ACTA ARITHMETICA
113.3 (2004)

On the torsion of elliptic curves over cubic number fields

by

Daeyeol Jeon, Chang Heon Kim and Andreas Schweizer (Seoul)

0. Introduction. A deep theorem, finally proved in [Ma], states 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:

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

Actually, each of these groups occurs infinitely often as $E(\mathbb{Q})_{\mathrm{tors}}$. (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 $j(E)$.) This is mainly due to the fact that the modular curves parametrizing elliptic curves with such a torsion structure are rational and hence have infinitely many $\mathbb{Q}$-rational points. See [Ku, Table 3] for the explicit parametrization of elliptic curves E such that $E(\mathbb{Q})_{\mathrm{tors}}$ contains such a group structure.

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 [Ka-Ma]:

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

Again, each of these 26 groups occurs infinitely often as $E(K)_{\mathrm{tors}}$, provided we allow the quadratic field K to vary as well. The main reason for this is that the modular curves which parametrize these torsion structures are rational, elliptic or hyperelliptic, and hence have infinitely many points that are rational or quadratic over $\mathbb{Q}$.

2000 *Mathematics Subject Classification*: Primary 11G05; Secondary 11G18.
Key words and phrases: elliptic curve, torsion, cubic number field, modular curve, trigonal.

It is not completely known which torsion groups are possible over cubic number fields, although there exist effective upper bounds. By [P2] and [P3], torsion points of prime order p exist only for $p = 2, 3, 5, 7, 11, 13$. (Actually, in [P2] the non-existence of certain p-torsion points is only proved conditionally; but as reported in [P3], that condition is now known to be true by a theorem of Kato.)

Moreover, [P1] gives explicit uniform bounds for p^n-torsion points over any number field of degree d. But when specialized to $d = 3$ without further fine-tuning, these bounds seem to be much too large. Momose [M] showed that over cubic number fields there exist no 64-torsion points and no 27-torsion points.

In this paper we solve the easier problem which torsion structures occur infinitely often if we vary over all cubic number fields (Theorem 3.4). Besides using some known deep results, the main step of the proof consists in determining which of the modular curves $X_1(N)$ are trigonal.

In analogy with the rational and the quadratic case one might suspect that the set of all possible torsion structures over cubic number fields consists exactly of the groups we have found, or at least is not much larger.

We thank Prof. Pierre Parent, who after seeing the first version of this paper sent us his preprint [P3]. We thank the referee for the careful reading of the manuscript and pointing out an inaccuracy.

1. The main tools. We start with the following easy observation.

LEMMA 1.1. *If E is an elliptic curve over a cubic number field K, then $E(K)_{\mathrm{tors}}$ is either cyclic or of the form $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2N\mathbb{Z}$.*

Proof. If $E(K)_{\mathrm{tors}} \cong \mathbb{Z}/M\mathbb{Z} \oplus \mathbb{Z}/N\mathbb{Z}$ with $M \mid N$, then by the Weil pairing K must contain the Mth roots of unity. But K has a real embedding. Thus $M \leq 2$. ∎

A point P on a curve X over a number field k is called a *point of degree* 3 over k if P is an L-rational point on X for some cubic extension L of k. This includes of course the k-rational points. In the special case $k = \mathbb{Q}$ we also use the term *cubic point*.

Now fix a natural number N. Saying "if K varies over all cubic number fields, there are infinitely many elliptic curves E/K with a K-rational N-torsion point" is tantamount to saying that the modular curve $X_1(N)$ has infinitely many cubic points.

For the non-cyclic torsion structures we have to investigate the modular curves $X_1(2N, 2)$ belonging to the congruence subgroups

$$\Gamma_1(2N) \cap \Gamma(2).$$

Infinitely many cubic points on $X_1(2N, 2)$ are equivalent to the existence

of infinitely many elliptic curves E over cubic number fields K such that $E(K)_{\mathrm{tors}}$ contains a subgroup $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2N\mathbb{Z}$.

But 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. Following [I-M], we write $X_\Delta(N)$ for the modular curve belonging to the group

$$\left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : N \mid c \text{ and } a \in \Delta \right\}.$$

Note that for $\Delta = \{\pm 1\}$ this is just $X_1(N)$. The paper [J-K] contains a formula for the genus of $X_\Delta(N)$ and a table with $g(X_1(N))$ for $N \leq 60$, which we do not want to repeat.

Conjugating the group $\Gamma_1(2N) \cap \Gamma(2)$ with the matrix $\left(\begin{smallmatrix} 1 & 0 \\ 0 & 2 \end{smallmatrix}\right)$ we obtain a birational map, defined over $\mathbb{Q}$, from $X_1(2N, 2)$ to $X_\Delta(4N)$ with $\Delta = \{\pm 1, \pm(2N+1)\}$. In the moduli interpretation this corresponds to dividing an elliptic curve with distinguished subgroup $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2N\mathbb{Z}$ by the 2-torsion point that generates $\mathbb{Z}/2\mathbb{Z}$, and obtaining an elliptic curve with a cyclic $4N$-isogeny and distinguished underlying $2N$-torsion point.

A smooth projective curve X over an algebraically closed field $\overline{k}$ is called *d-gonal* if there exists a finite morphism $f : X \to \mathbb{P}^1$ over $\overline{k}$ of degree d. For $d = 3$ we say that the curve is *trigonal*. Also, the smallest possible d is called the *gonality* of the curve.

For example, if k is a number field and X is trigonal over k, i.e., if there exists a k-rational map $X \to \mathbb{P}^1$ of degree 3, then X has infinitely many points of degree 3 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 L-rational for a suitable cubic extension L of k. Conversely, we have the following necessary criterion.

THEOREM 1.2. *Let X be a curve over a number field k. Suppose that X has at least one k-rational point P_0 and infinitely many points of degree 3 over k. Then the gonality of X is at most 6. Moreover, if the gonality is greater than 3, then the Jacobian variety $\mathrm{Jac}(X)/k$ contains an elliptic curve E which has positive rank over k.*

Proof. The first statement is Proposition 2 in [Fr]. In the proof of that proposition it is also shown that if the gonality of X is greater than 3, then the 3-fold symmetric product of X maps injectively (on points) as W_3 into the Jacobian $\mathrm{Jac}(X)$ and that by a result of Faltings, W_3 contains (a translate of) an abelian subvariety A of $\mathrm{Jac}(X)$ such that $A(k)$ is infinite. By [D-F, Section 3], A must be an elliptic curve. ∎

The best general lower bound for the gonality of a modular curve seems to be the one that 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 $\mathrm{PSL}_2(\mathbb{Z})$. Let D_Γ be the index of Γ in $\mathrm{PSL}_2(\mathbb{Z})$ and d_Γ the gonality of X_Γ. Abramovich [A] shows the following inequality:

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

Using the best known lower bound for λ_1, due to Henry Kim and Peter Sarnak, as reported on page 18 of [B-G-G-P], i.e. $\lambda_1 > 0.238$, we get the following result.

THEOREM 1.3. *Let X_Γ be the modular curve corresponding to a congruence subgroup $\Gamma \subset \mathrm{PSL}_2(\mathbb{Z})$ of index D_Γ and let d_Γ be the gonality of X_Γ. Then*

$$D_\Gamma < \frac{12000}{119}\, d_\Gamma.$$

In the following, we call the inequality in Theorem 1.3 *Abramovich's bound.*

COROLLARY 1.4. *If $X_1(N)$ is d-gonal, then we have*

$$N < \frac{20\sqrt{1190}}{119}\,\pi\sqrt{d} \le 18.22\sqrt{d}.$$

Proof. Note that $[\mathrm{PSL}_2(\mathbb{Z}) : \Gamma_1(N)] = \frac{1}{2}\psi(N)\varphi(N)$, where φ is the Euler function and $\psi(N) = N\prod_{p|N}(1+1/p)$. Our result follows from the inequality

$$\psi(N)\varphi(N) > \zeta(2)^{-1}N^2 = \frac{6}{\pi^2}\,N^2$$

where $\zeta(s)$ is the Riemann zeta function. ∎

When dealing with an individual curve, the following fact is very useful.

THEOREM 1.5 (Castelnuovo's inequality). *Let F be a function field with perfect constant field k. Suppose there are two subfields F_1 and F_2 with constant field k satisfying*

(1) *$F = F_1F_2$ 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

$$g \le n_1g_1 + n_2g_2 + (n_1 - 1)(n_2 - 1).$$

A proof can be found for example in [Sti] (Theorem III.10.3).

2. Trigonal modular curves. In [Ha-S] it is shown that the modular curve $X_0(N)$ is trigonal if and only if it is trivially trigonal, i.e., if $g(X_0(N)) \le 2$ or if $X_0(N)$ is non-hyperelliptic of genus 3 or 4. In this section we prove that the same holds for the modular curves $X_1(N)$ and $X_1(2N, 2)$.

(1) $X_1(N)$ is a rational curve if and only if $N = 1, \ldots, 10, 12$. In this case there obviously exists a $\mathbb{Q}$-rational map of degree 3 from $X_1(N)$ to $\mathbb{P}^1$.

(2) $X_1(N)$ is an elliptic curve if and only if $N = 11, 14, 15$. One can obtain a trigonal morphism defined over $\mathbb{Q}$ by mapping to the Y-coordinate in a Weierstrass equation.

(3) The genus of $X_1(N)$ is 2 if and only if $N = 13, 16, 18$. There are $\mathbb{Q}$-rational maps of degree 3 from $X_1(18)$ and $X_1(13)$ to the rational curves $X_0(18)$ resp. $X_\Delta(13)$ where $\Delta = \{\pm 1, \pm 3, \pm 9\}$. For $X_1(16)$, where we do not naturally see a trigonal map, we use the following lemma.

LEMMA 2.1. *Let X be a curve of genus 2 over a perfect field k. If X has at least three k-rational points, then there exists a map $X \to \mathbb{P}^1$ of degree 3 which is defined over k.*

Proof. We use the Riemann–Roch theorem over k. Let P_1, P_2, P_3 be three different k-rational points on X. If there is no k-rational function with pole divisor $P_1 + P_2 + P_3$, then the Riemann–Roch space of at least one of the divisors $P_i + P_j$, $i \neq j$, must have dimension 2 and hence $P_i + P_j$ must be in the canonical class. Similarly, if there is no k-rational function with pole divisor $3P_i$, then $2P_i$ must be in the canonical class. But then $2P_i$ would be equivalent to $P_i + P_j$, and hence $P_i - P_j$ would be a principal divisor, which is impossible on a curve of positive genus. ∎

We continue the discussion of $X_1(N)$.

(4) $X_1(20)$ has genus 3. Its canonical embedding is a smooth plane quartic curve and the projection from a $\mathbb{Q}$-rational point yields a trigonal morphism $X_1(20) \to \mathbb{P}^1$ over $\mathbb{Q}$.

(5) In all other cases (i.e. $N = 17, 19$ or $N > 20$) the genus of $X_1(N)$ is at least 5. Then a possible trigonal map would be defined over $\mathbb{Q}$. (This is a special case of [N-Sa, Theorem 2.1].) Thus the trigonality of $X_1(N)$ would imply the existence of infinitely many elliptic curves over cubic number fields L with an L-rational N-torsion point. But Momose [M, Theorem 4.1] proved that there are no N-torsion points at all over cubic number fields when $N = 19, 23, 27$. Hence for $N = 19, 23, 27$, $X_1(N)$ is not trigonal.

By Corollary 1.4, if $X_1(N)$ is trigonal, we must have $N \leq 31$. Using Abramovich's bound itself, one can also exclude the values $N = 31$ and $N = 29$.

In [J-K], the first two authors proved that there are eight bielliptic modular curves $X_1(N)$, namely for $N = 13, 16, 17, 18, 20, 21, 22, 24$. But by the Castelnuovo inequality the genus of a curve that is bielliptic and trigonal is bounded by 4. Thus $X_1(N)$ is not trigonal for $N = 17, 21, 22, 24$.

The Castelnuovo inequality also shows that the genus 9 curve $X_1(30)$ cannot be trigonal since it maps of degree 3 to the elliptic curve $X_1(15)$.

Similarly, for the genus 12 curve $X_1(25)$ the existence of a map of degree 5 to the rational curve $X_\Delta(25)$ where $\Delta = \{\pm 1, \pm 4, \pm 6, \pm 9, \pm 11\}$ rules out the existence of a trigonal map.

For the remaining two cases $N = 26$ and 28 we use the method described in Section 2 of [Ha-S]. Let X be a non-hyperelliptic modular curve of genus $g \geq 4$. Then X can be identified with the canonical curve which 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. Then X is trigonal if and only if a minimal generating system of the ideal $I(X)$ contains a cubic polynomial and X is not isomorphic to a smooth plane quintic curve. (This follows from Petri's Theorem, see e.g. [Ha-S, Theorem 2.1].)

To obtain a minimal generating system of $I(X)$, we only have to compute the relations of the $f_i f_j$ and $f_i f_j f_k$ $(1 \leq i, j, k \leq g)$. The space of linear relations among the $f_i f_j$ has dimension $(g-2)(g-3)/2$. Let $Q_1, \ldots, Q_{(g-2)(g-3)/2}$ be a system of quadratic generators of $I(X)$. Since the space of linear relations among the $f_i f_j f_k$ has dimension $(g-3)(g^2+6g-10)/6$, the number of cubic generators is given by

$$(g-3)(g^2+6g-10)/6 - \dim L'$$

where L' is the subspace generated by $x_i Q_j$ $(1 \leq i \leq g;\ 1 \leq j \leq (g-2) \times (g-3)/2)$ and x_i is the ith homogeneous coordinate of $\mathbb{P}^{g-1}$. Thus X is trigonal only if the above difference is non-zero.

LEMMA 2.2. *$X_1(26)$ and $X_1(28)$ are not trigonal.*

Proof. Let us consider the curve $X_1(26)$, which has genus 10. One can use the Fourier series of cusp forms to compute generators of the ideal $I(X_1(26))$. We get a basis of $S_2(X_1(26))$ and the corresponding Fourier coefficients from [St]. Using the computer algebra system MAPLE, we obtain 28 quadratic generators of the ideal $I(X_1(26))$, and find that the dimension of L' is exactly 175. It follows that there are no essential cubic generators. Therefore $X_1(26)$ is not trigonal.

By the same method we see that $X_1(28)$, which is also of genus 10, is not trigonal either. ∎

Summarizing the above results, we obtain the following result.

THEOREM 2.3. *The modular curve $X_1(N)$ is trigonal if and only if $g(X_1(N)) \leq 4$. Explicitly these N are*:

- *genus* 0: $N = 1, \ldots, 10, 12$;
- *genus* 1: $N = 11, 14, 15$;
- *genus* 2: $N = 13, 16, 18$;
- *genus* 3: $N = 20$.

For each of these curves there exists a morphism $X_1(N) \to \mathbb{P}^1$ of degree 3 which is defined over $\mathbb{Q}$.

The cover $X_1(2N,2) \to X_1(2N)$ implies by [N-Sa, Lemma 1.3] that if $X_1(2N,2)$ is trigonal, then $X_1(2N)$ must also be trigonal. Thus $X_1(2N,2)$ cannot be trigonal for $N > 10$. Alternatively, one could prove this by using Abramovich's bound.

Moreover, Theorem 1.5 shows that $X_1(2N,2)$ is not trigonal for $N = 8, 9, 10$. Namely, $X_1(2N,2)$ is a double cover of $X_1(2N)$ and the genera of $X_1(20,2)$, $X_1(20)$, $X_1(18,2)$ and $X_1(18)$ are 9, 3, 7 and 2 respectively. And $X_1(16,2)$ is isomorphic to the genus 5 curve $X_\Delta(32)$ with $\Delta = \{\pm 1, \pm 17\}$, which has a map of degree 2 onto the elliptic curve $X_{\widetilde{\Delta}}(32)$ with $\widetilde{\Delta} = \{\pm 1, \pm 7, \pm 17, \pm 23\}$ (compare [I-M, p. 419]).

On the other hand, for $N = 1, \ldots, 6$, the curve $X_1(2N,2)$ is rational or elliptic, and hence trigonal over $\mathbb{Q}$.

We are left with the curve $X_1(14,2)$, which has genus 4 and is not hyperelliptic (otherwise there would exist elliptic curves E over quadratic number fields K such that $E(K)_{\mathrm{tors}}$ contains a subgroup $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/14\mathbb{Z}$). So $X_1(14,2)$ is trigonal, but it is not clear where the degree 3 map is defined. Instead we investigate the curve $X_\Delta(28)$ corresponding to the group $\Gamma_\Delta = \Gamma_1(14) \cap \Gamma_0(28)$, which is birational to $X_1(14,2)$ over $\mathbb{Q}$.

LEMMA 2.4. *The curve $X_\Delta(28)$ with $\Delta = \{\pm 1, \pm 13\}$ is trigonal over $\mathbb{Q}$.*

Proof. The canonical embedding of $X_\Delta(28)$ in $\mathbb{P}^3$ is contained in a unique irreducible quadric surface Q, and is the complete intersection of Q with an irreducible cubic surface C (see Chap. IV, Example 5.2.2 of [H]). One can get a basis of $S_2(\Gamma_\Delta)$ and the corresponding Fourier coefficients from [St]. A proper linear combination gives a basis $\{f_1, f_2, f_3, f_4\}$ with rational Fourier coefficients. By computing the relations among the monomials $f_i f_j$ and $f_i f_j f_k$ using the computer algebra system MAPLE, we obtain defining equations of Q and C as follows:

$$\begin{cases} Q\colon & -x_1^2 - 4x_2^2 - 2x_1x_2 + x_3^2 + x_4^2 - x_3x_4 = 0, \\ C\colon & x_1^3 - 8x_2^3 - x_3^3 - x_4^3 - 6x_1x_2^2 + 3x_1^2x_2 - 12x_3x_4^2 + 15x_3^2x_4 = 0. \end{cases}$$

The following coordinate change over $\mathbb{Q}$ makes Q a ruled surface $XY - ZW = 0$:

$$\begin{aligned} x_1 &= \tfrac{1}{3}X + \tfrac{1}{4}Y + Z - \tfrac{1}{4}W, \\ x_2 &= \tfrac{1}{3}X + \tfrac{1}{8}Y - \tfrac{1}{2}Z + \tfrac{1}{4}W, \\ x_3 &= \tfrac{1}{3}X - \tfrac{1}{4}Y + Z + \tfrac{1}{4}W, \\ x_4 &= -\tfrac{1}{3}X + \tfrac{1}{4}Y + Z + \tfrac{1}{4}W. \end{aligned}$$

Let $F(X,Y,Z,W) = 0$ be the equation obtained from C by the above coordinate change. By dehomogenization of F with respect to W and substitu-

tions $Z = XY$, $X = x/4$ and $Y = -y/3$, we get a plane model of $X_\Delta(28)$ as follows:

$$(x^2-1)(y^3-9y)+(x^3-2x^2-9x-2)(y^2-1)=0.$$

This shows that the two trigonal maps (to the x-coordinate or to the y-coordinate) are defined over $\mathbb{Q}$. ∎

Again, we summarize:

THEOREM 2.5. *The modular curve $X_1(2N,2)$ is trigonal if and only if its genus is at most* 4. *This happens in and only in the following cases*:

- *genus* 0: $N = 1, 2, 3, 4$;
- *genus* 1: $N = 5, 6$;
- *genus* 4: $N = 7$.

In all these cases there exists a morphism $X_1(2N,2) \to \mathbb{P}^1$ of degree 3 *which is defined over $\mathbb{Q}$.*

3. Torsion of elliptic curves over cubic fields. Now we show that the modular curve $X_1(N)$ has infinitely many cubic points if and only if it is trigonal, and similarly for $X_1(2N,2)$.

THEOREM 3.1. (a) *The modular curve $X_1(N)$ has infinitely many cubic points if and only if $N = 1, \ldots, 16, 18, 20$.*

(b) *The modular curve $X_1(2N,2)$ has infinitely many cubic points if and only if $N = 1, \ldots, 7$.*

Proof. (a) If $X_1(N)$ has infinitely many cubic points, then by Theorem 1.2 the gonality of $X_1(N)$ can be at most 6 and hence $N \le 44$ by Corollary 1.4. Moreover, if the gonality of $X_1(N)$ is greater than 3, then the Jacobian $J_1(N)$ must contain an elliptic curve E with positive rank over $\mathbb{Q}$. As reported on page 2 of [B-G-G-P], the conductor of E divides N. From Cremona's table [C] we see that elliptic curves with conductor ≤ 44 and positive rank must have conductor 37 or 43. But for $N = 37$ and $N = 43$ the gonality of $X_1(N)$ is greater than 6 by Abramovich's bound. Since $X_1(N)$ is hyperelliptic only for $N = 13, 16, 18$ ([I-M]), the result follows by combining Theorems 1.2 and 2.3.

(b) If $X_1(2N,2)$ has infinitely many cubic points, then from the canonical cover $X_1(2N,2) \to X_1(2N)$, which is defined over $\mathbb{Q}$, we obtain infinitely many cubic points on $X_1(2N)$ as well. Therefore $N \le 10$. Also, $X_1(2N,2)$ is birational over $\mathbb{Q}$ to $X_\Delta(4N)$ with $\Delta = \{\pm 1, \pm(2N+1)\}$. In part (a) we have already seen that the elliptic curves in the Jacobian of $X_\Delta(4N)$ have rank 0 over $\mathbb{Q}$. From the torsion structures over quadratic number fields we see that $X_1(2N,2)$ is never hyperelliptic. Thus by Theorem 1.2, $X_1(2N,2)$ can only have infinitely many cubic points if it is trigonal. ∎

For lack of a reference we give a proof of the following (presumably well known) result which we will need later.

THEOREM 3.2. *Each of the* 15 *groups listed in the Introduction occurs infinitely often as the full torsion group* $E(\mathbb{Q})_{\mathrm{tors}}$.

Proof. The point that needs clarification is the following: Of the infinitely many $E/\mathbb{Q}$ with (say) a 6-torsion point, infinitely many will have $E(\mathbb{Q})_{\mathrm{tors}} \cong \mathbb{Z}/12\mathbb{Z}$ and infinitely many will have $E(\mathbb{Q})_{\mathrm{tors}} \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$. We have to make sure that there remain infinitely many with $E(\mathbb{Q})_{\mathrm{tors}} \cong \mathbb{Z}/6\mathbb{Z}$.

This can be seen as follows: From [Ku, Table 3] we take the parametrization of elliptic curves with a 6-torsion point and only consider values for the parameter c that are congruent to ± 2 modulo 5. Then E has good reduction modulo 5. Hence the prime-to-5 torsion reduces injectively into the group of $\mathbb{F}_5$-rational points of the reduced curve. But by the Hasse–Weil bound, there are at most 10 rational points over $\mathbb{F}_5$.

For all other groups that pose a similar problem, one can always restrict the parameter in [Ku, Table 3] to an infinite subset such that reduction modulo 5 and/or reduction modulo 3 guarantees that $E(\mathbb{Q})_{\mathrm{tors}}$ cannot be larger. ∎

Before coming to our main theorem we need one more auxiliary result.

LEMMA 3.3. *Let* E *be an elliptic curve over* $\mathbb{Q}$.

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

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

(b) *There are infinitely many cubic number fields* K_i *such that* $E(K_i)$ *has positive rank.*

Proof. (a) There exists a bound B such that no elliptic curve over a cubic number field K can have a K-rational N-torsion point with $N > B$ (see [Me]). Let L be the number field generated by all N-torsion points of E with $N \le B$. Then for every cubic number field K that is not contained in L we have $E(K)_{\mathrm{tors}} = E(\mathbb{Q})_{\mathrm{tors}}$.

(b) Of course, we can concentrate on the case where $E(\mathbb{Q})$ has rank 0. Moreover, we can assume E in the form $Y^2 = X^3 + AX + B$ with $A, B \in \mathbb{Z}$.

Suppose the fields $K_1, \dots, K_n$ are already constructed. Let p be a prime that is not ramified in any of $K_1, \dots, K_n$. If $X = \xi \in \mathbb{Q}$ were a solution of the equation $p^{-20} = X^3 + AX + B$, then (ξ, p^{-10}) would be a $\mathbb{Q}$-rational torsion point of E (since we assume rank 0). But this contradicts the Nagell–Lutz theorem [Si, p. 221].

So let $K_{n+1} = \mathbb{Q}(\xi)$ where ξ is a solution of $p^{-20} = X^3 + AX + B$. Then K_{n+1} is a cubic number field and different from K_i, $1 \le i \le n$, since p is ramified in K_{n+1} (Newton polygon). Moreover (ξ, p^{-10}) is a K_{n+1}-rational

point of E. By Theorem 7.1 on pp. 220–221 of [Si] it cannot be a torsion point. Hence $E(K_{n+1})$ has positive rank. ∎

Finally, we can prove the main result of this paper.

THEOREM 3.4. *If K varies over all cubic 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*:

$$\mathbb{Z}/N\mathbb{Z}, \qquad N = 1, \dots, 16, 18, 20,$$
$$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2N'\mathbb{Z}, \qquad N' = 1, \dots, 7.$$

Proof. So far we have proved that only these torsion structures can occur infinitely often. By the uniform boundedness theorem ([Me]) only finitely many other torsion structures are possible over cubic fields and for each of these other structures there are only finitely many E/K in total. We have also already shown 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 other ones we still have to take care of the same problem as in the proof of Theorem 3.2.

For the groups that occur already over $\mathbb{Q}$ (compare Theorem 3.2), each of the infinitely many elliptic curves over $\mathbb{Q}$ (compare Theorem 3.2) can by Lemma 3.3(a) be base-changed to a suitable cubic number field K without increasing the torsion.

There only remains the group $\mathbb{Z}/14\mathbb{Z}$ that has to be separated from $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/14\mathbb{Z}$. Now $X_1(14)$ is an elliptic curve and by Lemma 3.3(b) there exists a cubic number field K_1 over which it has infinitely many points. On the other hand, $X_1(14, 2)$ as a curve of genus 4 has only finitely many points over K_1 by Faltings's theorem. ∎

References

[A] D. Abramovich, *A linear lower bound on the gonality of modular curves*, Internat. Math. Res. Notices 1996, no. 20, 1005–1011.

[B-G-G-P] M. H. Baker, E. González-Jiménez, J. González and B. Poonen, *Finiteness results for modular curves of genus at least* 2, e-print arXiv: math.NT/0211394, preprint.

[C] J. E. Cremona, *Algorithms for Modular Elliptic Curves*, Cambridge Univ. Press, 1992.

[D-F] O. Debarre and R. Fahlaoui, *Abelian varieties in $W^r_d(C)$ and points of bounded degree on algebraic curves*, Compositio Math. 88 (1993), 235–249.

[Fr] G. Frey, *Curves with infinitely many points of fixed degree*, Israel J. Math. 85 (1994), 79–83.

[H] R. Hartshorne, *Algebraic Geometry*, Grad. Texts in Math. 52, Springer, 1977.

[Ha-S] Y. Hasegawa and M. Shimura, *Trigonal modular curves*, Acta Arith. 88 (1999), 129–140.

[I-M] N. Ishii and F. Momose, *Hyperelliptic modular curves*, Tsukuba J. Math. 15 (1991), 413–423.

[J-K] D. Jeon and C. H. Kim, *Bielliptic modular curves* $X_1(N)$, Acta Arith. 112 (2004), 75–86.

[Ka-Ma] S. Kamienny and B. Mazur, *Rational torsion of prime order in elliptic curves over number fields* (with an appendix by A. Granville), in: Columbia University Number Theory Seminar (New York, 1992), Astérisque 228 (1995), 81–100.

[Ku] D. Kubert, *Universal bounds on the torsion of elliptic curves*, Proc. London Math. Soc. (3) 33 (1976), 193–237.

[Ma] B. Mazur, *Modular curves and the Eisenstein ideal*, Inst. Hautes Études Sci. Publ. Math. 47 (1977), 33–186.

[Me] L. Merel, *Bornes pour la torsion des courbes elliptiques sur les corps de nombres*, Invent. Math. 124 (1996), 437–449.

[M] F. Momose, *p-torsion points on elliptic curves defined over quadratic fields*, Nagoya Math. J. 96 (1984), 139–165.

[N-Sa] K. V. Nguyen and M.-H. Saito, *d-gonality of modular curves and bounding torsions*, e-print arXiv: math.AG/9603024, preprint.

[P1] P. Parent, *Bornes effectives pour la torsion des courbes elliptiques sur les corps de nombres*, J. Reine Angew. Math. 506 (1999), 85–116.

[P2] —, *Torsion des courbes elliptiques sur les corps cubiques*, Ann. Inst. Fourier (Grenoble) 50 (2000), 723–749.

[P3] —, *No* 17*-torsion on elliptic curves over cubic number fields*, J. Théor. Nombres Bordeaux, to appear.

[Si] J. H. Silverman, *The Arithmetic of Elliptic Curves*, Grad. Texts in Math. 106, Springer, 1986.

[St] W. A. Stein, http://modular.fas.harvard.edu

[Sti] H. Stichtenoth, *Algebraic Function Fields and Codes*, Springer, 1993.

D. Jeon and A. Schweizer
Korea Institute for Advanced Study (KIAS)
207-43 Cheongnyangni 2-dong
Dongdaemun-gu
Seoul, 130-722 South Korea
E-mail: dyjeon@kias.re.kr
schweiz@kias.re.kr

C. H. Kim
Department of Mathematics
Seoul Women's University
126 Kongnung 2-dong
Nowon-gu
Seoul, 139-144 South Korea
E-mail: chkim@kias.re.kr

Received on 22.7.2003
and in revised form on 18.11.2003 (4580)