J. London Math. Soc. (2) 74 (2006) 1–12
doi:10.1112/S0024610706022940

ON THE TORSION OF ELLIPTIC CURVES OVER QUARTIC NUMBER FIELDS

DAEYEOL JEON, CHANG HEON KIM AND EUISUNG PARK

ABSTRACT

We determine which groups $\mathbb{Z}/M\mathbb{Z}\oplus\mathbb{Z}/N\mathbb{Z}$ occur infinitely often as torsion groups $E(K)_{\mathrm{tors}}$ when K varies over all quartic number fields and E varies over all elliptic curves over K.

0. *Introduction*

The first two authors and Schweizer [**19**] proved that if K varies over all cubic number fields and E varies over all elliptic curves over K, the group structures that appear infinitely often as torsion groups $E(K)_{\mathrm{tors}}$ are exactly the following:

$$\begin{aligned} &\mathbb{Z}/N\mathbb{Z}, && N = 1\text{–}16, 18, 20\\ &\mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/2N'\mathbb{Z}, && N' = 1\text{–}7. \end{aligned}$$

By infinitely often in this context we always mean for infinitely many absolutely non-isomorphic E or, in other words, for infinitely many different j-invariants $j(E)$. Their work started from the observation that the torsion group structures over the rational or quadratic number fields, which are described by [**22**] and [**20**] also occur infinitely often.

In their proof, the main step was the classification of the modular curves parametrizing elliptic curves with such a torsion structure that have infinitely many cubic points, which turns out to be determination of the trigonal modular curves $X_1(N)$ and $X_1(2, 2N)$.

This paper follows the same strategy as [**19**] to find torsion structures that occur infinitely often if we vary over all quartic number fields. Of course, in this case, the classification of tetragonal modular curves will play a central role.

The quartic case is in some sense more interesting than the cubic case, because not much is known which torsion groups exist at all. There are explicit bounds in Parent [**25**], but for $d = 4$ they give huge bounds for N and even for N' the bound by Merel [**23**] gives only $N \leqslant 100$ for $d = 4$. Thus, the results in the present paper give a more realistic picture of what torsion exists at all.

In this case, we fall into different situations. For example, the classification of tetragonal modular curves $X_1(N)$ requires more complicated calculations. Also, the non-cyclic torsion structures depend on the roots of unity in the number field, and so various non-cyclic groups may occur over quartic number fields. In fact, we need new methods such as the implementation of a computer algebra system SINGULAR.

Received 26 January 2005; revised 31 October 2005.

2000 *Mathematics Subject Classification* 11G05, 11G18, 11G30.

1. *Preliminaries*

A point P on a curve X over a number field k is called a *point of degree* 4 *over* k, if P is a K-rational point on X for some quartic extension K of k. This includes of course the k-rational points and the rational points over quadratic extensions of k. In the special case $k = \mathbb{Q}$ we also use the term *quartic point*.

For positive integers M and N with $M|N$, consider the congruence subgroup $\Gamma_1(M, N)$ of $\mathrm{SL}_2(\mathbb{Z})$ defined by

$$\Gamma_1(M,N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma(1) = \mathrm{SL}_2(\mathbb{Z}) \;\middle|\; \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \bmod N,\ M \mid b \right\}.$$

Let $X_1(M, N)$ denote the modular curve corresponding to $\Gamma_1(M, N)$. Of course $X_1(1, N)$ is the same as $X_1(N)$. Then there exist infinitely many quartic points on $X_1(M, N)$ if and only if there exist infinitely many elliptic curves E over quartic number fields K such that $E(K)_{\mathrm{tors}}$ contain a subgroup $\mathbb{Z}/M\mathbb{Z} \oplus \mathbb{Z}/N\mathbb{Z}$ (see [**5**]). Put $K_M = \mathbb{Q}(\zeta_M)$ where ζ_M is a primitive Mth root of unity. Note that the field of definition of $X_1(M, N)$ is equal to K_M.

Moreover, for the proofs we need some more modular curves, lying between $X_0(N)$ and $X_1(N)$. Let Δ be a subgroup of $(\mathbb{Z}/N\mathbb{Z})^*$ that contains -1. Let $X_\Delta(N)$ be the modular curve defined over $\mathbb{Q}$ associated to the congruence subgroup

$$\Gamma_\Delta(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma(1) \;\middle|\; a \in \Delta, N \mid c \right\}.$$

Note that for $\Delta = \{\pm 1\}$ this is just $X_1(N)$. A table of genera $g(X_1(N))$ for $N \leqslant 60$ can be found in [**16**], which we do not want to repeat.

Conjugating the group $\Gamma_1(M, N)$ with the matrix $\left(\begin{smallmatrix} 1 & 0 \\ 0 & M \end{smallmatrix}\right)$, we obtain a birational map from $X_1(M, N)$ to $X_\Delta(MN)$ with

$$\Delta = \{\pm 1, \pm(N+1), \pm(2N+1), \ldots, \pm((M-1)N+1)\}.$$

For $d|N$, let π_d be the natural projection from $(\mathbb{Z}/N\mathbb{Z})^*$ to $(\mathbb{Z}/\{d, N/d\}\mathbb{Z})^*$, where $\{d, N/d\}$ is the least common multiple of d and N/d.

THEOREM 1.1 [**18**]. *The genus of the modular curve $X_\Delta(N)$ is given by*

$$g(X_\Delta(N)) = 1 + \frac{\mu}{12} - \frac{\nu_2}{4} - \frac{\nu_3}{3} - \frac{\nu_\infty}{2}$$

where

$$\mu = N \cdot \prod_{\substack{p|N \\ \text{prime}}} \left(1 + \frac{1}{p}\right) \cdot \frac{\varphi(N)}{|\Delta|}$$

$$\nu_2 = |\{(b \mod N) \in \Delta \mid b^2 + 1 \equiv 0 \mod N\}| \cdot \frac{\varphi(N)}{|\Delta|}$$

$$\nu_3 = |\{(b \mod N) \in \Delta \mid b^2 - b + 1 \equiv 0 \mod N\}| \cdot \frac{\varphi(N)}{|\Delta|}$$

$$\nu_\infty = \sum_{\substack{d|N \\ d>0}} \frac{\varphi(d) \cdot \varphi(N/d)}{|\pi_d(\Delta)|}.$$

A smooth projective curve X over an algebraically closed field is called *d-gonal* if there exists a finite morphism $f : X \to \mathbb{P}^1$ of degree d. For $d = 4$, we say that the curve is *tetragonal*. Also, the smallest possible d is called the *gonality* of the curve X and we denote it by $\mathrm{Gon}(X)$.

The best general lower bound for the gonality of a modular curve seems to be that which is obtained in the following way.

Let λ_1 be the smallest positive eigenvalue of the Laplacian operator on the Hilbert space $L^2(X_\Gamma)$ where X_Γ is the modular curve corresponding to a congruence subgroup Γ of $\Gamma(1)$. Let D_Γ be the index of $\pm\Gamma$ in $\Gamma(1)$ and $d_\Gamma = \mathrm{Gon}(X_\Gamma)$. Abramovich [**1**] shows the following inequality:

$$\lambda_1 D_\Gamma \leqslant 24 d_\Gamma.$$

Using the best known lower bound for λ_1, due to Henry Kim and Peter Sarnak (as reported in [**3**, p. 187]), that is, $\lambda_1 > 0.238$, we get the following result.

THEOREM 1.2. *Let X_Γ be the modular curve corresponding to a congruence subgroup Γ of index $D_\Gamma = [\Gamma(1) : \pm\Gamma]$ and $d_\Gamma = \mathrm{Gon}(X_\Gamma)$. Then*

$$D_\Gamma < \frac{12\,000}{119} d_\Gamma.$$

In the following, we call the inequality in Theorem 1.2 *Abramovich's bound*.

REMARK 1.3. Applying Abramovich's bound we can get a good universal bound on the torsion of elliptic curves which occur infinitely often. Suppose that there exist infinitely many K-rational N-torsion points as K varies with $[K : \mathbb{Q}] = d$, which implies that $X_1(N)$ has infinitely many points of degree d over $\mathbb{Q}$. By Proposition 2 of [**11**]

$$\mathrm{Gon}(X_1(N)) \leqslant 2d.$$

Corollary 1.4 of [**19**] says that if $X_1(N)$ is d-gonal, then

$$N < \frac{20\sqrt{1190}}{119} \pi \sqrt{d}.$$

Therefore, we get the following universal bound:

$$N < 26\sqrt{d}.$$

When dealing with an individual curve, the following facts are very useful.

THEOREM 1.4 (Castelnuovo's inequality). *Let F be a function field with perfect constant field k. Suppose that there are two subfields F_1 and F_2 with constant field k satisfying:*

(1) *$F = F_1 F_2$ is the compositum of F_1 and F_2;*
(2) *$[F : F_i] = n_i$, and F_i has genus g_i $(i = 1, 2)$.*

Then the genus g of F is bounded by

$$g \leqslant n_1 g_1 + n_2 g_2 + (n_1 - 1)(n_2 - 1).$$

If k is a number field and X is tetragonal over k, that is, if there exists a k-rational map $X \to \mathbb{P}^1$ of degree 4, then X has infinitely many points of degree 4 over k.

Namely, over every k-rational point of $\mathbb{P}^1$ there lies at least one point of X that is k-rational or K-rational for a suitable quadratic or quartic extension K of k. Concerning this argument, there is a theorem by Abramovich and Harris [**2**].

THEOREM 1.5. *Let X be a curve over a number field k. Suppose that X is not of genus 7. Then X has infinitely many points of degree 4 or less over some finite extension K of k if and only if X admits a map of degree 4 or less to $\mathbb{P}^1$ or an elliptic curve.*

Proof. The proof follows from Theorem 1 in [**2**]. □

PROPOSITION 1.6. *Let X be a curve over a number field k. Suppose that X has infinitely many points of degree 4 over k. If the genus $g(X) \geqslant 7$ and gonality $\mathrm{Gon}(X) > 4$, then the Jacobian variety $J(X)$ contains an elliptic curve E which has positive rank over k.*

Proof. In the proof of Proposition 2 in [**11**] it is shown that if $\mathrm{Gon}(X) > 4$, then the four-fold symmetric product of X embeds as W_4 into the Jacobian $J(X)$ and that by the results of Faltings [**9**, **10**], W_4 contains (a translate of) an abelian subvariety A of $J(X)$ such that $A(k)$ is infinite. By Corollary 3.6 in [**7**], A must be an abelian variety of dimension 1 or 2. Suppose that A is of dimension 2. In Lemma 3.4 in [**7**] we take Z to be a translate of A contained in W_4. Then all of the conditions of the lemma are satisfied and we can conclude that there exists a map $X \to B$ of degree 2 where B is a curve of genus 2. This is a contradiction to the assumption of $\mathrm{Gon}(X) > 4$. □

Ishii and Momose [**15**] asserted that there exist no hyperelliptic modular curves $X_\Delta(N)$ with $\{\pm 1\} \subsetneq \Delta \subsetneq (\mathbb{Z}/N\mathbb{Z})^*$. However, the first two authors of the present paper [**17**] found a counterexample.

LEMMA 1.7. *The curve $X_\Delta(21)$ is a hyperelliptic where $\Delta = \{\pm 1, \pm 8\}$.*

REMARK 1.8. In [**15**] there was a mistake in treating Atkin–Lehner involutions on $X_\Delta(N)$. The Atkin–Lehner involutions define a unique involution on $X_0(N)$ but they do not hold for $X_\Delta(N)$.

In what follows, we have to treat whether $X_\Delta(N)$ and $X_1(M, N)$ are hyperelliptic or not individually.

2. *Tetragonal modular curves*

In this section we determine all of the modular curves $X_1(N)$ and $X_1(2, 2N)$ that are tetragonal. A smooth projective curve X of genus $g(X) \geqslant 2$ is called *bielliptic* (respectively *bi-hyperelliptic*) if it admits a map of degree 2 from X to an elliptic curve (respectively a hyperelliptic curve).

In [**16**, **17**] the first two authors of the present paper classified all bielliptic modular curves $X_1(M, N)$ as follows.

THEOREM 2.1. *The curve $X_1(M,N)$ is bielliptic only for the following (M,N):*

$$(1,13),(1,16),(1,17),(1,18),(1,20),(1,21),(1,22),(1,24),$$
$$(2,14),(2,16),(3,12),(4,12),(5,10),(7,7),(8,8).$$

Note that all bielliptic and bi-hyperelliptic curves are automatically tetragonal. We prove that $X_1(N)$ is tetragonal over $\mathbb{Q}$ if and only if it is rational, elliptic, hyperelliptic or bielliptic and that $X_1(2,2N)$ is tetragonal over $\mathbb{Q}$ if and only if it is rational, elliptic, bielliptic or bi-hyperelliptic. First we consider $X_1(N)$. It is easy to show that if a curve X defined over $\mathbb{Q}$ is rational, elliptic or hyperelliptic, then it admits a tetragonal map to $\mathbb{P}^1$ defined over $\mathbb{Q}$. Also, the first two of the present authors [**16**, **17**] proved that all bielliptic maps on $X_1(N)$ are defined over $\mathbb{Q}$. So the 'if' part follows.

Applying Abramovich's bound $X_1(N)$ can be tetragonal only when $N = 1,\dots,28,30,32$. Now we consider $X_1(25)$. Note that there is a natural map from $X_1(25)$ to $X_\Delta(25)$ of degree 2 where $\Delta = \{\pm1,\pm7\}$. Suppose that $X_1(25)$ is tetragonal. Then there is a map of degree 4 from $X_1(25)$ to $\mathbb{P}^1$. Let F_1 (respectively F_2, F_3) be the function field of $X_1(25)$ (respectively $X_\Delta(25), \mathbb{P}^1$). Note that $X_1(25)$ is of genus 12 and, by Theorem 1.1, $X_\Delta(25)$ is of genus 4. The proof for the non-hyperellipticity of $X_\Delta(25)$ in [**15**] is correct. Thus, we can apply Castelnuovo's inequality, then we get a contradiction. By a similar argument we get the following lemma.

LEMMA 2.2. *The curve $X_1(N)$ is not tetragonal for $N = 25, 27, 32$.*

Proof. The only thing we need is to find suitable maps, and so we suggest them. For $X_1(27)$, the map of degree 3 to $X_\Delta(27)$ that is of genus 1 where $\Delta = \{\pm1,\pm8,\pm10\}$. For $X_1(32)$, the map of degree 2 to $X_{\Delta'}(32)$ that is of genus 5 where $\Delta' = \{\pm1,\pm15\}$. Note that $X_{\Delta'}(32)$ is not hyperelliptic because it is birational to $X_1(2,16)$ and we will prove that there exist no hyperelliptic curves $X_1(2,2N)$ later. □

Now we will show that $X_1(N)$ is not tetragonal for $N = 19, 23, 26, 28, 30$. To this end we need some preparations.

Let X be a smooth projective curve of genus $g(X) \geqslant 3$. An invariant of X, closely related to the gonality, is the Clifford index, which is defined as follows:

$$\mathrm{Cliff}(X) := \min\{d - 2r \mid \exists\, L \in \mathrm{Pic}\, X, \deg(L) = d, h^0(L) = r+1 \geqslant 2, h^1(L) \geqslant 2\}.$$

Recall that it is known that

$$\mathrm{Cliff}(X) + 2 \leqslant \mathrm{Gon}(X) \leqslant \mathrm{Cliff}(X) + 3.$$

For details, see [**4**]. Thus, the following lemma shows that for $N = 19, 23, 26, 28, 30$, $\mathrm{Gon}(X_1(N)) \geqslant 5$ and, hence, $X_1(N)$ is not tetragonal.

LEMMA 2.3. *For $N = 19, 23, 26, 28, 30$, $\mathrm{Cliff}(X_1(N)) \geqslant 3$.*

REMARK 2.4. For a non-hyperelliptic curve X of $g(X) \geqslant 3$, the canonical line bundle defines a projectively normal embedding $X \hookrightarrow \mathbb{P}^{g-1}$. There is a well-known relation between the Clifford index of X and the higher syzygies of the canonical embedding of X. More precisely, let S be the homogeneous coordinate ring of $\mathbb{P}^{g-1}$, I_X the homogeneous ideal of X and $S_X = S/I_X$ the homogeneous coordinate ring of X.

Then one can consider a minimal free resolution

$$\cdots \to \oplus_j S^{\beta_{i,j}}(-i-j) \to \cdots \to \oplus_j S^{\beta_{1,j}}(-1-j) \to S \to S_X \to 0$$

of S_X as a finitely generated graded S-module. We call $\beta_{i,j}$ the *graded Betti numbers*. For a given $p \geqslant 1$, *property* N_p holds if $\beta_{i,j} = 0$ for $1 \leqslant i \leqslant p$ and all $j \geqslant 2$ due to Green and Lazarsfeld [**13**]. Equivalently, property N_p holds if the resolution is of the form

$$\cdots \to S^{\beta_{p,1}}(-p-1) \to \cdots \to S^{\beta_{2,1}}(-3) \to S^{\beta_{1,1}}(-2) \to S \to S_X \to 0.$$

Therefore, for projectively normal varieties, property N_1 holds if and only if the homogeneous ideal is generated by quadrics, and property N_p holds for $p \geqslant 2$ if and only if it has property N_1 and the kth syzygies among the quadrics are generated by linear syzygies for all $1 \leqslant k \leqslant p-1$. Now we recall the following theorem.

THEOREM 2.5 (Green and Lazarsfeld [**12**, Appendix]). *Let X be a smooth non-hyperelliptic curve of genus $g(X) \geqslant 3$. Then the canonical embedding $X \hookrightarrow \mathbb{P}^{g-1}$ fails to satisfy property N_e where $e := \mathrm{Cliff}(X)$.*

This result says that if $X \hookrightarrow \mathbb{P}^{g-1}$ satisfies property N_2, then $\mathrm{Cliff}(X) \geqslant 3$.

Proof of Lemma 2.3. From the above remark, it suffices to show that for $N = 19, 23, 26, 28, 30$, the canonical embedding of $X_1(N)$ satisfies property N_2. To compute the Betti numbers of the canonical embedding, we use the computer programs 'Maple' and SINGULAR.

Step 1. Calculate the homogeneous ideal of the canonical embedding of $X_1(N)$ by using 'Maple'.

Note that $X_1(N)$ is hyperelliptic if and only if $N = 13, 16, 18$ (see [**24**]). Thus, for $N = 19, 23, 26, 28, 30$, $X_1(N)$ can be identified with the canonical curve that is the image of the canonical embedding

$$X_1(N) \ni P \mapsto (f_1(P) : \ldots : f_g(P)) \in \mathbb{P}^{g-1}$$

where $\{f_1, \ldots, f_g\}$ is a basis of the space of cusp forms of weight 2. One can get such a basis and their Fourier coefficients from [**26**]. Then to obtain the homogeneous ideal $I(X_1(N))$, we only have to compute the relations of the $f_i f_j$ $(1 \leqslant i, j \leqslant g)$. There are $(g-2)(g-3)/2$ linear relations among the $f_i f_j$.

Step 2. Compute the Betti numbers by using SINGULAR. Note that because the canonical embedding is always projectively Cohen–Macaulay, the Betti numbers of the canonical curve are equal to those of the hyperplane section.

We show the so-called Betti table of the canonical embedding for our cases in Table 1. Thus, we conclude that property N_2 holds by definition. □

Therefore, we get the following result.

THEOREM 2.6. *The following are equivalent:*
(a) *$X_1(N)$ is tetragonal;*
(b) *$X_1(N)$ is rational, elliptic, hyperelliptic or bielliptic;*
(c) *the genus $g(X_1(N)) \leqslant 6$.*

Explicitly these N are:

- *rational:* $N = 1, \ldots, 10, 12$*;*
- *elliptic:* $N = 11, 14, 15$*;*
- *hyperelliptic:* $N = 13, 16, 18$*;*
- *bielliptic:* $N = 17, 20, 21, 22, 24$.

All hyperelliptic curves are also bielliptic. For each of these curves there exists a morphism $X_1(N) \to \mathbb{P}^1$ *of degree* 4 *that is defined over* $\mathbb{Q}$.

Now we consider $X_1(2, 2N)$. For convenience we state the list of $X_1(M, N)$ that are rational or elliptic as follows.

PROPOSITION 2.7. *The curve* $X_1(M, N)$ *with* $M \geqslant 2$ *is of genus* 0 *or* 1 *if and only if* (M, N) *is one of the* 13 *following ordered pairs:*

- *genus* 0 : $(2,2), (2,4), (2,6), (2,8), (3,3), (3,6), (4,4), (5,5)$.
- *genus* 1 : $(2,10), (2,12), (3,9), (4,8), (6,6)$.

Proof. Using the birationality between $X_1(M, N)$ and $X_\Delta(MN)$ and Theorem 1.1, one can easily obtain the result. □

Suppose that $X_1(2, 2N)$ is hyperelliptic, so is $X_\Delta(4N)$ where $\Delta = \{\pm 1, \pm(2N + 1)\}$. Applying Abramovich's bound $X_\Delta(4N)$ can only be hyperelliptic if $N \leqslant 8$. Note that the genera of $X_1(2, 14)$ and $X_1(2, 16)$ are 4 and 5, respectively. However, by Castelnuovo's inequality, the genus of a curve that is both hyperelliptic and bielliptic is bounded by 3. Thus, $X_1(2, 14)$ and $X_1(2, 16)$ are not hyperelliptic and, hence, we can conclude that there exist no hyperelliptic curves $X_1(2, 2N)$. Similarly to $X_1(N)$, if $X_1(2, 2N)$ is rational, elliptic or bielliptic, then it is tetragonal over $\mathbb{Q}$. The degree 2 cover $X_1(2, 18) \to X_1(18)$ over $\mathbb{Q}$ implies that $X_1(2, 18)$ is also tetragonal over $\mathbb{Q}$ because $X_1(18)$ is hyperelliptic.

TABLE 1. *The graded Betti numbers for the canonical embedding.*

	$\beta_{0,2}$	$\beta_{1,2}$	$\beta_{2,2}$	$\beta_{3,2}$	$\beta_{4,2}$	$\cdots$
$X_1(N)$	$\beta_{0,1}$	$\beta_{1,1}$	$\beta_{2,1}$	$\beta_{3,1}$	$\beta_{4,1}$	$\cdots$
	$\beta_{0,0}$	$\beta_{1,0}$	$\beta_{2,0}$	$\beta_{3,0}$	$\beta_{4,0}$	$\cdots$
	0	0	0	16	10	$\cdots$
$X_1(19)$	0	10	16	0	0	$\cdots$
	1	0	0	0	0	$\cdots$
	0	0	0	0	0	$\cdots$
$X_1(23)$	0	45	231	550	693	$\cdots$
	1	0	0	0	0	$\cdots$
	0	0	0	0	84	$\cdots$
$X_1(26)$	0	28	105	162	84	$\cdots$
	1	0	0	0	0	$\cdots$
	0	0	0	0	84	$\cdots$
$X_1(28)$	0	28	105	162	84	$\cdots$
	1	0	0	0	0	$\cdots$
	0	0	0	0	70	$\cdots$
$X_1(30)$	0	21	64	70	0	$\cdots$
	1	0	0	0	0	$\cdots$

Applying Abramovich's bound to $X_\Delta(4N)$ we know that $X_1(2,2N)$ can be only tetragonal if $N \leqslant 12$. The covers $X_1(2,2N) \to X_1(2N)$ with $N = 11, 12$ assure that $X_1(2,22)$ and $X_1(2,24)$ are not tetragonal by applying Castelnuovo's inequality as in the proof of Lemma 2.2. Finally, by using the Betti number argument one can show that $X_1(2,20)$ is not tetragonal.

THEOREM 2.8. *The following are equivalent:*
(a) $X_1(2,2N)$ *is tetragonal;*
(b) $X_1(2,2N)$ *is rational, elliptic, bielliptic or bi-hyperelliptic;*
(b) *the genus* $g(X_1(2,2N)) \leqslant 7$.
This happens in and only in the following cases:
- *rational:* $N = 1, 2, 3, 4$*;*
- *elliptic:* $N = 5, 6$*;*
- *bielliptic:* $N = 7, 8$*;*
- *bi-hyperelliptic:* $N = 9$.

For each of these curves there exists a morphism $X_1(2,2N) \to \mathbb{P}^1$ *of degree* 4 *that is defined over* $\mathbb{Q}$.

3. *Torsion of elliptic curves over quartic fields*

Let K be a quartic number field and E an elliptic curve over K. If $E(K)_{\text{tors}} \cong \mathbb{Z}/M\mathbb{Z} \oplus \mathbb{Z}/N\mathbb{Z}$ with $M|N$, then by the Weil pairing K must contain the Mth roots of unity. Thus, M will be one of the numbers $M = 1, 2, 3, 4, 5, 6, 8, 10, 12$. For determining the torsion structure that occurs infinitely often, it suffices to consider the existence of infinitely many quartic points on $X_1(M,N)$ for those M.

First we consider the cases $M = 1, 2$ in which the field of definition K_M is equal to $\mathbb{Q}$. We show that $X_1(N)$ has infinitely many quartic points if and only if it is tetragonal, and similarly for $X_1(2,2N)$.

THEOREM 3.1. *We have the following cases.*
(a) *The modular curve* $X_1(N)$ *has infinitely many quartic points if and only if* $N = 1, \ldots, 18, 20, 21, 22, 24$.
(b) *The modular curve* $X_1(2,2N)$ *has infinitely many quartic points if and only if* $N = 1, \ldots, 9$.

Actually, in all of these cases $X_1(N)$ *and* $X_1(2,2N)$ *are double covers of curves that have infinitely many quadratic points.*

Proof. (a) The 'if' part follows by Theorem 2.6. Suppose that $X_1(N)$ has infinitely many quartic points, then by Proposition 2 of [**11**] the gonality $\text{Gon}(X_1(N))$ can be at most 8, and hence $N = 1$–$40, 42, 44, 46, 48$ by Abramovich's bound. Assume that $g(X_1(N)) \geqslant 7$ and $\text{Gon}(X_1(N)) > 4$, which holds for $N = 19, 23$ and $N > 24$ by [**19**, Theorem 2.3] and Theorem 2.6. By Proposition 1.6, the Jacobian $J(X_1(N))$ must contain an elliptic curve E of positive rank over $\mathbb{Q}$. As reported in [**3**, p. 2], the conductor of E divides N. From Cremona's table [**6**] we see that elliptic curves with conductor $N \leqslant 48$ and positive rank must have conductor 37 or 43. Note that the case $N = 43$ is already omitted by Abramovich's bound. Now let us treat the case $N = 37$. Since the genus $g(X_1(37)) \neq 7$ and $\text{Gon}(X_1(37)) > 4$ by Abramovich's bound, it must admit a map of degree 3 or 4 to an elliptic curve by Theorem 1.5. Note that there is a natural map from $X_1(37)$

to $X_\Delta(37)$ of degree 2 where $\Delta = \{\pm 1, \pm 6\}$. Also $X_1(37)$ and $X_\Delta(37)$ are of genus 40 and 16, respectively. One can easily prove that $X_\Delta(37)$ is not bielliptic by the same method as in the proof of Lemma 2.9 of [**16**]. Thus, we can apply Castelnuovo's inequality, and then we get a contradiction.

(b) The 'if' part follows by Theorem 2.8. Suppose that $X_1(2, 2N)$ has infinitely many quartic points. Then the cover $X_1(2, 2N) \to X_1(2N)$ over $\mathbb{Q}$ implies the existence of infinitely many quartic points on $X_1(2N)$, and hence $N \leqslant 12$. Also, $X_1(2, 2N)$ is birational over $\mathbb{Q}$ to $X_\Delta(4N)$ with $\Delta = \{\pm 1, \pm(2N + 1)\}$. In part (a), if $N \leqslant 12$ we have already seen that the elliptic curves in the Jacobian of $X_\Delta(4N)$ have rank 0 over $\mathbb{Q}$. Combining Proposition 1.6, [**19**, Theorem 2.5] and Theorem 2.8, the result follows. □

Now we consider the cases $M = 3, 4, 6$. Since K_M is a quadratic number field for each M, $X_1(M, N)$ has infinitely many quartic points if and only if it has infinitely many quadratic points over K_M. Harris and Silverman [**14**] showed that if a curve X with $g(X) \geqslant 2$ defined over a number field K is neither hyperelliptic nor bielliptic, then the set of quadratic points on X over K is finite.

Suppose that $X_1(3, 3N)$ is hyperelliptic, so is $X_\Delta(9N)$ where $\Delta = \{\pm 1, \pm(3N+1), \pm(6N+1)\}$. Applying Abramovich's bound $X_\Delta(9N)$ can only be hyperelliptic if $N \leqslant 4$. Note that $X_1(3, 9)$ is an elliptic curve, and $X_1(3, 3), X_1(3, 6)$ are $\mathbb{P}^1$. By Castelnuovo's inequality the cover of degree 3 $X_1(3, 12) \to X_1(12)$ implies that $X_1(3, 12)$ is not hyperelliptic. Thus, there exist no hyperelliptic curves $X_1(3, 3N)$. Similarly, in the case $X_1(4, 4N)$, it suffices to prove that $X_1(4, 12)$ is not hyperelliptic. By the Castelnuovo's inequality the genus of a curve that is both hyperelliptic and bielliptic is bounded by 3, and so the result follows. Applying Abramovich's bound only one can show that there exist no hyperelliptic modular curves $X_1(6, 6N)$.

For the rational and elliptic $X_1(M, N)$ with $M = 3, 4, 6$, one can find a map of degree 2 to $\mathbb{P}^1$ over K_M that implies the existence of infinitely many quadratic points over K_M.

By Theorem 2.1 we have to consider the bielliptic curves $X_1(3, 12)$ and $X_1(4, 12)$. Suppose that $X_1(3, 12)$ has infinitely many quadratic points over K_3, then so is $X_\Delta(36)$ where $\Delta = \{\pm 1, \pm 13, \pm 25\}$. Following the same proofs as [**19**, Theorem 1.2] or Proposition 1.6 one can show that the Jacobian $J(X_\Delta(36))$ contains an elliptic curve of positive rank over K_3. However, the first two of the present authors [**17**] proved that such an elliptic curve cannot appear as a factor of $J(X_\Delta(36))$. Thus, $X_1(3, 12)$ has only finitely many quartic points. By similar arguments we can show that there are only finitely many quartic points on $X_1(4, 12)$ too.

Therefore we obtain the following.

THEOREM 3.2. *For $M = 3, 4, 6$, $X_1(M, N)$ has infinitely many quartic points if and only if (M, N) is one of the ordered pairs* $(3, 3), (3, 6), (3, 9), (4, 4), (4, 8), (6, 6)$.

Finally, we consider the cases $M = 5, 8, 10, 12$. In each case K_M is a quartic number field and so $X_1(M, N)$ has infinitely many quartic points if and only if it has infinitely many rational points over K_M. However, by Faltings [**8**] this can happen only when $X_1(M, N)$ is of genus 0 or an elliptic curve of positive rank. Only $X_1(5, 5)$ can satisfy the condition by Proposition 2.7. Thus, we get the following.

THEOREM 3.3. *Among $X_1(M,N)$ with $M = 5, 8, 10, 12$, only $X_1(5,5)$ has infinitely many quartic points.*

Before coming to our main theorem we need some auxiliary results.

LEMMA 3.4. *Let E be an elliptic curve over $\mathbb{Q}$ and E' an elliptic curve over a quadratic number field k.*

(a) *For almost all quadratic number fields K we have*

$$E(K)_{\mathrm{tors}} = E(\mathbb{Q})_{\mathrm{tors}}.$$

(b) *For almost all quadratic extensions L of k we have*

$$E'(L)_{\mathrm{tors}} = E'(k)_{\mathrm{tors}}.$$

Proof. Applying the same arguments as in [**19**, proof of Lemma 3.3(a)] the results follow. □

Mazur [**22**] proved that the torsion group $E(\mathbb{Q})_{\mathrm{tors}}$ of an elliptic curve E over the rational numbers must be isomorphic to one of the following 15 types:

$$\begin{aligned} &\mathbb{Z}/N\mathbb{Z}, && N = 1\text{–}10, 12\\ &\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2N'\mathbb{Z}, && N' = 1\text{–}4. \end{aligned}$$

One can find a proof of the fact that each group occurs infinitely often as the full torsion group $E(\mathbb{Q})_{\mathrm{tors}}$ in [**19**]. Also if E is an elliptic curve over a quadratic number field K, then $E(K)_{\mathrm{tors}}$ must be isomorphic to one of the following groups described in [**20**]:

$$\begin{aligned} &\mathbb{Z}/N\mathbb{Z}, && N = 1\text{–}16, 18\\ &\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2N'\mathbb{Z}, && N' = 1\text{–}6\\ &\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3N''\mathbb{Z}, && N'' = 1\text{–}2\\ &\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}. \end{aligned}$$

We can prove the same phenomenon as follows.

THEOREM 3.5. *Each of the 26 groups listed as above occurs infinitely often as the full torsion group $E(K)_{\mathrm{tors}}$ if K varies over all quadratic fields and E varies over all elliptic curves over K.*

Proof. Each of the cyclic groups listed above occurs infinitely often as a subgroup of $E(K)_{\mathrm{tors}}$ because $X_1(N)$ is rational, elliptic or hyperelliptic for $N = 1\text{–}16, 18$. One can easily check that the same holds for the non-cyclic groups.

First, the group that already occurs over $\mathbb{Q}$ must appear infinitely often because, by Lemma 3.4(a), we can find a suitable quadratic number field without increasing the torsion.

Thus, there only remains the group $\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$ that has to be separated from $\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$. Kubert [**21**, Table 1] suggested parametrizations of rational two 3-cycles as follows:

$$y^2 = x^3 + ax^2 + bx + c; \quad a = \tfrac{3}{4}(r+s), \quad b = \tfrac{1}{2}(rs+t), \quad c = \tfrac{1}{4}rt$$

where $r = 2t/(s-v), t = (v^2+3s^2)/12, v = s - f^2/2$ with $s \neq v, v \neq 0, v^2+3s^2 \neq 0$. Letting $s := -3$ and $f := 2^{k+1}\sqrt{s}$ $(k = 0, 1, 2, \dots)$ we get a family of non-isomorphic elliptic curves defined over $\mathbb{Q}(\sqrt{-3})$ whose torsion subgroups contain $\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$ and no 2-torsion. Thus, the result follows. □

Finally we can prove the main result of this paper.

THEOREM 3.6. *If K varies over all quartic number fields and E varies over all elliptic curves over K, the group structures which appear infinitely often as $E(K)_{\mathrm{tors}}$ are exactly the following:*

$$\begin{aligned}
&\mathbb{Z}/N_1\mathbb{Z}, && N_1 = 1\text{–}18, 20, 21, 22, 24\\
&\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2N_2\mathbb{Z}, && N_2 = 1\text{–}9\\
&\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3N_3\mathbb{Z}, && N_3 = 1\text{–}3\\
&\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4N_4\mathbb{Z}, && N_4 = 1, 2\\
&\mathbb{Z}/5\mathbb{Z} \oplus \mathbb{Z}/5\mathbb{Z},\\
&\mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}.
\end{aligned}$$

Actually, all of these torsion structures already occur infinitely often if K varies over all quadratic extensions of all quadratic number fields, that is, all biquadratic number fields.

Proof. Combining Theorems 3.1, 3.2 and 3.3 we know that only these torsion structures can occur infinitely often. We have already proved that each of the groups listed in the theorem occurs infinitely often as a subgroup of $E(K)_{\mathrm{tors}}$.

This proves the theorem for those groups that are maximal, whereas for the others we still have to take care of the same problem as in the proof of Theorem 3.5.

For the non-maximal groups, observe that they already occur over quadratic fields. Each of the infinitely many elliptic curves over quadratic fields can, by Lemma 3.4, be base-changed to a suitable quartic number field without increasing the torsion. Thus, the result follows. □

Acknowledgements. We want to express our heartfelt thanks to Andreas Schweizer for his kind and valuable comments in proving the results of this paper. We are also grateful to Hyungju Park for suggesting SINGULAR and letting us know that the Betti numbers of the canonical curve are equal to those of the hyperplane section.

References

1. D. ABRAMOVICH, 'A linear lower bound on the gonality of modular curves', *Internat. Math. Res. Notices* 20 (1996) 1005–1011.

2. D. ABRAMOVICH and J. HARRIS, 'Abelian varieties and curves in $W_d(C)$', *Compositio Math.* 78 (1991) 227–238.

3. M. H. BAKER, E. GONZÁLEZ-JIMÉNEZ, J. GONZÁLEZ and B. POONEN, 'Finiteness results for modular curves of genus at least 2', *Amer. J. Math.* 127 (2005) 1325–1387.

4. M. COPPENS and G. MARTENS, 'Secant spaces and Clifford's theorem', *Compositio Math.* 78 (1991) 193–212.

5. D. A. COX and W. R. PARRY, 'Torsion in elliptic curves over $k(t)$', *Compositio Math.* 41 (1980) 337–354.

6. J. E. Cremona, *Algorithms for modular elliptic curves* (Cambridge University Press, Cambridge, 1992).
7. O. Debarre and R. Fahlaoui, 'Abelian varieties in $W_d^r(C)$ and points of bounded degree on algebraic curves', *Compositio Math.* 88 (1993) 235–249.
8. G. Faltings, 'Endlichkeitssätze für abelsche Varietäten über Zahlkörpern', *Invent. Math.* 73 (1983) 349–366.
9. G. Faltings, 'Diophantine approximation on abelian varieties', *Ann. of Math.* (2) 133 (1991) 549–576.
10. G. Faltings, 'The general case of S. Lang's conjecture', *Barsotti Symposium in Algebraic Geometry*, Perspectives on Mathematics 15 (Academic Press, London, 1994) 175–182.
11. G. Frey, 'Curves with infinitely many points of fixed degree', *Israel J. Math.* 85 (1994) 79–83.
12. M. Green, 'Koszul cohomology and the geometry of projective varieties I' (with an Appendix by M. Green and R. Lazarsfeld), *J. Differential Geom.* 19 (1984) 125–171.
13. M. Green and R. Lazarsfeld, 'Some results on the syzygies of finite sets and algebraic curves', *Compositio Math.* 67 (1988) 301–314.
14. J. Harris and J. H. Silverman, 'Bielliptic curves and symmetric products', *Proc. Amer. Math. Soc.* 112 (1991) 347–356.
15. N. Ishii and F. Momose, 'Hyperelliptic modular curves', *Tsukuba J. Math.* 15 (1991) 413–423.
16. D. Jeon and C. H. Kim, 'Bielliptic modular curves $X_1(N)$', *Acta Arith.* 112 (2004) 75–86.
17. D. Jeon and C. H. Kim, 'Bielliptic modular curves $X_1(M, N)$', *Manuscripta Math.* 118 (2005) 455–466.
18. D. Jeon and C. H. Kim, 'On the arithmetic of certain modular curves', Preprint, 2005, arXiv:math.NT/0607611.
19. D. Jeon, C. H. Kim and A. Schweizer, 'On the torsion of elliptic curves over cubic number fields', *Acta Arith.* 113 (2004) 291–301.
20. S. Kamienny and B. Mazur, 'Rational torsion of prime order in elliptic curves over number fields' (with an appendix by A. Granville), Columbia University Number Theory Seminar, New York, 1992, *Astérisque* 228 (Société Mathématique de France, Paris, 1995) 81–100.
21. D. Kubert, 'Universal bounds on the torsion of elliptic curves', *Proc. London Math. Soc.* (3) 33 (1976) 193–237.
22. B. Mazur, 'Modular curves and the Eisenstein ideal', *Publ. Math. Inst. Hautes Études Sci.* 47 (1977) 33–168.
23. L. Merel, 'Bornes pour la torsion des courbes elliptiques sur les corps de nombres', *Invent. Math.* 124 (1996) 437–449.
24. J.-F. Mestre, 'Corps euclidiens, unités exceptionnelles et courbes élliptiques', *J. Number Theory* 13 (1981) 123–137.
25. P. Parent, 'Bornes effectives pour la torsion des courbes elliptiques sur les corps de nombres', *J. reine angew. Math.* 506 (1999) 85–116.
26. William A. Stein, 'The modular forms database', http://modular.math.washington.edu.

Daeyeol Jeon
Department of Mathematics Education
Kongju National University
182 Shinkwan-dong
Kongju, Chungnam, 314-701, Korea

dyjeon@kias.re.kr

Chang Heon Kim
Department of Mathematics
Seoul Women's University
126 Kongnung 2-dong
Nowon-gu
Seoul, 139-774, Korea

chkim@swu.ac.kr

Euisung Park
Korea Institute for Advanced Study (KIAS)
207-43 Cheongnyangni 2-dong
Dongdaemun-gu
Seoul, 130-722, Korea

puserdos@kias.re.kr