M. YASUDA
KODAI MATH. J.
**31** (2008), 385–403

# TORSION POINTS OF ELLIPTIC CURVES WITH GOOD REDUCTION

Masaya Yasuda

**Abstract**

We consider the torsion points of elliptc curves over certain number fields with good reduction everywhere.[1]

## Introduction

It is well known that there do not exist elliptic curves over $\mathbf{Q}$ with good reduction everywhere. The existence of elliptic curves with good reduction everywhere over quadratic fields was observed by Comalada [2]. We recall that an admissible elliptic curve over a number field $K$ is an elliptic curve defined over $K$, which has good reduction everywhere with a non-trivial 2-division point rational over $K$. Comalada classified admissible elliptic curves over real quadratic fields, dealing with certain diophantine equations in units of real quadratic fields (see [2]). In his paper [7], Kida computed the torsion subgroup of the Mordell-Weil group of admissible elliptic curves over certain real quadratic fields and showed that an admissible elliptic curve over a certain quadratic field $K$ has only $K$-rational points of order $p$ for small prime $p$. In this paper, we consider the torsion points of prime order of elliptic curves over certain number fields with good reduction everywhere. For each prime number $p$, we let $\zeta_p$ denote a primitive $p$-th root of unity. Our main result is the following:

Theorem 0.1. *Let $K$ be a number field having a real place and let $p$ be a prime number. Suppose that $p$ does not divide the class number of $K(\zeta_p)$ and the ramification index $e_{\mathfrak{p}}$ satisfies $e_{\mathfrak{p}} < p - 1$ for all primes $\mathfrak{p}$ of $K$ above $p$. Let $E$ be an elliptic curve over $K$ with good reduction everywhere. Then $E$ has no $K$-rational points of order $p$.*

Let $p$ be an odd prime number. Let $K$ be a number field and let $\mathcal{O}_K$ denote its ring of integers. Our main idea to prove above result is to examine the extensions of a diagonalizable group scheme $\mu_p$ by a constant group scheme $\mathbf{Z}/p\mathbf{Z}$ over the ring $\mathcal{O}_K$. Schoof studied the extensions of $\mu_p$ by $\mathbf{Z}/p\mathbf{Z}$ over $\mathcal{O}_K$,

---

[1] 2000 *Mathematics Subject Classification.* Primary 14L15; Secondary 11G05.

Received August 29, 2007; revised February 29, 2008.

using the equivalence of categories between the category of $\mathcal{O}_K$-group schemes and the category of triples $(G_1, G_2, \theta)$ where $G_1$ is a finite flat $\hat{\mathcal{O}}_K$-group scheme, $G_2$ is a finite flat $\mathcal{O}_K[1/p]$-group scheme and $\theta : G_1 \otimes \hat{\mathcal{O}}_K[1/p] \to G_2 \otimes \hat{\mathcal{O}}_K[1/p]$ is an isomorphism of $\hat{\mathcal{O}}_K[1/p]$-group schemes (see [9]). Here the ring $\hat{\mathcal{O}}_K$ is the inverse limit of the ring $\mathcal{O}_K/p^n\mathcal{O}_K$ for $n \in \mathbf{N}$. In a similar way, we consider the extensions of $\mathbf{Z}/p\mathbf{Z}$ by $\mu_p$ over $\mathcal{O}_K$. In order to study the extensions of $\mathbf{Z}/p\mathbf{Z}$ by $\mu_p$ over $\mathcal{O}_K$, we calculate the extensions of $\mathbf{Z}/p\mathbf{Z}$ by $\mu_p$ over the completion $\mathcal{O}_{K,\mathfrak{p}}$ at the prime $\mathfrak{p}$ of $K$ over $p$ by using Dieudonné theory (see [3]).

Finally we study the finite flat group schemes of prime order over the ring of integers of imaginary quadratic fields $K$ with class number one. In applications, we consider the existence of abelian varieties over $K$ with good reduction everywhere. The existence of such abelian varieties over cyclotomic fields was studied by Schoof (see [9]). According to Schoof's result, there do not exist non-zero abelian varieties over $K = \mathbf{Q}(\sqrt{m})$ with good reduction everywhere for $m \in \{-1, -2, -3, -7, -11\}$ under the Generalized Riemann Hypothesis (see [9]). Using Schoof's approach for the non-existence results of abelian varieties with good reduction everywhere, we get the following result:

THEOREM 0.2. *Let $K = \mathbf{Q}(\sqrt{m})$ be an imaginary quadratic field with class number one and let $p$ be an odd prime number such that $p$ does not divide $m$ and $(m/p) = 1$. Suppose that $p$ does not divide the class number of $K(\zeta_p)$. Let $A$ be an abelian variety over $K$ with bad reduction only at the primes of $K$ over $p$. Then $A$ has no complex multiplication over $K$.*

As a corollary, we get the following result:

COROLLARY 0.3. *There do not exist non-zero abelian varieties over $K = \mathbf{Q}(\sqrt{-19})$ with good reduction everywhere and complex multiplication over $K$.*

NOTATION. The symbols $\mathbf{Z}$, $\mathbf{Q}$, and $\mathbf{C}$ denote, respectively, the ring of rational integers, the field of rational numbers, and the field of complex numbers. If $G$ is a group scheme over a ring $R$, and $n \in \mathbf{Z}$, we write $G[n]$ for the kernel of multiplication $[n]_G : G \to G$.

## 1. Finite flat group schemes over complete discrete valuation rings with low ramification

Let $A = W(k)$ be the ring of Witt vectors over a perfect field $k$ of characteristic $p > 0$. Let $\sigma$ be the Frobenius automorphism on $k$ and $A$. We consider the Dieudonné ring $D_k = A[F, V]$, where $FV = VF = p$, and for each $\lambda \in A$, $F\lambda = \sigma(\lambda)F$ and $\lambda V = V\sigma(\lambda)$. Let $(A', \mathfrak{m})$ be the valuation ring of a finite totally ramified extension $K'$ of $K$, with $e = [K' : K]$ the absolute ramification index of $A'$. Assume $e < p - 1$. The category of finite flat commutative group schemes over $A$ with $p$-power order is denoted by $\mathcal{FF}_A$, and $\widetilde{\mathcal{FF}}_A$ is the full subcategory of objects killed by $p$. We define $\mathcal{FF}_{A'}$, $\widetilde{\mathcal{FF}}_{A'}$, etc.

in a similar manner. Using the anti-equivalence from $\widetilde{\mathscr{F}\mathscr{F}}_{A'}$ to the category of finite Honda systems killed by $p$, we calculate the extensions of group schemes over $A'$ of order $p$.

### 1.1. Review of Honda systems

We recall here the theory of Honda systems (cf. [3]).

For each finite $k$-algebra $R_k$ with radical $R_k^0$, we set

$$CW_k(R_k) = \{\bar{f} = (f_{-n})_{n \geq 0} \mid f_{-n} \in R_k \text{ and for almost all } n, f_{-n} \in R_k^0\}.$$

Let $S_m \in \mathbf{Z}[X_0, \dots, X_m; Y_0, \dots, Y_m]$ denote the $m$-th addition polynomial for $p$-Witt vectors. The functor $CW_k$ is a group functor with respect to the operation

$$(f_{-n})_{n \geq 0} + (g_{-n})_{n \geq 0} = (h_{-n})_{n \geq 0},$$

where

$$h_{-n} = \lim_{m \to \infty} S_m(f_{-n-m}, \dots, f_{-n}; g_{-n-m}, \dots, g_{-n}).$$

The structure of $D_k$-module on $CW_k$ is defined by the relations

$$F((f_{-n})_{n \geq 0}) = (\dots, f_{-n}^p, \dots, f_0^p),$$
$$V((f_{-n})_{n \geq 0}) = (\dots, f_{-n-1}, \dots, f_{-1}),$$
$$[\alpha]((f_{-n})_{n \geq 0}) = (\dots, (\sigma^{-n}\alpha)f_{-n}, \dots, \alpha f_0),$$

where $\alpha \in k$ and $[\alpha] = (\dots, 0, 0, \alpha) \in W(k) = A$ is the Teichmüller representative for $\alpha$. Let $G_k = \operatorname{Spec} R_k$ be a $p$-group scheme over $k$ and let $\triangle : R_k \to R_k \otimes R_k$ be the comultiplication. For each $\bar{f} = (f_{-n})_{n \geq 0} \in CW_k(R_k)$, we set $\triangle \bar{f} = (\triangle f_{-n})_{n \geq 0} \in CW_k(R_k \otimes R_k)$, similarly, $\bar{f} \otimes 1 = (f_{-n} \otimes 1)_{n \geq 0}$ and $1 \otimes \bar{f} = (1 \otimes f_{-n})_{n \geq 0}$. We set

$$M(G_k) = \{\bar{f} \in CW_k(R_k) \mid \triangle \bar{f} = \bar{f} \otimes 1 + 1 \otimes \bar{f}\} = \operatorname{Hom}(G_k, CW_k),$$

where the structure of $D_k$-module on $M(G_k)$ is induced by the corresponding structure on $CW_k$.

Let $M$ be a $D_k$-module. Define $M^{(1)} = A \otimes_A M$ as a $D_k$-module, using $\sigma : A \to A$, with operators $F(\lambda \otimes x) = \sigma(\lambda) \otimes F(x)$ and $V(\lambda \otimes x) = \sigma^{-1}(\lambda) \otimes V(x)$. We have $A$-linear maps $F_0 : M^{(1)} \to M$ and $V_0 : M \to M^{(1)}$, with $F_0 V_0 = p_M$ and $V_0 F_0 = p_{M^{(1)}}$. We define $M_{A'}$ to be the direct limit of the diagram

$$\begin{array}{ccc} \mathfrak{m} \otimes_A M & \xrightarrow{V^M} & p^{-1}\mathfrak{m} \otimes_A M^{(1)} \\ \downarrow \varphi_0^M & & \uparrow \varphi_1^M \\ A' \otimes_A M & \xleftarrow{F^M} & A' \otimes_A M^{(1)} \end{array}$$

in the category of $A'$-modules, where $\varphi_0^M$, $\varphi_1^M$ are the obvious maps, $V^M(\lambda \otimes x) = p^{-1}\lambda \otimes V_0(x)$, and $F^M(\lambda \otimes x) = \lambda \otimes F_0(x)$. More explicity, $M_{A'}$

is the quotient of $(A' \otimes_A M) \oplus (p^{-1}\mathfrak{m} \otimes_A M^{(1)})$ by the submodule

$$\{(\varphi_0^M(u) - F^M(w), \varphi_1^M(w) - V^M(u)) \mid u \in \mathfrak{m} \otimes_A M, w \in A' \otimes_A M^{(1)}\}.$$

There are canonical $A'$-linear maps

$$\iota_M : A' \otimes_A M \to M_{A'},$$
$$\mathscr{F}_M : p^{-1}\mathfrak{m} \otimes_A M^{(1)} \to M_{A'},$$
$$\mathscr{V}_M : M_{A'} \to A' \otimes_A M^{(1)}$$

(the last one induced by $1 \otimes V_0$ on $A' \otimes_A M$ and $p \otimes \mathrm{id}$ on $p^{-1}\mathfrak{m} \otimes_A M^{(1)}$). Using the natural $A$-linear maps $M \to A' \otimes_A M \xrightarrow{\iota_M} M_{A'}$ and $M^{(1)} \to p^{-1}\mathfrak{m} \otimes_A M^{(1)}$, we have the commutative diagram

$$\begin{array}{ccccc} M^{(1)} & \xrightarrow{F_0} & M & \xrightarrow{V_0} & M^{(1)} \\ \downarrow & & \downarrow & & \downarrow \\ p^{-1}\mathfrak{m} \otimes_A M^{(1)} & \xrightarrow{\mathscr{F}_M} & M_{A'} & \xrightarrow{\mathscr{V}_M} & A' \otimes_A M^{(1)}. \end{array}$$

When $M$ has finite $A$-length, the commutative diagram above induces $k$-linear isomorphisms

$$\mathrm{Ker}\, F_0 \simeq \mathrm{Ker}\, \mathscr{F}_M, \quad \mathrm{Coker}\, F_0 \simeq \mathrm{Coker}\, \mathscr{F}_M,$$
$$\mathrm{Ker}\, V_0 \simeq \mathrm{Ker}\, \mathscr{V}_M, \quad \mathrm{Coker}\, V_0 \simeq \mathrm{Coker}\, \mathscr{V}_M$$

(see [3, Lemma 2.4]). The functor $M \rightsquigarrow M_{A'}$ is exact on the category of $D_k$-modules of finite $A$-length (see [3, Lemma 2.2]).

Fix $G = \mathrm{Spec}\, R \in \mathscr{F}\mathscr{F}_{A'}$. We denote by $R_k$ and $R_{K'}$ the closed and generic fibers respectively of $R$ over $A'$. Set $M = M(G_k)$, where $G_k = \mathrm{Spec}\, R_k \in \mathscr{F}\mathscr{F}_k$. Define a continuous $A$-linear map

$$w_R : CW_k(R_k) \to R_{K'}/pR$$

by

$$w_R((a_{-n})) = \sum_{n \geq 0} p^{-n} \hat{a}_{-n}^{p^n} \pmod{pR},$$

where $\hat{a}_{-n} \in R$ is a lift of $a_{-n} \in R_k$ (see [5, Ch. II, Section 5.2]). We define $L_{A'}(G)$ to be the kernel of the $A'$-linear map

$$M_{A'} \to CW_{k,A'}(R_k) = (CW_k(R_k))_{A'} \xrightarrow{w'_R} R_{K'}/\mathfrak{m}R,$$

where $w'_R$ is induced by $w_R$ and a natural surjection $A' \otimes_A CW_k(R_k) \to CW_{k,A'}(R_k)$. The objects of the category $SH^f_{A'}$ of finite Honda systems over $A'$ consist of $(L, M)$ where $M$ is a $D_k$-module of finite $A$-length and where $L$ is an $A'$-submodule of $M_{A'}$ such that the canonical $k$-linear map

$$L/\mathfrak{m}L \to \mathrm{Coker}\, \mathscr{F}_M$$

is an isomorphism and the restriction of $\mathscr{V}_M$ to $L \subseteq M_{A'}$ is injective. The full subcategory of objects killed by $p$ is denoted by $\widetilde{SH}^f_{A'}$. For any $G$ in $\mathscr{F}\mathscr{F}_{A'}$, we define $LM_{A'}(G) = (L_{A'}(G), M(G_k))$. Note that $LM_{A'}(G)$ is an object in $SH^f_{A'}$ and the contravariant functor $LM_{A'} : \mathscr{F}\mathscr{F}_{A'} \to SH^f_{A'}$ is fully faithful and essentially surjective (see [3, Theorem 3.6]). The contravariant functor $LM_{A'}$ induces a functor $\widetilde{LM}_{A'}$ from $\widetilde{\mathscr{F}\mathscr{F}}_{A'}$ to $\widetilde{SH}^f_{A'}$ which is an anti-equivalence of categories.

### 1.2. Finite flat group schemes of order $p$

We now consider the finite flat group schemes over $A'$ of order $p$. Oort and Tate construct certain group schemes over $A'$ of order $p$ as follows (see [8, Theorem 2]): For any pair $a, b \in A'$ with $a \cdot b = p$, define

$$G_{a,b} = \operatorname{Spec} A'[x]/(x^p - ax)$$

and the comultiplication is given by

$$\triangle(x) = x \otimes 1 + 1 \otimes x + \frac{b}{1-p} \sum_{i=1}^{p-1} \frac{x^i}{w_i} \otimes \frac{x^{p-i}}{w_{p-i}},$$

in which $w_1, \ldots, w_{p-1}$ are certain units of $A'$. In particular, $G_{1,p} \simeq \mathbf{Z}/p\mathbf{Z}$ is a constant group scheme and $G_{p,1} \simeq \mu_p$ is a diagonalizable group scheme. Let $a$, $b$, $c$, $d$ be elements of $A'$ with $a \cdot b = p$ and $c \cdot d = p$. Then $G_{a,b}$ and $G_{c,d}$ are isomorphic to each other if and only if there is a unit $u \in (A')^\times$ with

$$c = u^{p-1}a, \quad d = u^{1-p}b.$$

According to the classification of finite group schemes of order $p$ due to Oort and Tate, for any group scheme $G$ over $A'$ of order $p$, there are $a, b \in A'$ with $a \cdot b = p$ such that $G$ is isomorphic to $G_{a,b}$ as group schemes over $A'$.

*Remark* 1.1. For any complete noetherian local ring $R$ with residue characteristic $p > 0$, Oort and Tate showed that $(a, b) \mapsto G_{a,b} = \operatorname{Spec} R[x]/(x^p - ax)$ gives a bijection between equivalence classes of factorizations $p = a \cdot b$ of $p$ in $R$ and the isomorphism classes of $R$-groups of order $p$.

For $a \in A'$, we let $\bar{a}$ denote the residue class in $k$ represented by $a$. According to the Dieudonné theory, finite flat group schemes over $k$ of order $p$ correspond in a one-to-one way to giving a module of length one over the ring $k[F, V]$. For any pair $a, b \in A'$ with $a \cdot b = p$, $(G_{a,b})_k$ corresponds to the Dieudonné module

$$k[F, V]/k[F, V] \cdot (F - \bar{a}, V - \bar{b}^{1/p}).$$

Fix a uniformizer $\pi$ of $A'$ and let $v$ be a valuation of $A'$ with $v(\pi) = 1$. For any pair $a, b \in A'$ with $a \cdot b = p$, consider the finite Honda system $LM_{A'}(G_{a,b})$. Fix $a, b \in A'$ with $a \cdot b = p$. For the convention, set $G = G_{a,b}$ and $R = A'[x]/(x^p - ax)$. We proceed case by case.

CASE $v(a) = 0$.

The Dieudonné module $M(G_k)$ is isomorphic to $k[F, V]$-module $M = k\mathbf{e}$ with $F\mathbf{e} = \bar{a}\mathbf{e}$ and $V\mathbf{e} = 0$. In this case, $A'$-linear map $\mathscr{F}_M : p^{-1}\mathfrak{m} \otimes_A M^{(1)} \to M_{A'}$ is an isomorphism. Since $(L_{A'}(G), M)$ consists of a finite Honda system, we see that $A'$-submodule $L_{A'}(G)$ of $M_{A'}$ is trivial.

CASE $v(b) = 0$.

The Dieudonné module $M(G_k)$ is isomorphic to $k[F, V]$-module $M = k\mathbf{e}$ with $F\mathbf{e} = 0$ and $V\mathbf{e} = \bar{b}^{1/p}\mathbf{e}$. Since the Cartier dual of $G_{a,b}$ is $G_{b,a}$, we see that $L_{A'}(G) = M_{A'}$ due to the construction of the dual Honda system (see [3, p. 292–293]).

CASE $v(a), v(b) > 0$.

Let $v(a) = \ell$ $(1 \le \ell \le e-1)$. The Dieudonné module $M(G_k)$ is isomorphic to $k[F, V]$-module $M = k\mathbf{e}$ with $F\mathbf{e} = 0$ and $V\mathbf{e} = 0$, in which $\mathbf{e}$ corresponds to the element $(\dots, 0, 0, x) \in M(G_k) = M(R_k)$. In this case, any $u \in M_{A'}$ can be uniquely written in the form

$$u = \left(1 \otimes \alpha_0\mathbf{e}, \frac{\pi}{p} \otimes \alpha_1\mathbf{e} + \cdots + \frac{\pi^{p-1}}{p} \otimes \alpha_{e-1}\mathbf{e}\right),$$

with $\alpha_0, \dots, \alpha_{e-1} \in k$. Easy calculation shows that

$$w'_R(u) = \hat{\alpha}_0 x + \frac{\pi}{p}\hat{\alpha}_1^p ax + \cdots + \frac{\pi^{e-1}}{p}\hat{\alpha}_{e-1}^p ax \pmod{\mathfrak{m}R} \in R_{K'}/\mathfrak{m}R,$$

with $\hat{\alpha}_n \in A'$ any lift of $\alpha_n \in k$. We can see that $w'_R(u) = 0$ if and only if

$$\alpha_1 = \cdots = \alpha_{e-\ell-1} = 0 \quad \text{and} \quad \alpha_0 + \overline{\left(\frac{a\pi^{e-\ell}}{p}\right)}\alpha_{e-\ell}^p = 0.$$

Therefore, by definition, $A'$-submodule $L_{A'}(G)$ of $M_{A'}$ is equal to the set

$$\left\{\left(1 \otimes \alpha_0\mathbf{e}, \frac{\pi^{e-\ell}}{p} \otimes \alpha_{e-\ell}\mathbf{e} + \cdots + \frac{\pi^{p-1}}{p} \otimes \alpha_{e-1}\mathbf{e}\right) \in M_{A'} \,\middle|\, \alpha_0 + \overline{\left(\frac{a\pi^{e-\ell}}{p}\right)}\alpha_{e-\ell}^p = 0\right\}.$$

**1.3. Extensions of group schemes of order $p$**

The category $SH^f_{A'}$ is an abelian category. More precisely, if

$$\varphi : (L_1, M_1) \to (L_2, M_2)$$

is a morphism in $SH^f_{A'}$, then $\operatorname{Ker}\varphi = (L', M')$ and $\operatorname{Coker}\varphi = (L'', M'')$ satisfy

$$M' = \operatorname{Ker}[M_1 \to M_2], \quad M'' = \operatorname{Coker}[M_1 \to M_2]$$

and

$$L' = (M')_{A'} \cap L_1, \quad L'' = \mathrm{image}[L_2 \hookrightarrow (M_2)_{A'} \to (M'')_{A'}],$$

and the natural map $\mathrm{Coker}[L_1 \to L_2] \to L''$ is an isomorphism (see [3, Theorem 4.3]). Let $\mathfrak{M}_1, \mathfrak{M}_2 \in \widetilde{SH}^f_{A'}$. Consider the group $\mathrm{Ext}^1_{\widetilde{SH}^f_{A'}}(\mathfrak{M}_2, \mathfrak{M}_1)$ of equivalence classes of exact sequences $0 \to \mathfrak{M}_1 \to \mathfrak{M} \to \mathfrak{M}_2 \to 0$ in the category $\widetilde{SH}^f_{A'}$. Put $\mathfrak{M}_1 = (L_1, M_1)$, $\mathfrak{M} = (L, M)$ and $\mathfrak{M}_2 = (L_2, M_2)$. Then the above sequence is exact if and only if the induced sequences of $D_k$-modules $0 \to M_1 \to M \to M_2 \to 0$ and of $A'$-modules $0 \to L_1 \to L \to L_2 \to 0$ have this property.

Let $a$, $b$, $c$, $d$ be elements of $A'$ with $a \cdot b = p$ and $c \cdot d = p$. Using the anti-equivalence $\widetilde{LM}_{A'} : \widetilde{\mathscr{F}\mathscr{F}}_{A'} \to \widetilde{SH}^f_{A'}$, we obtain that

$$\mathrm{Ext}^1_{\widetilde{\mathscr{F}\mathscr{F}}_{A'}}(G_{a,b}, G_{c,d}) \simeq \mathrm{Ext}^1_{\widetilde{SH}^f_{A'}}(LM_{A'}(G_{c,d}), LM_{A'}(G_{a,b})).$$

We now consider the group $\mathrm{Ext}^1_{\widetilde{SH}^f_{A'}}(LM_{A'}(G_{c,d}), LM_{A'}(G_{a,b}))$. Set $LM_{A'}(G_{a,b}) = (L_1, M_1)$ and $LM_{A'}(G_{c,d}) = (L_2, M_2)$. Fix

$$(L, M) \in \mathrm{Ext}^1_{\widetilde{SH}^f_{A'}}((L_2, M_2), (L_1, M_1)).$$

Since $M_1$ and $M_2$ are $k[F, V]$-modules of length one, we write $M_1 = k\mathbf{e}_1$ and $M_2 = k\mathbf{e}_2$ as before. Then we can choose a basis $\{\mathbf{e}, \mathbf{e}'\}$ for $M$ as a $k$-vector space as follows:

$$0 \to M_1 \xrightarrow{f} M \xrightarrow{g} M_2 \to 0, \tag{1}$$

where $f(\mathbf{e}_1) = \mathbf{e}$, $g(\mathbf{e}) = 0$ and $g(\mathbf{e}') = \mathbf{e}_2$. Since the exact sequence

$$0 \to (M_1)_{A'} \to M_{A'} \to (M_2)_{A'} \to 0$$

is split as $A'$-modules, the $A'$-submodule $L$ of $M_{A'}$ is uniquely determined by $L_1$ and $L_2$. Therefore it suffices to consider the structure of $k[F, V]$-module on $M$. If the actions $F$ and $V$ on $M$ are given by

$$F\mathbf{e} = \alpha\mathbf{e} + \beta\mathbf{e}', \quad V\mathbf{e} = \alpha'\mathbf{e} + \beta'\mathbf{e}',$$
$$F\mathbf{e}' = \gamma\mathbf{e} + \delta\mathbf{e}', \quad V\mathbf{e}' = \gamma'\mathbf{e} + \delta'\mathbf{e}',$$

with $\alpha, \beta, \gamma, \delta, \alpha', \beta', \gamma', \delta' \in k$, we simply write

$$F = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}, \quad V = \begin{pmatrix} \alpha' & \beta' \\ \gamma' & \delta' \end{pmatrix}.$$

We proceed case by case.

Case $v(a) = v(c) = 0$.

Since the sequence (1) is exact as $k[F, V]$-modules, we obtain that the actions of $F$ and $V$ on $M$ are given by

$$F = \begin{pmatrix} \bar{a} & \alpha \\ 0 & \bar{c} \end{pmatrix}, \quad V = \begin{pmatrix} 0 & \beta \\ 0 & 0 \end{pmatrix},$$

with $\alpha, \beta \in k$. Since $FV = VF = 0$ on $M$, we get $\beta = 0$. Therefore the actions of $F$ and $V$ on $M$ are given by

$$F = \begin{pmatrix} \bar{a} & \alpha \\ 0 & \bar{c} \end{pmatrix}, \quad V = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix},$$

with $\alpha \in k$. Note that by these actions on $M$, $(L, M)$ becomes a finite Honda system.

Case $v(a) = v(d) = 0$.

A similar calculation shows that the actions of $F$ and $V$ on $M$ are given by

$$F = \begin{pmatrix} \bar{a} & \alpha \\ 0 & 0 \end{pmatrix}, \quad V = \begin{pmatrix} 0 & 0 \\ 0 & \bar{d}^{1/p} \end{pmatrix},$$

with $\alpha \in k$.

Case $v(a) = 0$, $1 \leq v(c) \leq e - 1$.

A similar calculation shows that the actions of $F$ and $V$ on $M$ are given by

$$F = \begin{pmatrix} \bar{a} & \alpha \\ 0 & 0 \end{pmatrix}, \quad V = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix},$$

with $\alpha \in k$.

Case $1 \leq v(a), v(c) \leq e - 1$.

Since the sequence (1) is exact as $k[F, V]$-modules, we obtain that the actions of $F$ and $V$ on $M$ are given by

$$F = \begin{pmatrix} 0 & \alpha \\ 0 & 0 \end{pmatrix}, \quad V = \begin{pmatrix} 0 & \beta \\ 0 & 0 \end{pmatrix},$$

with $\alpha, \beta \in k$. Since the canonical $k$-linear map $L/\mathfrak{m}L \to \operatorname{Coker} \mathscr{F}_M$ is an isomorphism, we get $\alpha = 0$. Therefore the actions of $F$ and $V$ on $M$ are given by

$$F = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \quad V = \begin{pmatrix} 0 & \beta \\ 0 & 0 \end{pmatrix},$$

with $\beta \in k$. Note that by these actions on $M$, $(L, M)$ becomes a finite Honda system.

Considering the Cartier dual, we get the following results:

Theorem 1.2. *Let $q = p^f$ and assume $k = \mathbf{F}_q$. Let $a$, $b$, $c$, $d$ be elements of $A'$ with $a \cdot b = p$ and $c \cdot d = p$.*

(1) *If* $v(a) \neq 0$ *and* $v(c) = 0$, *we have* $\mathrm{Ext}^1_{\mathscr{F}\mathscr{F}_{A'}}(G_{a,b}, G_{c,d}) = 0$.
(2) *If* $v(a) = 0$ *or* $v(c) \neq 0$, *we have*

$$\dim_{\mathbf{F}_p} \mathrm{Ext}^1_{\widetilde{\mathscr{F}\mathscr{F}_{A'}}}(G_{a,b}, G_{c,d}) = f.$$

*Proof*. (1) In this case, we see that $G_{a,b}$ is connected while $G_{c,d}$ is étale. This implies that $\mathrm{Ext}^1_{\mathscr{F}\mathscr{F}_{A'}}(G_{a,b}, G_{c,d}) = 0$.

(2) This follows from calculations above. □

## 2. Extensions of $\mu_p$ by $\mathbf{Z}/p\mathbf{Z}$ and of $\mathbf{Z}/p\mathbf{Z}$ by $\mu_p$

Let $K$ be a number field and $p$ be a prime number. In this section, we consider the groups of extensions of a diagonalizable group scheme $\mu_p$ by a constant group scheme $\mathbf{Z}/p\mathbf{Z}$ and of extensions of $\mathbf{Z}/p\mathbf{Z}$ by $\mu_p$ over the ring of integers $\mathcal{O}_K$ of $K$.

### 2.1. An equivalence of categories

Let $R$ be a Noetherian ring, let $p \in R$ and let $\underline{Gr}_R$ denote the category of finite flat $R$-group schemes. Let

$$\hat{R} = \varprojlim R/p^n R$$

and let $\underline{C}$ be the category of triples $(G_1, G_2, \theta)$ where $G_1$ is a finite flat $\hat{R}$-group scheme, $G_2$ is a finite flat $R[1/p]$-group scheme and

$$\theta : G_1 \otimes_{\hat{R}} \hat{R}[1/p] \to G_2 \otimes_{R[1/p]} \hat{R}[1/p]$$

is an isomorphism of $\hat{R}[1/p]$-group schemes. Morphisms in $\underline{C}$ are pairs of morphisms of group schemes that are compatible with the morphisms $\theta$. The functor $\underline{Gr}_R \to \underline{C}$ that sends an $R$-group scheme $G$ to the triple

$$(G \otimes_R \hat{R}, G \otimes_R R[1/p], \mathrm{id} \otimes_R \hat{R}[1/p])$$

is an equivalence of categories (see [1, Theorem 2.6]). The equivalence of categories above gives the following result (see [9, Corollary 2.4]):

Theorem 2.1. *Let* $G$ *and* $H$ *be two finite flat group schemes over* $R$. *There is a natural exact "Mayer-Vietoris" sequence*

$$0 \to \mathrm{Hom}_R(G,H) \to \mathrm{Hom}_{\hat{R}}(G,H) \times \mathrm{Hom}_{R[1/p]}(G,H) \to \mathrm{Hom}_{\hat{R}[1/p]}(G,H)$$

$$\xrightarrow{\delta} \mathrm{Ext}^1_R(G,H) \to \mathrm{Ext}^1_{\hat{R}}(G,H) \times \mathrm{Ext}^1_{R[1/p]}(G,H) \to \mathrm{Ext}^1_{\hat{R}[1/p]}(G,H),$$

*where* $\delta$ *maps an* $\hat{R}[1/p]$*-morphism* $\varphi : G \to H$ *to the extension of* $G$ *by* $H$ *that corresponds to the triple*

$$((H \times G)_{\hat{R}}, (H \times G)_{R[1/p]}, \theta),$$

*where* $\theta(h,g) = (h + \varphi(g), g)$.

In the applications, $R$ is the ring of integers of a number field $K$, the element $p$ is a prime number, and $G$ and $H$ are $p$-group schemes. Then $G$ and $H$ are étale over $R[1/p]$ and we can identify them with their Galois modules. The Galois action is unramified outside $p$. The ring $\hat{R}$ is a finite product of finite extensions of $\mathbf{Z}_p$. Finally, the ring $\hat{R}[1/p] \cong K \otimes \mathbf{Q}_p$ is a product of $p$-adic fields. Over each of these fields the group schemes can be identified with their local Galois modules.

### 2.2. Extensions of $\mu_p$ by $\mathbf{Z}/p\mathbf{Z}$ and of $\mathbf{Z}/p\mathbf{Z}$ by $\mu_p$

Let $p$ be a prime number and let $\zeta_p$ denote a primitive $p$-th root of unity. Let $K$ be a number field and let $\mathcal{O}_K$ and $\mathcal{O}_K^\times$ denote its ring of integers and its group of units. For each prime $\mathfrak{p}$ of $K$ over $p$, let $e_\mathfrak{p}$ and $f_\mathfrak{p}$ denote the ramification index and the residue degree of $\mathfrak{p}$ in the extension $K/\mathbf{Q}$, respectively.

THEOREM 2.2. *Let $K$ be a number field and let $p$ be a prime number. Suppose that $p$ does not divide the class number of $K(\zeta_p)$ and the ramification index $e_\mathfrak{p}$ satisfies $e_\mathfrak{p} < p-1$ for all primes $\mathfrak{p}$ of $K$ over $p$. Then we have*
(1) $\mathrm{Ext}^1_{\mathcal{O}_K}(\mu_p, \mathbf{Z}/p\mathbf{Z}) = 0$.
(2) $\dim_{\mathbf{F}_p} \mathrm{Ext}^1_{\mathcal{O}_K,p}(\mathbf{Z}/p\mathbf{Z}, \mu_p) \le \sum_{\mathfrak{p}|p} f_\mathfrak{p}$.
*Here the index '$p$' means 'the $p$-torsion part'.*

*Proof.* (1) This is proved by Schoof (see [9, Theorem 2.6]).

(2) Since $e_\mathfrak{p} < p-1$ for all primes $\mathfrak{p}$ over $p$, the $p$-th roots of unity are not contained in any of the completions at $\mathfrak{p}$. This implies that $\mathrm{Hom}_{\hat{\mathcal{O}}_K[1/p]}(\mathbf{Z}/p\mathbf{Z}, \mu_p) = 0$. Therefore, by Theorem 2.1, there is an exact sequence

$$0 \to \mathrm{Ext}^1_{\mathcal{O}_K}(\mathbf{Z}/p\mathbf{Z}, \mu_p) \to \mathrm{Ext}^1_{\hat{\mathcal{O}}_K}(\mathbf{Z}/p\mathbf{Z}, \mu_p) \times \mathrm{Ext}^1_{\mathcal{O}_K[1/p]}(\mathbf{Z}/p\mathbf{Z}, \mu_p)$$
$$\to \mathrm{Ext}^1_{\hat{\mathcal{O}}_K[1/p]}(\mathbf{Z}/p\mathbf{Z}, \mu_p).$$

Fix $G \in \mathrm{Ext}^1_{\mathcal{O}_K,p}(\mathbf{Z}/p\mathbf{Z}, \mu_p)$, which is split over $\hat{\mathcal{O}}_K$. Since $G$ is killed by $p$ and split over $\hat{\mathcal{O}}_K$, the extension $L$ obtained by adjoining the points of $G$ to $K(\zeta_p)$ has degree dividing $p$ and is unramified at all primes. Since $p$ does not divide the class number of $K(\zeta_p)$, it follows that $L = K(\zeta_p)$. Therefore $G$ is split over $\mathcal{O}_K[1/p]$ and hence $G$ is split over $\mathcal{O}_K$. Therefore we have

$$\dim_{\mathbf{F}_p} \mathrm{Ext}^1_{\mathcal{O}_K,p}(\mathbf{Z}/p\mathbf{Z}, \mu_p) \le \dim_{\mathbf{F}_p} \mathrm{Ext}^1_{\hat{\mathcal{O}}_K,p}(\mathbf{Z}/p\mathbf{Z}, \mu_p).$$

This completes the proof by Theorem 1.2. □

The group $\mathrm{Ext}^1_{\mathcal{O}_K,p}(\mathbf{Z}/p\mathbf{Z}, \mu_p)$ may be non-trivial when the ring $\mathcal{O}_K$ contains certain units. The group schemes constructed by Katz and Mazur provide examples of such non-trivial extensions (see [6, Interlude (8.7)]). Let $R$ be a ring and let $\varepsilon \in R^\times$. Consider the $R$-algebra

$$A = \bigoplus_{i=0}^{p-1} R[X_i]/(X_i^p - \varepsilon^i).$$

For any $R$-algebra $S$ with connected spectrum, the $S$-points of $T_\varepsilon = \operatorname{Spec} A$ are pairs $(s,i)$ with $0 \le i \le p-1$ and $s \in S$ satisfying $s^p = \varepsilon^i$. The scheme $T_\varepsilon$ is a finite flat $R$-algebra scheme with multiplication of two pairs $(s,i)$ and $(t,j)$ given by

$$(s,i)\cdot(t,j) = \begin{cases} (st, i+j) & \text{if } i+j < p, \\ (st/\varepsilon, i+j-p) & \text{if } i+j \ge p. \end{cases}$$

The group scheme $T_\varepsilon$ is killed by $p$. The projection $A \to R[X_0]/(X_0^p - 1)$ induces a closed flat immersion of $\mu_p$ in $T_\varepsilon$. There is an exact sequence

$$0 \to \mu_p \to T_\varepsilon \to \mathbf{Z}/p\mathbf{Z} \to 0.$$

Two extensions $T_\varepsilon$ and $T_{\varepsilon'}$ are isomorphic whenever $\varepsilon/\varepsilon'$ is a $p$-th power. If $R$ is a field, the points of $T_\varepsilon$ generate the field extension $R(\zeta_p, \sqrt[p]{\varepsilon})$.

## 3. Finite flat group schemes of prime order over certain number fields

Let $K$ be a number field. Let $\mathcal{O}_K$ and $\mathcal{O}_K^\times$ denote its ring of integers and its group of units. We shall review here the classification of group schemes of prime order over $\mathcal{O}_K$ due to Oort and Tate (see [8]). Fix a prime number $p$. Let $M$ be the set of non-generic points of $\operatorname{Spec}(\mathcal{O}_K)$ and let $M_p$ denote the set of $\mathfrak{p} \in M$ such that $\mathfrak{p}$ divides $p$. For each $\mathfrak{p} \in M$, let $\mathcal{O}_{K,\mathfrak{p}}$ denote the completion of $\mathcal{O}_K$ at $\mathfrak{p}$, let $K_\mathfrak{p}$ denote the field of fractions of $\mathcal{O}_{K,\mathfrak{p}}$, and let $U_\mathfrak{p}$ denote the group of units in $\mathcal{O}_{K,\mathfrak{p}}$. For each $\mathfrak{p} \in M_p$, we let $v_\mathfrak{p}$ denote the corresponding normalized discrete valuation of $K$, let $k_\mathfrak{p}$ denote the residue field of $\mathcal{O}_{K,\mathfrak{p}}$ and let $u \mapsto \bar{u}$ denote the residue class map $\mathcal{O}_{K,\mathfrak{p}} \to k_\mathfrak{p}$. Let $C_K$ denote the idèle class group of $K$. Let $E$ denote the functor which associates with commutative ring $R$ with unity the set $E(R)$ of isomorphism classes of $R$-groups of order $p$. Then they showed that the square

$$\begin{array}{ccc} E(\mathcal{O}_K) & \longrightarrow & \prod_{\mathfrak{p}\in M} E(\mathcal{O}_{K,\mathfrak{p}}) \\ \downarrow & & \downarrow \\ E(K) & \longrightarrow & \prod_{\mathfrak{p}\in M} E(K_\mathfrak{p}) \end{array} \tag{2}$$

is cartesian (see [8, Lemma 4]). Using class field theory, there are canonical bijections

$$E(K) \simeq \operatorname{Hom}_{\text{cont}}(C_K, \mathbf{F}_p^\times),$$
$$E(K_\mathfrak{p}) \simeq \operatorname{Hom}_{\text{cont}}(K_\mathfrak{p}^\times, \mathbf{F}_p^\times) \quad (\mathfrak{p} \in M) \quad \text{and}$$
$$E(\mathcal{O}_{K,\mathfrak{p}}) \simeq \operatorname{Hom}_{\text{cont}}(K_\mathfrak{p}^\times/U_\mathfrak{p}, \mathbf{F}_p^\times) \quad (\mathfrak{p} \in M\backslash M_p),$$

where $\operatorname{Hom}_{\text{cont}}$ denotes the continuous homomorphisms (see [8, Lemma 6]). Via these bijections the arrows in the diagram (2) are induced by the canonical homomorphisms $K_{\mathfrak{p}}^{\times} \to C_K$ and $K_{\mathfrak{p}}^{\times} \to K_{\mathfrak{p}}^{\times}/U_{\mathfrak{p}}$. If $G$ is an $\mathcal{O}_K$-group scheme of order $p$, we shall denote by $\psi^G \in \mathrm{Hom}_{\mathrm{cont}}(C_K, \mathbf{F}_p^{\times})$ the idéle class character determined by $G \otimes_{\mathcal{O}_K} K$, and by $\psi_{\mathfrak{p}}^G$ the corresponding character of $K_{\mathfrak{p}}^{\times}$, for each $\mathfrak{p} \in M$. For each $\mathfrak{p} \in M_p$, we let $n_{\mathfrak{p}}^G = v(a)$, where $a \in \mathcal{O}_{K,\mathfrak{p}}$ is such that $G \otimes_{\mathcal{O}_K} \mathcal{O}_{K,\mathfrak{p}} \simeq (G_{a,b})_{\mathcal{O}_{K,\mathfrak{p}}}$ in the notation of remark 1.1. Note that $a$ is determined up to $U_{\mathfrak{p}}^{p-1}$ by $G \otimes_{\mathcal{O}_K} \mathcal{O}_{K,\mathfrak{p}}$, hence $n_{\mathfrak{p}}^G$ is uniquely determined by $G$. They showed the following theorem (see [8, Theorem 3]):

Theorem 3.1. *The map $G \mapsto (\psi^G, (n_{\mathfrak{p}}^G)_{\mathfrak{p} \in M_p})$ gives a bijection between the isomorphism classes of $\mathcal{O}_K$-groups of order $p$ and the systems $(\psi, (n_{\mathfrak{p}})_{\mathfrak{p} \in M_p})$ consisting of a continuous homomorphism $\psi : C_K \to \mathbf{F}_p^{\times}$ and for each $\mathfrak{p} \in M_p$ an integer $n_{\mathfrak{p}}$ such that $0 \le n_{\mathfrak{p}} \le v_{\mathfrak{p}}(p)$, which satisfy the following conditions*:

(1) *For $\mathfrak{p} \in M \backslash M_p$, $\psi$ is unramified at $\mathfrak{p}$, i.e. $\psi_{\mathfrak{p}}(U_{\mathfrak{p}}) = 1$,*

(2) *For $\mathfrak{p} \in M_p$, $\psi_{\mathfrak{p}}(u) = (\mathrm{Nm}_{k_{\mathfrak{p}}/\mathbf{F}_p}(\bar{u}))^{-n_{\mathfrak{p}}}$.*

*Here $\psi_{\mathfrak{p}} : K_{\mathfrak{p}}^{\times} \to \mathbf{F}_p^{\times}$ denotes the local character induced by $\psi$ via the canonical map $K_{\mathfrak{p}}^{\times} \to C_K$ and $\mathrm{Nm}_{k_{\mathfrak{p}}/\mathbf{F}_p}$ denotes the norm map.*

For a given family of integers $(n_{\mathfrak{p}})_{\mathfrak{p} \in M_p}$, there is either no idèle class character $\psi$ satisfying (1) and (2) of Theorem 3.1, or the set of all idèle characters is a principal homogeneous space under the group of homomorphisms of the ideal class group $\mathrm{Cl}(K)$ of $K$ into $\mathbf{F}_p^{\times}$. Therefore, if the class number of $K$ is prime to $(p-1)$, there is at most one $\psi$ for each family $(n_{\mathfrak{p}})_{\mathfrak{p} \in M_p}$.

### 3.1. Imaginary quadratic fields of class number one

Let $K = \mathbf{Q}(\sqrt{m})$ be a quadratic field, where $m$ is a square-free integer. Let $\zeta_n$ denote a primitive $n$-th root of unity. Set

$$N = \begin{cases} |m| & \text{if } m \equiv 1 \pmod 4, \\ 4|m| & \text{if } m \equiv 2, 3 \pmod 4. \end{cases}$$

We have $K \subset \mathbf{Q}(\zeta_N)$. For an odd prime $p$ and integer $a$ not divisible by $p$, we let $(a/p)$ denote the quadratic residue symbol. We give here a lemma which we use later.

Lemma 3.2. *Let $p$ be an odd prime number. Let $n$ denote the degree of the extension $\mathbf{Q}(\zeta_{p \cdot N})/K(\zeta_p)$. Suppose $p$ divides neither $n$ nor the class number of the cyclotomic field $\mathbf{Q}(\zeta_{p \cdot N})$. Then the class number of the field $K(\zeta_p)$ is not divisible by $p$.*

*Proof.* If the class number of the field $K(\zeta_p)$ is divisible by $p$, then there exists an abelian extension $H/K(\zeta_p)$ which is unramified everywhere of $p$-power degree. Since $p$ is prime to $n$, the abelian extension $H \cdot \mathbf{Q}(\zeta_{p \cdot N})/\mathbf{Q}(\zeta_{p \cdot N})$ is unramified everywhere of $p$-power degree. By assumption, this is a contadiction. □

Assume that $K$ is an imaginary quadratic field of class number one. As is well known, there are nine imaginary quadratic fields of class number one. These fields are

$$\mathbf{Q}(\sqrt{-1}),\ \mathbf{Q}(\sqrt{-2}),\ \mathbf{Q}(\sqrt{-3}),\ \mathbf{Q}(\sqrt{-7}),\ \mathbf{Q}(\sqrt{-11}),$$
$$\mathbf{Q}(\sqrt{-19}),\ \mathbf{Q}(\sqrt{-43}),\ \mathbf{Q}(\sqrt{-67}),\ \mathbf{Q}(\sqrt{-163}).$$

We consider the finite flat group schemes over $\mathcal{O}_K$ of prime order.

Proposition 3.3. *Let $p$ be an odd prime number such that $p$ does not ramify in $K$. Then the only group schemes of order $p$ over $\mathcal{O}_K$ are $\mu_p$ and $\mathbf{Z}/p\mathbf{Z}$.*

*Proof.* In the case that $(m/p) = -1$, this is proved by Oort and Tate (see [8, Corollary of Theorem 3]). In the case that $(m/p) = 1$, there are two primes $\mathfrak{p}$, $\bar{\mathfrak{p}}$ in $K$ over $p$. We introduce the usual notation. For any integral ideal $\mathfrak{a}$ of $K$, we let $U(\mathfrak{a})$ be the subgroup of the idéle group $\mathbf{A}_K^\times$ of $K$ defined by

$$U(\mathfrak{a}) = \{s \in \mathbf{A}_K^\times \mid s_\mathfrak{p} \in U_\mathfrak{p} \text{ and } s_\mathfrak{p} \equiv 1 \pmod{\mathfrak{a}\mathcal{O}_{K,\mathfrak{p}}} \text{ for all primes } \mathfrak{p}\}.$$

Let $\overline{U}(\mathfrak{a})$ be the image of $U(\mathfrak{a})$ of the canonical map $\mathbf{A}_K^\times \to C_K$ and set

$$\mathrm{Cl}(K, \mathfrak{a}) = C_K/\overline{U}(\mathfrak{a}).$$

Since the field $K$ has no real places, there is an exact sequence

$$1 \to (\mathcal{O}_K/\mathfrak{a})^\times/\mathrm{img}\,\mathcal{O}_K^\times \to \mathrm{Cl}(K, \mathfrak{a}) \to \mathrm{Cl}(K) \to 0,$$

where img $\mathcal{O}_K^\times$ denotes the image of $\mathcal{O}_K^\times$ of the natural map $\mathcal{O}_K^\times \to (\mathcal{O}_K/\mathfrak{a})^\times$.

For the family $(n_\mathfrak{p}, n_{\bar{\mathfrak{p}}}) = (1, 0)$, we assume that there is a continuous homomorphism $\psi : C_K \to \mathbf{F}_p^\times$ satisfying the conditions (1) and (2) of Theorem 3.1. Then we have a surjective homomorphism $\bar{\psi} : \mathrm{Cl}(K, \mathfrak{p}) \to \mathbf{F}_p^\times$ induced by $\psi$. Since the class number of $K$ is equal to 1, we have an isomorphism

$$(\mathcal{O}_K/\mathfrak{p})^\times/\mathrm{img}\,\mathcal{O}_K^\times \simeq \mathrm{Cl}(K, \mathfrak{p}).$$

Since $\pm 1 \in \mathcal{O}_K^\times$, this is a contradiction. In a similar way, there is no idèle class character $\psi$ satisfying the conditions (1) and (2) of Theorem 3.1 for the family $(n_\mathfrak{p}, n_{\bar{\mathfrak{p}}}) = (0, 1)$. Therefore the $\mathcal{O}_K$-group schemes of order $p$ are $\mu_p$ and $\mathbf{Z}/p\mathbf{Z}$. □

An abelian variety over a number field $k$ is said to have *good reduction* if it has good reduction at every finite place of the ring of integers of $k$. We now consider an abelian variety $A$ over $K$ with good reduction. Recently, Schoof proved that for every conductor $f \in \{1, 3, 4, 5, 7, 8, 9, 12\}$ there do not exist non-zero abelian varieties over $\mathbf{Q}(\zeta_f)$ with good reduction (see [9, Theorem 1.1]). Assuming the Generalized Riemann Hypothesis (GRH), he proved the same results when $f = 11$ and 15 (see [9, Theorem 1.1]). Therefore there do not exist non-zero abelian varieties over $K = \mathbf{Q}(\sqrt{m})$ with good reduction everywhere for $m \in \{-1, -2, -3, -7, -11\}$ under the GRH.

Let $K = \mathbf{Q}(\sqrt{m})$ be an imaginary quadratic field with class number one. Let $p$ be an odd prime number such that $p$ does not ramify in $K$. We now consider an abelian variety $A$ over $K$ with bad reduction only at the primes of $K$ over $p$. Let $\mathscr{A}$ be the Néron model of $A$ over $\mathcal{O}_K$. Since $A$ has bad reduction only at the primes of $K$ over $p$, note that $\mathscr{A}[p^n]$ is a finite flat group scheme over $\mathcal{O}_K[1/p]$. Let $\mathfrak{p}$ be a prime of $K$ over $p$. Note that any finite flat group scheme over $K_{\mathfrak{p}}$ of $p$-power order admits a prolongation over $\mathcal{O}_{K,\mathfrak{p}}$ (see [5, Théorème 3.3.3]). Therefore there is a finite flat group scheme $G$ over $\mathcal{O}_K$ such that $G$ is isomorphic to $\mathscr{A}[p^n]$ over $\mathcal{O}_K[1/p]$, using the equivalence of categories between the category $\underline{Gr}_{\mathcal{O}_K}$ of $\mathcal{O}_K$-group schemes and the category $\underline{C}$ of triples $(G_1, G_2, \theta)$ where $G_1$ is a finite flat $\hat{\mathcal{O}}_K$-group scheme, $G_2$ is a finite flat $\mathcal{O}_K[1/p]$-group scheme and $\theta : G_1 \otimes \hat{\mathcal{O}}_K[1/p] \to G_2 \otimes \hat{\mathcal{O}}_K[1/p]$ is an isomorphism of $\hat{\mathcal{O}}_K[1/p]$-group schemes. For the convention, we simply write $\mathscr{A}[p^n]$ for $G$.

Lemma 3.4. *Let $p$ be an odd prime number such that $p$ does not ramify in $K$ and $(m/p) = 1$. Assume $A$ has complex multiplication over $K$. Then the finite flat group scheme $\mathscr{A}[p^n]$ admits a filtration*

$$0 = G_s \subset G_{s-1} \subset \cdots \subset G_1 \subset G_0 = \mathscr{A}[p^n]$$

*by closed flat subgroup schemes such that successive subquotients $G_i/G_{i+1}$ have order $p$.*

*Proof.* Let $G$ be a simple subgroup scheme of $\mathscr{A}[p^n]$. Set $L = K(G(\overline{K}))$ and let $S_p$ be the $p$-Sylow subgroup of $\mathrm{Gal}(L/K)$. Since $A$ has complex multiplication over $K$, it follows that the group $\mathrm{Gal}(K(A[p^n])/K)$ is abelian (see [10, Corollar 2 of Theorem 5]).

Therefore the group $\mathrm{Gal}(L/K)$ is abelian and hence the $S_p$-fixed points $G(\overline{K})^{S_p}$ is a $\mathrm{Gal}(L/K)$-submodule of $G(\overline{K})$. Since

$$\#G(\overline{K}) \equiv \#G(\overline{K})^{S_p} \pmod{p},$$

we see that $G(\overline{K})^{S_p}$ is non-trivial. Since $G$ is simple, it follows that $G(\overline{K}) = G(\overline{K})^{S_p}$. Let $L'$ be the fixed field of $S_p$. Then $G(\overline{K})$ is a $\mathrm{Gal}(L'/K)$-module. By assumption, there are two primes $\mathfrak{p}$, $\bar{\mathfrak{p}}$ of $K$ over $p$. If $v$ is a non-archimedean place, set $U_v^{(n)} = \{x \in U_v \mid v(x-1) \geq n\}$. Let $\mathscr{N}$ be the norm subgroup of $\mathbf{A}_K^\times$ defined by

$$\mathscr{N} = \left( U_{\mathfrak{p}}^{(1)} \times U_{\bar{\mathfrak{p}}}^{(1)} \times \prod_{v \neq \mathfrak{p}, \bar{\mathfrak{p}}} U_v \right) \cdot \mathbf{K}^\times,$$

where $U_v = \mathbf{C}^\times$ for the archimedean places $v$ and $\mathbf{K}^\times$ is the image of $K^\times$ on the diagonal. By class field theory, there is a surjection $\mathbf{A}_K^\times/\mathscr{N} \to \mathrm{Gal}(L'/K)$. Let $V_K$ be the image of the global units of $K$ in

$$\Gamma = U_{\mathfrak{p}}/U_{\mathfrak{p}}^{(1)} \times U_{\bar{\mathfrak{p}}}/U_{\bar{\mathfrak{p}}}^{(1)}.$$

Then we have the exact sequence

$$0 \to \Gamma/V_K \to \mathbf{A}_K^\times/\mathcal{N} \to \mathbf{A}_K^\times \Big/ \left( \left( \prod_v U_v \right) \cdot \mathbf{K}^\times \right) \to 0.$$

Here, the last quotient is isomorphic to the ideal class group of $K$, which is trivial. Therefore the group $\mathrm{Gal}(L'/K)$ has exponent dividing $p-1$. The $\mathbf{F}_p[\mathrm{Gal}(L'/K)]$-module $G(\bar{K})$ is therefore a product of 1-dimensional eigenspaces. Since $G$ is simple, there is only one such eigenspaces and $G$ has order $p$. In a similar way, the finite flat group scheme $\mathscr{A}[p^n]$ admits a filtration

$$0 = G_s \subset G_{s-1} \subset \cdots \subset G_1 \subset G_0 = \mathscr{A}[p^n]$$

by closed flat subgroup schemes such that successive subquotients $G_i/G_{i+1}$ have order $p$. □

THEOREM 3.5. *Let $K = \mathbf{Q}(\sqrt{m})$ be an imaginary quadratic field with class number one and let $p$ be an odd prime number such that $p$ does not ramify in $K$ and $(m/p) = 1$. Suppose that $p$ does not divide the class number of $K(\zeta_p)$. Let $A$ be an abelian variety over $K$ with bad reduction only at the primes of $K$ over $p$. Then $A$ has no complex multiplication over $K$.*

*Proof.* Assume $A$ has complex multiplication over $K$. Since the class number of $K$ is equal to 1, any extension over $\mathcal{O}_K$ of constant $p$-group schemes by one another is constant. Considering the Cartier dual, any extension over $\mathcal{O}_K$ of diagonalizable $p$-group schemes by one another is diagonalizable. Note that the only group schemes over $\mathcal{O}_K$ of order $p$ are $\mu_p$ and $\mathbf{Z}/p\mathbf{Z}$ by Proposition 3.3. By Lemma 3.4 and the proof of [9, Theorem 2.1], there is an exact sequence

$$0 \to M \to \mathscr{A}[p^n] \to C \to 0$$

with $M$ diagonalizable and $C$ constant. By the proof of [9, Theorem 2.1], we have that $\dim A = 0$. □

Let $K = \mathbf{Q}(\sqrt{-19})$ and set $p = 5$. Since the class number of the cyclotomic field $\mathbf{Q}(\zeta_{95})$ is not divisible by $p$ (see [13]), it follows that the class number of $K(\zeta_p)$ is not divisible by $p$ by Lemma 3.2. As a corollary, we get the following.

THEOREM 3.6. *There do not exist non-zero abelian varieties over $K = \mathbf{Q}(\sqrt{-19})$ with good reduction everywhere and complex multiplication over $K$.*

**3.2. Elliptic curves over certain number fields with good reduction**

It is well known that there is no elliptic curves over $\mathbf{Q}$ with good reduction. On the other hand, several examples of such curves over quadratic fields are known. An elliptic curve defined over a number field $k$ is called *g-admissible* if it satisfies the conditions below:

1. it has good reduction over $k$,
2. it has a $k$-rational point of order 2,
3. it admits a global minimal model.

If it satisfies only (1) and (2), then it is called *admissible*. In his paper [2], Comalada showed that there exists an admissible elliptic curve over $K = \mathbf{Q}(\sqrt{m})$ $(0 < m < 100)$ if and only if

$$m = 6, 7, 14, 22, 38, 41, 65, 77, 86.$$

*Example*. The elliptic curve $E$ over $K = \mathbf{Q}(\sqrt{6})$ with Weierstrass equation

$$y^2 + \sqrt{6}xy - y = x^3 - (2 + \sqrt{6})x^2$$

is $g$-admissible. This can be seen from the fact that the discriminant of $E$ is equal to the unit $(5 + 2\sqrt{6})^3$. The three points of order 2 of $E$ have their $x$-coodinates equal to $x = -\dfrac{1}{2}$ and $\dfrac{1 + \sqrt{6} \pm (\sqrt{-2} + \sqrt{-3})i}{2}$ respectively. Their $y$-coordinates are given by $y = \dfrac{-\sqrt{6}x + 1}{2}$. The point with $x = -\dfrac{1}{2}$ is the only 2-rational point that is rational over $K$. The curve $E$ has exactly six points defined over $K$. They are $(0, 0)$ and its multiples $(2 + \sqrt{6}, -5 - 2\sqrt{6})$, $\left(-\dfrac{1}{2}, \dfrac{1}{2(\sqrt{6} - 2)}\right)$, $(2 + \sqrt{6}, 0)$, $(0, 1)$ and $\infty$.

Let $K$ be a number field and let $p$ be an odd prime number. Let $E$ be an elliptic curve over $K$ with good reduction. We now consider the $K$-rational points of order $p$ in the elliptic curve $E$. Suppose there exists a $K$-rational point $P$ of order $p$ in the elliptic curve $E$. Using the Weil pairing $e_p : E[p] \times E[p] \to \mu_p$, we can define a map $E[p] \to \mu_p$ by $Q \mapsto e_p(P, Q)$. Since the point $P$ is rational over $K$, this map gives an exact sequence

$$0 \to \mathbf{Z}/p\mathbf{Z} \to E[p] \to \mu_p \to 0. \tag{3}$$

of $\mathrm{Gal}(\overline{K}/K)$-modules. Let $\mathscr{E}$ be the Néron model of the elliptic curve $E$ over $\mathcal{O}_K$. Since the elliptic curve $E$ has good reduction over $K$, note that $\mathscr{E}[p]$ is a finite flat group scheme over $\mathcal{O}_K$.

Lemma 3.7. *Suppose that the ramification index $e_{\mathfrak{p}}$ satisfies $e_{\mathfrak{p}} < p - 1$ for all primes $\mathfrak{p}$ of $K$ over $p$. Then the exact sequence* (3) *of* $\mathrm{Gal}(\overline{K}/K)$*-modules induces an exact sequence*

$$0 \to \mathbf{Z}/p\mathbf{Z} \to \mathscr{E}[p] \to \mu_p \to 0$$

*of finite flat group schemes over $\mathcal{O}_K$.*

*Proof*. For any finite flat group schemes $G$ over $\mathcal{O}_K$, there is a one-to-one correspondence between closed flat subgroup schemes between $G$ over $\mathcal{O}_K$ and $G \otimes_{\mathcal{O}_K} K$ over $K$. For any finite flat group schemes $G$ over $\mathcal{O}_{K,\mathfrak{p}}$ of $p$-power order, by the assumption, $G$ is uniquely determined up to isomorphism by the isomorphism type of its generic fiber (see [12, Propositon 4.5.1]). Therefore a constant group scheme $\mathbf{Z}/p\mathbf{Z}$ is a subgroup scheme of $\mathscr{E}[p]$ over $\mathcal{O}_K$. There exists an exact sequence

$$0 \to \mathbf{Z}/p\mathbf{Z} \to \mathscr{E}[p] \to G \to 0 \tag{4}$$

of finite flat group schemes over $\mathcal{O}_K$. Since $G \otimes K$ is isomorphic to a diagonalizable group scheme $\mu_p$ by the exact sequence (3), $G$ is isomorphic to a diagonalizable group scheme $\mu_p$ over $\mathcal{O}_K$. This completes the proof. □

Combining the above result with Theorem 2.2, we get the following result:

THEOREM 3.8. *Let $K$ be a number field having a real place and let $p$ be a prime number. Suppose that $p$ does not divide the class number of $K(\zeta_p)$ and the ramification index $e_{\mathfrak{p}}$ satisfies $e_{\mathfrak{p}} < p - 1$ for all primes $\mathfrak{p}$ of $K$ above $p$. Let $E$ be an elliptic curve over $K$ with good reduction. Then $E$ has no $K$-rational points of order $p$.*

*Proof.* Suppose there exists a $K$-rational point of order $p$ in the elliptic curve $E$. By Lemma 3.7, there exists an exact sequence

$$0 \to \mathbf{Z}/p\mathbf{Z} \to \mathscr{E}[p] \to \mu_p \to 0$$

of finite flat group schemes over $\mathcal{O}_K$. Set $E = E_1$. Since the above exact sequence of finite flat group schemes over $\mathcal{O}_K$ is split by Theorem 2.2, there exists an elliptic curve $E_2$ over $K$ and a $K$-isogeny $E_1 \to E_2$ with kernel $\mu_p$. Then the image of the Galois submodule $\mathbf{Z}/p\mathbf{Z}$ gives a point of order $p$ in $E_2$. Continuing in this fashion, we obtain a sequence of $K$-isogenies

$$E_1 \to E_2 \to \cdots,$$

where each isogeny has kernel $\mu_p$. Since all the $E_i$ has good reduction over $K$, we see that $E_i \simeq E_j$ for some $i < j$ (see [4, Satz 6]). Composing our $K$-isogenies gives a endomorphism $f : E_i \to E_i$ defined over $K$. If $P_i \in E_i(K)$ is the image of $P \in E(K)$, then by construction $P_i \notin \operatorname{Ker} f$. Since $\deg f$ is a power of $p$, we see that $f$ is a non-scalar endomorphism. Therefore the elliptic curve $E_i$ has complex multiplication by some order $\mathcal{O}$ in an imaginary quadratic field $K'$, and we have an isomorphism (see [11, Ch. 2, Proposition 1.1])

$$[\cdot] : \mathcal{O} \simeq \operatorname{End}(E_i)$$

such that for any invariant differential $\omega \in \Omega_{E_i}$ on $E_i$,

$$[\alpha]^* \omega = \alpha\omega \quad \text{for all } \alpha \in \mathcal{O}.$$

Let $\alpha$ be the element of $\mathcal{O}$ such that $[\alpha] = f \in \operatorname{End}_K(E_i)$. Considering the action of $\operatorname{End}_K(E_i)$ on $\mathrm{H}^0(E_i/K, \Omega_{E_i}) \simeq K$, we have $\alpha \in K \cap K' = \mathbf{Q}$. This is a contradiction. □

As a corollary, we get the following result:

COROLLARY 3.9. *Let $K = \mathbf{Q}(\sqrt{6})$ or $\mathbf{Q}(\sqrt{7})$. Let $E$ be an elliptic curve over $K$ with good reduction. Then $E$ has no $K$-rational points of order $p$ for any prime number $p \geq 5$.*

*Proof.* Let $\mathscr{E}$ be the Néron model of $E$ over $\mathcal{O}_K$. Since $E$ has good reduction at the prime of $K$ over 2, the elliptic curve $\mathscr{E}(\mathbf{F}_2)$ has at most $3 + 2\sqrt{2} < 7$ points. Therefore $E$ has no $K$-rational points of order $p$ for any prime number $p \geq 7$. Set $p = 5$. We consider the case $K = \mathbf{Q}(\sqrt{6})$. Since the class number of the cyclotomic field $\mathbf{Q}(\zeta_{120})$ is not divisible by $p$ (see [13]), the class number of $K(\zeta_p)$ is not divisible by $p$ by Lemma 3.2. By Theorem 3.8, the elliptic curve $E$ has no $K$-rational points of order $p$. We now consider the case $K = \mathbf{Q}(\sqrt{7})$. Since the class number of the cyclotomic field $\mathbf{Q}(\zeta_{140})$ is not divisible by $p$ (see [13]), the class number of $K(\zeta_p)$ is not divisible by $p$ by Lemma 3.2. This completes the proof by Theorem 3.8. □

The following table is all taken from [2] and [7]. In the table, all the isomorphism classes of $g$-admissible elliptic curves having good reduction over the three fields $K = \mathbf{Q}(\sqrt{m})$ $(m = 6, 7, 14)$ are listed. Each isomorphism class contains a curve having a Weierstrass equation of the form

$$y^2 = x^3 + a_2x^2 + a_4x,$$

on which the point $(0,0)$ is of order 2. For each curve, the data given in the table are Comalada's code $E_i$, $m$, $a_2$, $a_4$, the $j$-invariant, and the torsion subgroup $T$ of the Mordell-Weil group. The coefficients $a_2$, $a_4$ and the $j$-invariant are given by expressions containing the fundamental unit $\varepsilon$ of $K$ and its conjugate $\bar{\varepsilon}$.

Table 1. Elliptic curves having good reduction over $\mathbf{Q}(\sqrt{6})$, $\mathbf{Q}(\sqrt{7})$, $\mathbf{Q}(\sqrt{14})$

| | $m$ | $a_2$ | $a_4$ | $j$ | $T$ |
|---|---|---|---|---|---|
| $E_1$ | 6 | $-2(\varepsilon - 1)$ | $4\varepsilon$ | $(20)^3$ | $\mathbf{Z}/6\mathbf{Z}$ |
| $E_3$ | 6 | $-14(\varepsilon - 1)$ | $4\bar{\varepsilon}$ | $64(4\varepsilon^4 + 1)^3/\varepsilon^4$ | $\mathbf{Z}/2\mathbf{Z}$ |
| $E_5$ | 6 | $14(\varepsilon - 1)\varepsilon$ | $4\varepsilon$ | $64(4\varepsilon^4 + 1)^3/\varepsilon^4$ | $\mathbf{Z}/6\mathbf{Z}$ |
| $E_7$ | 7 | $-(1 + 2\varepsilon^2)$ | $16\varepsilon^3$ | $(255)^3$ | $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$ |
| $E_9$ | 7 | $2(1 + 2\varepsilon^2)$ | 1 | $(256\varepsilon^2 + \bar{\varepsilon})^3$ | $\mathbf{Z}/4\mathbf{Z}$ |
| $E_{11}$ | 7 | $-2(1 + 2\varepsilon^2)$ | 1 | $(256\varepsilon^2 + \bar{\varepsilon})^3$ | $\mathbf{Z}/2\mathbf{Z}$ |
| $E_{13}$ | 7 | $8\varepsilon - 1$ | $16\varepsilon^2$ | $(-15)^3$ | $\mathbf{Z}/4\mathbf{Z}$ |
| $E_{14}$ | 7 | $-(8\varepsilon - 1)$ | $16\varepsilon^2$ | $(-15)^3$ | $\mathbf{Z}/4\mathbf{Z}$ |
| $E_{15}$ | 14 | $-3(\varepsilon - 1)/2$ | $16\varepsilon$ | $(-15)^3$ | $\mathbf{Z}/2\mathbf{Z}$ |
| $E_{17}$ | 14 | $3(\varepsilon - 1)$ | $-\varepsilon$ | $(255)^3$ | $\mathbf{Z}/2\mathbf{Z}$ |

*Acknowledgement*. I would like to thank Professor Toshiyuki Katura, who gave me various advice and useful comments.

## References

[1] M. Artin, Algebraization of formal moduli, II, Existence of modifications, Ann. of Math. **91** (1970), 88–135.
[2] S. Comalada, Elliptic curves with trivial conductor over quadratic fields, Pacific J. Math. **144** (1990), 237–258.
[3] B. Conrad, Finite group schemes over base with low ramification, Compos. Math. **119** (1999), 239–320.
[4] G. Faltings, Endlichkeitssätze für abelsche Varietäten über Zahlkörpern, Invent. Math. **83** (1983), 349–366.
[5] J.-M. Fontaine, Groupes *p*-divisible sur les corps locaux, Astérisque (1977), 47–48.
[6] N. Katz and B. Mazur, Arithmetic moduli of elliptic curves, Ann. of Math. Stud. **108**, Princeton University Press, Princeton, 1985.
[7] M. Kida, Reduction of elliptic curves over certain real quadratic number fields, Math. Comp. **68** (1999) 228, 1679–1685.
[8] F. Oort and J. Tate, Group schemes of prime order, Ann. Sci. École Norm. Sup. **3** (1970), 1–21.
[9] R. Schoof, Abelian varieties over cyclotomic fields with good reduction, Math. Ann. **325** (2003), 413–448.
[10] J.-P. Serre and J. Tate, Good reduction of abelian varieties, Ann. of Math. **88** (1968), 492–517.
[11] J. H. Silvermann, Advanced topics in the arithmetic of elliptic curves, Graduate texts in math. **151**, Springer-Verlag, Berlin-Heidelberg-New York, 1994.
[12] J. Tate, Finite flat group schemes, Modular forms and Fermat's last theorem, Springer-Verlag, Berlin-Heidelberg-New York, 1997, 121–154.
[13] L. C. Washington, Introduction to cyclotomic fields, Graduate texts in math. **83**, Springer-Verlag, Berlin-Heidelberg-New York, 1982.

Masaya Yasuda
Fujitsu Laboratories Ltd.
1-1, Kamikodanaka 4-chome
Nakahara-ku, Kawasaki 211-8588
Japan
E-mail: myasuda@labs.fujitsu.com