manuscripta math. 113, 507–529 (2004) © Springer-Verlag 2004

Frank Calegari

Semistable abelian varieties over $\mathbb{Q}$

Received: 2 October 2002 / Revised Version: 17 November 2003
Published online: 3 March 2004

Abstract. We prove that for $N = 6$ and $N = 10$, there do not exist any non-zero semistable abelian varieties over $\mathbb{Q}$ with good reduction outside primes dividing N. Our results are contingent on the GRH discriminant bounds of Odlyzko. Combined with recent 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 $\mathbb{Q}$ with good reduction outside primes dividing N precisely when $N \notin \{1, 2, 3, 5, 6, 7, 10, 13\}$.

1. Introduction

In 1985, Fontaine [3] proved a conjecture of Shafarevich to the effect that there do not exist any nonzero abelian varieties over $\mathbb{Z}$ (or equivalently, abelian varieties $A/\mathbb{Q}$ with good reduction everywhere). Fontaine's approach was via finite group schemes over local fields. In particular, he proved the following theorem:

Theorem 1.1 (Fontaine). *Let G_ℓ be a finite flat group scheme over $\mathbb{Z}_\ell$ killed by ℓ. Let $L = \mathbb{Q}_\ell(G_\ell) := \mathbb{Q}_\ell(G_\ell(\overline{\mathbb{Q}}_\ell))$. Then*

$$v(\mathfrak{D}_{L/\mathbb{Q}_\ell}) < 1 + \frac{1}{\ell - 1}$$

where v is the valuation on L such that $v(\ell) = 1$, and $\mathfrak{D}_{L/\mathbb{Q}_\ell}$ is the different of $L/\mathbb{Q}_\ell$.

If G_ℓ is the restriction of some finite flat group scheme $G/\mathbb{Z}$ then $\mathbb{Q}(G)$ is *a fortiori* unramified at primes outside ℓ. In this context, the result of Fontaine is striking since it implies that the field $\mathbb{Q}(G)$ has particularly small root discriminant. If $A/\mathbb{Q}$ has good reduction everywhere, then it has a smooth proper Néron model $\mathcal{A}/\mathbb{Z}$, and $G := \mathcal{A}[\ell]/\mathbb{Z}$ is a finite flat group scheme. Using the discriminant bounds of Odlyzko [8], Fontaine showed that for certain small primes ℓ, for every n, either $A/\mathbb{Z}$ or some isogenous abelian variety has a rational ℓ^n-torsion point. Reducing A modulo p for some prime p of good reduction (in this case, any prime), one finds abelian varieties over $\mathbb{F}_p$ with at least ℓ^n rational points. One knows, however, that

F. Calegari: Department of Mathematics, Harvard University, Cambridge, MA 02138, USA. e-mail: fcale@math.harvard.edu

Mathematics Subject Classification (2000): 14K15

DOI: 10.1007/s00229-004-0445-1

isogenous abelian varieties over $\mathbb{F}_p$ have an equal and thus bounded number of points. This contradiction proves that $A/\mathbb{Q}$ cannot exist.

If one considers abelian varieties $A/\mathbb{Q}$ such that A has good reduction outside a single prime p, one can no longer expect nonexistence results. Indeed, there exist abelian varieties with good reduction everywhere except at p. One such class of examples are the Jacobians of modular curves $X_0(p^n)$, which have positive genus for every p and sufficiently large n. A natural subclass of abelian varieties, however, are the semistable ones. By considering the modular abelian varieties $J_0(N)$, one finds nonzero semistable abelian varieties over $\mathbb{Q}$ which have good reduction outside N for all squarefree $N \notin \{1, 2, 3, 5, 6, 7, 10, 13\}$. A reasonable conjecture to make is that there are no semistable abelian varieties over $\mathbb{Z}[1/N]$ for N in this set. Fontaine's Theorem is the case $N = 1$. Recently Brumer and Kramer [1] proved this statement for $N \in \{2, 3, 5, 7\}$, and (by quite different methods) Schoof [12] for $N \in \{2, 3, 5, 7, 13\}$. In this paper, we treat the remaining cases $N \in \{6, 10\}$, and prove the following theorems:

Theorem 1.2. *Let $A/\mathbb{Q}$ be an abelian variety with everywhere semistable reduction, and good reduction outside* 2 *and* 3. *If the GRH discriminant bounds of Odlyzko hold, then A has dimension* 0.

Theorem 1.3. *Let $A/\mathbb{Q}$ be an abelian variety with everywhere semistable reduction, and good reduction outside* 2 *and* 5. *If the GRH discriminant bounds of Odlyzko hold, then A has dimension* 0.

We note that in Fontaine [3], Brumer–Kramer [1] and Schoof [12], the GRH is *not* assumed. Our technique for proving these results is linked strongly to the ideas in Brumer–Kramer [1] and Schoof [12], and thus we consider it important to briefly recall the main ideas of these papers now. Schoof's approach is similar in spirit to Fontaine's. Instead of working with finite flat group schemes over $\mathbb{Z}$, one considers finite flat group schemes over $\mathbb{Z}[\frac{1}{p}]$, where p is prime. In order to restrict to the class of group schemes possibly arising from non-semistable abelian varieties, one uses the following fact due to Grothendieck ([4], Exposé IX, Prop. 3.5):

Theorem 1.4 (Grothendieck). *Let A be an abelian variety over $\mathbb{Q}$ with semistable reduction at p. Let $\mathcal{I}_p \subset \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ denote a choice of inertia group at p. Then the action of $\mathcal{I}_p$ on the ℓ^n-division points of A for $\ell \neq p$ is rank two unipotent; i.e., as an endomorphism, for $\sigma \in \mathcal{I}_p$,*

$$(\sigma - 1)^2 A[\ell^n] = 0.$$

In particular, $\mathcal{I}_p$ acts through its maximal pro-ℓ quotient, which is procyclic.

Thus one may restrict attention to finite flat group schemes $G/\mathbb{Z}[\frac{1}{p}]$ of ℓ-power order such that inertia at p acts through its maximal pro-ℓ quotient. The key step of Schoof's approach is to show that any such group scheme admits a filtration by the group schemes $\mathbb{Z}/\ell\mathbb{Z}$ and μ_ℓ. Using this filtration, along with various extension results (in the spirit of Mazur [9], in particular Proposition 2.1 pg. 49 and Proposition 4.1 pg. 58) for group schemes over $\mathbb{Z}[\frac{1}{p}]$, one shows as in Fontaine that for each n, some abelian variety isogenous to A has rational torsion points of order ℓ^n. The approach of Brumer and Kramer is quite different. Although, as in Schoof and Fontaine, they use discriminant bounds to control $\mathbb{Q}(A[\ell])$ for particular ℓ, they seek a contradiction not to any local bounds but to a theorem of Faltings. Namely, they construct infinitely many pairwise non isomorphic but isogenous abelian varieties, contradicting the finiteness of this set (as follows from Faltings [2], Satz 6, pg. 363). The essential difference in the two approaches, however, is that Brumer and Kramer use the explicit description of the Tate module $\mathbb{T}_\ell$ of A at a prime p of semistable reduction. Such a description is once more due to Grothendieck [4].

Both of these approaches fail (at least naïvely) to work when $N = 6$ or 10. Using Schoof's approach one runs into a problem (when $N = 10$) because μ_3 admits non-isomorphic finite flat group scheme extensions by $\mathbb{Z}/3\mathbb{Z}$ over $\mathbb{Z}[\frac{1}{10}]$, whereas no nontrivial extensions exist over either $\mathbb{Z}[\frac{1}{2}]$ or $\mathbb{Z}[\frac{1}{5}]$. One difficulty that arises in Brumer and Kramer's approach is that the field $\mathbb{Q}(A[3])$ fails to have a unique prime above the bad primes 2 or 5, as fortuitously happens in the cases they consider. We combine both methods, as well as some new ideas, to prove our results. In the next section we recall some definitions and results from Brumer and Kramer's paper.

1.1. Notation

Let p be a prime number. Let $\mathcal{D}_p = \mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ denote the local Galois group at p. For a Galois extension of global fields $L/\mathbb{Q}$, we denote a decomposition group at p by $\mathcal{D}_p(L/\mathbb{Q})$. This is well defined up to conjugation, or equivalently, up to an embedding $L \hookrightarrow \overline{\mathbb{Q}}_p$ which we shall fix when necessary. In the same spirit, let $\mathcal{I}_p = \mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p^{unr})$, and let $\mathcal{I}_p(L/\mathbb{Q})$ be an inertia group at p as a subgroup of $\mathcal{D}_p(L/\mathbb{Q})$ and of $\mathrm{Gal}(L/\mathbb{Q})$. One notes that $\mathcal{I}_p$ is normal in $\mathcal{D}_p$. For any $\mathcal{D}_p$-module $\mathcal{M}$, let $\overline{\mathcal{M}}$ denote $\mathcal{M}/\ell\mathcal{M}$; it is a $\mathcal{D}_p$-module killed by ℓ. We shall use $\widehat{\mathcal{M}}$ to denote a $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-module killed by ℓ constructed functorially from $\overline{\mathcal{M}}$. A "finite" group scheme G/R will always mean a group scheme G finite and flat over Spec R. For an abelian variety A, let $\hat{A}$ denote the dual abelian variety.

2. Local Considerations

2.1. Preliminaries

In this section we introduce some notation and results from the paper of Brumer and Kramer [1].

Let $A/\mathbb{Q}$ be an abelian variety of dimension $d > 0$ with semistable reduction at p. Let ℓ be a prime different from p, and consider the Tate module $\mathbb{T}_\ell(A/\mathbb{Q}_p)$. Let $\mathcal{M}_f(p) = \mathbb{T}_\ell(A/\mathbb{Q}_p)^{\mathcal{I}_p}$, and let $\mathcal{M}_t(p)$ be the submodule of $\mathbb{T}_\ell(A/\mathbb{Q}_p)$ orthogonal to $\mathcal{M}_f(p)(\hat{A})$ under the Weil paring

$$e : \mathbb{T}_\ell(A) \times \mathbb{T}_\ell(\hat{A}) \longrightarrow \mathbb{Z}_\ell(1).$$

In Brumer and Kramer, these modules were referred to as $\mathcal{M}_1$ and $\mathcal{M}_2$ respectively. Following a suggestion, we use instead the hopefully more suggestive notation $\mathcal{M}_f$ (f for finite or fixed) and $\mathcal{M}_t$ (t for toric). Since A is semistable, there are inclusions

$$0 \subseteq \mathcal{M}_t(p) \subseteq \mathcal{M}_f(p) \subseteq \mathbb{T}_\ell(A/\mathbb{Q}_p).$$

Since $\mathcal{I}_p$ is normal in $\mathcal{D}_p$, the groups $\mathcal{M}_f(p)$ and $\mathcal{M}_t(p)$ are $\mathcal{D}_p = \mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$-modules. Let $\mathcal{A}/\mathbb{Z}$ be the Néron model for A. Let $\mathcal{A}^0_{\mathbb{F}_p}$ be the connected component of the special fibre of $\mathcal{A}$ at p. It is an extension of an abelian variety of dimension a_p by a torus of dimension $t_p = d - a_p$. One has $\mathrm{rank}(\mathcal{M}_t(p)) = t_p$ and $\mathrm{rank}(\mathcal{M}_f(p)) = t_p + 2a_p = d + a_p$.

Definition 2.1 (Brumer–Kramer). *Let A be an abelian variety with bad reduction at p. Let $i(A, \ell, p)$ denote the minimal integer $n \geq 1$ such that $\mathbb{Q}_p(A[\ell^n])$ is ramified at p. Call $i(A, \ell, p)$ the "effective stage of inertia".*

We note that $i(A, \ell, p)$ is finite by the criterion of Néron–Ogg–Shafarevich.

Let $\Phi_A(p) = (\mathcal{A}/\mathcal{A}^0)(\overline{\mathbb{F}}_p)$ be the component group of A at p. For a finite group G, let $\mathrm{ord}_\ell(G)$ denote the largest exponent d such that ℓ^d divides the order of G. Recall the following result from [1]:

Theorem 2.2 (Brumer–Kramer). *Let A be a semistable abelian variety with bad reduction at p. Let $\overline{\mathcal{M}_f}(p)$ and $\overline{\mathcal{M}_t}(p)$ denote the projections of $\mathcal{M}_f(p)$ and $\mathcal{M}_t(p)$ to $A[\ell]$. Suppose that κ is a $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$-submodule of $A[\ell]$ and let $\phi : A \longrightarrow A'$ be a $\mathbb{Q}_p$-isogeny with kernel κ. Then*

$$\mathrm{ord}_\ell(\Phi_{\hat{A}'}(p)) - \mathrm{ord}_\ell(\Phi_{\hat{A}}(p)) = \dim(\kappa \cap \overline{\mathcal{M}_t}(p)) + \dim(\kappa \cap \overline{\mathcal{M}_f}(p)) - \dim\ \kappa.$$

Moreover, if $\overline{\mathcal{M}_t}(p) \subseteq \kappa \subseteq \overline{\mathcal{M}_f}(p)$, then $i(A', \ell, p) = i(A, \ell, p) + 1$.

By taking κ to be a proper $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ submodule of $A[\ell]$, Brumer and Kramer use this theorem to construct infinitely many non-isomorphic varieties isogenous to A over $\mathbb{Q}$. This contradicts Faltings' Theorem. Although we shall also use Faltings' Theorem, our final contradiction will come from showing that A (or some isogenous abelian variety) has too many points over some finite field, contradicting Weil's Riemann hypothesis, much as in the approach of Schoof [12]. We shall also make use of the following lemma.

Lemma 2.3. *Let $\sigma \in \mathcal{I}_p$. The image of $(\sigma - 1)$ acting on $\mathbb{T}_\ell(A)$ lies in $\mathcal{M}_t(A)$. The image of $(\sigma - 1)$ on $A[\ell]$ lies in $\overline{\mathcal{M}_t}(p)$.*

Proof. Let $y \in \mathcal{M}_f(p)(\hat{A})$, and $x \in \mathbb{T}_\ell(A)$. Then $e((\sigma-1)x, y) = e(x^\sigma, y)/e(x, y)$. Since both y and $\mathbb{Z}_\ell(1)$ are fixed by σ, we conclude that

$$e((\sigma - 1)x, y) = e(x^\sigma, y^\sigma)/e(x, y) = e(x, y)^\sigma/e(x, y) = 1.$$

Thus $(\sigma - 1)x \in \mathcal{M}_t(p)$. The second statement of Lemma 2.3 follows from the first. □

2.2. *Results*

In proving Theorem 1.2 (or 1.3), we may assume that A has bad reduction at both 2 and 3 (respectively, both 2 and 5), since otherwise we may apply the previous results of Brumer–Kramer [1], Schoof [12], or Fontaine [3].

The proof of Theorem 1.3 is very similar to the proof of Theorem 1.2, although some additional complications arise. Thus we restrict ourselves first to the case $N = 6$, and then later explain how our proof can be adapted to work for $N = 10$. One main ingredient is the following result, proved in section 3:

Theorem 2.4. *Let $G/\mathbb{Z}[\frac{1}{6}]$ be a finite group scheme of 5-power order such that:*

1. *Inertia at 2 and 3 acts through a cyclic 5-group.*
2. *The action of inertia on the subquotients $G[5^n](\overline{\mathbb{Q}})/G[5^{n-1}](\overline{\mathbb{Q}})$ is through an order 5 quotient for all n.*

Assume the GRH discriminant bounds of Odlyzko. Then G has a filtration by the group schemes $\mathbb{Z}/5\mathbb{Z}$ and μ_5. Moreover, if G is killed by 5, then $\mathbb{Q}(G) \subseteq K$, where $K := \mathbb{Q}(\sqrt[5]{2}, \sqrt[5]{3}, \zeta_5)$.

In particular, if $A/\mathbb{Q}$ is a semistable abelian variety with good reduction outside 2 and 3, and $\mathcal{A}/\mathbb{Z}$ is its Néron model, then by Theorem 1.4 the conditions of Theorem 2.4 are satisfied by the finite group scheme $\mathcal{A}[5^n]/\mathbb{Z}[\frac{1}{6}]$ for each n. Thus $\mathcal{A}[5^n]$ has a filtration by the group schemes $\mathbb{Z}/5\mathbb{Z}$ and μ_5, and $\mathbb{Q}(A[5]) \subseteq K$. These results and their proofs are of the same flavour as results in Schoof [12]. One such result from that paper we use explicitly is the following (a special case of Theorem 3.3 and the proof of Corollary 3.4 in *loc. cit.*):

Theorem 2.5 (Schoof). *Let $p = 2$ or 3. Let $G/\mathbb{Z}[\frac{1}{p}]$ be a finite group scheme of 5-power order such that inertia at p acts through a cyclic 5-group. Then G has a filtration by the group schemes $\mathbb{Z}/5\mathbb{Z}$ and μ_5. Moreover, the extension group* $\mathrm{Ext}^1(\mu_5, \mathbb{Z}/5\mathbb{Z})$ *of group schemes over $\mathbb{Z}[\frac{1}{p}]$ is trivial, and there exists an exact sequence of group schemes*

$$0 \longrightarrow M \longrightarrow G \longrightarrow C \longrightarrow 0$$

where M is a diagonalizable group scheme over $\mathbb{Z}[\frac{1}{p}]$, and C is a constant group scheme.

In sections 2.3, 2.4 and 2.5 we shall assume there exists a semistable abelian variety $A/\mathbb{Z}[\frac{1}{6}]$, and derive a contradiction using Theorem 2.4.

2.3. *Construction of Galois Submodules*

The proof of Brumer and Kramer relies on the fact that for abelian varieties with bad semistable reduction at one prime $p \in \{2, 3, 5, 7\}$, there exists an ℓ such that there is a unique prime above p in $\mathbb{Q}(A[\ell])$. In this case, the $\mathcal{D}_p$-modules $\overline{\mathcal{M}_f}(p)$ and $\overline{\mathcal{M}_t}(p)$ are automatically $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-modules, and so one has a source of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-modules with which to apply Theorem 2.2. This approach fails in our case, (at least if $\ell = 5$) since Theorem 2.4 allows the possibility that $\mathbb{Q}(A[5])$ could be as big as $K := \mathbb{Q}(2^{1/5}, 3^{1/5}, \zeta_5)$, and 2 and 3 split into 5 distinct primes in $\mathcal{O}_K$. On the other hand, something fortuitous does happen, and that is that the inertia subgroups $\mathcal{I}_p(K/\mathbb{Q})$ for $p = 2, 3$ are *normal* subgroups of $\mathrm{Gal}(K/\mathbb{Q})$, when *a priori* they are only normal subgroups of $\mathcal{D}_p(K/\mathbb{Q})$. Using this fact we may construct global Galois modules from the local $\mathcal{D}_p(K/\mathbb{Q})$-modules $\overline{\mathcal{M}}_f(p)$ as follows.

Lemma 2.6. *Let* $F = \mathbb{Q}(A[\ell])$, $\Gamma = \mathrm{Gal}(F/\mathbb{Q})$, *and* $H \subseteq \Gamma$ *be a normal subgroup of* Γ. *Let* $\overline{\mathcal{M}}$ *be a subgroup of* $A[\ell]$ *fixed pointwise by* H. *Let* $\widehat{\mathcal{M}}$ *be the* $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$*-submodule generated by the points of* $\overline{\mathcal{M}}$. *Then* $\mathbb{Q}(\widehat{\mathcal{M}}) \subseteq E$, *where* E *is the fixed field of* H.

Proof. By Galois theory, it suffices to show that $\widehat{\mathcal{M}}$ is fixed by H. This result is a special case of the more general fact: If H is any normal subgroup of Γ, then any Γ-module generated by H-invariant elements is itself H-invariant. Any sum of elements fixed by H is clearly fixed by H. Thus it remains to show that any element gP with $g \in \Gamma$ is also fixed by H. For this we observe that

$$h(gP) = g(g^{-1}hgP) = gP$$

since $g^{-1}hg \in H$. □

Definition 2.7. *Let* $\widehat{\mathcal{M}}_f(p)$ *be the* $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$*-module generated by* $\overline{\mathcal{M}}_f(p)$, *considered as a subgroup of* $A[\ell]$ *after choosing some embedding* $\overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_p$.

Since all embeddings $\overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_p$ differ by an automorphism of $\overline{\mathbb{Q}}$, we find that $\widehat{\mathcal{M}}_f(p)$ does not depend on the choice of embedding, although $\overline{\mathcal{M}}_f(p)$ does, in general. We note that by Faltings theorem, there exist only finitely many abelian varieties over $\mathbb{Q}$ isogenous to A. Thus is makes sense to chose a representative from the isogeny class of A that is *maximal* with respect to any well defined property.

Lemma 2.8. *Suppose that* $\mathrm{ord}_5(\Phi_{\hat{A}}(2))$ *is maximal amongst all abelian varieties isogenous to* A. *Then*

1. $A[5]$ *is unramified at* 2
2. *There is an exact sequence*

$$0 \longrightarrow \mu_5^m \longrightarrow A[5] \longrightarrow (\mathbb{Z}/5\mathbb{Z})^n \longrightarrow 0$$

with $m + n = 2d$. *Moreover,* $m = n = d$.

Similarly, if A *is chosen such that* $\mathrm{ord}_5(\Phi_{\hat{A}}(3))$ *is maximal, then* $A[5]$ *is unramified at* 3 *and statement* 2 *still holds. Finally,* A *and any variety isogenous to* A *has ordinary reduction at* 5.

Since $\mathcal{I}_p(K/\mathbb{Q})$ is a normal subgroup of $\mathrm{Gal}(K/\mathbb{Q})$, Lemma 2.6 implies that

$$\mathbb{Q}(\widehat{\mathcal{M}}_f(2)) \subseteq \mathbb{Q}(\zeta_5, 3^{1/5}), \qquad \mathbb{Q}(\widehat{\mathcal{M}}_f(3)) \subseteq \mathbb{Q}(\zeta_5, 2^{1/5}).$$

We now apply Theorem 2.2 with $\kappa = \widehat{\mathcal{M}}_f(2)$. Let $A' = A/\kappa$. Since κ is a $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ module A' is an abelian variety over $\mathbb{Q}$. We see that

$$\mathrm{ord}_5(\Phi_{\hat{A}'}(2)) - \mathrm{ord}_5(\Phi_{\hat{A}}(2)) = \dim\, \kappa \cap \overline{\mathcal{M}}_t(2) + \dim\, \kappa \cap \overline{\mathcal{M}}_f(2) - \dim\, \kappa.$$

Since by construction $\overline{\mathcal{M}}_t(2) \subseteq \overline{\mathcal{M}}_f(2) \subseteq \kappa$, the right hand side is equal to

$$2d - \dim\ \kappa \geq 0.$$

Yet from the maximality of $\mathrm{ord}_5(\Phi_{\hat{A}}(2))$, it follows that $2d - \dim\ \kappa \leq 0$. Thus $\dim\ \kappa = d$, and in particular $\widehat{\mathcal{M}}_f(2) = \kappa = A[5]$. Thus by Lemma 2.6 $A[5]$ is unramified at 2. Note that this same construction can be applied *mutatis mutandis* when 2 is replaced by 3. Since $A[5]$ is unramified at 2, it follows from a standard patching argument ([9], 1.2(b), p. 44) that $A[5]$ prolongs to a finite group scheme over $\mathbb{Z}[\frac{1}{3}]$. Thus we may now apply Theorem 2.5, and conclude that there exists an exact sequence of group schemes over $\mathbb{Z}[\frac{1}{3}]$

$$0 \longrightarrow \mu_5^m \longrightarrow A[5] \longrightarrow (\mathbb{Z}/5\mathbb{Z})^n \longrightarrow 0$$

where $m + n = 2d$. It now remains to show that $m = n = d$.

Let $A' = A/\mu_5^m$. The morphism $A \to A'$ induces a proper map $(\mathbb{Z}/5\mathbb{Z})^n = A[5]/\mu_5^m \to A'$. By an fppf abelian sheaf argument, we see that this map is a categorical monomorphism and hence by EGA IV$_3$ 8.11.5 ([5]) a closed immersion. Specializing to the fibre over $\mathbb{F}_5$ we find that

$$(\mathbb{Z}/5\mathbb{Z})^n \hookrightarrow A'_{\mathbb{F}_5}[5].$$

The p-rank of the p-torsion subgroup of an abelian variety over an algebraically closed field of characteristic p is at most the dimension d, with equality only if A is ordinary at p. Thus $n \leq d$. Applying the same argument to $\hat{A}$ we find that $m \leq d$ and thus $n = m = d$, and A has ordinary reduction at 5. Since ordinary reduction is preserved under isogeny, we are done. □

We now divide our proof by contradiction into two cases. In the first case we assume that A has mixed reduction at at least one of 2 or 3 (i.e. the connected component of the special fibre is the extension of a *non-trivial* abelian variety of dimension $a_p \neq 0$ by a torus of dimension $t_p = d - a_p$). In the second case we assume that A has purely toric reduction at both 2 and 3.

2.4. A has Mixed Reduction at 2 *or* 3

Let $\mathrm{ord}_5(\Phi_{\hat{A}}(2))$ be maximal. Then from Lemma 2.8 there is an exact sequence over $\mathbb{Z}[\frac{1}{3}]$

$$0 \longrightarrow \mu_5^d \longrightarrow A[5] \longrightarrow (\mathbb{Z}/5\mathbb{Z})^d \longrightarrow 0.$$

If A has mixed reduction at 2 then $a_2 > 0$, and $\mathcal{M}_f(2)$ has rank $t_2 + 2a_2 = d + a_2 > d$. In particular, $\kappa := \overline{\mathcal{M}}_f(2) \cap \mu_5^d$ is nontrivial and defines a diagonalizable $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-submodule of $A[5]$ (here we use the fact that every subgroup of $\mu_5^d(\overline{\mathbb{Q}})$ is $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ stable). We now apply Theorem 2.2. Let $A' = A/\kappa$. We find that

$$\mathrm{ord}_5(\Phi_{\hat{A}'}(2)) - \mathrm{ord}_5(\Phi_{\hat{A}}(2)) = \dim\ \kappa \cap \overline{\mathcal{M}}_t(2) + \dim\ \kappa \cap \overline{\mathcal{M}}_f(2) - \dim\ \kappa.$$

Since $\kappa \subseteq \overline{\mathcal{M}}_f(2)$, the last two terms cancel, and $\mathrm{ord}_5(\Phi_{\hat{A}'}(2))$ is also maximal. Hence we may repeat this process, thereby constructing morphisms $A \longrightarrow A^{(n)}$ with larger and larger kernels κ_n, where κ_n has a filtration by copies of the finite group scheme μ_5.

Lemma 2.9. *Any extension of diagonalizable group schemes of* 5*-power order over* $\mathbb{Z}[\frac{1}{6}]$ *is diagonalizable.*

Proof. By taking Cartier duals, it suffices to prove the analogous statement for constant group schemes: Any extension of 5-power order constant group schemes over $\mathbb{Z}[\frac{1}{6}]$ is constant. The action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on any such extension is unramified outside 2 and 3, and acts via a 5-group. Since p-groups are solvable, it suffices to prove that there are no Galois 5-extensions of $\mathbb{Q}$ unramified outside 2 and 3. Easy class field theory (for example, the Kronecker–Weber theorem) shows that no such extensions exist. □

Thus we have proven that for all n, there exist exact sequences

$$0 \longrightarrow \kappa_n \longrightarrow A[5^{k(n)}] \longrightarrow M_n \longrightarrow 0.$$

where κ_n is a diagonalizable group scheme, $k(n)$ the smallest integer such that $5^{k(n)}$ kills κ_n, and M_n is the cokernel. Hence the variety $\hat{A}/M_n^{\vee}$ contains the arbitrarily large constant group scheme $\kappa_n^{\vee}$, and so, after choosing some auxiliary prime q of good reduction, we see that $(\hat{A}/M_n^{\vee})(\mathbb{F}_q)$ can be arbitrarily large. This contradicts the uniform boundedness of the number of points over $\mathbb{F}_q$ for all varieties isogenous to $\hat{A}$ (indeed, the number of points for all such varieties is equal).

If A does not have purely toric reduction at 3, a similar argument applies.

2.5. A has Purely Toric Reduction at 2 *and* 3

Under this assumption, for $p \in \{2, 3\}$, we have $\mathcal{M}_t(p) = \mathcal{M}_f(p)$, and so we write both as $\mathcal{M}(p)$. Again we assume that $\mathrm{ord}_5(\Phi_{\hat{A}}(2))$ is maximal. In particular, we may assume that $\widehat{\mathcal{M}}(2) = A[5]$, that $\mathbb{Q}(A[5])$ is contained in $\mathbb{Q}(\zeta_5, 3^{1/5})$, and that we have an exact sequence of group schemes over $\mathbb{Z}[\frac{1}{3}]$:

$$0 \longrightarrow \mu_5^d \longrightarrow A[5] \longrightarrow (\mathbb{Z}/5\mathbb{Z})^d \longrightarrow 0.$$

By abuse of notation we may also think of this as an exact sequence of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-modules.

Lemma 2.10. *The Galois modules* $\widehat{\mathcal{M}}(3)$ *and* μ_5^d *coincide. Equivalently, there is an equality of Galois modules:* $\widehat{\mathcal{M}}(3) = \mu_5^d$.

Proof. First we show that $\overline{\mathcal{M}}(2) \cap \mu_5^d = \{0\}$. If not, then since $\dim \overline{\mathcal{M}}(2) = d$, the module $\overline{\mathcal{M}}(2)$ would not surject onto $(\mathbb{Z}/5\mathbb{Z})^d$, and the elements of $\overline{\mathcal{M}}(2)$ could not possibly generate $A[5]$ as a $\mathrm{Gal}(K/\mathbb{Q})$-module[1]. Thus by dimension considerations, as a $\mathbb{F}_5$-vector space, we have that $A[5] = \mu_5^d \oplus \overline{\mathcal{M}}(2)$.

Let $L := \mathbb{Q}(\zeta_5, 3^{1/5})$. Then as we have noted, $\mathbb{Q}(A[5]) \subseteq L$. Let σ generate $\mathcal{I}_3(L/\mathbb{Q})$. From Grothendieck's Theorem (Theorem 1.4), we have $(\sigma - 1)^2 = 0$ as an endomorphism on $A[5]$. Thus $\overline{\mathcal{M}}(2) + \sigma\overline{\mathcal{M}}(2)$ is a well defined $\mathcal{I}_3$-module. On the other hand, $\overline{\mathcal{M}}(2)$ is a $\mathcal{D}_2(L/\mathbb{Q})$-module, and $\mathcal{I}_3$ is a set of representatives for the left cosets of $\mathcal{D}_2(L/\mathbb{Q})$ in $\mathrm{Gal}(L/\mathbb{Q})$. Thus $\overline{\mathcal{M}}(2)+\sigma\overline{\mathcal{M}}(2)$ is a $\mathrm{Gal}(L/\mathbb{Q})$-module, and so

$$\widehat{\mathcal{M}}(2) = \overline{\mathcal{M}}(2) + \sigma\overline{\mathcal{M}}(2).$$

Since $\dim_{\mathbb{F}_5} \widehat{\mathcal{M}}(2) = \dim_{\mathbb{F}_5}(A[5]) = 2d$, by dimension considerations one must have $\sigma\overline{\mathcal{M}}(2) \cap \overline{\mathcal{M}}(2) = 0$.

The decomposition group of $L := \mathbb{Q}(\zeta_5, 3^{1/5})$ at 3 is the entire Galois group $\mathrm{Gal}(L/\mathbb{Q})$, and the inertia group $\mathcal{I}_3$ is equal to $\langle\sigma\rangle$. We show that $\mu_5^d \subset \widehat{\mathcal{M}}(3)$ and $\widehat{\mathcal{M}}(3) \subset \mu_5^d$.

Since $\sigma\overline{\mathcal{M}}(2) \cap \overline{\mathcal{M}}(2) = \{0\}$, we have $\ker(\sigma - 1) \cap \overline{\mathcal{M}}(2) = \{0\}$. An element killed by $\sigma - 1$ is exactly fixed by $\mathcal{I}_3$. Thus the only elements of $A[5]$ fixed by $\mathcal{I}_3$ are those in μ_5^d. Since (by Lemma 2.6) $\widehat{\mathcal{M}}(3)$ is unramified at 3, we have $\widehat{\mathcal{M}}(3) \subseteq \mu_5^d$. On the other hand, $|\widehat{\mathcal{M}}(3)| \geq |\overline{\mathcal{M}}(3)| = 5^d = |\mu_5^d|$. Thus we are done. □

We now apply Theorem 2.2 again with $\kappa = \widehat{\mathcal{M}}(3) = \mu_5^d$. If $A' = A/\mu_5^d$, then since $\overline{\mathcal{M}}(3) = \widehat{\mathcal{M}}(3)$, we have $i(A', 5, 3) = i(A, 5, 3) + 1 \geq 2$. On the other hand, we see from the exact sequence for $A[5]$ that $(\mathbb{Z}/5\mathbb{Z})^d \subset A'[5]$. By Theorem 2.4 and the proof of Lemma 2.8 we infer that there exists an exact sequence of group schemes over $\mathbb{Z}[\frac{1}{6}]$:

$$0 \longrightarrow (\mathbb{Z}/5\mathbb{Z})^d \longrightarrow A'[5] \longrightarrow \mu_5^d \longrightarrow 0.$$

Replace A by A'. Since $\mathbb{Q}(A[5])$ is unramified at 3, we know that is must be contained within $\mathbb{Q}(\zeta_5, 2^{1/5})$. Since A is ordinary at 5, however, we may prove more.

Lemma 2.11. *The field $\mathbb{Q}(A[5])$ is $\mathbb{Q}(\zeta_5)$. There is only one prime above 3 in the extension $\mathbb{Q}(A[5])/\mathbb{Q}$.*

Proof. Consider the action of $\mathcal{I}_5$ on $A[5]$. By Lemma 2.8, A is ordinary at 5. Thus $A[5]$ as an $\mathcal{I}_5$-module is an extension of a constant module of rank d by a cyclotomic module of rank d. The $(\mathbb{Z}/5\mathbb{Z})^d$ inside $A[5]$ must intersect trivially with this cyclotomic module. Thus it provides a splitting of $A[5]$ as an $\mathcal{I}_5$-module into a product of a cyclotomic module and a constant module. Thus $\mathbb{Q}_5(A[5])$ is unramified over $\mathbb{Q}_5(\zeta_5)$. The maximal extension of $\mathbb{Q}(\zeta_5)$ inside K unramified at $1 - \zeta_5$ is $\mathbb{Q}(\zeta_5, 18^{1/5})$. Since $\mathbb{Q}(A[5])$ is also unramified over 3 (as $i(A, 5, 3) \geq 2$), $\mathbb{Q}(A[5])$ must be exactly $\mathbb{Q}(\zeta_5)$. The second statement of the lemma clearly follows from the first. □

[1] Another way to reduce to the case where $\overline{\mathcal{M}}(2) \cap \mu_5^d = \{0\}$ is as follows: if this intersection was nontrivial, we could take quotients repeatedly until the resulting intersection *was* trivial. If this process repeated indefinitely, we could apply the arguments of section 2.4 to produce a contradiction.

The second part of Lemma 2.11 implies that $\overline{\mathcal{M}}(3)$ is a Gal($\overline{\mathbb{Q}}/\mathbb{Q}$)-module, as in [1]. Applying Theorem 2.2 once more, with $\kappa = \widehat{\mathcal{M}}(3) = \overline{\mathcal{M}}(3)$, and setting $A' = A/\kappa$, we find that

$$i(A', 5, 3) = i(A, 5, 3) + 1 \geq 3.$$

Replace A by A'. In particular, $\mathbb{Q}(A[5^2])$ is unramified at 3. Thus by Theorem 2.5 there exists a filtration of group schemes over $\mathbb{Z}[\frac{1}{2}]$:

$$0 \longrightarrow M \longrightarrow A[5^2] \longrightarrow C \longrightarrow 0$$

where M is a diagonalizable group scheme, and C is a constant group scheme. Let $q \in \mathbb{Z}$ be a prime of good reduction. We observe that the varieties A/M and $\hat{A}/C^\vee$ contain constant subgroup schemes of order $\#C$ and $\#M$ respectively. It follows from Weil's Riemann Hypothesis that abelian varieties of dimension d over $\mathbb{F}_q$ have at most $(1 + \sqrt{q})^{2d}$ points. Thus $\#C \leq (1 + \sqrt{q})^{2d}$ and $\#M \leq (1 + \sqrt{q})^{2d}$, and

$$5^{4d} = \#A[5^2] = \#C\#M \leq (1 + \sqrt{q})^{4d}.$$

Choosing $q = 7$, say, then since $5 > 1 + \sqrt{7}$, we have a contradiction if $d > 0$. This completes the proof of Theorem 1.2 except for Theorem 2.4, which we prove now.

3. Group Schemes over $\mathbb{Z}$[1/6]

First, some preliminary remarks on group schemes. Here we follow Schoof [12].

Let $(\ell, N) = 1$. Let $\underline{C}$ be the category of finite group schemes G over $\mathbb{Z}[1/N]$ satisfying the following properties:

1. G is killed by ℓ: $G = G[\ell]$.
2. For all $p|N$, the action of $\sigma \in \mathcal{I}_p$ on $G(\overline{\mathbb{Q}}_p)$ is either trivial or cyclic of order ℓ.

For example, $\mathbb{Z}/\ell\mathbb{Z}$ and μ_ℓ are objects of $\underline{C}$. As remarked in [12], this category is closed under direct products, flat subgroups and flat quotients. Thus, to prove that any object of $\underline{C}$ has a filtration by $\mathbb{Z}/\ell\mathbb{Z}$ and μ_ℓ it suffices to show that the only simple objects of $\underline{C}$ are $\mathbb{Z}/\ell\mathbb{Z}$ and μ_ℓ. If $A/\mathbb{Q}$ is a semistable abelian variety with good reduction at primes not dividing N, then from Theorem 1.4, we have $\mathcal{A}[\ell] \in \underline{C}$. Another class of examples are the group schemes G_ϵ defined by Katz–Mazur ([7] Chapter 8, Interlude 8.7, [12]); for any unit $\epsilon \in \mathbb{Z}[1/N]$ they construct a group scheme $G_\epsilon \in \underline{C}$ of order ℓ^2 killed by ℓ. G_ϵ is an extension of $\mathbb{Z}/\ell\mathbb{Z}$ by μ_ℓ, and $G_\epsilon(\overline{\mathbb{Q}}) = \mathbb{Q}(\zeta_\ell, \epsilon^{1/\ell})$.

Let $N = 6$ and $\ell = 5$. To prove that the only simple objects of $\underline{C}$ are μ_5 and $\mathbb{Z}/5\mathbb{Z}$, it suffices to show that the $\overline{\mathbb{Q}}$ points of any object of $\underline{C}$ are defined over the field K, where $K = \mathbb{Q}(\zeta_5, 2^{1/5}, 3^{1/5})$, because of the following result:

Lemma 3.1. *Let $G/\mathbb{Z}[1/N]$ be a simple group scheme killed by ℓ, where $(N, \ell) = 1$. Let $L = \mathbb{Q}(G(\overline{\mathbb{Q}}))$ and suppose that* Gal$(L/\mathbb{Q}(\zeta_\ell))$ *is an ℓ-group. Then G is either $\mathbb{Z}/\ell\mathbb{Z}$ or μ_ℓ.*

Proof. Since any ℓ-group acting on $(\mathbb{Z}/\ell\mathbb{Z})^d$ has at least one (in fact $\ell - 1$) nontrivial fixed point, there exists a point P of G defined over $\mathbb{Q}(\zeta_\ell)$. Since G is simple, P generates G as a Galois module and thus $\mathbb{Q}(G) \subseteq \mathbb{Q}(\zeta_\ell)$. In particular, G is unramified outside ℓ, hence unramified at each prime dividing N. Thus G prolongs to a finite group scheme over $\mathbb{Z}$, killed by ℓ, and with $\mathbb{Q}(G) \subseteq \mathbb{Q}(\zeta_\ell)$. Since the $(\ell - 1)$th roots of unity are in $\mathbb{F}_\ell^*$, and since all irreducible $\mathbb{F}_\ell$ representations of the abelian group $\mathrm{Gal}(\mathbb{Q}(\zeta_\ell)/\mathbb{Q})$ are one dimensional, any simple subgroup scheme of G has order ℓ. From Oort–Tate [11], the finite group schemes of order ℓ over $\mathbb{Z}$ are $\mathbb{Z}/\ell\mathbb{Z}$ and μ_ℓ. □

Let G be an object of $\underline{C}$. To prove that $\mathbb{Q}(G) \subseteq K$ it clearly suffices to prove the same inclusion for any group scheme which contains G as a direct factor. Consider the field $L = \mathbb{Q}(G \times G_{-1} \times G_2 \times G_3)$. One sees from the definition of G_ϵ that $K := \mathbb{Q}(\zeta_5, 2^{1/5}, 3^{1/5}) \subseteq L$. We prove that $L = K$. Using the estimates of Fontaine [3] we obtain an upper bound on the ramification of L at 5. Since inertia at 2 and 3 acts through a cyclic subgroup of order 5, we also have ramification bounds at 2 and 3. As in Schoof [12] and Brumer–Kramer [1], we obtain the following estimate of the root discriminant

$$\delta_L := |\Delta_L|^{1/[L:\mathbb{Q}]} < 5^{1+\frac{1}{5-1}} 2^{1-\frac{1}{5}} 3^{1-\frac{1}{5}} = 5^{5/4} 6^{4/5} = 31.349 < 31.645.$$

Note that this is not only an inequality of real numbers: one also has that as algebraic integers $5^{5/4}6^{4/5}$ is *divisible* by δ_L, and the ratio has nontrivial 5-adic valuation. From the discriminant bounds of Odlyzko [8], under the assumption of GRH, one concludes that $[L : \mathbb{Q}] < 2400$ and thus $[L : K] < 24$. In particular, $L/\mathbb{Q}$ is a solvable extension, and thus we can apply tools from class field

Remark. The methods of Odlyzko [8] give a general technique to bound the root discriminant of a number field $K/\mathbb{Q}$. One obtains an estimate of the form $\delta_K \geq \gamma(n)$, where $n = [K : \mathbb{Q}]$ and $\gamma(x)$ is an explicitly calculable continuous convex function of x. Under the assumption of the Generalized Riemann Hypothesis, one obtains similar bounds, with γ replaced by some larger (still convex) function $\gamma'(x)$. Both γ and γ' have finite limit as x goes to ∞. In fact,

$$\lim_{x \longrightarrow \infty} \gamma(x) = 4\pi e^\gamma = 22.38, \qquad \lim_{x \longrightarrow \infty} \gamma'(x) \sim 41.$$

In particular, without the GRH, the estimate $\delta_L < 31.349$ does not imply the degree $[L : \mathbb{Q}]$ is bounded, which might allow us to compute L explicitly. In the calculations of Fontaine, Schoof and Brumer–Kramer, all root discriminant estimates fall within the unconditional (on GRH) bounds of Odlyzko and so allow the use of unconditional estimates.

Our calculations in this section could be shortened by more reliance on computer calculation. However, for exposition we include as much class field theory as we can do by hand. This leads us to consider several group theory lemmata which allow us to do computations in smaller fields.

The root discriminant of K is $\delta_K = 5^{23/20}6^{4/5}$. Since the exponents of 2 and 3 in δ_K equal those for δ_L, the extension L/K is unramified outside primes lying above

5. Let $F = \mathbb{Q}(\zeta_5, 576^{1/5})$ (F can also be written as $\mathbb{Q}(\zeta_5, 18^{1/5})$ or $\mathbb{Q}(\zeta_5, 24^{1/5})$). Then $F/\mathbb{Q}(\zeta_5)$ is unramified at $1 - \zeta_5$. The prime $1 - \zeta_5$ splits completely in F. If $\pi_{F,i}$ for $i = 1, \ldots, 5$ are the primes above $1 - \zeta_5$, then $N_{F/\mathbb{Q}}(\pi_{F,i}) = 5$. The extension K/F is totally ramified at all primes $\pi_{F,i}$. Equivalently, $\pi_{F,i} = \pi_{K,i}^5$ for all i, and $N_{K/\mathbb{Q}}(\pi_{K,i}) = 5$. Let us consider the factorization of $\pi_{K,i}$ in L. Since $L/\mathbb{Q}$ is Galois, the ramification exponents are equal for all i. Thus we may write

$$\pi_{K,i} = \prod_{j=1}^{r_{L/K}} \mathfrak{p}_{i,j}^{e_{L/K}}, \qquad N_{L/K}(\mathfrak{p}_{i,j}) = \pi_{K,i}^{f_{L/K}}, \qquad N_{L/\mathbb{Q}}(\mathfrak{p}_{i,j}) = 5^{f_{L/K}},$$

$$r_{L/K} e_{L/K} f_{L/K} = [L : K].$$

3.1. L/K Tame

In this section we assume that L/K is a *tame* extension, and prove that $L = K$.

Lemma 3.2. $[L : K] < 10$.

Proof. Since L/K is tame, $\mathfrak{D}_{L/K} = \prod_{i=1}^{5} \prod_{j=1}^{r_{L/K}} \mathfrak{p}_{i,j}^{e_{L/K}-1}$, where $\mathfrak{D}_{L/K}$ is the different. Thus

$$\Delta_{L/K} = N_{L/K}(\mathfrak{D}_{L/K}) = \prod_{i=1}^{5} \pi_{K,i}^{r_{L/K} f_{L/K}(e_{L/K}-1)}.$$

Since $N_{K/\mathbb{Q}}(\pi_{K,i}) = 5$, $\mathrm{ord}_5(N_{K/\mathbb{Q}}(\Delta_{L/K})) = 5[L : K](1 - 1/e_{L/K}) < 5[L : K]$. Using the transitivity property of the discriminant [13] we find

$$\delta_L = \delta_K \cdot N_{K/\mathbb{Q}}(\Delta_{L/K})^{1/[L:\mathbb{Q}]} < \delta_K \cdot 5^{5/[K:\mathbb{Q}]} = 5^{23/20} 6^{4/5} 5^{5/100} = 28.925.$$

If $[L : \mathbb{Q}] \geq 1000$, then assuming the GRH, $\delta_L > 29.094$ by [8]. This is a contradiction to the above upper bound, so $[L : K] < 10$. □

Remark. If $5 \mid [L : K]$ and $[L : K] < 10$ then $[L : K] = 5$ and $\mathrm{Gal}(L/K)$ is tame if and only if it is unramified. We shall consider the case L/K unramified of degree 5 in section 3.3. Therefore we assume for now that $[L : K]$ has order coprime to 5.

Lemma 3.3. *Let* Γ *be a finite group, and let* $\Gamma' = [\Gamma, \Gamma]$ *be its commutator subgroup. Suppose moreover that* $\Gamma/\Gamma' \cong \mathbb{Z}/5\mathbb{Z}$*, and* $|\Gamma'| \geq 10$*. Then* $\Gamma \cong \mathbb{Z}/5\mathbb{Z}$*.*

Proof. Assume that $|\Gamma'| < 10$. It suffices to show that Γ is abelian, since then $\Gamma' = \langle 1 \rangle$ and $\Gamma \simeq \mathbb{Z}/5\mathbb{Z}$. If Γ' has order 5, then Γ has order 5^2 and is necessarily abelian. Thus Γ' has order coprime to 5, and thus there exists a section $\mathbb{Z}/5\mathbb{Z} \to \Gamma$. The action of $\mathbb{Z}/5\mathbb{Z}$ on Γ' by conjugation induces an automorphism of Γ'. Since for all groups Γ' of order less than 10, $|\mathrm{Aut}(\Gamma')|$ is coprime to 5, this action must be trivial, and thus Γ is abelian. □

Lemma 3.4. *If the extension* L/K *is tame and of degree coprime to* 5*, then* $L = K$*.*

Proof. Let J be the field $\mathbb{Q}(\zeta_5, 2^{1/5})$. We have the following exact sequence of groups

$$0 \longrightarrow \mathrm{Gal}(L/K) \longrightarrow \mathrm{Gal}(L/J) \longrightarrow \mathbb{Z}/5\mathbb{Z} \longrightarrow 0.$$

The extension L/J is Galois since $L/\mathbb{Q}$ is Galois. By Lemma 3.2, $[L : K] < 10$. Thus by Lemma 3.3, either $L = K$ or $\mathrm{Gal}(L/K)$ is not the commutator subgroup of $\mathrm{Gal}(L/J)$. Since by assumption $[L : K]$ has order coprime to 5, either $L = K$ (in which case we are done) or $\mathrm{Gal}(L/J)^{ab}$ is not a 5-group. Hence J admits a Galois extension E/J contained in L, and of order coprime to 5.

Sub-lemma 1. *E/J is unramified at* 2 *and* 3.

Proof. Let $p \in \{2, 3\}$. Consider ramification degrees e_p. One has

$$e_p(E/J) \mid e_p(L/J) = e_p(L/K)e_p(K/J).$$

Moreover, L/K is unramified at primes above 2 and 3, and $[K : J] = 5$. Thus $e_p(E/J)$ is either 1 or 5, and thus must be 1, since $5 \nmid [E : J]$. □

Continuation of Proof of Lemma 3.4. Thus E/J is a non-trivial abelian extension of degree coprime to 5, unramified outside the unique prime π_J above 5, and tamely ramified at π_J. Such extensions are classified by class field theory. One has by `pari` that $\mathrm{Cl}(\mathcal{O}_J) = 1$. On the other hand, $J/\mathbb{Q}$ is totally ramified at 5, and so $(\mathcal{O}_J/\pi_J\mathcal{O}_J)^* \simeq \mathbb{F}_5^*$ which is generated by the global unit $(1 + \sqrt{5})/2 \equiv -2$. Thus E does not exist. This proves that $L = K$. □

3.2. L/K Wild

Recall that $[L : K] < 24$. In this section, we assume that L/K is wildly ramified and of degree 10, 15 or 20, and leave $[L : K] = 5$ until the next section.

Lemma 3.5. *Let H be a group of order* 10, 15 *or* 20. *Let Γ be an extension of $\mathbb{Z}/5\mathbb{Z}$ by H. Then Γ^{ab} is not a* 5*-group.*

Proof. Let $H' \simeq \mathbb{Z}/5\mathbb{Z}$ be a 5-Sylow subgroup of H. Since $5(1+5) > 20$, H' is the unique 5-Sylow subgroup of H. Thus H' is preserved under automorphisms of H. Conjugation on H by an element of Γ is an automorphism, and thus $gH'g^{-1} = H'$ for any g in Γ. In particular, H' is normal in Γ. The quotient group Γ/H' has order equal to $|H|$. Thus Γ/H', like H, has a normal 5-Sylow subgroup and hence has an abelian quotient of order 2, 3 or 4. Since this quotient is also a quotient of Γ, the lemma is proved. □

Let J be the field $\mathbb{Q}(\zeta_5, 2^{1/5})$. We have the following exact sequence of groups

$$0 \longrightarrow \mathrm{Gal}(L/K) \longrightarrow \mathrm{Gal}(L/J) \longrightarrow \mathrm{Gal}(K/J) \longrightarrow 0.$$

By Lemma 3.5, $\mathrm{Gal}(L/J)^{ab}$ is not a 5-group. Thus J admits an abelian extension of degree coprime to 5, contained in L. The non-existence of such an extension was proved during the proof of Lemma 3.4.

3.3. L/K of degree 5

To finish the proof of Theorem 2.4, we must consider the cases where L/K is either wildly ramified of degree 5, or unramified of degree 5. Assume that we are in one of these cases; we shall arrive at a contradiction. $\mathrm{Gal}(L/\mathbb{Q}(\zeta_5))$ is a group of order 125 that surjects onto $\mathbb{Z}/5\mathbb{Z} \oplus \mathbb{Z}/5\mathbb{Z}$. There are three groups up to isomorphism with this property. All of them admit at least one morphism to $\mathbb{Z}/5\mathbb{Z}$ with kernel $\mathbb{Z}/5\mathbb{Z} \oplus \mathbb{Z}/5\mathbb{Z}$ that factor through the map to $\mathrm{Gal}(K/\mathbb{Q}(\zeta_5))$. Thus there exists a field $D/\mathbb{Q}(\zeta_5)$, contained within K, such that $\mathrm{Gal}(L/D) \simeq \mathbb{Z}/5\mathbb{Z} \oplus \mathbb{Z}/5\mathbb{Z}$.

Lemma 3.6. *There exists an intermediate field E contained in L and containing D such that E is not equal to K and E/D is unramified at primes above* 2 *and* 3.

Proof. Since the root discriminant of L locally at 2 and 3 is bounded by $2^{4/5}$ and $3^{4/5}$ respectively, this lemma is obvious if the root discriminant for D attains these bounds, since then any subgroup of $\mathrm{Gal}(L/D) = \mathbb{Z}/5\mathbb{Z} \oplus \mathbb{Z}/5\mathbb{Z}$ not corresponding to K will produce the required E. Thus we may assume that $D = \mathbb{Q}(p^{1/5}, \zeta_5)$ with p equal to 2 or 3. Assume that $p = 2$. The inertia group $\mathcal{I}_3(L/D)$ is of order 5, since $e_3(L/K) = 1$ and $e_3(K/D) = 5$. Thus we see that the fixed field E of $\mathcal{I}_3(L/D) \subset \mathrm{Gal}(L/D)$ *is* unramified at 3 above D. Moreover, E/D is unramified above 2, since L/K and K/D are. Finally, E is not K since K/D is ramified at 3. An identical argument works for $p = 3$. □

Lemma 3.7. *If $D/\mathbb{Q}$ is wildly ramified at* 5 *then either E/D is unramified at* 5 *or $\Delta_{E/D} = \pi_D^8$ where π_D is the unique prime above* 5 *in D. If D is tamely ramified at* 5, *then $D = \mathbb{Q}(\zeta_5, 24^{1/5})$ and $\Delta_{E/D}$ divides $(\pi_{D,1} \ldots \pi_{D,5})^8$, where $\pi_{D,i}$ are the primes in D above* 5.

Proof. Either $D/\mathbb{Q}$ is tamely ramified at 5 (in which case it is $\mathbb{Q}(\zeta_5, 24^{1/5})$) or it is not. Suppose first that $D/\mathbb{Q}$ is wildly ramified. We may assume also that E/D is wildly ramified, since otherwise it is unramified, and we are done. Let $v_{E/D}$ denote the exponent of π_D in $\Delta_{E/D}$. Suppose that $v_{E/D} \geq 10$. Then $N_{D/\mathbb{Q}}(\Delta_{E/D}) = 5^{v_{E/D}} \geq 5^{10}$, so

$$\delta_{E,5} = \delta_{D,5} N_{D/\mathbb{Q}}(\Delta_{E/D})^{1/100} \geq 5^{23/20} 5^{10/100} = 5^{5/4}.$$

Since $\delta_{E,5}$ divides $\delta_{L,5}$, this estimate contradicts the bound given by Fontaine (Theorem 1.1). Hence $v_{E/D} < 10$. On the other hand, we have the following equality regarding the different ([13], IV. Prop. 4):

$$\sum_{i=0}^{\infty} (|\Gamma_i| - 1) = v_{\pi_E}(\mathfrak{D}_{E/D})$$

where π_E is the prime in E above π_D, and Γ_i is the higher ramification group (in the lower numbering) at π_E. Thus if $v_{E/D}$ is the exponent of π_E in the different $\mathfrak{D}_{E/D}$ (equivalently, the exponent of π_D in the discriminant $\Delta_{E/D}$),

$$v_{E/D} \equiv 0 \bmod 4$$

since $|\Gamma_i| - 1$ is either equal to 4 or 0. Thus since $v_{E/D} < 10$, we have $v_{E/D} = 4$ or 8. Since we have wild ramification, $v_{E/D} > e_{E/D} - 1$. Thus $v_{E/D} = 8$, and $\Delta_{E/D} = \pi_D^8$.

Suppose now that $D = \mathbb{Q}(\zeta_5, 24^{1/5})$. Let $\pi_{K,i}$ be the unique prime above $\pi_{D,i}$ in $\mathcal{O}_K$. Let $\Delta_{L/K} = (\pi_{K,1} \dots \pi_{K,5})^v$ (note all exponents are equal since $L/\mathbb{Q}$ is Galois). If $v \geq 10$ then

$$\delta_{L,5} = \delta_{K,5} N_{K/\mathbb{Q}}(\Delta_{L/K})^{1/500} \geq 5^{23/20} 5^{50/500} = 5^{5/4}$$

contradicting the bound of Fontaine as above. Note that the only ramification in L/D occurs at primes above 5. Thus since $v < 10$,

$$\Delta_{L/D} = \Delta_{K/D}^5 N_{K/D}(\Delta_{L/K}) \mid (\pi_{D,1} \dots \pi_{D,5})^{40+10}$$

where the left hand side *strictly* divides the right as ideals in $\mathcal{O}_D$. If $\pi_{D,i}$ occurs in $\Delta_{E/D}$ with exponent $v_{E/D}$ then

$$\Delta_{L/D} > \Delta_{E/D}^5 = \pi_{D,i}^{5v_{E/D}}$$

and thus $v_{E/D} < 10$. Since $[L : K] = 5$, all ramification groups have order 5 or 1, so as above, $4|v_{E/D}$ and thus $v_{E/D} = 0$ or 8 for each prime $\pi_{D,i}$. In particular $\Delta_{E/D}$ divides $(\pi_{D,1} \dots \pi_{D,5})^8$. □

Since $E/\mathbb{Q}$ is not necessarily Galois, we can not infer in the proof above that $v_{E/D}$ is the same for each $\pi_{D,i}$. However, that will not be necessary for the sequel.

Let us recall now the conductor-discriminant formula (see for example [10], 11.9, p. 557).

Lemma 3.8 (Conductor-Discriminant Formula). *Let B/A be an abelian extension of algebraic number fields. Then*

$$\Delta_{B/A} = \prod_{\chi} \mathfrak{f}(\chi)$$

where the product runs over all characters of Gal(B/A).

Lemma 3.9. *If E/D is ramified, and $D/\mathbb{Q}$ is wildly ramified at* 5 *then the conductor $\mathfrak{f}_{E/D}$ is equal to π_D^2. If $D/\mathbb{Q}$ is tamely ramified (and so $D = \mathbb{Q}(\zeta_5, 24^{1/5})$), then the conductor $\mathfrak{f}_{E/D}$ divides $(\pi_{D,1} \dots \pi_{D,5})^2$.*

Proof. The four nontrivial characters of Gal$(E/D) \simeq \mathbb{Z}/5\mathbb{Z}$ are faithful, and have conductor $\mathfrak{f}_{E/D}$. Thus by the conductor-discriminant formula (Lemma 3.8), $\Delta_{E/D} = (\mathfrak{f}_{E/D})^4$. The result then follows from Lemma 3.7. □

By Lemma 3.9, the possibilities for E will be constrained by the ray class group of $\mathfrak{f} := \pi_D^2$ or $(\pi_{D,1} \dots \pi_{D,5})^2$. We may calculate these groups with the aid of `pari`. The results are tabulated in the table in the appendix (section 5.1), and they indicate the proof of Theorem 2.4 is complete, after noting that all cases where the ray class field is nontrivial, K is the ray class field, contradicting the definition of E.

4. $N = 10$

Let us begin by stating the analogs for $N = 10$ of Theorems 2.4 and 2.5 (another special case of Theorem 3.3 and the proof of Corollary 3.4 in [12]):

Theorem 4.1. *Let $G/\mathbb{Z}[\frac{1}{10}]$ be a finite group scheme of 3-power order such that:*

1. *Inertia at 2 and 5 acts through a cyclic 3-group.*
2. *The action of Inertia on the subquotients $G[3^n](\overline{\mathbb{Q}})/G[3^{n-1}](\overline{\mathbb{Q}})$ is through an order 3 quotient for all n.*

Assume the GRH discriminant bounds of Odlyzko. Then G has a filtration by the group schemes $\mathbb{Z}/3\mathbb{Z}$ and μ_3. Moreover, if G is killed by 3, then $\mathbb{Q}(G) \subseteq H$, where $K := \mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{5}, \zeta_3)$, and H is the Hilbert class field of K, which is of degree 3 over K.

Theorem 4.2 (Schoof). *Let $p = 2$ or 5. Let $G/\mathbb{Z}[\frac{1}{p}]$ be a finite group scheme of 3-power order such that inertia at p acts through a cyclic 3-group. Then G has a filtration by the group schemes $\mathbb{Z}/3\mathbb{Z}$ and μ_3. Moreover, the extension group $\mathrm{Ext}^1(\mu_3, \mathbb{Z}/3\mathbb{Z})$ of group schemes over $\mathbb{Z}[\frac{1}{p}]$ is trivial, and there exists an exact sequence of group schemes*

$$0 \longrightarrow M \longrightarrow G \longrightarrow C \longrightarrow 0$$

where M is a diagonalizable group scheme over $\mathbb{Z}[\frac{1}{p}]$, and C is a constant group scheme.

We delay the proof of theorem 4.1 until Section 4.1.

The situation for $N = 10$ is analogous to $N = 6$, but one technical difficulty is that $\mathcal{I}_p(H/\mathbb{Q})$ is not a normal subgroup of $\mathrm{Gal}(H/\mathbb{Q})$, for either $p = 2$ or $p = 5$. We do however prove the following:

Lemma 4.3. *The primes 2 and 5 split into exactly 3 distinct primes in H.*

Proof. The equivalent statement is true with H replaced by K. Thus it suffices to prove that 2 and 5 remain inert in the extension H/K. The easiest way to see this is by comparing residue field degrees. H is the compositum of K and the Hilbert class field B of $\mathbb{Q}(20^{1/3})$. In $\mathbb{Q}(20^{1/3})$, the primes above 2 and 5 are not principal (a simple check with `pari`), and so remain inert in B. Thus for $p = 2$ and $p = 5$ the residue field degree $f_{B/\mathbb{Q}} = 9$. Since for $p = 2$ and $p = 5$ one finds that $f_{K/\mathbb{Q}} = 3$, it follows that the the primes above 2 and 5 in K remain inert in H. □

It follows from Lemma 4.3 that the subgroups $\mathcal{D}_p(H/\mathbb{Q})$ are of index three in $\mathrm{Gal}(H/\mathbb{Q})$. One sees that $\mathcal{I}_{p'}(H/\mathbb{Q})$ is a set of representatives for the cosets of $\mathcal{D}_p(H/\mathbb{Q})$ in $\mathrm{Gal}(H/\mathbb{Q})$, where $\{p, p'\} = \{2, 5\}$ (as an unordered pair), since the possible fixed fields of $\mathcal{D}_p(H/\mathbb{Q})$ are never fixed by $\mathcal{I}_{p'}(H/\mathbb{Q})$. This leads to the following construction:

Lemma 4.4. *Let $\{p, p'\} = \{2, 5\}$. Let $\overline{\mathcal{M}} \subset A[3]$ be a $\mathcal{D}_p(H/\mathbb{Q})$-module. Let $\sigma \in \mathcal{I}_{p'}(H/\mathbb{Q})$ be a nontrivial element. Then*

$$\widehat{\mathcal{M}} = \overline{\mathcal{M}} + \sigma\overline{\mathcal{M}} = \overline{\mathcal{M}} + (\sigma - 1)\overline{\mathcal{M}}$$

is a $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$*-module. Moreover,* $\dim(\widehat{\mathcal{M}}) \leq 2\dim(\overline{\mathcal{M}})$ *with equality if and only if* $\overline{\mathcal{M}}$ *and* $(\sigma - 1)\overline{\mathcal{M}}$ *have trivial intersection inside* $A[3]$.

Proof. By Grothendieck (Theorem 1.4) one finds that as an endomorphism, for $\sigma \in \mathcal{I}_{p'}$, we have $(\sigma - 1)^2 = 0$ on $A[3]$. Thus $\widehat{\mathcal{M}}$ is an $\mathcal{I}_{p'}$-module. On the other hand, $\overline{\mathcal{M}}$ is a $\mathcal{D}_p$-module, and the coset space $\mathrm{Gal}(H/\mathbb{Q})/\mathcal{D}_p(H/\mathbb{Q})$ is given by $\mathcal{I}_{p'}(H/\mathbb{Q})$. Thus $\widehat{\mathcal{M}}$ is a $\mathrm{Gal}(H/\mathbb{Q})$-module. The final claim is clear from the construction of $\widehat{\mathcal{M}}$. □

.

We now apply this construction not to $\overline{\mathcal{M}}_f(p)$, as in section 2.3, but to $\overline{\mathcal{M}}_t(p)$.

Lemma 4.5. *Fix* $p \in \{2, 5\}$ *and assume that* $\mathrm{ord}_3(\Phi_{\hat{A}}(p))$ *is maximal. Then*

$$A[3] = \widehat{\mathcal{M}}_t(p) + \overline{\mathcal{M}}_f(p).$$

If $\kappa = \widehat{\mathcal{M}}_t(p)$, then from Theorem 2.2,

$$\mathrm{ord}_3(\Phi_{\hat{A}'}(p)) - \mathrm{ord}_5(\Phi_{\hat{A}}(p)) = \dim\ \kappa \cap \overline{\mathcal{M}}_t(p) + \dim\ \kappa \cap \overline{\mathcal{M}}_f(p) - \dim\ \kappa.$$

Since $\overline{\mathcal{M}}_t(p) \subseteq \kappa \cap \overline{\mathcal{M}}_f(p)$, we find that this quantity is at least $2t_p - \dim\ \kappa$. By the maximality assumption on $\mathrm{ord}_3(\Phi_{\hat{A}}(p))$ we conclude that $2t_p - \dim\ \kappa \leq 0$. On the other hand, by Lemma 4.4 we see that $\dim \kappa \leq 2t_p$, with equality if and only if $\overline{\mathcal{M}}$ and $(\sigma - 1)\overline{\mathcal{M}}$ have trivial intersection inside $A[3]$. Thus $\dim \kappa = 2t_p$, and $\overline{\mathcal{M}}$ and $(\sigma - 1)\overline{\mathcal{M}}$ have trivial intersection inside $A[3]$. By Lemma 2.3, the image of $(\sigma - 1)$ on $A[3]$ for $\sigma \in \mathcal{I}_{p'}$ is contained within $\overline{\mathcal{M}}_2(p')$, and thus has dimension at most $t_{p'}$. This immediately proves that $t_p \leq t_{p'}$, and by symmetry, that $t_2 = t_5$. Moreover, equality also forces $\overline{\mathcal{M}}_t(p) = \kappa \cap \overline{\mathcal{M}}_f(p)$. In particular, $\dim(\overline{\mathcal{M}}_f(p) + \widehat{\mathcal{M}}_t(p)) = \dim(\overline{\mathcal{M}}_f(p) + \kappa)$ is at least

$$\dim \overline{\mathcal{M}}_f(p) + \dim \kappa - \dim \kappa \cap \overline{\mathcal{M}}_f(p) = \dim \overline{\mathcal{M}}_f(p) + \dim \kappa - \dim \overline{\mathcal{M}}_t(p)$$

which equals $(2d - t_p) + 2t_p - t_p = 2d$. In other words,

$$A[3] = \widehat{\mathcal{M}}_t(p) + \overline{\mathcal{M}}_f(p).$$

□

Lemma 4.6. *Let* $\{p, p'\} = \{2, 5\}$. *For* $\mathrm{ord}_3(\Phi_{\hat{A}}(p))$ *maximal,* $\mathbb{Q}(A[3])$ *is unramified at p.*

Proof. From Lemma 4.5, we have that $A[3] = \widehat{\mathcal{M}}_t(p) + \overline{\mathcal{M}}_f(p)$. Moreover, we have a direct sum decomposition

$$\widehat{\mathcal{M}}_t(p) = \overline{\mathcal{M}}_t(p) \oplus (\sigma - 1)\overline{\mathcal{M}}_t(p)$$

which follows from the discussion above, since for $\widehat{\mathcal{M}}_t(p)$ to have dimension $2t_p$, $\overline{\mathcal{M}}_t(p)$ and $(\sigma - 1)\overline{\mathcal{M}}_t(p)$ must have trivial intersection. By definition, $\mathcal{I}_p$ acts trivially on $\overline{\mathcal{M}}_f(p)$. Thus it suffices to show that $\mathcal{I}_p$ acts trivially on $\widehat{\mathcal{M}}_t(p)$.

Since $\mathcal{I}_p(H/\mathbb{Q}) = \mathcal{I}_p(H/\mathbb{Q}(\zeta_3))$ for $p \in \{2, 5\}$ it clearly suffices to show that $\mathcal{I}_p(H/\mathbb{Q}(\zeta_3))$ acts trivially on $\widehat{\mathcal{M}}_t(p)$ considered as a $\mathrm{Gal}(H/\mathbb{Q}(\zeta_3))$-module.

Fix a basis for $\overline{\mathcal{M}}_t(p)$, and choose the corresponding basis for $(\sigma - 1)\overline{\mathcal{M}}_t(p)$ whose basis elements are $(\sigma - 1)$ of our chosen basis for $\overline{\mathcal{M}}_t(p)$. Note that $(\sigma - 1)$ *fixes* $(\sigma - 1)\overline{\mathcal{M}}_t(p)$ since $(\sigma - 1)^2 = 0$. Thus with respect to this basis, the action of σ on $\widehat{\mathcal{M}}_t(p)$ is given by the following matrix

$$\rho(\sigma) = \begin{pmatrix} \mathrm{Id}_t & 0 \\ \mathrm{Id}_t & \mathrm{Id}_t \end{pmatrix}$$

where Id_t is an element of $M_t(\mathbb{F}_p)$, the $t \times t$ matrices over $\mathbb{F}_p$, and $\rho(\sigma)$ denotes the image of σ in $\mathrm{Gal}(\mathbb{Q}(\widehat{\mathcal{M}}_t(p))/\mathbb{Q}(\zeta_3))$. By Lemma 2.3, for $\tau \in \mathcal{I}_p$, the module $(\tau - 1)A[3]$ lies within $\overline{\mathcal{M}}_t(p)$. Moreover, $\overline{\mathcal{M}}_t(p) \subseteq \overline{\mathcal{M}}_f(p)$ is fixed by τ. Thus with respect to our basis the action of $\tau \in \mathcal{I}_p$ is given by a matrix

$$\rho(\tau) = \begin{pmatrix} \mathrm{Id}_t & a \\ 0 & \mathrm{Id}_t \end{pmatrix}$$

for some $a \in M_t(\mathbb{F}_p)$. It suffices to prove that $a = 0$, since then we have shown $\mathcal{I}_p$ acts trivially on $A[3]$. Since

$$\mathbb{Q}(\widehat{\mathcal{M}}_t(p)) \subseteq \mathbb{Q}(A[3]) \subseteq H$$

and since $[H : \mathbb{Q}(\zeta_3)] = 27$, the group U generated by $\langle \rho(\sigma), \rho(\tau) \rangle$ is a group of order dividing 27. Moreover, since all powers of a commute with one another, U is a subgroup of $\mathrm{GL}_2(\mathbb{F}_3[a])$. Thus our desired conclusion ($a = 0$) follows from the following result:

Sub-lemma 2. *Let $U \subseteq \mathrm{GL}_2(\mathbb{F}_3[a])$ be a subgroup of order dividing 27 containing the elements*

$$\left\langle \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \right\rangle$$

then $a = 0$.

Proof. If U is abelian, then the commutator $[\sigma, \tau] = 1$, and one computes immediately that $a = 0$. Thus U has order 27. From a classification of all non-abelian groups of order 27, we find that $[U, U]$ is central. From $[\sigma, \tau]\sigma - \sigma[\sigma, \tau] = 0$, we infer that that $a^2 = 2a + a^2 = 0$. In characteristic 3, this proves that $a = 0$. □

Remark. The utility in Lemma 4.6 is that it allows us to reduce arguments for $N = 10$ to the exact analogs of arguments for $N = 6$. The reason is as follows. When $\mathrm{ord}_3(\Phi_{\hat{A}}(p))$ is maximal, Lemma 4.6 implies that $\mathbb{Q}(A[3])$ is unramified at p. Thus $\mathbb{Q}(A[3])$ must be a Galois (over $\mathbb{Q}$) subfield of H fixed by all conjugates of the inertia group $\mathcal{I}_p(H/\mathbb{Q})$. The only such fields are the subfields of $\mathbb{Q}(\zeta_3, p'^{1/3})$. Thus we obtain the desired results of section 2.3 *without* the hypothesis that $\mathcal{I}_p(H/\mathbb{Q})$ is normal in $\mathrm{Gal}(H/\mathbb{Q})$.

We may now establish Theorem 1.3 in much the same way as Theorem 1.2. Let $\{p, p'\} = \{2, 5\}$. Here are the extra steps required to complete the proof:

1. For $\mathrm{ord}_3(\Phi_{\hat{A}}(p))$ maximal, $\mathbb{Q}(A[3])$ is unramified at p by Lemma 4.6. Thus $A[3]$ prolongs to a finite group scheme over $\mathbb{Z}[1/p']$, and from Theorem 4.2 we infer there exists an exact sequence of group schemes (over $\mathbb{Z}[1/p']$)

$$0 \longrightarrow \mu_3^m \longrightarrow A[3] \longrightarrow (\mathbb{Z}/3\mathbb{Z})^n \longrightarrow 0.$$

   The arguments of Lemma 2.8 apply *mutatis mutandis* to show that $m = n = d$ and A has ordinary reduction at 3.
2. The arguments of section 2.4 and Lemma 2.9 hold with 5 replaced by 3 and "2 and 3" replaced by "2 and 5". It suffices to show that $\mathbb{Q}$ does not admit any Galois extensions of order 3 unramified outside 2 and 5. This follows from the Kronecker–Weber theorem.
3. The maximal Galois extension of $\mathbb{Q}$, contained within H and unramified at 2 is $\mathbb{Q}(\zeta_3, 5^{1/3})$. Hence the proof of Lemma 2.10 still applies, since the inertia subgroups of $\mathrm{Gal}(\mathbb{Q}(A[3])/\mathbb{Q})$ when $\mathbb{Q}(A[3]) \subseteq \mathbb{Q}(\zeta_3, 5^{1/3})$ are *normal*. Similarly, a proof of Lemma 2.11 requires us only to note that the maximal unramified at 3 extension of $\mathbb{Q}(\zeta_3)$ inside H is $\mathbb{Q}(\zeta_3, 10^{1/3})$, which *is* ramified at 5.
4. A final contradiction is reached because

$$3^{4d} \leq (1 + \sqrt{3})^{4d}$$

   is not true for $d > 0$. One might remark at this point that since A has good reduction at 3, and since A is defined over $\mathbb{Q}$, the rational 3-torsion injects into $A(\mathbb{F}_p)[3^\infty]$, as follows from standard facts about formal groups (see, for example, [6]). Note this fact is not essential, however, since for any prime q of good reduction, an inclusion of a constant group scheme C into A *automatically* reduces to an inclusion $C(\mathbb{F}_q) \hookrightarrow A(\mathbb{F}_q)$.

Thus it remains to prove Theorem 4.1.

4.1. Group Schemes over $\mathbb{Z}[1/10]$

Since $\mathrm{Gal}(H/\mathbb{Q}(\zeta_3))$ is a 3-group, the discussion at the beginning of section 3 shows that it suffices to prove that if $L = \mathbb{Q}(G \times G_{-1} \times G_2 \times G_5)$ then $L \subseteq H$. One has the following estimate of the root discriminant for L

$$\delta_L < 3^{1+\frac{1}{3-1}} 2^{1-\frac{1}{3}} 5^{1-\frac{1}{3}} = 3^{3/2} 10^{2/3} = 24.118 < 24.258.$$

From the estimates of [8] one finds that $[L : \mathbb{Q}] < 280$, and so $[L : K] < 16$. One sees that that $K := \mathbb{Q}(\sqrt{-3}, \sqrt[3]{2}, \sqrt[3]{5}) \subseteq L$. We wish to prove that $\mathrm{Gal}(L/K)$ is a 3-group. The root discriminant of K is $\delta_K = 3^{7/6} 10^{2/3}$, and so L/K is at most ramified at primes above 3. Let $F = \mathbb{Q}(\sqrt{-3}, \sqrt[3]{10})$. Then $F/\mathbb{Q}(\sqrt{-3})$ is unramified at $\sqrt{-3}$. The prime $\sqrt{-3}$ splits completely in F, and we write $(\sqrt{-3}) = \pi_{F,1}\pi_{F,2}\pi_{F,3}$, $N_{F/\mathbb{Q}}(\pi_{F,i}) = 3$. The extension K/F is totally ramified at each $\pi_{F,i}$. One has $\pi_{F,i} = \pi_{K,i}^3$ for all i, and $N_{K/\mathbb{Q}}(\pi_{K,i}) = 3$.

4.2. L/K Tame

In this section we assume that L/K is a *tame* extension.

Lemma 4.7. *One has* $[L : K] \leq 6$.

Proof. Arguing as in Lemma 3.2 we find that $N_{K/\mathbb{Q}}(\Delta_{L/K}) < 3^{3[L:K]}$. Thus

$$\delta_L = \delta_K N_{K/\mathbb{Q}}(\Delta_{L/K})^{1/[L:\mathbb{Q}]} \leq 3^{7/6} 10^{2/3} 3^{3/18} = 20.082.$$

Yet from the GRH Odlyzko bound, if $[L : \mathbb{Q}] \geq 126$, then $\delta_L > 20.221$. Thus we find $[L : K] \leq 6$. □

If $[L : K] \leq 6$, then either $\mathrm{Gal}(L/K)$ is a 3-group or it surjects onto a nontrivial group of order coprime to 3. In the latter case, L would contain an abelian extension J/K tamely ramified and of degree coprime to 3. Moreover, since L/K is unramified at primes above 2 and 5, a similar conclusion holds for J.

Lemma 4.8. *There are no abelian extensions J/K tamely ramified at primes above* 3 *in K, of order coprime to* 3*, and unramified outside* 3.

Proof. We proceed via class field theory. According to `pari`, the class number of K is 3, its Hilbert class field H being the compositum of K and the Hilbert class field of $\mathbb{Q}(\sqrt{-3}, \sqrt[3]{20})$. Thus by class field theory it suffices (since J/K has order prime to 3) to show that global units of $\mathcal{O}_K$ generate $(\mathcal{O}_K/\pi_{K,1}\pi_{K,2}\pi_{K,3})^*$. On the other hand, since K/F is totally ramified, we have an isomorphism

$$(\mathcal{O}_K/\pi_{K,1}\pi_{K,2}\pi_{K,3})^* \simeq (\mathcal{O}_F/\pi_{F,1}\pi_{F,2}\pi_{F,3})^* \simeq \mathbb{F}_3^* \times \mathbb{F}_3^* \times \mathbb{F}_3^*$$

Hence it suffices to use global units from $\mathcal{O}_F$. Let $v = (\sqrt[3]{10} - 1)/\sqrt{-3}$. Then from `pari` we find that the 2 fundamental units of $\mathcal{O}_F$ are given by

$$\epsilon_1 = \frac{1}{4}v^4 - \frac{1}{2}v^2 + \frac{3}{2}v - \frac{1}{4}$$
$$\epsilon_2 = \frac{1}{4}v^4 - \frac{1}{2}v^3 + \frac{3}{2}v^2 - \frac{1}{4}$$

We find that the images of -1, ϵ_1, and ϵ_2 in $\mathcal{O}_F/\pi_1 \times \mathcal{O}_F/\pi_2 \times \mathcal{O}_F/\pi_3$ are $(-1, -1, -1)$, $(1, 1, -1)$ and $(1, -1, 1)$ respectively. Since these elements generate the group $(\mathbb{F}_3^*)^3$, we are done. □

4.3. L/K Wild

We assume that L/K is wildly ramified at 3, and (for the moment) not a 3-group. If $\mathrm{Gal}(L/K)^{ab}$ is not a 3-group, then there would exist a corresponding extension J/K tame of order coprime to 3. Since no such extensions exist (see the tame case), we may also assume that $\mathrm{Gal}(L/K)^{ab}$ is a 3-group. Let Γ denote the group $\mathrm{Gal}(L/K)$. There should be no confusion between the group Γ and the group scheme Γ, which will not appear again. Let $n = |\Gamma|$. Since $n < 16$, we have $n \in \{6, 12, 15\}$. All groups of order 15 are abelian. If $n = 6$, the only non-abelian group is S_3. Yet $S_3^{ab} = \mathbb{Z}/2\mathbb{Z}$. Thus $n = 12$. The only group Γ of order 12 such that $\Gamma^{ab} = \mathbb{Z}/3\mathbb{Z}$ is the alternating group A_4, which is a nontrivial extension of $\mathbb{Z}/3\mathbb{Z}$ by $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Lemma 4.9. *One has $N_{K/\mathbb{Q}}(\Delta_{L/K}) \geq 3^{66}$, and $N_{K/\mathbb{Q}}(\Delta_{L/K}) \leq 3^{69}$.*

Assume the first bound is violated. Then since $N_{K/\mathbb{Q}}(\Delta_{L/K}) = 3^{3k}$ for some k, it must be bounded by 3^{63}. Since $[L : \mathbb{Q}] = 12 \times 18 = 216$,

$$\delta_L = \delta_K N_{K/\mathbb{Q}}(\Delta_{L/K})^{1/[L:\mathbb{Q}]} \leq 3^{7/6}10^{2/3}3^{63/216} = 23.039 < 23.089.$$

Yet from the GRH Odlyzko bound, $\delta_L > 23.089$. The other inequality is violated if and only if $N_{L/K}(\Delta_{L/K}) \geq 3^{72}$. Yet in this case,

$$\delta_L = \delta_K N_{K/\mathbb{Q}}(\Delta_{L/K})^{1/[L:\mathbb{Q}]} \geq 3^{7/6}10^{2/3}3^{72/216} = 3^{3/2}10^{2/3}.$$

Since $\delta_L < 3^{3/2}10^{2/3}$ by the Fontaine bound, this is a contradiction and thus we are done. □

Denote the primes in L above $\pi_{K,i}$ by $\mathfrak{p}_{i,j}$. Fix a prime $\mathfrak{p} = \mathfrak{p}_{i,j}$, and let $\Gamma_0 \subseteq \Gamma$ (respectively, $\Gamma_1 \subseteq \Gamma$) be the inertia (respectively wild inertia) subgroup corresponding to $\mathfrak{p}$. Since $L/\mathbb{Q}$ is Galois, these groups are well defined up to conjugation. Moreover, Γ_1 is normal in Γ_0, and Γ_0/Γ_1 has prime to 3 order. Since $L/\mathbb{Q}$ is Galois, Γ_i is determined by $\mathfrak{p}$ up to conjugation. Let us simplify some notation. Let $v = v_{\mathfrak{p}}(\mathfrak{D}_{L/K})$, $f = f_{L/K}$, $e = e_{L/K}$, $r = r_{L/K}$. We have standard equalities

$$\mathfrak{D}_{L/K} = \prod_{i=1}^{3}\prod_{j=1}^{r}\mathfrak{p}_{i,j}^{v} \qquad \Delta_{L/K} = \prod_{i=1}^{3}\pi_{K,i}^{frv} \qquad N_{K/\mathbb{Q}}(\Delta_{L/K}) = 3^{3frv}.$$

From the previous lemma, $22 \leq frv \leq 23$. Moreover, $fre = [L : K] = 12$. Since K/L is wildly ramified, 3 divides e. Hence it suffices to show that $e = 3$, $e = 6$ and $e = 12$ all lead to contradictions. If $e = 3$, then $fr = 4$. Yet fr divides 23 or 22, which is impossible. Suppose that $e = 6$. Then $|\Gamma_0| = 6$, and Γ_0 must be a normal subgroup of Γ since it is a subgroup of index 2. If Γ had such a subgroup, then Γ^{ab} would not be a 3-group. Thus we may assume that $e = 12$. If $e = 12$ then the 3-group Γ_1 would be a normal subgroup of $\Gamma_0 = \Gamma$. Since Γ has no such subgroup, we are done, and $\mathrm{Gal}(L/K)$ is a 3-group.

We may therefore assume that L/K is Galois of degree dividing 9, and thus abelian. Let $\mathfrak{f}_{L/K}$ be the conductor of this extension.

Lemma 4.10. *The conductor $\mathfrak{f}_{L/K}$ divides $(\pi_{K,1}\pi_{K,2}\pi_{K,3})^2$.*

Proof. Assume otherwise. Since $L/\mathbb{Q}$ is Galois we infer that $(\pi_{K,1}\pi_{K,2}\pi_{K,3})^3 | \mathfrak{f}_{L/K}$. We consider separately the three possible Galois groups.

Suppose that $\mathrm{Gal}(L/K) \simeq \mathbb{Z}/9\mathbb{Z}$. Then since $\mathbb{Z}/9\mathbb{Z}$ has six faithful characters, by the conductor-discriminant formula (Lemma 3.8), $(\mathfrak{f}_{L/K})^6 | \Delta_{L/K}$. In particular, if $(\pi_{K,1}\pi_{K,2}\pi_{K,3})^3 | \mathfrak{f}_{L/K}$, then $(\pi_{K,1}\pi_{K,2}\pi_{K,3})^{18} | \Delta_{L/K}$ and so

$$\delta_{L,3} = \delta_{K,3} N_{K/\mathbb{Q}}(\Delta_{L/K})^{1/[L:\mathbb{Q}]} \geq 3^{7/6}3^{54/162} = 3^{3/2}$$

contradicting the Fontaine bound.

Suppose that $\mathrm{Gal}(L/K) \simeq \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$. Let χ_i for $i = 1, \dots, 4$ be the four characters of order 3 corresponding to the four degree 3 extensions K_i of K

inside L. Since the compositum $K_i.K_j = L$ for $i \neq j$, the lowest common divisor $(\mathfrak{f}(\chi_i), \mathfrak{f}(\chi_j))$ must equal $\mathfrak{f}_{L/K}$ for all $i \neq j$. In particular, $(\mathfrak{f}_{L/K})^2 | \prod_{i=1}^4 \mathfrak{f}(\chi_i)$, and thus since there are four non-trivial characters of $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$, by the conductor-discriminant formula (Lemma 3.8), $(\mathfrak{f}_{L/K})^6 | \Delta_{L/K}$, and (as above) this contradicts the Fontaine bound.

Suppose that $\mathrm{Gal}(L/K) \simeq \mathbb{Z}/3\mathbb{Z}$. Then by the conductor-discriminant formula (Lemma 3.8), $(\mathfrak{f}_{L/K})^2 | \Delta_{L/K}$, and so

$$\delta_{L,3} = \delta_{K,3} N_{K/\mathbb{Q}}(\Delta_{L/K})^{1/[L:\mathbb{Q}]} \geq 3^{7/6} 3^{18/54} = 3^{3/2}$$

contradicting the Fontaine bound. □

By Lemma 4.10, since L/K has conductor $\mathfrak{f}_{L/K}$ dividing $\mathfrak{f} := (\pi_{K,1}\pi_{K,2}\pi_{K,3})^2$, the possible L are constrained by the ray class group of $\mathfrak{f}$. The result is tabulated in the table in the appendix (section 5.1). In particular, we find that the ray class field of conductor $\mathfrak{f}$ is exactly equal to H, the Hilbert class field of K, completing our proof of Theorem 4.1.

5. Appendix

5.1. Ray Class Fields

Here are some class field computations done using `pari`. They took between fifteen minutes and an hour each on a Sparc–II ULTRA machine running at 333 MHz. The essentials of the `pari` script are below.

K	δ_K	$\mathfrak{f}$	$\lvert\mathrm{Cl}_{\mathfrak{f}}\rvert$
$\mathbb{Q}(\zeta_5, 2^{1/5})$	$5^{23/20}2^{4/5}$	π_K^2	1
$\mathbb{Q}(\zeta_5, 3^{1/5})$	$5^{23/20}3^{4/5}$	π_K^2	1
$\mathbb{Q}(\zeta_5, 6^{1/5})$	$5^{23/20}6^{4/5}$	π_K^2	5
$\mathbb{Q}(\zeta_5, 12^{1/5})$	$5^{23/20}6^{4/5}$	π_K^2	5
$\mathbb{Q}(\zeta_5, 24^{1/5})$	$5^{3/4}6^{4/5}$	$(\pi_{K,1} \ldots \pi_{K,5})^2$	5
$\mathbb{Q}(\zeta_5, 48^{1/5})$	$5^{23/20}6^{4/5}$	π_K^2	5
$\mathbb{Q}(\zeta_3, 2^{1/3}, 5^{1/3})$	$3^{7/6}10^{2/3}$	$(\pi_{K,1}\pi_{K,2}\pi_{K,3})^2$	3

5.2. Pari Script

Here is the `pari` script for fields other than $\mathbb{Q}(\zeta_5, 24^{1/5})$ and $\mathbb{Q}(\zeta_3, 2^{1/3}, 5^{1/3})$, where an adjustment must be made since the conductor is of a slightly different form. The calculation of the discriminant was included as a check against typographical errors in the defining polynomials[2].

[2] Bjorn Poonen points out to me that as written, this `pari` program assumes the GRH during computation. One may remove this assumption from the calculation using `bnfcertify`.

```
allocatemem()
allocatemem()
allocatemem()
allocatemem()
nf=nfinit(poly defining K);
factor(nf[3])
bnf=bnfinit(nf[1],1);
pd=idealprimedec(nf,5);
pd1=idealhnf(nf,pd[1]);
idealnorm(nf,pd1)
pd2=idealmul(nf,pd1,pd1);
bnrclassno(bnf,pd1)
bnrclassno(bnf,pd2)
```

References

[1] Brumer, A., Kramer, K.: Non-existence of certain semistable abelian varieties. Manuscripta Math. **106** (3), 291–304 (2001)

[2] Faltings, G.: Endlichkeitssätze für abelsche Varietäten über Zahlkörpern. Invent. Math. **73**, 349–366 (1983)

[3] Fontaine, J.: Il n'y a pas de variété abélienne sur $\mathbb{Z}$. Invent. Math. **81** (3), 515–538 (1985)

[4] Grothendieck, A.: Groups de monodromie en géométrie algébrique I. (SGA VII), Séminaire de Géométrie Algébrique du Bois-Marie, 1967-1969, Lecture Notes in Math., Vol. **288**. Springer-Verlag, Berlin and New York, 1972, pp. 313–523

[5] Grothendieck, A.: Éléments de géométrie algébrique. IV. Étude locale des schémas et des morphismes de schémas IV. (EGA IV). Inst. Hautes Études Sci. Publ. Math. **32**, 1967

[6] Katz, N.: Galois properties of torsion points on abelian varieties. Invent. Math. **62** (3), 481–502 (1981)

[7] Katz, N., Mazur, B.: Arithmetic Moduli of Elliptic Curves. Annals of Math. Studies **108**, Princeton University Press, Princeton, 1985

[8] Martinet, J.: Petits discriminants des corps de nombres. Journées Arithmétiques 1980, London Math. Soc. Lecture Note Series **56**, Cambridge Univ. Press, 1982

[9] Mazur, B.: Modular curves and the Eisenstein ideal. Publ. Math. I.H.E.S. **47**, 33–186 (1977)

[10] Neukirch, J.: Algebraische Zahlentheorie. Springer–Verlag, 1992

[11] Oort, F., Tate, J.: Group schemes of prime order. Ann. Scient. École. Norm. Sup. (4) **3**, 1–21 (1970)

[12] Schoof, R.: Semi-stable abelian varieties over $\mathbb{Q}$ with bad reduction in one prime only. Preprint

[13] Serre, J-P.: Local Fields. Springer-Verlag, Graduate Texts in Math. **67**