ACTA ARITHMETICA
176.1 (2016)

Torsion points and reduction of elliptic curves

by

Masaya Yasuda (Fukuoka)

1. Introduction. In 1977, Mazur [9, 10] first showed that no elliptic curve over $\mathbb{Q}$ can have $\mathbb{Q}$-rational p-torsion points for any prime $p \geq 11$. Then Kenku–Momose [8] and Kamienny [7] classified the possible torsion subgroups of elliptic curves over quadratic fields K, and in particular they showed that no elliptic curve over K can have K-rational p-torsion points for any primes $p \geq 17$. For cubic fields, Parent [13, 14] proved the same result on p-torsion points as in the case of quadratic fields. In 2010, it was announced in [19] that Kamienny, Stein and Stoll proved that 17 is the largest prime dividing the order of the K-rational torsion subgroup of an elliptic curve over any quartic field K (see also Derickx's master thesis [3] for number fields of higher degree).

In addition to the above progress on p-torsion points, the notion of *reduction* plays an important role in the study of the structure of the Mordell–Weil group of an elliptic curve. Let E be an elliptic curve over $\mathbb{Q}$ of conductor n (in particular, E has bad reduction at all primes dividing n). For $p = 5$ or 7 with $p \nmid n$, Agashe [1, Theorem 1.1] proved that if n is square free and p divides the order of the torsion subgroup of $E(\mathbb{Q})$, then p divides the cuspidal class number of the modular curve $X_0(n)$ (see Section 3 below for details). In [20, Theorem 5.1], T. Takagi gave a formula for the cuspidal class number for square free n. By combining Agashe's result [1, Theorem 1.1] with [20, Theorem 5.1], T. Takagi [21, Theorem] gave a relation between the prime order p of torsion points and the conductor n of E. In a quite different way from Agashe's method, Yasuda [23] proved the non-existence of $\mathbb{Q}$-rational p-torsion points of an elliptic curve over $\mathbb{Q}$ with bad reduction only at certain primes. Given $p = 5$ or 7, if E has bad reduction only at primes $\ell \not\equiv 0, \pm 1 \bmod p$, then E has no $\mathbb{Q}$-rational p-torsion points [23, The-

2010 *Mathematics Subject Classification*: Primary 14H52; Secondary 14G05.
Key words and phrases: elliptic curves, torsion points, finite flat group schemes.
Received 26 January 2016.
Published online 29 September 2016.

DOI: 10.4064/aa8425-6-2016

orem 1.1]. This generalizes Agashe–Takagi's result [21, Theorem]. In [23, Theorem 1.2], Yasuda further extended [23, Theorem 1.1] by proving the non-existence of K-rational torsion points of elliptic curves over a number field K with bad reduction only at certain primes.

In this paper, we improve [23, Theorem 1.2]. Given an elliptic curve E over a number field K, let $\mathcal{E}$ denote its Néron model over the ring $\mathcal{O}_K$ of integers of K. Let $\mathcal{E}[m]$ denote the kernel of multiplication by an integer $m > 0$. Let N be the product of the primes over which E has bad reduction. Our method is different from [23]. In the proof of [23, Theorem 1.2], the ramification of the extension $K(E[p])$ over $K(\zeta_p)$ is studied to deduce the non-existence of p-torsion points of E for primes $p \nmid N$, where $K(E[p])$ denotes the field generated by the points of the p-torsion subgroup $E[p]$. In contrast, we analyze the structure of the finite flat group scheme $\mathcal{E}[p]$ over the ring $\mathcal{O}_K[1/N]$, by using Schoof's results [15, Section 2] on p-group schemes over $\mathcal{O}_K$. The main ingredient in our analysis is to show that for certain N, the group scheme $\mathcal{E}[p]$ has a prolongation over $\mathcal{O}_K$ if E has a K-rational p-torsion point. Our main result is:

Main Theorem 1.1. *Let K be a number field and $p \geq 5$ a prime not dividing the class number of the field $F = K(\zeta_p)$. Assume either of the following two conditions holds:*

(A) *The ramification index $e_{\mathfrak{p}}$ satisfies $e_{\mathfrak{p}} < p - 1$ for all primes $\mathfrak{p}$ of K over p.*
(B) *$\zeta_p \in K$ and there is only one prime of K over p.*

Let E be an elliptic curve over K with good reduction outside the set

$$\mathfrak{S}_{K,p} := \{\mathfrak{q} : \text{prime of } K \text{ over a prime } \ell \mid \ell \neq p \text{ and } \ell^{f_{\mathfrak{q}}} \not\equiv \pm 1 \bmod p\},$$

where $f_{\mathfrak{q}}$ denotes the residue degree of the prime $\mathfrak{q}$ of K. If E has a K-rational p-torsion point, then E has complex multiplication (CM) *by some imaginary quadratic subfield of K and everywhere good reduction* (EGR) *over K. In particular, if K has a real place, then E has no K-rational p-torsion points.*

Compared to the previous result [23, Theorem 1.2], condition (B) is new (for $p = 5$ and 7, condition (A) was used in [24, 25] to find real quadratic fields K such that the class number of $K(\zeta_p)$ is divisible by p, by constructing elliptic curves with good reduction outside $\mathfrak{S}_{K,p}$). For a *regular* prime $p \geq 5$, set $K = \mathbb{Q}(\zeta_p)$. In this setting, the class number of $F = K$ is not divisible by p and condition (B) is clearly satisfied. Furthermore, the set $\mathfrak{S}_{K,p}$ is empty since $\ell^{f_{\mathfrak{q}}} \equiv 1 \bmod p$ for any prime $\mathfrak{q}$ of K over a prime $\ell \neq p$. Note that the only quadratic field included in the cyclotomic field $\mathbb{Q}(\zeta_p)$ is $\mathbb{Q}(\sqrt{p})$ (resp. $\mathbb{Q}(\sqrt{-p})$) if $p \equiv 1 \bmod 4$ (resp. $p \equiv 3 \bmod 4$). As a corollary of Main Theorem 1.1, we obtain the following result:

COROLLARY 1.2. *Let $p \geq 11$ be a regular prime. Let E be an elliptic curve over $\mathbb{Q}(\zeta_p)$ with EGR. Then:*

- *In case $p \equiv 1 \bmod 4$, the curve E has no $\mathbb{Q}(\zeta_p)$-rational p-torsion points.*
- *In case $p \equiv 3 \bmod 4$, if E has a $\mathbb{Q}(\zeta_p)$-rational p-torsion point, then E has CM by $\mathbb{Q}(\sqrt{-p})$.*

Schoof [15] determined all cyclotomic fields over which there exist non-zero abelian varieties with EGR. In particular, he showed that there do not exist non-zero abelian varieties over $\mathbb{Q}(\zeta_m)$ with EGR for every $m \in \{1, 3, 4, 5, 7, 8, 9, 12\}$ (i.e. the condition $p \geq 11$ is sufficient for Corollary 1.2), and the same result holds for $m = 11$ and 15 under the generalized Riemann hypothesis. For the regular prime $p = 13$, set $\lambda = \zeta_{13} + \zeta_{13}^{-1}$. Let $E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$, where

$$\begin{cases} a_1 = \lambda^2 + \lambda + 1, \quad a_2 = -\lambda^3 + \lambda^2 + \lambda, \ a_3 = \lambda^5 + \lambda^3 + \lambda, \\ a_4 = \lambda^5 - \lambda^4 - 11\lambda^3 - \lambda^2 + 3\lambda, \\ a_6 = 13\lambda^5 - 31\lambda^4 - 48\lambda^3 + 52\lambda^2 + 33\lambda - 10. \end{cases}$$

The elliptic curve E has EGR over the totally real field $\mathbb{Q}(\lambda) = \mathbb{Q}(\zeta_{13})^+$ (the curve E arises from a cusp form of weight 2 and level 1), and it has a $\mathbb{Q}(\lambda)$-rational 19-torsion point (see e.g. [2, Example 6.8, p. 168]). In contrast, the result of Corollary 1.2 shows that E has no $\mathbb{Q}(\zeta_{13})$-rational 13-torsion points.

It is well known that there are no elliptic curves over $\mathbb{Q}$ with EGR. On the other hand, there exist elliptic curves over certain quadratic fields with EGR. In particular, for every prime $p \in S = \{29, 41, 109, 133\}$, there exists an elliptic curve over $\mathbb{Q}(\sqrt{p})$ with EGR (see the database of [26] for more details). Every $p \in S$ is a regular prime satisfying $p \equiv 1 \bmod 4$, and hence $\mathbb{Q}(\sqrt{p}) \subset \mathbb{Q}(\zeta_p)$. Therefore, for each prime $p \in S$, no elliptic curve E over $\mathbb{Q}(\sqrt{p})$ with EGR has $\mathbb{Q}(\zeta_p)$-rational p-torsion points by Corollary 1.2.

The organization of this paper is as follows: In Section 2, we prove Theorem 1.1. In Section 3, we give a sketch of proof of Agashe's result [1, Theorem 1.1] and compare our strategy with Agashe's. In Section 4, we apply Corollary 1.2 to obtain some results on the non-existence of $\mathbb{Q}(\zeta_p)$-rational p-torsion points of certain elliptic curves. In particular, for every regular prime $p \geq 11$, we show the non-existence of $\mathbb{Q}(\zeta_p)$-rational p-torsion points of elliptic curves over $\mathbb{Q}$ with EGR over $\mathbb{Q}(\zeta_p)$.

NOTATION. The symbols $\mathbb{Z}$ and $\mathbb{Q}$ denote the ring of integers and the field of rational numbers, respectively. For a prime p, the finite field with p elements is denoted by $\mathbb{F}_p$. Let ζ_p be a fixed primitive pth root of unity, and μ_p denote the set of pth roots of unity. If G is a group scheme over a ring R, and $n \in \mathbb{Z}$, we write $G[n]$ for the kernel of multiplication $[n]_G : G \to G$.

2. Proof of Main Theorem 1.1. In this section, we prove Main Theorem 1.1. Let us give some lemmas:

LEMMA 2.1. *Let E be an elliptic curve over a number field K. If E has a K-rational p-torsion point for a prime $p \geq 5$, then E has semistable (i.e. good or multiplicative) reduction at $\mathfrak{q}$ for all primes $\mathfrak{q}$ of K with $\mathfrak{q} \nmid p$.*

Proof. See the proof of [6, Lemma 1.3]. ∎

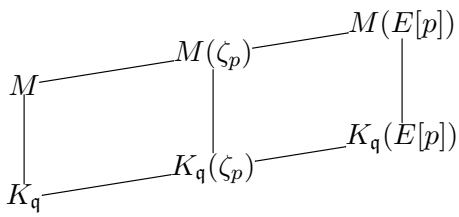
LEMMA 2.2. *Let E be an elliptic curve over a number field K. If E has a K-rational p-torsion point for a prime $p \geq 5$, then the field $K(E[p])$ is unramified over K at any prime $\mathfrak{q} \in \mathfrak{S}_{K,p}$.*

Proof. The proof is based on the second proof of [23, Theorem 1.1], in which only the case $K = \mathbb{Q}$ is studied (see [23, Section 3]). By Lemma 2.1, the curve E has either good or multiplicative reduction at any prime $\mathfrak{q} \in \mathfrak{S}_{K,p}$ (note $\mathfrak{q} \nmid p$). If E has good reduction at $\mathfrak{q}$, then $K(E[p])$ is unramified over K at $\mathfrak{q}$ by the criterion of Néron–Ogg–Shafarevich (see [16, Chapter VII]).

We next consider the case of multiplicative reduction. Let $K_\mathfrak{q}$ denote the completion of K at $\mathfrak{q}$. By the theory of Tate curves, there exists an unramified extension M over $K_\mathfrak{q}$ of degree at most 2 such that E is isomorphic to the Tate curve E_q over M, where q is the Tate parameter (see [17, Chapter V] for details). More precisely, we have an isomorphism

$$\Phi : E(\overline{M}) \simeq \overline{M}^*/q^{\mathbb{Z}},$$

and so the p-torsion subgroup $E(\overline{M})[p]$ is isomorphic to $(\zeta_p^{\mathbb{Z}} \cdot Q^{\mathbb{Z}})/q^{\mathbb{Z}}$ under Φ, where $Q = q^{1/p} \in \overline{M}$ is a fixed primitive pth root of q. In other words, when we view $E(\overline{M})[p]$ as an $\mathbb{F}_p$-vector space, the set $\{\zeta_p, Q\}$ gives a basis of $E(\overline{M})[p]$ under the isomorphism Φ. Now consider the following extensions:



Note that the extensions $M/K_\mathfrak{q}$ and $M(\zeta_p)/M$ are unramified since $K_\mathfrak{q}(\zeta_p)/K_\mathfrak{q}$ is unramified as $\mathfrak{q} \nmid p$. Here we focus on the extension $M(E[p])$ over $M(\zeta_p)$, which is a Kummer extension of degree either 1 or p. If the extension degree equals 1, the extension $M(E[p])/M(\zeta_p)$ is trivial, and hence $K(E[p])/K$ is unramified at $\mathfrak{q}$.

Next we consider the case $M(E[p]) \neq M(\zeta_p)$. Suppose that $M(E[p]) = M(\zeta_p, Q)$ is a ramified extension over $M(\zeta_p)$ of degree p. Then the totally

ramified extension $M(E[p])/M(\zeta_p)$ is defined by the polynomial

$$X^p - q = \prod_{i=0}^{p-1}(X - Q \cdot \zeta_p^i),$$

and hence $Q \cdot \zeta_p^i \notin M$ for any $0 \le i \le p-1$. However, we have $\zeta_p \in M$ since E has one K-rational p-torsion point and the point is also M-rational. Therefore $[K_{\mathfrak{q}}(\zeta_p) : K_{\mathfrak{q}}] \le [M : K_{\mathfrak{q}}] \le 2$, and hence $\ell^{f_{\mathfrak{q}}} \equiv \pm 1 \bmod p$. This contradicts $\mathfrak{q} \in \mathfrak{S}_{K,p}$. Thus $M(E[p])$ is unramified over $M(\zeta_p)$, and hence $K(E[p])$ is also unramified over K at $\mathfrak{q}$. ∎

Let K be a number field and $p \ge 5$ a prime. Let E be an elliptic curve over K with good reduction outside the set $\mathfrak{S}_{K,p}$. Assume that E has a K-rational p-torsion point P. Using the p-torsion point P, we can define a group homomorphism

$$\phi : E[p] \to \mu_p \quad \text{by} \quad T \mapsto e_p(P, T),$$

where $e_p : E[p] \times E[p] \to \mu_p$ is the Weil pairing (see [16, Chapter III]). Let G_K denote the absolute Galois group $\mathrm{Gal}(\overline{K}/K)$. Since the point P is K-rational, the map ϕ gives an exact sequence

$$0 \to \mathbb{Z}/p\mathbb{Z} \to E[p] \xrightarrow{\phi} \mu_p \to 0 \tag{2.1}$$

of G_K-modules, where $\mathbb{Z}/p\mathbb{Z}$ is the constant G_K-module generated by P. The action of G_K on $E[p]$ gives an associated Galois modulo p representation

$$\overline{\rho}_{E,p} : G_K \to \mathrm{Aut}(E[p]) \simeq \mathrm{GL}_2(\mathbb{F}_p).$$

Set $L = K(E[p])$ and $F = K(\zeta_p)$. Then the representation $\overline{\rho}_{E,p}$ induces a faithful representation $\rho : \mathrm{Gal}(L/K) \to \mathrm{GL}_2(\mathbb{F}_p)$. By the exact sequence (2.1) of G_K-modules, the representation ρ has the form $\left(\begin{smallmatrix} 1 & * \\ 0 & \chi \end{smallmatrix}\right)$, where

$$\chi : \Delta \to \mathbb{F}_p^\times, \quad \Delta := \mathrm{Gal}(F/K),$$

denotes the cyclotomic character defined by $\sigma(\zeta_p) = \zeta_p^{\chi(\sigma)}$ for every $\sigma \in \Delta$. Since E has good reduction at all primes of K over p (recall that $\mathfrak{S}_{K,p}$ contains no prime of K over p), the curve E has everywhere semistable reduction by Lemma 2.1. Let $\mathcal{E}$ denote the Néron model of E over $\mathcal{O}_K$. A commutative finite flat group scheme of order p over a commutative ring R is called a *p-group scheme* over R (see [15, Section 2]). Let $N \in \mathbb{Z}$ be the product of all primes ℓ over which E has bad reduction. Then $\mathcal{E}[p]$ is a p-group scheme over the ring $\mathcal{O}_K[1/N]$.

We now give a lemma on prolongation of the p-group scheme $\mathcal{E}[p]$:

LEMMA 2.3. *The p-group scheme $\mathcal{E}[p]$ over $\mathcal{O}_K[1/N]$ prolongs to a p-group scheme over $\mathcal{O}_K$.*

Proof. A similar argument about patching of finite flat group schemes in [9, (I.2), pp. 44–45] shows that the p-group scheme $\mathcal{E}[p]$ over $\mathcal{O}_K[1/N]$ prolongs to a finite flat group scheme over $\mathcal{O}_K$ since the inertia group of $\mathrm{Gal}(K(E[p]/K))$ at every prime $\mathfrak{q}$ over N (i.e. $\mathfrak{q} \in \mathfrak{S}_{K,p}$) is trivial by Lemma 2.2. ∎

Lemma 2.4. *Let G denote a prolongation of the p-group scheme $\mathcal{E}[p]$ over $\mathcal{O}_K$. Then we have an extension*

$$0 \to (\mathbb{Z}/p\mathbb{Z})_{\mathcal{O}_K} \to G \to (\mu_p)_{\mathcal{O}_K} \to 0 \tag{2.2}$$

of p-group schemes over $\mathcal{O}_K$, where $(\mathbb{Z}/p\mathbb{Z})_{\mathcal{O}_K}$ and $(\mu_p)_{\mathcal{O}_K}$ denote the constant and the diagonalizable group schemes of order p over $\mathcal{O}_K$, respectively.

Proof. Let G_0 be a simple subgroup scheme of G. Since the order of the group $\Gamma := \mathrm{Gal}(L/F)$ is divisible by p, this group acts trivially on $G_0(\overline{K})$ by the same argument as in the proof of [15, Proposition 2.2]. Since G_0 is simple, the $\mathbb{F}_p[\Delta]$-module $G_0(\overline{K})$ is a one-dimensional eigenspace over $\mathbb{F}_p$. Therefore the group scheme G_0 has order p. By the Oort–Tate classification [12, Theorem 3] of finite flat group schemes over $\mathcal{O}_K$ of prime order, the structure of a finite flat group scheme H over $\mathcal{O}_K$ of order p is uniquely determined up to isomorphism by its generic fiber $H \otimes K$, or its Galois module $H(\overline{K})$. Then by the exact sequence (2.1) of G_K-modules, we can take for G_0 the constant group scheme $(\mathbb{Z}/p\mathbb{Z})_{\mathcal{O}_K}$, which is generated by the p-torsion point P. Let C denote the finite flat group scheme given by the cokernel of $G_0 = (\mathbb{Z}/p\mathbb{Z})_{\mathcal{O}_K} \hookrightarrow G$. Then the group scheme C also has exact order p, and its Galois module $C(\overline{K})$ is isomorphic to μ_p by the exact sequence (2.1) again. Hence C is isomorphic to the diagonalizable group scheme $(\mu_p)_{\mathcal{O}_K}$ over $\mathcal{O}_K$. ∎

Now we recall a key result proved by Schoof (the field K in the proposition below is assumed to be a complex number field in [15, Proposition 2.6], but the result holds for any number field when $p \geq 3$).

Proposition 2.5 (Schoof [15, Proposition 2.6]). *Let K be a number field and $p \geq 3$ a prime not dividing the class number of $K(\zeta_p)$. If either* (A) *or* (B) *of Main Theorem* 1.1 *is satisfied, then any extension of $(\mu_p)_{\mathcal{O}_K}$ by $(\mathbb{Z}/p\mathbb{Z})_{\mathcal{O}_K}$ over $\mathcal{O}_K$ is split.*

We are now ready to prove Main Theorem 1.1 (our strategy is based on Mazur's work [10, §3]).

Proof of Main Theorem 1.1. Let K be a number field and $p \geq 5$ a prime. As in Theorem 1.1, we assume that p does not divide the class number h_F of $F = K(\zeta_p)$, and either (A) or (B) holds. Let E be an elliptic curve over K with good reduction outside $\mathfrak{S}_{K,p}$. Let $\mathcal{E}$ denote its Néron model over $\mathcal{O}_K$ as above.

Suppose E has a K-rational p-torsion point. By Lemma 2.2, there exists a p-group scheme G over $\mathcal{O}_K$ extended from $\mathcal{E}[p]$. Then G has an extension (2.2) over $\mathcal{O}_K$ by Lemma 2.3, and the extension is split by Proposition 2.5. This implies that the exact sequence (2.1) of G_K-modules is split, that is,

$$E[p] = \mathbb{Z}/p\mathbb{Z} \oplus \mu_p \tag{2.3}$$

as G_K-modules. Set $E_1 = E$. Then there exists an elliptic curve E_2 over K and a K-isogeny $E_1 \to E_2$ with kernel μ_p. Note that the image of the Galois submodule $\mathbb{Z}/p\mathbb{Z} \subset E_1$ gives a K-rational p-torsion point of E_2 again. By repeating this procedure, we obtain a sequence of K-isogenies

$$E_1 \to E_2 \to E_3 \to \cdots,$$

each with kernel μ_p. By Shafarevich's Theorem [16, Theorem 6.1 in Chapter IX], we have $E_i \simeq E_j$ for some $i < j$. Composing some K-isogenies gives an endomorphism $f : E_i \to E_i$ defined over K. If $P_i \in E_i(K)$ is the image of the p-torsion point $P \in E(K)$, then $P_i \notin \ker f$ by construction. Since $\deg f$ is a power of p, we see that f is a non-scalar endomorphism. This implies that E_i has CM, and E also has CM. Recall that E has everywhere semistable reduction, which implies that E has EGR (see e.g. [16, Proposition 5.4 in Chapter VII] for details). Furthermore, since E_i has CM, there exists an imaginary quadratic field K' such that E_i has CM by some order $\mathcal{O}$ in K'. By [17, Proposition 1.1 in Chapter II], we have an isomorphism

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

such that for any invariant differential $\omega \in \Omega_{E_i}$ on E_i, we have $[\alpha]^*\omega = \alpha\omega$ for every $\alpha \in \mathcal{O}$. Let α denote the element of $\mathcal{O}$ such that $[\alpha] = f \in \mathrm{End}_K(E_i)$. By considering the action of $\mathrm{End}_K(E_i)$ on $H^0(E_i/K, \Omega_{E_i}) \simeq K$, we have $\alpha \in K \cap K'$ and $K' = \mathbb{Q}(\alpha) \subset K$ since $\alpha \notin \mathbb{Q}$ and $[K' : \mathbb{Q}] = 2$. Then both E_i and E have CM by the imaginary quadratic subfield K' of K. In case K has a real place, we have $\alpha \in K \cap K' = \mathbb{Q}$, a contradiction. Therefore E has no K-rational p-torsion points in this case. This completes the proof of Main Theorem 1.1. ∎

3. Agashe's result and strategy for $K = \mathbb{Q}$. In the case $K = \mathbb{Q}$, Main Theorem 1.1 shows that given $p = 5$ or 7, an elliptic curve E over $\mathbb{Q}$ has no $\mathbb{Q}$-rational p-torsion points if E has bad reduction only at primes $\ell \not\equiv 0, \pm 1 \bmod p$. In contrast, as stated in Section 1, Agashe proved the following result for elliptic curves over $\mathbb{Q}$ of square free conductor [1, Theorem 1.1] (see [5] for the definition of the optimal curve of an elliptic curve over $\mathbb{Q}$):

THEOREM 3.1 (Agashe). *Let E be an elliptic curve over $\mathbb{Q}$ of square free conductor n. Let E' denote the optimal curve in the isogeny class of E. Suppose p is a prime with $p \nmid 6n$.*

(i) *If p divides the order of the torsion part $E'(\mathbb{Q})_{\mathrm{tor}}$ of $E'(\mathbb{Q})$, then p divides the order of $E' \cap C$, where C is the cuspidal subgroup (i.e. the group of degree zero divisors on $X_0(n)(\mathbb{C})$ that are supported on the cusps). In particular, p divides the order of C.*

(ii) *If p divides the order of $E(\mathbb{Q})_{\mathrm{tor}}$, then p divides the order of C.*

By combining (ii) with the cuspidal class number formula of [20], we can obtain a part of our result in the case $K = \mathbb{Q}$. In this section, we give a sketch of the proof of Theorem 3.1 by Agashe, and compare our proof with Agashe's strategy.

The result (ii) of Theorem 3.1 easily follows from (i) in view of the fact that if the optimal curve E' has a $\mathbb{Q}$-rational p-torsion point, then so does E [5, Theorem 1.2]. In the proof of (i) by Agashe, the key results are the following two propositions:

PROPOSITION 3.2 ([1, Proposition 2.1]). *Let $n > 0$ be a square free integer. Given $\delta_r \in \{1, r\}$ for every prime $r \mid n$, with $\delta_\ell = 1$ for at least one $\ell \mid n$, there exists an Eisenstein series G of weight 2 on $\Gamma_0(n)$, which is an eigenfunction for all the Hecke operators such that $a_s(G) = s + 1$ for all primes $s \nmid n$, and $a_r(G) = \delta_r$ for all primes $r \mid n$, where $G(q) = \sum_{k=0}^{\infty} a_k(G) q^k$ denotes the Fourier expansion of G at the cusp ∞ with $q = e^{2\pi i z}$.*

PROPOSITION 3.3 ([1, Proposition 3.6]). *Let E' and n be as in Theorem 3.1. Let f denote the cuspform of weight 2 on $\Gamma_0(n)$ associated to E'. Suppose that there is a prime $p \geq 5$ such that p divides the order of $E'(\mathbb{Q})_{\mathrm{tor}}$. Then there is a prime $\ell \mid n$ such that $w_\ell = -1$, where w_ℓ is the sign of the Atkin–Lehner involution W_ℓ acting on f.*

Here we give a sketch of the proof of Theorem 3.1(i) by Agashe.

Sketch of proof of Theorem 3.1(i). Let f denote the cuspform of weight 2 on $\Gamma_0(n)$ associated to the optimal curve E'. Assume that there is a prime $p \nmid 6n$ dividing the order of $E'(\mathbb{Q})_{\mathrm{tor}}$. By Proposition 3.3, there exists a prime $\ell \mid n$ such that $w_\ell = -1$. For every prime r, we set $\delta_r = -w_r$ if $w_r = -1$, and $\delta_r = r$ if $w_r = 1$. Since $\delta_\ell = -w_\ell = 1$, by Proposition 3.2 there is an Eisenstein series G such that $a_s(G) = s + 1$ for all primes $s \nmid n$, and for all primes $r \mid n$,

$$a_r(G) = \begin{cases} r & \text{if } w_r = 1, \\ 1 & \text{if } w_r = -1. \end{cases}$$

In particular, if $r \mid n$ and $w_r = 1$, we have $p \mid (r + 1)$ by [1, Lemma 3.2], and hence $a_r(G) = r \equiv -1 = -w_r \bmod p$ (the result of [1, Lemma 3.2] is basically due to [5, Section 4], and its proof is related to that of Lemma 2.2). As in Proposition 3.2, let $f(q) = \sum_{k=0}^{\infty} a_k(f) q^k$ denote the Fourier expansion of the cuspform f. Then $a_k(f) \equiv a_k(G) \bmod p$ for all primes k. Furthermore,

since f and G are eigenfunctions for all the Hecke operators, we see that $a_k(f) \equiv a_k(G) \bmod p$ for all $k \geq 1$. By [9, Lemma II 5.6(a)], we also have $a_0(f) \equiv a_0(G) \bmod p$ and hence $f \equiv E \bmod p$. Let C_G denote the subgroup of the cuspidal subgroup C associated to G defined by Stevens [18, Definition 1.8.5]. By the assumption $p \nmid n$, the cuspform f is ordinary at p since $a_p(f) = a_p(G) \equiv p + 1 \equiv 1 \bmod p$. Then it follows from [22, Theorem 0.4] that $E'[p] \cap C_G \neq 0$, and thus p divides the order of $E' \cap C$. ∎

In order to study the structure of the torsion part of an elliptic curve E over $\mathbb{Q}$, Agashe investigates the coefficients of the Fourier expansion of the cuspform f corresponding to E. Our strategy is quite different: we study the structure of finite flat group schemes obtained from the Néron model of E.

4. Non-existence of $\mathbb{Q}(\zeta_p)$-rational p-torsion points. In this section, we apply Corollary 1.2 to obtain some results on the non-existence of $\mathbb{Q}(\zeta_p)$-rational p-torsion points of certain elliptic curves. For a regular prime $p \geq 11$, let E be an elliptic curve over $\mathbb{Q}(\zeta_p)$ with EGR (recall that it is shown in [15] that there do not exist non-zero abelian varieties over $\mathbb{Q}(\zeta_p)$ with EGR for $p = 3$, 5 or 7). Here we study the non-existence of $\mathbb{Q}(\zeta_p)$-rational p-torsion points of E. By Corollary 1.2, the curve E has no $\mathbb{Q}(\zeta_p)$-rational p-torsion points if $p \equiv 1 \bmod 4$. Hence we focus on $p \equiv 3 \bmod 4$. We begin with the following lemma:

LEMMA 4.1. *For a regular prime $p \geq 11$ with $p \equiv 3 \bmod 4$, let E denote an elliptic curve over $\mathbb{Q}(\zeta_p)$ with EGR. Assume that E has a $\mathbb{Q}(\zeta_p)$-rational p-torsion point. Then E has CM by a non-maximal order of $\mathbb{Q}(\sqrt{-p})$.*

Proof. By Corollary 1.2, the curve E has CM by $K' := \mathbb{Q}(\sqrt{-p})$. Suppose that E has CM by the maximal order R of K', i.e., the ring of integers of K' (we have $R = \mathbb{Z}[\sqrt{-p}]$ for $p \equiv 3 \bmod 4$). By the theory of CM elliptic curves [17, Theorem 5.6], the field $K'(j(E), h(E[p]))$ is the ray class field of K' modulo p, where $j(E)$ is the j-invariant of E and $h : E \to \mathbb{P}^1$ is the Weber function defined over $K'(j(E))$ (see [17, §5 in Chapter II] for the construction of h). Let $Cl(K')$ and $Cl(K', p)$ denote the class group and the ray class group of K' modulo p, respectively. By [11, Exercise 13 in Chapter VI], we have an exact sequence

$$1 \to R^*/R^{(p)} \to (R/pR)^* \to Cl(K', p) \to Cl(K') \to 1,$$

where R^* is the group of units of R, and $R^{(p)}$ the group of units $a \in R^*$ satisfying $a \equiv 1 \bmod p$. Since $R^*/R^{(p)} = \{\pm 1\}$ for $R = \mathbb{Z}[\sqrt{-p}]$ and $p \geq 11$, we have

$$\begin{aligned}[K'(j(E), h(E[p])) : K'] = \#Cl(K', p) &= \frac{\#(R/pR)^* \cdot \#Cl(K')}{2} \\ &\geq \#(R/pR)^*/2 \geq p(p-1)/2\end{aligned}$$

by the above exact sequence. On the other hand, we have $j(E) \in \mathbb{Q}(\zeta_p)$ and all points of $E[p]$ are defined over $\mathbb{Q}(\zeta_p)$ by (2.3). Consequently, the ray class field $K'(j(E), h(E[p]))$ is included in $\mathbb{Q}(\zeta_p)$ (note that the Weber function h is defined over $K'(j(E)) \subset \mathbb{Q}(\zeta_p)$), and hence

$$[K(j((E), h(E[p])) : K'] \leq (p-1)/2,$$

a contradiction. Hence E cannot have CM by the maximal order of K'. ∎

By combining Corollary 1.2 with Lemma 4.1, we obtain the following non-existence result for $\mathbb{Q}(\zeta_p)$-rational p-torsion points of elliptic curves over $\mathbb{Q}$:

THEOREM 4.2. *Let E be an elliptic curve over $\mathbb{Q}$. If E has EGR over $\mathbb{Q}(\zeta_p)$ for a regular prime $p \geq 11$, then E has no $\mathbb{Q}(\zeta_p)$-rational p-torsion points. Conversely, if E has a $\mathbb{Q}(\zeta_p)$-rational p-torsion point, then E has bad reduction at some primes of $\mathbb{Q}(\zeta_p)$.*

Proof. By Corollary 1.2, we only need to consider $p \equiv 3 \bmod 4$. Assume E has EGR over $\mathbb{Q}(\zeta_p)$. Suppose that E has a $\mathbb{Q}(\zeta_p)$-rational p-torsion point. Then E has CM by $\mathbb{Q}(\sqrt{-p})$ by Corollary 1.2. It is well known that there are 13 isomorphic classes of elliptic curves over $\mathbb{Q}$ with CM. All representative elliptic curves over $\mathbb{Q}$ with CM, denoted by $E_{D,f}$, are listed in [17, §3 in Appendix A]. Note that $E_{D,f}$ has CM by an order of conductor f of the imaginary quadratic field $\mathbb{Q}(\sqrt{-D})$, and $D \in T = \{3, 4, 7, 8, 11, 19, 43, 67, 163\}$. Furthermore, it follows from [16, §5 in Chapter X] that any CM elliptic curve over $\mathbb{Q}$ is $\mathbb{Q}$-isomorphic to a twist of some $E_{D,f}$. From these facts, the curve E is $\mathbb{Q}$-isomorphic to a twist of $E_{p,f}$ for some conductor f. According to the list of $E_{D,f}$ in [17, §3 in Appendix A], we always have $f = 1$ for $D \geq 8$. Thus E has CM by the *maximal* order of $\mathbb{Q}(\sqrt{-p})$ for the primes $p \geq 11$. This contradicts Lemma 4.1. ∎

For $d \in \mathbb{Q}^*$, we let E^d denote the twist of an elliptic curve E over $\mathbb{Q}$ (see [16, Proposition 5.4 in Chapter X] for details). As mentioned in the proof of Proposition 4.2, any CM elliptic curve over $\mathbb{Q}$ is given by a twisted curve $E^d_{D,f}$ for some d, f and $D \in T$ (the curve $E_{D,f}$ and the set T are introduced in the proof of Proposition 4.2). Dieulefait et al. [4] gave some information about the field of definition of p-torsion points of CM elliptic curves $E^d_{D,f}$ for primes p dividing the discriminant D. According to [4, Theorem 3], given any CM curve $E = E^d_{p,f}$ for a prime $p \geq 11$, there are p-torsion points of E defined over $\mathbb{Q}(\zeta_p + \zeta_p^{-1}, \sqrt{d})$. Furthermore, $d = -p$ is the only case where any Galois number field containing p-torsion points of E contains $\mathbb{Q}(\sqrt{-p})$. In other words, the curve $E^d_{p,f}$ with $d = -p$ has a p-torsion point defined over $\mathbb{Q}(\zeta_p + \zeta_p^{-1}, \sqrt{-p}) = \mathbb{Q}(\zeta_p)$ for $p = 11, 19, 43, 67$ and 163. In contrast, Theorem 4.2 implies that $E^d_{p,f}$ with $d = -p$ has bad reduction at some

primes of $\mathbb{Q}(\zeta_p)$ for $p = 11, 19, 43$ and 163 (note that $p = 67$ is irregular). More precisely, for $p = 11, 19, 43$ and 163, the curve $E = E^d_{p,f}$ with $d = -p$ still has bad reduction at the prime $(1 - \zeta_p)$ of $\mathbb{Q}(\zeta_p)$ over p (note that E has bad reduction only at p).

References

[1] A. Agashe, *Rational torsion in elliptic curves and the cuspidal subgroup*, arXiv: 0810.5181 (2008).

[2] L. Berger, G. Böckle, L. Dembélé, M. Dimitrov, T. Dokchitser and J. Voight, *Elliptic Curves, Hilbert Modular Forms and Galois Deformations*, Springer Science & Business Media, 2013.

[3] M. Derickx, *Torsion points on elliptic curves and gonalities of modular curves*, Master's Thesis, Univ. Leiden, 2012.

[4] L. Dieulefait, E. González-Jiménez, and J. Urroz, *On fields of definition of torsion points of elliptic curves with complex multiplication*, Proc. Amer. Math. Soc. 139 (2011), 1961–1969.

[5] N. Dummigan, *Rational torsion on optimal curves*, Int. J. Number Theory 4 (2005), 513–531.

[6] T. A. Fisher, *On 5 and 7 descents for elliptic curves*, PhD thesis, Univ. Cambridge, 2000.

[7] S. Kamienny, *Torsion points on elliptic curves and q-coefficients of modular forms*, Invent. Math. 109 (1992), 221–229.

[8] M. Kenku and F. Momose, *Torsion points on elliptic curves defined over quadratic fields*, Nagoya Math. J. 109 (1988), 125–149.

[9] B. Mazur, *Modular curves and the Eisenstein ideal*, IHES Publ. Math. 47 (1977), 33–186.

[10] B. Mazur, *Rational points on modular curves*, in: Modular Functions of one Variable V, Lecture Notes in Math. 601, Springer, 1977, 107–148.

[11] J. Neukirch, *Algebraic Number Theory*, Grundlehren Math. Wiss. 322, Springer, Berlin, 1999.

[12] F. Oort and J. Tate, *Group schemes of prime order*, Ann. Sci. École Norm. Sup. 3 (1970), 1–21.

[13] P. Parent, *Torsion des courbes elliptiques sur les corps cubiques*, Ann. Inst. Fourier (Grenoble) 50 (2000), 723–749.

[14] P. Parent, *No 17-torsion on elliptic curves over cubic number fields*, J. Théor. Nombres Bordeaux 15 (2003), 831–838.

[15] R. Schoof, *Abelian varieties over cyclotomic fields with good reduction everywhere*, Math. Ann. 325 (2003), 413–448.

[16] J. H. Silverman, *The Arithmetic of Elliptic Curves*, Grad. Texts in Math. 106, Springer, Berlin, 1994.

[17] J. H. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*, Grad. Texts in Math. 151, Springer, Berlin, 1994.

[18] G. Stevens, *Arithmetic on Modular Curves*, Springer Science & Business Media, 2012.

[19] M. Stoll, *Torsion points on elliptic curves over quartic number fields*, invited talk at the 9th Algorithmic Number Theory Symposium (ANTS-IX), 2010; http://www.mathe2.uni-bayreuth.de/stoll/talks/ANTS2010-1-EllTorsion.pdf.

[20] T. Takagi, *The cuspidal class number formula for the modular curves $X_0(M)$ with M square-free*, J. Algebra 193 (1997), 180–213.
[21] T. Takagi, *Erratum to "The cuspidal class number formula for the modular curves $X_1(2p)$"*, J. Math. Soc. Japan 64 (2012), 87–89.
[22] S. L. Tang, *Congruences between modular forms, cyclic isogenies of modular elliptic curves, and integrality of p-adic L-functions*, Trans. Amer. Math. Soc. 349 (1997), 837–856.
[23] M. Yasuda, *Torsion points of elliptic curves with bad reduction at some primes*, Comment. Math. Univ. St. Pauli 61 (2012), 1–7.
[24] M. Yasuda, *Torsion points of elliptic curves with bad reduction at some primes II*, Bull. Korean Math. Soc. 50 (2013), 83–96.
[25] M. Yasuda, *Kummer generators and torsion points of elliptic curves with bad reduction at some primes*, Int. J. Number Theory 9 (2013), 1743–1752.
[26] S. Yokoyama, *Database project LMFDB: Elliptic curves with everywhere good reduction over number fields*, http://www2.math.kyushu-u.ac.jp/~s-yokoyama/ECtable.html.

Masaya Yasuda
Institute of Mathematics for Industry
Kyushu University
744 Motooka Nishi-ku
Fukuoka 819-0395, Japan
E-mail: yasuda@imi.kyushu-u.ac.jp