ACTA ARITHMETICA
152.3 (2012)

Torsion groups of elliptic curves over quadratic fields

by

Sheldon Kamienny (Los Angeles)
and Filip Najman (Leiden and Zagreb)

1. Introduction. For an elliptic curve E over a number field K, it is well known, by the Mordell–Weil theorem, that the set $E(K)$ of K-rational points on E is a finitely generated abelian group. The group $E(K)$ is isomorphic to $T \oplus \mathbb{Z}^r$, where r is a nonnegative integer and T is the torsion subgroup. When $K = \mathbb{Q}$, by Mazur's Theorem [7], the torsion subgroup is either cyclic of order m, where $1 \leq m \leq 10$ or $m = 12$, or of the form $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2m\mathbb{Z}$, where $1 \leq m \leq 4$.

If K is a quadratic field, then the following theorem of Kenku and Momose [5] and the first author [4] classifies the possible torsions.

Theorem 1. *Let K be a quadratic field and E an elliptic curve over K. Then the torsion subgroup $E(K)_{\mathrm{tors}}$ of $E(K)$ is isomorphic to one of the following* 26 *groups:*

$$\begin{aligned}
&\mathbb{Z}/m\mathbb{Z} && \text{for } 1 \leq m \leq 18,\ m \neq 17,\\
&\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2m\mathbb{Z} && \text{for } 1 \leq m \leq 6,\\
&\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/2m\mathbb{Z} && \text{for } m = 1, 2,\\
&\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}.
\end{aligned}$$

While this theorem settles the question which torsion groups appear if the field varies through all quadratic fields, it tells us nothing about the possible torsion subgroups if we fix a certain quadratic field.

The second author found all the possible torsions over each of the two cyclotomic quadratic fields, $\mathbb{Q}(i)$ and $\mathbb{Q}(\sqrt{-3})$, in [8] and [9]. The torsion groups appearing over $\mathbb{Q}(i)$ are the ones from Mazur's theorem and $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$, while the torsion groups appearing over $\mathbb{Q}(\sqrt{-3})$ are the ones from Mazur's theorem, $\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$ and $\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$.

2010 *Mathematics Subject Classification*: 11G05, 14H52.
Key words and phrases: torsion group, elliptic curves, quadratic fields.

DOI: 10.4064/aa152-3-5

In this paper we describe methods that can be used to obtain results of this type, i.e. find all possible torsions over a given quadratic field. The problem amounts to finding whether certain modular curves that are either elliptic or hyperelliptic have K-rational points that are not cusps for the given quadratic field K.

We use these techniques to find, for each possible torsion group, the exact field with the smallest absolute value of the discriminant such that there exists an elliptic curve with that torsion group. This is done by searching through fields with ascending discriminant until we find one over which the torsion group is possible.

Over the rationals, there are infinitely many nonisomorphic elliptic curves with each torsion group. This is not generally the case for all torsion groups over quadratic fields. Some torsion groups will appear for only finitely many elliptic curves (up to isomorphism) for each field, some will always appear infinitely many times if they appear at all, while some will appear finitely many times over some fields and infinitely many times over others.

A folklore conjecture is that the rank of an elliptic curve over the rationals with any possible torsion can be arbitrarily large. In contrast, we will find the maximum rank that an elliptic curve with prescribed torsion can have over certain quadratic fields. This is done with torsion groups that appear finitely often over the given fields.

2. Finding the possible torsions over a fixed quadratic field. Let K be a quadratic field. Denote by $Y_1(m,n)$ the affine curve whose K-rational points classify isomorphism classes of the triples (E, P_m, P_n), where E is an elliptic curve (over K) and P_m and P_n are torsion points (over K) which generate a subgroup isomorphic to $\mathbb{Z}/m\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$. For simplicity, we write $Y_1(n)$ instead of $Y_1(1,n)$. Let $X_1(m,n)$ be the compactification of the curve $Y_1(m,n)$ obtained by adjoining its cusps.

Nice models of the curves $X_1(n)$ can be found, for example, in [1], while the curves $X_1(2,n)$ that we will need can be found in [13]. We list the curves (and their cusps) that correspond to the torsion points that appear over quadratic field, but not over the rationals. We also exclude the curves $X_1(3,3)$, $X_1(3,6)$ and $X_1(4,4)$ since they appear only over the cyclotomic quadratic fields, which are dealt with in [8] and [9]. The curves are as follows:

- $X_1(11) : y^2 - y = x^3 - x$, where the cusps satisfy
$$x(x-1)(x^5 - 18x^4 + 35x^3 - 16x^2 - 2x + 1) = 0;$$
- $X_1(13) : y^2 = x^6 - 2x^5 + x^4 - 2x^3 + 6x^2 - 4x + 1$, where the cusps satisfy
$$x(x-1)(x^3 - 4x^2 + x + 1) = 0;$$

- $X_1(14) : y^2 + xy + y = x^3 - x$, where the cusps satisfy
$$x(x-1)(x+1)(x^3 - 9x^2 - x + 1)(x^3 - 2x^2 - x + 1) = 0;$$
- $X_1(15) : y^2 + xy + y = x^3 + x^2$, where the cusps satisfy
$$x(x+1)(x^4 + 3x^3 + 4x^2 + 2x + 1)(x^4 - 7x^2 - 6x^2 + 2x + 1) = 0;$$
- $X_1(16) : y^2 = x(x^2 + 1)(x^2 + 2x - 1)$, where the cusps satisfy
$$x(x-1)(x+1)(x^2 - 2x - 1)(x^2 + 2x - 1) = 0;$$
- $X_1(18) : y^2 = x^6 + 2x^5 + 5x^4 + 10x^3 + 10x^2 + 4x + 1$, where the cusps satisfy
$$x(x+1)(x^2 + x + 1)(x^2 - 3x - 1) = 0;$$
- $X_1(2, 10) : y^2 = x^3 + x^2 - x$, where the cusps satisfy
$$x(x-1)(x+1)(x^2 + x - 1)(x^2 - 4x - 1) = 0;$$
- $X_1(2, 12) : y^2 = x^3 - x^2 + x$, where the cusps satisfy
$$x(x-1)(2x-1)(2x^2 - x + 1)(3x^2 - 3x - 1)(6x^2 - 6x - 1) = 0.$$

In order to find whether there exists a curve with torsion $\mathbb{Z}/m\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$ over a quadratic field K, one needs to determine whether $X_1(m, n)$ has a K-rational point that is not a cusp.

If $X_1(m, n)$ is an elliptic curve, then a usual method of computing the rank is to perform 2-descent. One can use an implementation [17] of Simon in PARI/GP. If the rank is positive then there will be infinitely many elliptic curves with torsion $\mathbb{Z}/m\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$ over K. If the rank is zero, then one has to check whether all the torsion points are cusps. If not, then there will be finitely many, explicitly computable elliptic curves with the given torsion subgroup.

If $X_1(m, n)$ is a hyperelliptic curve, there are, by Faltings' theorem, finitely many K-rational points, implying that there are finitely many elliptic curves (up to isomorphism) with torsion $\mathbb{Z}/m\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$ over K. To find all the points one can sometimes proceed to compute the rank of the Jacobian using 2-descent on Jacobians. This can be done in MAGMA (see [18]). Although this will often work, 2-descent is not an algorithm, as one has no guarantee that one will obtain the exact rank using it, only upper bounds.

Because of this we give an alternative approach, using the method of Mazur in Section 4, that will give us a criterion when the Jacobians of $X_1(13)$ and $X_1(18)$ have rank 0.

If the rank is equal to zero, after finding the torsion of the Jacobian, one has to check whether any of the torsion points arises from a K-rational point that is not a cusp. If the rank is positive, this significantly complicates the problem and one can try to apply the Chabauty method [16] (if the rank is 1) or some other similar method.

Note that the only other hyperelliptic curve, $X_1(16)$, is generally easier to deal with, since $f(x)$ (where $y^2 = f(x)$ is a model of $X_1(16)$) is not irreducible. This enables one to try to find all the points with more elementary methods, like covering the hyperelliptic curve with 2 elliptic curves (this is essentially what is done in [8]).

Note that once a K-rational point on $Y_1(m,n)$ is found, one can find in [13] how to actually construct an elliptic curve with torsion $\mathbb{Z}/m\mathbb{Z}\oplus\mathbb{Z}/n\mathbb{Z}$ over K.

3. Smallest field with a given torsion. We now apply methods described in Section 2 to find the field with the smallest $|\Delta|$ over which each torsion group appears, where Δ is the discriminant. We start with the group $\mathbb{Z}/11\mathbb{Z}$.

THEOREM 2. *The quadratic field K with smallest $|\Delta|$ such that $\mathbb{Z}/11\mathbb{Z}$ appears as a torsion group over K is $K = \mathbb{Q}(\sqrt{-7})$.*

Proof. The torsion group of $X_1(11)(K)$ is isomorphic to $\mathbb{Z}/5\mathbb{Z}$ for all quadratic fields K (see [13, Lemme 4.1, p. 28]). All the torsion points have $x = 0$ or $x = 1$, implying that the torsion points are cusps. We now compute, using 2-descent, that $\operatorname{rank}(X_1(11)(\mathbb{Q}(\sqrt{d}))) = 0$ for $d = -1,\ -3$ and 5, and $\operatorname{rank}(X_1(11)(\mathbb{Q}(\sqrt{-7}))) = 1$. Taking a nontorsion point on $X_1(11)(\mathbb{Q}(\sqrt{-7}))$, we get the curve

$$y^2 + \frac{85+33\sqrt{-7}}{128}xy + \frac{85\sqrt{-7}-999}{16384}y = x^3 + \frac{89\sqrt{-7}-275}{4096}x^2,$$

where $(0,0)$ is a torsion point of order 11. ∎

THEOREM 3. *The quadratic field K with smallest $|\Delta|$ such that $\mathbb{Z}/13\mathbb{Z}$ appears as a torsion group over K is $K = \mathbb{Q}(\sqrt{17})$.*

Proof. First note that from [9] we can see that $\mathbb{Z}/13\mathbb{Z}$ does not appear over $\mathbb{Q}(i)$ and $\mathbb{Q}(\sqrt{-3})$, the two fields with the smallest $|\Delta|$. As $X_1(13)$ is a hyperelliptic curve, we are led to the study of its Jacobian $J_1(13)$. We deduce via 2-descent that $\operatorname{rank}(J_1(13)(\mathbb{Q}(\sqrt{d}))) = 0$ for $d = 5, -7, 2, -2, -11, 3, 13$ and -15. The torsion of $J_1(13)(\mathbb{Q})$ is isomorphic to $\mathbb{Z}/21\mathbb{Z}$ and all the points on $J_1(13)(\mathbb{Q})_{\text{tors}}$ are generated by the cusps of $X_1(13)$. We will prove $J_1(13)(\mathbb{Q}(\sqrt{d}))_{\text{tors}} = J_1(13)(\mathbb{Q})_{\text{tors}}$ for $d = 5, -7, 2, -2, -11, 3, 13$ and thus complete our proof. Note that if p is an inert (in $\mathbb{Q}(\sqrt{d})$) prime of good reduction, then the prime-to-p part of $J_1(13)(\mathbb{Q}(\sqrt{d}))_{\text{tors}}$ injects into $J_1(13)(\mathbb{F}_p(\sqrt{d})) \simeq J_1(13)(\mathbb{F}_{p^2})$. If p splits, let $\mathfrak{p}$ be a prime over p. Then $O_K/\mathfrak{p} \simeq \mathbb{F}_p$, so the prime-to-$p$ part of $J_1(13)(K)_{\text{tors}}$ injects into $J_1(13)(\mathbb{F}_p)$.

As 3 and 47 are inert in $\mathbb{Q}(\sqrt{5})$, $|J_1(13)(\mathbb{F}_9)| = 3\cdot 19$ and $|J_1(13)(\mathbb{F}_{47^2})| = 2^8 \cdot 7^2 \cdot 19^2$, we conclude $J_1(13)(\mathbb{Q}(\sqrt{5}))_{\text{tors}} = J_1(13)(\mathbb{Q})_{\text{tors}}$.

As 3 and 5 are inert in $\mathbb{Q}(\sqrt{-7})$, $|J_1(13)(\mathbb{F}_9)| = 3 \cdot 19$ and $|J_1(13)(\mathbb{F}_{25})| = 19^2$, we conclude $J_1(13)(\mathbb{Q}(\sqrt{-7}))_{\text{tors}} = J_1(13)(\mathbb{Q})_{\text{tors}}$.

As 3 and 11 are inert in $\mathbb{Q}(\sqrt{2})$, $|J_1(13)(\mathbb{F}_9)| = 3 \cdot 19$ and $|J_1(13)(\mathbb{F}_{121})| = 7^2 \cdot 19^2$, we conclude $J_1(13)(\mathbb{Q}(\sqrt{2}))_{\text{tors}} = J_1(13)(\mathbb{Q})_{\text{tors}}$.

As 5 and 29 are inert in $\mathbb{Q}(\sqrt{-2})$, $|J_1(13)(\mathbb{F}_{25})| = 19^2$ and $|J_1(13)(\mathbb{F}_{29^2})| = 2^6 \cdot 3^2 \cdot 19 \cdot 61$, we conclude $J_1(13)(\mathbb{Q}(\sqrt{-2}))_{\text{tors}} = J_1(13)(\mathbb{Q})_{\text{tors}}$.

As 3 splits and 41 is inert in $\mathbb{Q}(\sqrt{13})$ and $\mathbb{Q}(\sqrt{-11})$, and $|J_1(13)(\mathbb{F}_3)| = 19$ and $|J_1(13)(\mathbb{F}_{41^2})| = 2^6 \cdot 7^4 \cdot 19$, we conclude $J_1(13)(\mathbb{Q}(\sqrt{-11}))_{\text{tors}} = J_1(13)(\mathbb{Q}(\sqrt{13}))_{\text{tors}} = J_1(13)(\mathbb{Q})_{\text{tors}}$.

As 5 and 17 are inert in $\mathbb{Q}(\sqrt{3})$, $|J_1(13)(\mathbb{F}_{25})| = 19^2$ and $|J_1(13)(\mathbb{F}_{17^2})| = 2^6 \cdot 3^2 \cdot 7 \cdot 19$, we conclude $J_1(13)(\mathbb{Q}(\sqrt{3}))_{\text{tors}} = J_1(13)(\mathbb{Q})_{\text{tors}}$.

As 17 splits and 41 is inert in $\mathbb{Q}(\sqrt{-15})$, $|J_1(13)(\mathbb{F}_{17})| = 2^2 \cdot 3 \cdot 19$ and $|J_1(13)(\mathbb{F}_{41^2})| = 2^6 \cdot 7^4 \cdot 19$, we conclude $J_1(13)(\mathbb{Q}(\sqrt{-15}))_{\text{tors}} = J_1(13)(\mathbb{Q})_{\text{tors}}$.

Note that Reichert [14] already found an elliptic curve with torsion $\mathbb{Z}/13\mathbb{Z}$ over $\mathbb{Q}(\sqrt{17})$,

$$y^2 = x^3 - (4323 + 1048\sqrt{17})x + 227630 + 55208\sqrt{17},$$

where $(-49 - 12\sqrt{-7}, -296 - 72\sqrt{-7})$ is a point of order 13. ∎

THEOREM 4. *The quadratic field K with smallest $|\Delta|$ such that $\mathbb{Z}/14\mathbb{Z}$ appears as a torsion group over K is $K = \mathbb{Q}(\sqrt{-7})$.*

Proof. Note that from [8] we can see that $\mathbb{Z}/14\mathbb{Z}$ does not appear over $\mathbb{Q}(i)$ and $\mathbb{Q}(\sqrt{-3})$. Now, $X_1(14)(\mathbb{Q})_{\text{tors}} \simeq \mathbb{Z}/6\mathbb{Z}$, and all the points in $X_1(14)(\mathbb{Q})_{\text{tors}}$ are cusps. From [13, Lemme 4.4, p. 33], we see that $X_1(14)(\mathbb{Q}(\sqrt{-7}))_{\text{tors}} \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$, and $X_1(14)(K)_{\text{tors}} \simeq \mathbb{Z}/6\mathbb{Z}$ for all other quadratic fields K. We compute $\text{rank}(X_1(14)(\mathbb{Q}(\sqrt{5}))) = 0$, so all the points on $X_1(14)(\mathbb{Q}(\sqrt{5}))$ are cusps.

By examining torsion points on $X_1(14)(\mathbb{Q}(\sqrt{-7}))$ that are not rational, we find noncuspidal points on $X_1(14)(\mathbb{Q}(\sqrt{-7}))$. This induces the curve

$$y^2 + \frac{63 + \sqrt{-7}}{56}xy + \frac{11 + \sqrt{-7}}{112}y = x^3 + \frac{11 + \sqrt{-7}}{112}x^2,$$

where the point $(0, 0)$ is of order 14. ∎

THEOREM 5. *The quadratic field K with smallest $|\Delta|$ such that $\mathbb{Z}/15\mathbb{Z}$ appears as a torsion group over K is $K = \mathbb{Q}(\sqrt{5})$.*

Proof. Note that from [8] we can see that $\mathbb{Z}/15\mathbb{Z}$ does not appear over $\mathbb{Q}(i)$ and $\mathbb{Q}(\sqrt{-3})$. Now $X_1(15)(\mathbb{Q})_{\text{tors}} \simeq \mathbb{Z}/4\mathbb{Z}$, and all the points in $X_1(15)(\mathbb{Q})_{\text{tors}}$ are cusps. The only quadratic fields K such that $X_1(15)(K)_{\text{tors}} \not\simeq \mathbb{Z}/4\mathbb{Z}$ are $K = \mathbb{Q}(\sqrt{-3})$, $\mathbb{Q}(\sqrt{5})$ and $\mathbb{Q}(\sqrt{-15})$. One easily checks that the points on $X_1(15)(\mathbb{Q}(\sqrt{-3}))_{\text{tors}}$ are cusps, while the points on $X_1(15)(\mathbb{Q}(\sqrt{5}))_{\text{tors}}$ and $X_1(15)(\mathbb{Q}(\sqrt{-15}))_{\text{tors}}$ are not. From a noncuspidal

point on $X_1(15)(\mathbb{Q}(\sqrt{5}))_{\text{tors}}$ we obtain an elliptic curve (already found by Reichert [14])

$$y^2 = x^3 + (281880\sqrt{5} - 630315)x + 328392630 - 146861640\sqrt{5},$$

with a point $(264\sqrt{5} - 585, 5076\sqrt{5} - 11340)$ of order 15. ∎

REMARK 6. Note that the two example curves in Theorems 4 and 5 prove that [5, Example 2.5] is wrong. We believe that the reason for this is that the bad reduction of the modular curve $X_0(N)$ (for $N = 14, 15$) at the primes 7 and 5 respectively was not taken into account.

THEOREM 7. *The quadratic field K with smallest $|\Delta|$ such that $\mathbb{Z}/16\mathbb{Z}$ appears as a torsion group over K is $K = \mathbb{Q}(\sqrt{-15})$.*

Proof. Note that from [8] we can see that $\mathbb{Z}/16\mathbb{Z}$ does not appear over $\mathbb{Q}(i)$ and $\mathbb{Q}(\sqrt{-3})$. The torsion $J_1(16)(\mathbb{Q})_{\text{tors}}$ of the Jacobian of $X_1(16)(\mathbb{Q})$ is isomorphic to $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/10\mathbb{Z}$. All of these torsion points are induced by cusps of $X_1(16)$. We compute that $\text{rank}(J_1(16)(\mathbb{Q}(\sqrt{d}))) = 0$ for $d = 5, -7, 2, -2, -11, 3$ and 13, and in much the sense manner as in Theorem 3, we obtain $J_1(16)(\mathbb{Q}(\sqrt{d}))_{\text{tors}} = J_1(16)(\mathbb{Q})_{\text{tors}}$ for all the listed values d, with the exception of $d = 2$. For $d = 2$, we obtain $J_1(16)(\mathbb{Q})_{\text{tors}} = \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/10\mathbb{Z}$, but again all the points on the curve $X_1(16)(\mathbb{Q}(\sqrt{2}))$ are cusps.

The elliptic curve (taken from [14])

$$y^2 = x^3 + 272133x + 41173974$$

has a point $(3 - 144\sqrt{-15}, -6480 - 432\sqrt{-15})$ of order 16 over $\mathbb{Q}(\sqrt{-15})$. ∎

THEOREM 8. *The quadratic field K with smallest $|\Delta|$ such that $\mathbb{Z}/18\mathbb{Z}$ appears as a torsion group over K is $K = \mathbb{Q}(\sqrt{33})$.*

Proof. Note that from [8] and [9] we can see that $\mathbb{Z}/18\mathbb{Z}$ does not appear over $\mathbb{Q}(i)$ and $\mathbb{Q}(\sqrt{-3})$. We can immediately disregard the fields $\mathbb{Q}(\sqrt{d})$ for $d = 2, -19, -31, 17, 21$ as a consequence of [5, Proposition 2.4(i)], $d = -11, 13, 21$ as a consequence of [5, Proposition 2.4(ii)] and $d = -7, -15$ as a consequence of [5, Proposition 2.4(iii)]. One is left to deal with the cases $d = -2, 3, 23, 6, -6$. Computing $\text{rank}(J_1(18)(\mathbb{Q}(\sqrt{d}))) = 0$ and $J_1(18)(\mathbb{Q}(\sqrt{d}))_{\text{tors}} = J_1(18)(\mathbb{Q}(\sqrt{d})) = \mathbb{Z}_{21}$ for all these cases, we find that there are no non-cuspidal points on $X_1(18)$ for any of these fields.

For an example of an elliptic curve with torsion $\mathbb{Z}/18\mathbb{Z}$ over $\mathbb{Q}(\sqrt{33})$ we take another example of Reichert [14],

$$y^2 = x^3 + (28296\sqrt{33} - 162675)x + 35441118 - 6168312\sqrt{33},$$

where $(147 - 24\sqrt{33}, 540 - 108\sqrt{33})$ is a point of order 18. ∎

THEOREM 9. *The quadratic field K with smallest $|\Delta|$ such that $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/10\mathbb{Z}$ appears as a torsion group over K is $K = \mathbb{Q}(\sqrt{-2})$.*

Proof. Note that from [8] we can see that $\mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/10\mathbb{Z}$ does not appear over $\mathbb{Q}(i)$ and $\mathbb{Q}(\sqrt{-3})$. All the points on $X_1(2,10)(\mathbb{Q}(\sqrt{-7})) = X_1(2,10)(\mathbb{Q})$ $\simeq \mathbb{Z}/6\mathbb{Z}$ are cusps, as are all the points on $X_1(2,10)(\mathbb{Q}(\sqrt{5})) \simeq \mathbb{Z}/2\mathbb{Z}$ $\oplus\,\mathbb{Z}/6\mathbb{Z}$. Both $X_1(2,10)(\mathbb{Q}(\sqrt{-7}))$ and $X_1(2,10)(\mathbb{Q}(\sqrt{5}))$ have rank 0, while $X_1(2,10)(\mathbb{Q}(\sqrt{-2}))$ has rank 1.

For an elliptic curve with torsion $\mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/10\mathbb{Z}$ over $\mathbb{Q}(\sqrt{-2})$ we take a nontorsion point on $X_1(2,10)(\mathbb{Q}(\sqrt{-2}))$ and obtain the curve

$$y^2 + \frac{5}{11}xy + \frac{6}{121}y = x^3 + \frac{6}{121}x^2,$$

where the points $((-2-8\sqrt{-2})/121, (20\sqrt{-2}-28)/1331)$ and $(6/11, -72/121)$ generate the torsion group $\mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/10\mathbb{Z}$. ∎

THEOREM 10. *The quadratic field K with smallest $|\Delta|$ such that $\mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/12\mathbb{Z}$ appears as a torsion group over K is $K=\mathbb{Q}(\sqrt{13})$.*

Proof. Note that from [8] we can see that $\mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/12\mathbb{Z}$ does not appear over $\mathbb{Q}(i)$ and $\mathbb{Q}(\sqrt{-3})$. The field with smallest $|\Delta|$ such that $X_1(2,12)$ has positive rank over it is $\mathbb{Q}(\sqrt{13})$. Note that for all quadratic fields K except for $K=\mathbb{Q}(i)$, $\mathbb{Q}(\sqrt{3})$ or $\mathbb{Q}(\sqrt{-3})$, we have $X_1(2,12)(K)_{\mathrm{tors}} = X_1(2,12)(\mathbb{Q})_{\mathrm{tors}}$ $\simeq \mathbb{Z}/4\mathbb{Z}$ (see [13, Lemme 4.11, p. 44]). For $K=\mathbb{Q}(i)$, $\mathbb{Q}(\sqrt{3})$ and $\mathbb{Q}(\sqrt{-3})$ all the points on $X_1(2,12)(K)_{\mathrm{tors}}$ are cusps.

For an elliptic curve with torsion $\mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/12\mathbb{Z}$ over $\mathbb{Q}(\sqrt{13})$ we take a nontorsion point on $X_1(2,12)(\mathbb{Q}(\sqrt{13}))$ and obtain the curve

$$y^2 + (134025 - 37172\sqrt{13})xy + (47915630355840 - 13289404780320\sqrt{13})y = x^3 + (3775925760\sqrt{13} - 13614293940)x^2,$$

where the points

$$(954691712 - 264783840\sqrt{13}, 42132429627392\sqrt{13} - 151910635381440)$$

and

$$(3993089880 - 1107483870\sqrt{13}, 176222937989280\sqrt{13} - 635380838833260)$$

generate the torsion group $\mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/12\mathbb{Z}$. ∎

4. The method of Mazur for $X_1(13)$ and $X_1(18)$. As mentioned earlier, the curves $X_1(13)$ and $X_1(18)$ are the hardest to deal with. One can expect that for a large number of fields, 2-descent will not be able to prove the finiteness of $J_1(N)$. We use a different method to obtain a criterion for the finiteness of $J_1(N)$ that will be satisfied for many imaginary quadratic fields.

In [3] the first author carried out a 19-Einstein prime descent on $J_1(13)$ over a quadratic imaginary field K. Here we perform an analogous task,

a 7-Eisenstein prime descent on $J_1(18)$ over a quadratic imaginary field. We describe the results of these descents in Theorem 11.

When $N = 13$ or 18, the curve $X_1(N)$ is of genus 2. We let G be the Galois group of the cover $X_1(N) \to X_0(N)$, so $G \approx (\mathbb{Z}/N\mathbb{Z})^*/(\pm 1)$. In each case the Hecke algebra $\mathbb{T}$ (see [3]) is isomorphic to $\mathbb{Z}[G] \approx \mathbb{Z}[\zeta_3]$. When $N = 13$, the $\mathbb{Q}(\zeta_N)^+$-rational cuspidal group C has order 19, and when $N = 18$, C has order 21. The Eisenstein ideal I is the ideal of $\mathbb{T}$ that annihilates C. We set $q = 19$ if $N = 13$, and $q = 7$ if $N = 18$. The q-Eisenstein prime π is the prime ideal of $\mathbb{T}$, above q, and in the support of I. It is the annihilator of the q-Sylow subgroup C_q of C. We write ε for the character via which G acts on C_q, and we write $\mathbb{Q}_\varepsilon$ for the field cut out by ε (by identifying G with $\mathrm{Gal}(\mathbb{Q}(\zeta_N)^+/\mathbb{Q})$).

Let K be an imaginary quadratic field with associated character ψ, and suppose ψ is disjoint from $\mathbb{Q}_\varepsilon$. We write E for the composition $K \cdot \mathbb{Q}_\varepsilon$. We decompose the q-Sylow subgroup $\mathbf{C}$ of the ideal class group of E into eigenspaces under the action of $\mathrm{Gal}(E/\mathbb{Q})$,

$$\mathbf{C} = \bigoplus \mathbf{C}(\varepsilon^a \psi^b)$$

where $\mathbf{C}(\varepsilon^a\psi^b) = \{c \in \mathbf{C} : \sigma c = \varepsilon^a\psi^b(\sigma)c \text{ for all } \sigma \in \mathrm{Gal}(E/Q)\}$. We note that $\mathbf{C}(\varepsilon^{-a}\psi^{-b}) \neq 0$ if and only if $\mathbb{B}_{1,\varepsilon^a\psi^b} \equiv 0 \pmod{\pi}$, where $\mathbb{B}_{1,\chi}$ is the first generalized Bernoulli number.

THEOREM 11. *If $N = 18$ we assume that 2 does not split in K. If $\mathbf{C}(\psi)$ and $\mathbf{C}(\psi\varepsilon^{-1})$ are both zero then the Mordell–Weil group $J_1(N)(K)$ is finite.*

Proof. When $N = 13$, this is Theorem 6.1 of [3]. For the remainder of the proof we will assume that $N = 18$. The Hecke algebra is $\mathbb{Z}[\zeta_3]$, so the ideal (7) splits into a product $(7) = \pi\overline{\pi}$ of two primes. One of these is the Eisenstein prime π, and the other is the annihilator $\overline{\pi}$ of the $\mathbb{Q}$-rational cuspidal subgroup of order 7. The 7-torsion in $J_1(N)$ has a corresponding decomposition $J[7] = J[\pi] \oplus J[\overline{\pi}]$ into the direct sum of the π- and $\overline{\pi}$-torsion subgroups. As a $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-module C is isomorphic to $\mathbb{Z}/7\mathbb{Z}[\varepsilon]$, the twist of the constant Galois module by the character ε. By the Eichler–Shimura relation the quotient $J[\pi]/C$ is isomorphic to $\boldsymbol{\mu}_7$, the $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-module of 7th roots of unity (see [3] for details).

We will carry out a π-descent in the style of Mazur. One might think that the descent would be made easier if we utilize the potential good reduction at 3, and then take $\mathrm{Gal}(\mathbb{Q}_\varepsilon/\mathbb{Q})$-invariants (which is easy since $[\mathbb{Q}_\varepsilon : \mathbb{Q}]$ is prime to 7). However, it turns out that one does not actually gain anything by doing this. As we shall see, the contribution to the relevant cohomology groups coming from the prime 3 turns out to be trivial.

Since $\mathbb{T} = \mathbb{Z}[\zeta_3]$ is a P.I.D., the ideal π is principal, say $\pi = (\eta)$. Let $\triangle_K = \{\wp : \wp \,|\, 2 \text{ or } 3 \text{ in } \mathcal{O}_K\}$, and let $S = \mathrm{Spec}\,\mathcal{O}_K - \triangle_K$. Write A for the

open subscheme of the Néron model $\mathcal{A}_{/\operatorname{Spec}\mathcal{O}_K}$ whose fibers are connected. We examine the sequence

$$0 \to A[\eta] \to A \xrightarrow{\cdot\eta} A \to 0 \to \cdots \tag{1}$$

over the base $\operatorname{Spec}\mathcal{O}_K$. The group scheme $A[\eta]$ is a quasi-finite flat group scheme over $\operatorname{Spec}\mathcal{O}_K$. We will also need to study the sequence (1) over the base S where A is an abelian scheme, and $A[\eta]$ is a finite flat group scheme.

LEMMA 12.

(a) *There is a short exact sequence of finite flat group schemes*

$$0 \to C \to A[\eta] \to \boldsymbol{\mu}_7 \to 1$$

over the base S.

(b) *There is a short exact sequence of quasi-finite flat group schemes*

$$0 \to \overline{C} \to A[\eta] \to \overline{\boldsymbol{\mu}}_7 \to 1$$

over the base $\operatorname{Spec}\mathcal{O}_K$. *Here $\overline{C}$ and $\overline{\boldsymbol{\mu}}_7$ are extensions of $C_{/S}$ and $\boldsymbol{\mu}_{7/S}$ to* $\operatorname{Spec}\mathcal{O}_K$.

Proof. Part (a) follows from the comments at the beginning of the proof of Theorem 11, together with the Oort–Tate classification of group schemes of prime order.

Part (b) is just obtained by taking the closure of the group schemes in (a). ∎

We use the sequence from 12(b) to analyze the *f.p.q.f.* cohomology of (1), i.e., we study the exact sequence

$$A(\operatorname{Spec}\mathcal{O}_K) \xrightarrow{\cdot\eta} A(\operatorname{Spec}\mathcal{O}_K) \to H^1(\operatorname{Spec}\mathcal{O}_K, A[\eta])$$

with the goal of showing that the right hand group is trivial. This implies that $A(\operatorname{Spec}\mathcal{O}_K)$ is finite. Together with the fact that $A(\operatorname{Spec}\mathcal{O}_K)$ is of finite index in $\mathcal{A}(\operatorname{Spec}\mathcal{O}_K) = J_1(18)(K)$ we see that the latter group is finite.

In order to compute $H^1(\operatorname{Spec}\mathcal{O}_K, A[\eta])$ we compute $H^1(\operatorname{Spec}\mathcal{O}_K, \overline{C})$ and $H^1(\operatorname{Spec}\mathcal{O}_K, \overline{\boldsymbol{\mu}}_7)$. To analyze the latter we use the sequence

$$1 \to \overline{\boldsymbol{\mu}}_7 \to \boldsymbol{\mu}_7 \to \boldsymbol{\mu}_{7^\cdot} \to 1$$

where $\boldsymbol{\mu}_{7^\cdot}$ is a skyscraper sheaf concentrated at the points of $\triangle$. As usual, $H^1(\operatorname{Spec}\mathcal{O}_K, \boldsymbol{\mu}_7)$ fits into a Kummer sequence

$$1 \to \mathcal{O}_K^*/(\mathcal{O}_K^*)^7 \to H^1(\operatorname{Spec}\mathcal{O}_K, \boldsymbol{\mu}_7) \to \operatorname{Pic}(\mathcal{O}_K)[7] \to 1.$$

The left hand group is trivial since K is an imaginary quadratic field, and the right is trivial since the class number of K is assumed to be relatively prime to 7 (i.e., $\mathbf{C}(\psi) = 0$). Thus $H^1(\operatorname{Spec}\mathcal{O}_K, \boldsymbol{\mu}_7) = 0$.

Now $H^0(\operatorname{Spec}\mathcal{O}_K, \boldsymbol{\mu}_{7^\cdot}) = \bigoplus_{\wp\in\triangle} \boldsymbol{\mu}_7(\mathcal{O}_K/\wp)$, and so this group is also trivial. Thus, the sequence

$$\to H^0(\operatorname{Spec}\mathcal{O}_K, \boldsymbol{\mu}_{7^\cdot}) \to H^1(\operatorname{Spec}\mathcal{O}_K, \overline{\boldsymbol{\mu}}_7) \to H^1(\operatorname{Spec}\mathcal{O}_K, \boldsymbol{\mu}_7)$$

shows that the middle group is trivial.

We turn our attention to the group $H^1(\operatorname{Spec}\mathcal{O}_K, \overline{C})$. Let $\triangle_E = \{\wp \in \operatorname{Spec}\mathcal{O}_E : \wp \,|\, 2 \text{ or } 3\}$, and let $T = \operatorname{Spec}\mathcal{O}_E - \triangle_E$. Mazur [6] shows that $H^1(\operatorname{Spec}\mathcal{O}_K, \overline{C})$ injects into $H^1(S, C)$, and the latter group injects into $H^1(T, C_{/T})^{\mathrm{Gal}(T/S)} \approx H^1(T, \mathbb{Z}/7\mathbb{Z})^{\mathrm{Gal}(T/S)}$ (since $C_{/T} \approx \mathbb{Z}/7\mathbb{Z}$). The latter injection follows from the Hochschild–Serre spectral sequence $H^p(\mathrm{Gal}(T/S), H^q(T, C_{/T})) \Rightarrow H^{p+q}(S, C)$, which degenerates since $\mathrm{Gal}(T, S)$ has order prime to 7.

We examine the long exact relative cohomology sequence

$$(2) \qquad 0 \to H^1(\operatorname{Spec}\mathcal{O}_E, \mathbb{Z}/7\mathbb{Z}) \to H^1(T, \mathbb{Z}/7\mathbb{Z}) \to H^2_{\triangle}(\operatorname{Spec}\mathcal{O}_E, \mathbb{Z}/7\mathbb{Z}) \to H^2(\operatorname{Spec}\mathcal{O}_E, \mathbb{Z}/7\mathbb{Z}) \to \cdots$$

Now $H^2_{\triangle}(\operatorname{Spec}\mathcal{O}_E, \mathbb{Z}/7\mathbb{Z}) \approx \bigoplus_{\wp\in\triangle} H^2(\operatorname{Spec}\mathcal{O}_{E,\wp}, \mathbb{Z}/\mathbb{Z})$, which is isomorphic to the Pontryagin dual $\bigoplus_{\wp\in\triangle} H^1(\operatorname{Spec}\mathcal{O}_{E,\wp}, \boldsymbol{\mu}_7)^*$ by local flat duality.

The map $H^2_{\triangle}(\operatorname{Spec}\mathcal{O}_{E,\wp}, \mathbb{Z}/7\mathbb{Z}) \to H^2/(\operatorname{Spec}\mathcal{O}_E, \mathbb{Z}/7\mathbb{Z})$ in (2) is dual to the map $H^1(\operatorname{Spec}\mathcal{O}_E, \boldsymbol{\mu}_7) \xrightarrow{\alpha} H^1(\operatorname{Spec}\mathcal{O}_{E,\wp}, \boldsymbol{\mu}_7)$, where $\wp$ is the unique prime of E dividing 2. Under α the group $\mathcal{O}_E^*/(\mathcal{O}_E^*)^7$ maps surjectively onto $k_\wp^*/(k_\wp^*)^7$ (where $k_\wp = \mathcal{O}_E/\wp$). Then $H^2_{\triangle}(\operatorname{Spec}\mathcal{O}_E, \mathbb{Z}/7\mathbb{Z})$ maps injectively to $H^2(\operatorname{Spec}\mathcal{O}, \mathbb{Z}/7\mathbb{Z})$, which tells us (from (2)) that $H^1(\operatorname{Spec}\mathcal{O}_E, \mathbb{Z}/7\mathbb{Z})$ surjects onto $H^1(T, \mathbb{Z}/7\mathbb{Z})$, i.e.

$$\begin{aligned} &H^1(\operatorname{Spec}\mathcal{O}_E, \mathbb{Z}/7\mathbb{Z}) \approx H^1(T, \mathbb{Z}/7\mathbb{Z}) \\ &\approx | \\ &\mathrm{Hom}(\mathcal{C}l_E, \mathbb{Z}/7\mathbb{Z}) \end{aligned}$$

Taking $\mathrm{Gal}(T/S)$-invariants and using the assumption $\mathcal{C}(\psi\varepsilon^{-1}) = 0$ we find $H^1(T, \mathbb{Z}/7\mathbb{Z})^{\mathrm{Gal}(T/S)} = 0$, as desired. This completes the proof that $J_1(N)(K)$ is finite. ∎

Finally, we wish to use the results on the descents to study K-rational points on $X_1(N)$. Let $R = \operatorname{Spec}\mathbb{Z}$ if $N = 13$, and $\operatorname{Spec}\mathbb{Z}[1/3]$ if $N = 18$. Mazur's argument [6, 3.1] works mutatis mutandis in this case and proves the following.

PROPOSITION 13. *The morphism $f : X_1(N)^{\mathrm{smooth}}_{/R} \to J_1(N)$ is a formal immersion away from characteristic 2 and 13 if $N = 13$, and away from characteristic 2 if $N = 18$.*

We recall that K is a quadratic imaginary field such that $J_1(N)(K)$ is finite. If $N = 13$ let $p = 3$ or 5, and if $N = 18$ let $p = 5$ or 7, and assume that

p splits or ramifies in K. We let $\wp$ be a prime above p in $\mathcal{O}_K$, and write k for $\mathcal{O}_K/\wp$. Proposition 13, together with the argument of [6, Corollary 4.3], shows that if E is an elliptic curve over K with a K-rational point P of order N then E has potentially good reduction at $\wp$. The reduction cannot be good because N is too large for the reduction of P to exist on $E_{/k}$. The reduction must therefore be additive. However, N is also too large to divide $[E : E^\circ]$ in the additive case, which forces P to specialize to $E^\circ_{/k} \approx G_a$. This is clearly impossible since $\gcd(N, p) = 1$, so the pair (E, P) cannot exist.

5. Interplay of rank and torsion. In this section we will study how often a torsion group appears over a fixed quadratic field if it appears at all. All three possibilities will happen: some groups will appear infinitely often over a fixed quadratic field K, some finitely often, and some can appear finitely or infinitely often, depending on K.

THEOREM 14. *Suppose that over a quadratic field K, the group $\mathbb{Z}/13\mathbb{Z}$, $\mathbb{Z}/16\mathbb{Z}$ or $\mathbb{Z}/18\mathbb{Z}$ appears as torsion group of an elliptic curve. Then there are finitely many elliptic curves (up to isomorphism) over K with that torsion group.*

Proof. As $X_1(N)$ is a curve of genus > 1 for $N = 13, 16, 18$, by Faltings' theorem, $X_1(N)(K)$ has finitely many points. ∎

THEOREM 15. *Suppose that over a quadratic field K, the group $\mathbb{Z}/11\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/10\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/12\mathbb{Z}$ appears as torsion group of an elliptic curve. Then there are infinitely many elliptic curves over K with that torsion group.*

Proof. Since $X_1(m, n)$ for $(m, n) = (1, 11), (2, 10), (2, 12)$ are elliptic curves, one has to prove that there does not exist a field where $X_1(m, n)$ has a noncuspidal torsion point and rank 0.

As was mentioned in Theorem 2, $X_1(11)(K)_{\text{tors}} = X_1(11)(\mathbb{Q})_{\text{tors}} \simeq \mathbb{Z}/5\mathbb{Z}$ and all the torsion points are cusps. Thus if $X_1(11)(K)$ has a noncuspidal point, it is of infinite order.

As mentioned in Theorems 9 and 10, all the points on $X_1(2, 10)(K)_{\text{tors}}$ and $X_1(2, 12)(K)_{\text{tors}}$ are cusps, for all quadratic fields K. ∎

THEOREM 16.

(i) *There are two elliptic curves with torsion $\mathbb{Z}/14\mathbb{Z}$ over $\mathbb{Q}(\sqrt{-7})$. Over all other quadratic fields, if there exists one elliptic curve with torsion $\mathbb{Z}/14\mathbb{Z}$, there exist infinitely many.*

(ii) *There is one elliptic curve with torsion $\mathbb{Z}/15\mathbb{Z}$ over the fields $\mathbb{Q}(\sqrt{5})$ and $\mathbb{Q}(\sqrt{-15})$. Over all other quadratic fields, if there exists one elliptic curve with torsion $\mathbb{Z}/15\mathbb{Z}$, there exist infinitely many.*

Proof. (i) As mentioned in Theorem 4, $\mathbb{Q}(\sqrt{-7})$ is the only field over which the elliptic curve $X_1(14)$ has torsion that is larger than $X_1(14)(\mathbb{Q})_{\mathrm{tors}}$ and there are points on $X_1(14)(\mathbb{Q}(\sqrt{-7}))_{\mathrm{tors}}$ that are not cusps. Moreover, $\mathrm{rank}(X_1(14)(\mathbb{Q}(\sqrt{-7}))) = 0$, so there are finitely many points on $X_1(14)$ over $\mathbb{Q}(\sqrt{-7})$. By checking the curves generated by the torsion points of $X_1(14)(\mathbb{Q}(\sqrt{-7}))$ one easily sees that there are, up to isomorphism, exactly two elliptic curves with torsion $\mathbb{Z}/14\mathbb{Z}$ over $\mathbb{Q}(\sqrt{-7})$. The curves have the following equations:

$$y^2 + \frac{14+3\sqrt{-7}}{7}xy + \frac{-3+\sqrt{-7}}{7}y = x^3 + \frac{-3+\sqrt{-7}}{7}x^2,$$
$$y^2 + \frac{7+2\sqrt{-7}}{7}xy + \frac{1+\sqrt{-7}}{7}y = x^3 + \frac{1+\sqrt{-7}}{7}x^2,$$

where $(0,0)$ is a point of order 14 on both curves.

For all other quadratic fields, a noncuspidal point on $X_1(14)(\mathbb{Q}(\sqrt{-7}))$ will have infinite order.

(ii) As mentioned in Theorem 5, the only fields over which the elliptic curve $X_1(15)$ has torsion larger than $X_1(15)(\mathbb{Q})_{\mathrm{tors}}$ are the fields $\mathbb{Q}(\sqrt{-3})$, $\mathbb{Q}(\sqrt{5})$ and $\mathbb{Q}(\sqrt{15})$. One checks that the points on $X_1(15)(\mathbb{Q}(\sqrt{-3}))_{\mathrm{tors}}$ are cusps, while the points on $X_1(15)(\mathbb{Q}(\sqrt{5}))_{\mathrm{tors}}$ and $X_1(15)(\mathbb{Q}(\sqrt{-15}))_{\mathrm{tors}}$ are not. One computes that $\mathrm{rank}(X_1(15)(\mathbb{Q}(\sqrt{5}))) = \mathrm{rank}(X_1(15)(\mathbb{Q}(\sqrt{-15}))) = 0$, proving that there are only finitely many curves with torsion $\mathbb{Z}/15\mathbb{Z}$ over these fields. By checking the curves generated by the torsion points of $X_1(15)(\mathbb{Q}(\sqrt{5}))$ and $X_1(15)(\mathbb{Q}(\sqrt{-15}))$, we find that over both of these fields there is exactly one curve with 15-torsion. Over $\mathbb{Q}(\sqrt{-15})$ this is the elliptic curve

$$y^2 + \frac{145+7\sqrt{-15}}{128}xy + \frac{265+79\sqrt{-15}}{4096}y = x^3 + \frac{265+79\sqrt{-15}}{4096}x^2,$$

where $((95-9\sqrt{-15})/512, (255+65\sqrt{-15})/16384)$ is a point of order 15.

The only curve with 15-torsion over $\mathbb{Q}(\sqrt{5})$ can be found in the proof of Theorem 5. ∎

One can examine not just the torsion group, but the whole Mordell–Weil group of these exceptional curves. One can easily compute that the rank of all four curves from Theorem 16 is equal to zero.

This proves the following corollary.

Corollary 17.

(a) *All elliptic curves with torsion* $\mathbb{Z}/14\mathbb{Z}$ *over* $\mathbb{Q}(\sqrt{-7})$ *have rank zero.*
(b) *All elliptic curves with torsion* $\mathbb{Z}/15\mathbb{Z}$ *over* $\mathbb{Q}(\sqrt{5})$ *and* $\mathbb{Q}(\sqrt{-15})$ *have rank zero.*

Note that this is in stark contrast to what happens over the rationals, where it is a widely believed conjecture that an elliptic curve with prescribed torsion can have arbitrarily large rank. Moreover, for any torsion group appearing over the rationals, there exists an elliptic curve with that torsion group and rank at least 3 (see [2]).

An upper limit on the rank of an elliptic curve with given torsion over a fixed quadratic field can exist and be positive. For example, by Theorem 14, there are only finitely many elliptic curves with torsion $\mathbb{Z}/13\mathbb{Z}$ over $\mathbb{Q}(\sqrt{193})$, and by [13, Théorème 4.3], there exists a curve with rank at least 2.

6. Number of fields having given torsion. It is natural to wonder what is the density of the fields having some fixed group as a torsion group of elliptic curves. For torsion groups such that the curve X_1 inducing them is an elliptic curve, this will depend on the rank of the quadratic twists of X_1. If $T = \mathbb{Z}/m\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$ is a torsion group that is generated by an elliptic modular curve $X_1(m,n)$, then for all except finitely many quadratic fields K, T will appear as a torsion group over K if and only if X_1 has positive rank over K. This means that the standard conjecture [15, Corollary 7.4] implies that the group T will appear over $1/2$ of the quadratic fields, when ordered by discriminant. However, the best one can unconditionally prove at the moment is an asymptotical lower bound on the number of fields $\mathbb{Q}(\sqrt{d})$ with $|d| \le X$ for some bound X, having or not having T as a torsion group.

PROPOSITION 18.

(a) *Let $T = \mathbb{Z}/14\mathbb{Z}$, $\mathbb{Z}/15\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/10\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/12\mathbb{Z}$. Then the number of quadratic fields $\mathbb{Q}(\sqrt{d})$ such that $0 < |d| \le X$ and T does not appear as the torsion group of an elliptic curve over $\mathbb{Q}(\sqrt{d})$ is $\gg X/\log X$.*

(b) *The number of quadratic fields $\mathbb{Q}(\sqrt{d})$ such that $0 < |d| \le X$ and $\mathbb{Z}/11\mathbb{Z}$ does not appear as the torsion group of an elliptic curve over $\mathbb{Q}(\sqrt{d})$ is $\gg X/(\log X)^{1-\alpha}$ for some $0 < \alpha < 1$.*

(c) *Let $\epsilon > 0$ and $T = \mathbb{Z}/11\mathbb{Z}$, $\mathbb{Z}/14\mathbb{Z}$, $\mathbb{Z}/15\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/10\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/12\mathbb{Z}$. Then the number of quadratic fields $\mathbb{Q}(\sqrt{d})$ such that $0 < |d| \le X$ and T appears as a torsion group (for infinitely many nonisomorphic curves) over $\mathbb{Q}(\sqrt{d})$ is $\gg X^{1-\epsilon}$.*

Proof. (a) As $X_1(14)$, $X_1(15)$, $X_1(2,10)$ and $X_1(2,12)$ are elliptic curves, by [11, Corollary 3] we see that $\gg X/\log X$ of the twists of the appropriate curve X_1 will have rank 0, and thus there will be no elliptic curves with given torsion over the corresponding quadratic field.

(b) The proof is the same as in (a) with the difference that since $X_1(11)$ does not have a rational 2-torsion point, we can apply the stronger result of [10, Corollary 3] and thus prove the theorem.

(c) By [12, Theorem 1], $\gg X^{1-\epsilon}$ of the twists of each of the elliptic curves X_1 will have positive rank, and thus there will exist infinitely many elliptic curves with the appropriate torsion over this field. ∎

If T is a torsion group induced by a hyperelliptic curve, then one expects this torsion group not to appear much more often than it appears. Indeed, one can prove that for a large density of quadratic fields, if the fields $\mathbb{Q}(\sqrt{d})$ are ordered by the largest prime appearing in d, $\mathbb{Z}/18\mathbb{Z}$ will not appear as a torsion group.

We will use the following proposition of Kenku and Momose [5, Proposition (2.4)].

PROPOSITION 19. *Let K be a quadratic field. If K satisfies one of the conditions* (i), (ii) *or* (iii) *listed below, then there are no elliptic curves over K with torsion $\mathbb{Z}/18\mathbb{Z}$.*

(i) 3 *remains prime in K.*
(ii) 3 *splits in K and* 2 *does not split in K.*
(iii) 5 *or* 7 *ramifies in K.*

We now define the function ψ that will give us an ordering of quadratic fields that will be more suitable for our purposes.

DEFINITION 20. Let d be a square-free integer and write $d_1 = (-1)^{\alpha_0} 2^{\alpha_1} \dots p_k^{\alpha_k}$. We define the bijection ψ from the set of all quadratic fields to the positive integers by $\psi(\mathbb{Q}(\sqrt{d})) = (\alpha_k \dots \alpha_0)_2$.

THEOREM 21. *Define $N_t = \{\mathbb{Q}(\sqrt{d}) : \mathbb{Z}/18\mathbb{Z}$ does not appear as the torsion group of an elliptic curve over $\mathbb{Q}(\sqrt{d})$ and $\psi(\mathbb{Q}(\sqrt{d})) \le t\}$ and $A_t = \{\mathbb{Q}(\sqrt{d}) : \psi(\mathbb{Q}(\sqrt{d})) \le t\}$. Then*

$$\lim_{t\to\infty} \frac{N_t}{A_t} \ge \frac{55}{64}.$$

Proof. When ordered by the ψ-function, 1/4 of quadratic fields will satisfy part (i) of Proposition 19, and 3/16 will satisfy (ii). Since the set of fields satisfying (i) and the set of fields satisfying (ii) are disjoint, 7/16 of the fields will satisfy either one. Condition (iii) is satisfied by 3/4 of the fields and the probability that this condition is satisfied does not depend on whether (i) or (ii) are satisfied, and thus we conclude that at least $7/16 + 3/4 - 7/16 \cdot 3/4 = 55/64$ of quadratic fields (when ordered by ψ) do not have $\mathbb{Z}/18\mathbb{Z}$ as a torsion subgroup appearing over them. ∎

Acknowledgements. We are grateful to Andrej Dujella and Matija Kazalicki for helpful comments. The second author was financed by the National Foundation for Science, Higher Education and Technological Development of the Republic of Croatia.

References

[1] H. Baaziz, *Equations for the modular curve $X_1(N)$ and models of elliptic curves with torsion points*, Math. Comp. 79 (2010), 2371–2386.

[2] A. Dujella, *Infinite families of elliptic curves with high rank and prescribed torsion*, http://web.math.hr/~duje/tors/generic.html.

[3] S. Kamienny, *On $J_1(p)$ and the conjecture of Birch and Swinnerton-Dyer*, Duke Math. J. 49 (1982), 329–340.

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

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

[6] B. Mazur, *Rational points of abelian varieties with values in towers of number fields*, Invent. Math. 18 (1972), 183–266.

[7] —, *Rational isogenies of prime degree*, ibid. 44 (1978), 129–162.

[8] F. Najman, *Torsion of elliptic curves over quadratic cyclotomic fields*, Math. Univ. J. Okayama 53 (2011) 75–82.

[9] —, *Complete classification of torsion of elliptic curves over quadratic cyclotomic fields*, J. Number Theory 130 (2010), 1964–1968.

[10] K. Ono, *Nonvanishing of quadratic twists of modular L-functions and applications to elliptic curves*, J. Reine Angew. Math. 533 (2001), 81–97.

[11] K. Ono and C. Skinner, *Non-vanishing of quadratic twists of modular L-functions*, Invent. Math. 134 (1998), 651–660.

[12] A. Perelli and J. Pomykała, *Averages of twisted elliptic L-functions*, Acta Arith. 80 (1997), 149–163.

[13] F. P. Rabarison, *Structure de torsion des courbes elliptiques sur les corps quadratiques*, ibid. 144 (2010), 17–52.

[14] M. A. Reichert, *Explicit determination of nontrivial torsion structures of elliptic curves over quadratic number fields*, Math. Comp. 46 (1986), 637–658.

[15] K. Rubin and A. Silverberg, *Ranks of elliptic curves*, Bull. Amer. Math. Soc. 39 (2002), 455–474.

[16] S. Siksek, *Explicit Chabauty over number fields*, arXiv:10102603.

[17] D. Simon, Le fichier gp, http://www.math.unicaen.fr/~simon/ell.gp.

[18] M. Stoll, *Implementing 2-descent for Jacobians of hyperelliptic curves*, Acta Arith. 98 (2001), 245–277.

Sheldon Kamienny
Department of Mathematics
University of Southern California
3620 S. Vermont Ave.
Los Angeles, CA 90089-2532, U.S.A.
E-mail: kamienny@usc.edu

Filip Najman
Mathematisch Instituut
P.O. Box 9512
2300 RA Leiden, The Netherlands
E-mail: fnajman@math.leidenuniv.nl
and
Department of Mathematics
University of Zagreb
Bijenička Cesta 30
10000 Zagreb, Croatia
E-mail: fnajman@math.hr

Received on 4.6.2011
and in revised form on 16.8.2011 (6716)