LMS J. Comput. Math. 17 (1) (2014) 509–535
doi:10.1112/S1461157014000072

Computation on elliptic curves with complex multiplication

Pete L. Clark, Patrick Corn, Alex Rice and James Stankewicz

Abstract

We give the complete list of possible torsion subgroups of elliptic curves with complex multiplication over number fields of degree 1–13. Additionally we describe the algorithm used to compute these torsion subgroups and its implementation.

1. *Introduction*

1.1. *The main results*

The goal of this paper is to present a complete list of possible torsion subgroups of elliptic curves with complex multiplication over number fields of small degree. Our main tool is an algorithm whose input is a positive integer d. The output is a (necessarily finite) list of isomorphism classes of finite abelian groups G such that G is isomorphic to $E(K)[\mathrm{tors}]$ for some number field K of degree d and some elliptic curve E defined over K with complex multiplication.

Our algorithm requires a complete list of imaginary quadratic fields of class number h for all integers h which properly divide d. Fortunately, Watkins [**26**] has enumerated all imaginary quadratic fields with class number $h \leqslant 100$, which would in theory allow us to run our algorithm for all $d \leqslant 201$ (and for infinitely many other values of d, for instance all prime values).

We implemented our algorithm using the MAGMA programming language [**2**] and ran it on Unix servers in the University of Georgia Department of Mathematics. The result, after doing some additional analysis, is a complete list of torsion subgroups for degree d with $1 \leqslant d \leqslant 13$. This list, for each degree d, is described in § 4. Note in particular the relative scarcity when d is prime. This phenomenon will be explored in a further paper.

For $d = 1$ these computations were first done by Olson in 1974 [**17**], whereas for $d = 2$ and 3 they are a special case of work of Zimmer and his collaborators over a ten year period from the late 1980s to the late 1990s [**5**, **16**, **19**]. We believe that our results are new for $4 \leqslant d \leqslant 13$.

1.2. *Connections to prior work*

According to the celebrated *uniform boundedness theorem* of Merel [**14**], for any fixed $d \in \mathbf{Z}_{>0}$, the supremum of the size of all rational torsion subgroups of all elliptic curves defined over all number fields of degree d is finite.

In 1977, Mazur proved uniform boundedness for $d = 1$ (that is, for elliptic curves $E_{/\mathbf{Q}}$) [**13**]. Moreover, Mazur gave a complete classification of the possible torsion subgroups:

$$E(\mathbf{Q})[\mathrm{tors}] \in \begin{cases} \mathbf{Z}/m\mathbf{Z} & \text{for } m = 1, \ldots, 10, 12, \\ \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/2m\mathbf{Z} & \text{for } m = 1, \ldots, 4. \end{cases}$$

Received 23 July 2013; revised 14 March 2014.

2010 Mathematics Subject Classification 11-04, 11G05, 11G15, 14H52 (primary).

Alex Rice and James Stankewicz were partially supported by NSF VIGRE grant DMS-0738586 during this work. James Stankewicz was also partially supported by the Van Vleck fund at Wesleyan University and the Villum Fonden through the network for Experimental Mathematics in Number Theory, Operator Algebras and Topology.

Work of Kamienny [8, 9] and of Kenku and Momose [10] gives the following result when K is a quadratic number field:

$$E(K)[\text{tors}] \in \begin{cases} \mathbf{Z}/m\mathbf{Z} & \text{for } m = 1, \dots, 16, 18, \\ \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/2m\mathbf{Z} & \text{for } m = 1, \dots, 6, \\ \mathbf{Z}/3\mathbf{Z} \oplus \mathbf{Z}/m\mathbf{Z} & \text{for } m = 3, 6, \\ \text{and} & \mathbf{Z}/4\mathbf{Z} \oplus \mathbf{Z}/4\mathbf{Z}. \end{cases}$$

This and similar subsequent enumeration results over varying number fields are to be understood in the following sense. First, for any quadratic field K and any elliptic curve $E_{/K}$, the torsion subgroup of $E(K)$ is isomorphic to one of the groups listed. Second, for each of the groups G listed, there exists at least one quadratic field K and an elliptic curve $E_{/K}$ with $E(K)[\text{tors}] \cong G$. A complete classification of torsion subgroups of elliptic curves over cubic fields is not yet known.

Further results come from focusing on particular classes of elliptic curves. Notably H. Zimmer and his collaborators have done extensive computations on torsion in elliptic curves with j-invariant in the ring of algebraic integers. In [16], Müller, Stroher and Zimmer proved that in the case of integral j-invariant, if K is a quadratic number field then

$$E(K)[\text{tors}] \in \begin{cases} \mathbf{Z}/m\mathbf{Z} & \text{for } m = 1, \dots, 8, 10, \\ \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/m\mathbf{Z} & \text{for } m = 2, 4, 6, \\ \text{and} & \mathbf{Z}/3\mathbf{Z} \oplus \mathbf{Z}/3\mathbf{Z}. \end{cases}$$

In [19] Pethö, Weis and Zimmer showed that if E has integral j-invariant and K is a cubic number field then

$$E(K)[\text{tors}] \in \begin{cases} \mathbf{Z}/m\mathbf{Z} & \text{for } m = 1, \dots, 10, 14, \\ \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/m\mathbf{Z} & \text{for } m = 2, 4, 6. \end{cases}$$

Here we study elliptic curves with complex multiplication (CM). Such curves form a subclass of curves with integral j-invariant [24, Theorem. II.6.4], so our results are subsumed by the above results for $d \leqslant 3$; but, as we will see, the CM hypothesis allows us to extend our computations to higher values of d, up to $d = 13$.

2. *Background*

2.1. *Kubert–Tate normal form*

The fundamental result on which our algorithm rests is the following elementary theorem, which gives a parameterization of all elliptic curves with an N-torsion point for $N \geqslant 4$.

THEOREM 2.1 (Kubert). *Let E be an elliptic curve over a field K and $P \in E(K)$ a point of order at least 4. Then E has an equation of the form*

$$y^2 + (1 - c)xy - by = x^3 - bx^2 \tag{1}$$

for some $b, c \in K$, and $P = (0, 0)$.

Proof. This first appeared in [11]. See for instance [16, § 3]. □

https://doi.org/10.1112/S1461157014000072 Published online by Cambridge University Press

We will call the equation (1) the *Kubert–Tate normal form* of E, and our notation for a curve in Kubert–Tate normal form with parameters b, c as above will be simply $E(b, c)$. The j-invariant of this elliptic curve is

$$j(b,c) = \frac{(16b^2 + 8b(1-c)(c+2) + (1-c)^4)^3}{b^3(16b^2 - b(8c^2+20c-1) - c(1-c)^3)}. \tag{2}$$

REMARK 1. This form is unique for a given curve with a fixed point of order at least 4. In practice we use this to find elliptic curves with some primitive N-torsion point, so an elliptic curve E may have many isomorphic Kubert–Tate normal forms, depending on which torsion point we choose to send to $(0, 0)$.

EXAMPLE 1. Here are some small multiples of the point $(0, 0)$ on $E(b, c)$:

$$[2](0,0) = (b, bc),$$

$$[3](0,0) = (c, b-c),$$

$$[4](0,0) = \left(\frac{b(b-c)}{c^2}, \frac{b^2(c^2+c-b)}{c^3}\right),$$

$$[5](0,0) = \left(\frac{bc(c^2+c-b)}{(b-c)^2}, \frac{bc^2(b^2-bc-c^3)}{(b-c)^3}\right),$$

$$[6](0,0) = \left(\frac{(b-c)(b^2-bc-c^3)}{A^2}, \frac{c(b-c)^2(2b^2-bc(c-3)+c^2)}{A^3}\right),$$

$$[7](0,0) = \left(\frac{Abc((b-c)^2+Ab)}{(b^2-bc-c^3)^2}, \frac{(Ab)^2((b-c)^3+c^3A)}{(b^2-bc-c^3)^3}\right),$$

where $A = b - c - c^2$. In particular we see that for $N \leqslant 3$, $(0, 0)$ cannot be an N-torsion point on $E(b, c)$.

2.2. *Modular curves*

The affine modular curve $Y_1(N)$ for $N \geqslant 4$ is a fine moduli space for pairs (E, P) where E is an elliptic curve and P is a point of exact order N on E. We will search for CM-points on $Y_1(N)$ for various values of $N \geqslant 4$; that is, points over various number fields which correspond to CM elliptic curves with an N-torsion point(the $Y_1(N)$ for $1 \leqslant N \leqslant 3$ are coarse moduli spaces and so will only give us the information we desire over an algebraically closed field). Kubert curves give a down-to-earth way of constructing a defining equation for $Y_1(N)$.

DEFINITION 2.2. Let $\mathbf{Q}(b, c)$ be a rational function field, and let $E_{/\mathbf{Q}(b,c)}$ denote the elliptic curve given by equation (1). If $N \geqslant 3$ is an integer, let $n_1, d_1, n_2, d_2 \in \mathbf{Q}[b, c]$ be such that $(n_i, d_i) = 1$, d_i is monic, and

$$x\left(\left[\left\lceil\frac{N}{2}\right\rceil - 1\right](0,0)\right) = \frac{n_1(b,c)}{d_1(b,c)}, \qquad x\left(\left[\left\lfloor\frac{N}{2}\right\rfloor + 1\right](0,0)\right) = \frac{n_2(b,c)}{d_2(b,c)}.$$

Then we let $f_N(b, c) = n_1d_2 - n_2d_1 \in \mathbf{Q}[b, c]$.

LEMMA 2.3. *Let k be a field, let $Y_{/k}$ be an integral algebraic variety, let $q : A \to Y$ be a relative abelian variety, and let y be a closed point of Y. Then the specialization map $\mathfrak{s} : A(K(Y)) \to A_y(k(y))$ is a group homomorphism.*

https://doi.org/10.1112/S1461157014000072 Published online by Cambridge University Press

Proof. This result appears in [**12**, p. 40]. Lang's (wonderful) text is rather informally written: many results, including this one, are given there without proof or reference. For the convenience of the reader we give a proof. It suffices to show this when $k = \overline{k}$, which we assume hereon.

Step 1. Suppose Y is a nonsingular curve. Then $A_{/Y}$ is equal to the *Néron model* of its generic fiber, so the map $\mathfrak{s}$ is a homomorphism by [**1**, Proposition I.2.8].

Step 2. Suppose Y is a singular curve. Let $\pi : \tilde{Y} \to Y$ be its normalization, and let $\tilde{y}$ be a closed point of $\tilde{Y}$ with $\pi(\tilde{y}) = y$. Let $\tilde{A} = \pi^*(q) \to \tilde{Y}$ be the pullback of the family to $\tilde{Y}$. Then the fiber of $\tilde{A}$ over $\tilde{y}$ is canonically identified with the fiber of A over y, and thus the specialization map $\tilde{s} : \tilde{A}(K(\tilde{Y})) \to A_{\tilde{y}}(k(\tilde{y}))$ is canonically identified with $\mathfrak{s}$. We have reduced to Step 1.

Step 3. In the general case we choose a chain of closed irreducible subvarieties $Y_0 = \{y\} \subset Y_1 \subset \ldots \subset Y_d = Y$ containing y, with $\dim Y_i = i$. We apply Step 2 repeatedly, specializing from the generic point of Y_i to the generic point of Y_{i-1}. □

LEMMA 2.4. *If $b_0, c_0 \in \overline{\mathbf{Q}}$ and $E(b_0, c_0)$ is an elliptic curve given by equation (1) then the point $(0,0)$ on $E(b_0, c_0)$ is an N-torsion point if and only if $f_N(b_0, c_0) = 0$.*

Proof. By Example 1 we must have $N \geqslant 4$.
Step 1. Suppose $[N](0,0) = O$. We claim that $[\lceil N/2 \rceil - 1](0,0)$ and $[\lfloor N/2 \rfloor + 1](0,0)$ are finite and have equal x-coordinates. Indeed, if $[\lceil N/2 \rceil - 1](0,0) = O$, then $(0,0)$ is $(2 - 2\lceil N/2 \rceil + N)$-torsion, that is, 2-torsion if N is even and 1-torsion if N is odd, contradicting Example 1. A similar argument shows that $[\lfloor N/2 \rfloor + 1](0,0)$ is finite. Moreover, we have

$$\left[\left\lceil \frac{N}{2} \right\rceil - 1\right](0,0) + \left[\left\lfloor \frac{N}{2} \right\rfloor + 1\right](0,0) = \left[\left\lceil \frac{N}{2} \right\rceil + \left\lfloor \frac{N}{2} \right\rfloor\right](0,0) = [N](0,0) = O,$$

so $[\lceil N/2 \rceil - 1](0,0)) = -[\lfloor N/2 \rfloor + 1](0,0)$. As for any points P, Q on a Weierstrass elliptic curve, $P = \pm Q$ if and only if $x(P) = x(Q)$, this establishes the claim. Now, since $x([\lceil N/2 \rceil - 1](0,0)) = x([\lfloor N/2 \rfloor + 1](0,0)) \in \overline{\mathbf{Q}}$, if $d_1(b_0, c_0) = 0$ then also $n_1(b_0, c_0) = 0$ hence $f_N(b_0, c_0) = n_1(b_0, c_0)d_2(b_0, c_0) - n_2(b_0, c_0)d_2(b_0, c_0) = 0$. Similarly if $d_2(b_0, c_0) = 0$. Finally, if $d_1(b_0, c_0)d_2(b_0, c_0) \neq 0$, then

$$x\left(\left[\left\lceil \frac{N}{2} \right\rceil - 1\right](0,0)\right) = \frac{n_1(b_0, c_0)}{d_1(b_0, c_0)} = \frac{n_2(b_0, c_0)}{d_2(b_0, c_0)} = x\left(\left[\left\lfloor \frac{N}{2} \right\rfloor + 1\right](0,0)\right),$$

so $f_N(b_0, c_0) = 0$.

Step 2. Suppose that $f_N(b_0, c_0) = 0$. Thus there must be at least one irreducible factor $g(b, c)$ of $f_N(b, c)$ such that $g(b_0, c_0) = 0$. Then $Z = \mathbf{Q}[b, c]/\langle g(b, c) \rangle$ is an irreducible curve, and let Y be obtained from Z by removing the finite set of closed points on which the Kubert curve $E(b_0, c_0)$ becomes singular. Then $E(b, c)$ gives a relative elliptic curve over Y, and the elliptic curve $E(b_0, c_0)$ is its specialization at the closed point (b_0, c_0). By construction, $[N](0,0) = O$ on the generic fiber of Y, so by Lemma 2.3, $[N](0,0) = O$ on $E(b_0, c_0)$. □

EXAMPLE 2. We will make use of the explicit formulas of Example 1.
(a) Let $N = 4$. Setting $x((0,0)) = x([3](0,0))$ gives $f_4(b, c) = c$.
(b) Let $N = 5$. The condition that $(0,0)$ is a 5-torsion point is $b - c = 0$. Setting $x([2](0,0)) = x([3](0,0))$ gives $f_5(b, c) = b - c$.
(c) Let $N = 7$. The condition that $(0,0)$ is a 7-torsion point is $b^2 - bc - c^3 = 0$. Setting $x([3](0,0)) = x([4](0,0))$ gives $f_7(b, c) = b(b - c) - c(c^2)$.

https://doi.org/10.1112/S1461157014000072 Published online by Cambridge University Press

As Examples 1 and 2 illustrate, the complexity of the rational functions giving the coordinates of $[N](0,0)$ increases rapidly with N. Our trick of computing $[\lceil N/2\rceil - 1](0,0)$ and $[\lfloor N/2\rfloor + 1](0,0)$ instead becomes a critical one to extend the range of our calculations.

In general, $f_N(b,c) = 0$ is not the defining equation for $Y_1(N)$ as $[N]P = 0$ implies only that P has order d for some $d \mid N$. The polynomial $f_N(b,c)$ will have as irreducible factors defining equations for $Y_1(d)$ for $d \mid N$, $d > 3$. However a simple Möbius inversion will furnish such an equation. Although we do not explicitly write down equations for $Y_1(N)$ in our algorithm, one could do so with relative ease. A more sophisticated version of this computation has been undertaken by Sutherland [**25**].

EXAMPLE 3. We computed $4(0,0)$ and $2(0,0)$ as part of our above examples, so $f_6(b,c) = b^2 - bc - bc^2$. The divisors of 6 are $1, 2, 3$ and 6. Thus by Möbius inversion, the equation for $Y_1(6)$ in the (b,c)-plane is $b - c - c^2$, a smooth plane curve. For higher N, $Y_1(N)$ is not naturally a plane curve (for example, the genus of $Y_1(N)$ will usually not be of the form $(d-1)(d-2)/2$) and so there will often be singularities in this plane model.

We note in general that if $d \geqslant 3$ and $d \mid N$ then $f_d \mid f_N$. This is easy to see using the group law when $d \geqslant 4$. For $d = 3$ we can see this by computing on the elliptic curve $E(b,c)$ over the function field $\mathbf{Q}(b,c)$. Namely, if (x,y) is any non-identity point it is possible to compute that $[3](x,y) \pm (0,0)$ has x-coordinate with b-adic valuation 1. Therefore b but not b^2 divides $f_N(b,c)$ when $3 \mid N$. Therefore performing a Möbius inversion on the f_N furnishes a factorization $f_N = \prod_{\substack{d \mid N \\ d \geqslant 3}} \phi_d$ where if $N \geqslant 4$ then $\phi_N(b,c)$ is a defining equation for $Y_1(N)$ in the (b,c)-plane.

2.3. *Complex multiplication and bounds on j-invariants*

If $E(b,c)$ is a CM elliptic curve defined over a number field of degree d, then its j-invariant $j(b,c)$ must lie in a number field of degree dividing d. The degree of $\mathbf{Q}(j(b,c))$ is equal to the class number of End E, which is an order in an imaginary quadratic field.

THEOREM 2.5 (Heilbronn [**7**]). *For any positive integer d, there are only finitely many imaginary quadratic fields with class number d.*

COROLLARY 2.6. *For any positive integer d, there are only finitely many imaginary quadratic orders $\mathcal{O}$ such that the class number $h(\mathcal{O})$ satisfies $h(\mathcal{O}) \leqslant d$.*

Proof. Since every quadratic order $\mathcal{O}$ must be of the form $\mathbf{Z} + f\mathcal{O}_K$, this follows from Gauss's class number formula [**4**, Theorem 7.24]. □

EXAMPLE 4. We find the least possible degrees for an elliptic curve over a number field K with 7-torsion and j-invariant 0. If we have such a curve E, we can find a pair $(b,c) \in K^2$ such that $E \cong E(b,c)$. Since $j(b,c) = 0$, we have

$$16b^2 + 8b(1-c)(c+2) + (1-c)^4 = 0, \tag{3}$$

and since $(0,0)$ is a nontrivial 7-torsion point, we have

$$b^2 - bc - c^3 = 0. \tag{4}$$

The real solutions to equation (3) in the (b,c) affine plane may be seen in Figure 1, and equation (4) in Figure 2.

https://doi.org/10.1112/S1461157014000072 Published online by Cambridge University Press

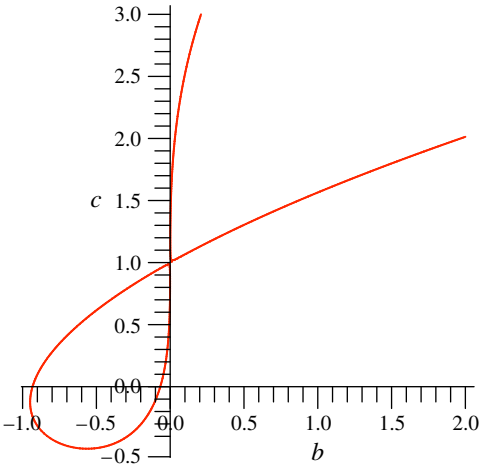

FIGURE 1. *The real* (b, c) *such that* $E(b, c)$ *has* j*-invariant* 0.

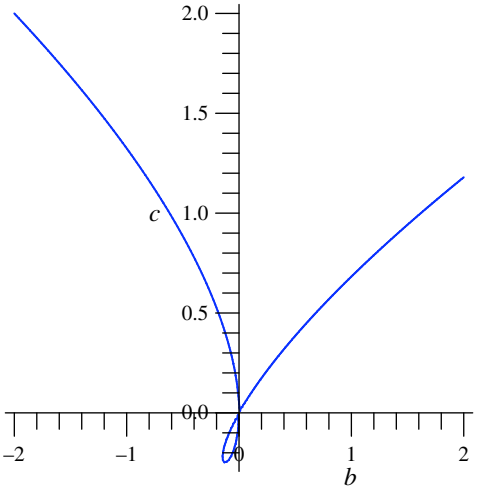

FIGURE 2. *The real* (b, c) *such that* $(0, 0)$ *is a* 7*-torsion point on* $E(b, c)$.

The resultant of these two polynomials with respect to c is

$$(b^2 + b + 1)(b^6 - 325b^5 + 5518b^4 + 3655b^3 + 718b^2 + 51b + 1).$$

The roots of this *Kubert resultant* identify the intersection points of our two affine curves, as shown in Figure 3. We should note here that the first irreducible factor has no real roots. Instead, the b-coordinates of the intersection points we see are four of the six real roots of the second factor. In any case, looking at the first irreducible factor over $\mathbf{Q}$, we see that we can take $b = \zeta_3$.

We plug in ζ_3 for b in the above polynomials and compute the greatest common divisor, which is $c+1$. So the elliptic curve $E(\zeta_3, -1)$ has a 7-torsion point over $\mathbf{Q}(\zeta_3)$. That is, on the curve

$$y^2 + 2xy - \zeta_3 y = x^3 - \zeta_3 x^2,$$

https://doi.org/10.1112/S1461157014000072 Published online by Cambridge University Press

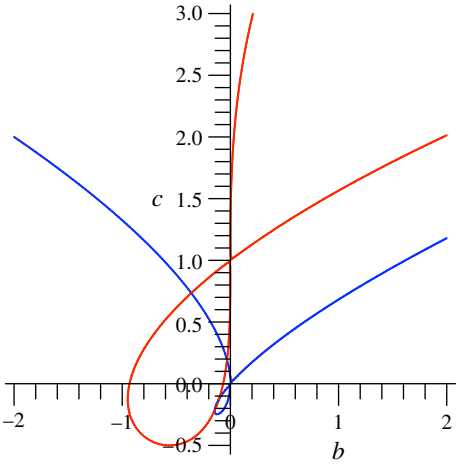

FIGURE 3. *The real* (b, c) *such that* $(0, 0)$ *is a* 7*-torsion point on* $E(b, c)$ *with* j*-invariant* 0.

the point $(0, 0)$ is a 7-torsion point[†]. Moreover, this curve acquires full 7-torsion over the degree-12 cyclotomic field $\mathbf{Q}(\zeta_{21})$.

We generalize the above construction as follows: writing $j(b, c) = n_j(b, c)/d_j(b, c)$ as the quotient of two polynomials, we see that there is an elliptic curve $E(b, c)$ with j-invariant j_0 and $[N](0, 0) = O$ if and only if (b, c) satisfy the equations

$$\begin{aligned} n_j(b, c) &= j_0 d_j(b, c), \\ f_N(b, c) &= 0. \end{aligned} \tag{5}$$

If there are only finitely many pairs (j_0, N) that we have to check, then since the resultant of these equations with respect to c is a one-variable polynomial in b, there are only finitely many elliptic curves $E(b, c)$ over a small-degree number field with j-invariant j_0 and with $(0, 0)$ an N-torsion point. To determine if $\mathbf{Z}/n\mathbf{Z} \oplus \mathbf{Z}/N\mathbf{Z}$ with $n \mid N$ is a torsion subgroup of an elliptic curve over a small-degree number field, we need only check the nth *division polynomial* [**23**, Exercise 3.7] to see if $E(b, c)$ acquires an additional n-torsion point over a small-degree number field. There are finitely many $n \mid N$ and for each such n, there are algorithms to compute the nth division polynomial.

In this way, we see how a rough algorithm for enumerating torsion subgroups of CM elliptic curves presents itself. Fix a degree d, so that we aim to tabulate CM torsion subgroups over number fields of degree d. By Heilbronn's theorem, there are only finitely many j-invariants of elliptic curves with CM over all number fields of degree at most d. By Merel's bound, we have only finitely many possible torsion subgroups to check. Since there are only finitely many j_0 and N, the procedure described above terminates for each d.

We note here that Merel's bound is quite large and often impractical. We mention it only to note that the above procedure terminates for any finite number of j-invariants, CM or not. In the CM case, we have much better bounds to consider.

2.4. *Possible torsion of CM elliptic curves*

Let E be an elliptic curve over a number field F with CM. If $E(F)$ contains an N-torsion point, then the size of N is severely restricted by the degree of F; the following

[†]The reader who prefers standard Weierstrass models may verify that the origin corresponds to the 7-torsion point $(12(1 - \zeta_3), -108\zeta_3)$ on the isomorphic elliptic curve $y^2 = x^3 - (1296\zeta_3 + 6480)$.

https://doi.org/10.1112/S1461157014000072 Published online by Cambridge University Press

theorems of Silverberg [22] and Prasad–Yogananda [20] can be used to give an explicit upper bound on N.

THEOREM 2.7 (Silverberg, Prasad–Yogananda). *Let E be an elliptic curve over a number field F of degree d, and suppose that E has CM by the order $\mathcal{O}$ in the imaginary quadratic field K. Let $w(\mathcal{O}) = \#\mathcal{O}^\times$ and e be the exponent of the torsion subgroup of $E(F)$. Then:*
(a) $\varphi(e) \leqslant w(\mathcal{O})d$;
(b) *if $K \subseteq F$, then* $\varphi(e) \leqslant w(\mathcal{O})d/2$;
(c) *if $K \nsubseteq F$, then* $\varphi(\#E(F)[\mathrm{tors}]) \leqslant w(\mathcal{O})d$.

Proof. See [20, 22]. It can be deduced from Silverberg's work that all above occurrences of $w(\mathcal{O})$ may be replaced with $w(\mathcal{O})/h(\mathcal{O})$. □

We will refer henceforth to the bounds obtained from the above theorem and proof as the *SPY bounds*. Using merely the bound of part (a) and the well-known inequality $\sqrt{N} \leqslant \phi(N)$ for $N \geqslant 7$, we see that we need only consider values of N that are at most $w(\mathcal{O})^2 d^2$. The SPY bounds also lead us to expect that the largest torsion subgroups occur when $w(\mathcal{O})$ is largest, namely when $j = 0, 1728$.

Any bound on the exponent above gives a bound on the size of the torsion subgroup. If the exponent of $E(F)[\mathrm{tors}]$ is at most N, since $E(\mathbf{C})[\mathrm{tors}] \cong (\mathbf{Q}/\mathbf{Z})^2$ [23, Corollary V.1.1], we have $\#E(F)[\mathrm{tors}] \leqslant N^2$. In fact, there exist integers $n \mid N$ such that $E(F)[\mathrm{tors}] \cong \mathbf{Z}/n\mathbf{Z} \oplus \mathbf{Z}/N\mathbf{Z}$. Moreover in that case, the Weil Pairing [23, § III.8] shows that $F \supset \mathbf{Q}(\zeta_n)$ and thus $\varphi(n) \mid [F : \mathbf{Q}] = d$.

In the case that E has CM by $\mathcal{O}$, note that $j(E) \in F$ so that $\mathbf{Q}(j(E)) \subset F$ and thus $h(\mathcal{O}) \mid [F : \mathbf{Q}] = d$. Therefore, let $\deg = d/h(\mathcal{O})$. The strengthening of the SPY bounds as noted in the proof of Theorem 2.7 implies that if e is the exponent of $E(F)[\mathrm{tors}]$ then $\varphi(e) \leqslant w(\mathcal{O}) \deg$. Note also that if deg is odd, $K \not\subset F$ since K and $\mathbf{Q}(j(E))$ are linearly disjoint.

If $\deg = 2$ then we may assume that $j \neq 0, 1728$ because the possible groups in that case have already been determined [16]. Thus $w(\mathcal{O}) = 2$, hence either $E(F)[\mathrm{tors}]$ is among the 12 possible torsion subgroups G such that $\varphi(\#G) \leqslant 4$ or F is the compositum of $\mathbf{Q}(j(E))$ with K, otherwise known as $H(\mathcal{O})$, the ring class field of $\mathcal{O}$. In the latter case, we have the following theorem.

THEOREM 2.8 (Parish). *Let $\mathcal{O}$ be an imaginary quadratic order, j the j-invariant of an elliptic curve with CM by $\mathcal{O}$, $L = \mathbf{Q}(j)$. Then if E is an elliptic curve defined over H with CM by $\mathcal{O}$ then $E(H(\mathcal{O}))[\mathrm{tors}]$ contains only points of order $1, 2, 3, 4$, or 6. Moreover, if E is defined over L then $E(L)[\mathrm{tors}]$ can only be isomorphic to one of $0, \mathbf{Z}/2\mathbf{Z}, \mathbf{Z}/3\mathbf{Z}, \mathbf{Z}/4\mathbf{Z}, \mathbf{Z}/6\mathbf{Z}$, or $\mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/2\mathbf{Z}$.*

Proof. See [18, § VI]. □

Much finer information is available in Parish's paper. Except for $j = 0$ and $\mathbf{Z}/3\mathbf{Z} \oplus \mathbf{Z}/3\mathbf{Z}$ or $\mathbf{Z}/7\mathbf{Z}$, each torsion subgroup G which is possible over $H(\mathcal{O})$ has $\varphi(\#G) \leqslant 4$. Note that as a further consequence, if E is an elliptic curve with CM by $\mathcal{O}$ over a number field F and $[F : \mathbf{Q}] = h(\mathcal{O})$, then the only possible torsion subgroups are those found in degree 1. By the Weil pairing, if $E(F)[\mathrm{tors}] \cong \mathbf{Z}/n\mathbf{Z} \oplus \mathbf{Z}/N\mathbf{Z}$ with $n \mid N$ then $\varphi(n) \mid d$. In most cases though, $\varphi(n) \mid \deg$. We can however determine exactly the intersection of $\mathbf{Q}(\zeta_n)$ with $\mathbf{Q}(j(\mathcal{O}))$ and thus get closer to the ideal that $\varphi(n) \mid \deg$.

Let H denote the ring class field of $\mathcal{O}$ and G the maximal abelian sub-extension of H over $\mathbf{Q}$, which is necessarily multiquadratic [4, § 6]. Hence G', the intersection of $\mathbf{Q}(j(\mathcal{O}))$ with G,

https://doi.org/10.1112/S1461157014000072 Published online by Cambridge University Press

must also be multiquadratic. Since any abelian extension must be contained in some $\mathbf{Q}(\zeta_m)$ [4, Theorem 8.8], the intersection of $\mathbf{Q}(\zeta_n)$ with $\mathbf{Q}(j(\mathcal{O}))$ must be contained in G'. This G' may be numerically determined via discriminants, but it is not computationally difficult to simply list the discriminants of the quadratic subfields of $\mathbf{Q}(j(\mathcal{O}))$, which are all necessarily real. If Δ is a discriminant of a real quadratic field K, then $K \subset \mathbf{Q}(\zeta_n)$ if and only if $\Delta \mid n$ [15, Example V.3.11]. Finally, if M is a multiquadratic field extension of degree 2^m, then the number of quadratic sub-extensions is $2^m - 1$.

FUNCTION 2.9 (CyclotomicIntersectionDegree). Let $\mathcal{O}$ be an imaginary quadratic order and n a positive integer.

(1) Let $L = \{\mathrm{disc}(K) : [K : \mathbf{Q}] = 2, K \subset \mathbf{Q}(j(\mathcal{O}))\}$, the discriminants of the quadratic subfields of the multiquadratic field G' above.
(2) Let $M = \{D : D \in L, D \mid n\}$, the discriminants of the quadratic subfields of $G' \cap \mathbf{Q}(\zeta_n)$.
(3) Return $\#\ M + 1$.

These steps restrict the groups which could possibly occur as torsion subgroups of an elliptic curve with CM by $\mathcal{O}$. We combine these steps into a function, which takes as input an imaginary quadratic order $\mathcal{O}$, a degree d, and a list of integers N which could be the exponent of a torsion subgroup of an elliptic curve E over a number field F with CM by $\mathcal{O}$. The output of this function is a list of finite abelian groups G such that $E(F)[\mathrm{tors}] \cong G$ for an elliptic curve E with CM by $\mathcal{O}$.

FUNCTION 2.10 (PossibleGroups). Let $d \in \mathbf{Z}_{>1}$, $\mathcal{O}$ an imaginary quadratic order such that $h(\mathcal{O}) \mid d$, and L a list of positive integers N.

(1) Set $L' = \{\mathbf{Z}/n\mathbf{Z} \oplus \mathbf{Z}/N\mathbf{Z} : N \in L, n \mid N\}$, $h = h(\mathcal{O})$, and $\deg = d/h$.
(2) If $\deg = 1$ then remove $\mathbf{Z}/n\mathbf{Z} \oplus \mathbf{Z}/N\mathbf{Z}$ from L' unless $n = N = 2$ or $n = 1$ and $N \in \{1, 2, 3, 4, 6\}$.
(3) If $\deg = 2$ then remove $\mathbf{Z}/n\mathbf{Z} \oplus \mathbf{Z}/N\mathbf{Z}$ from L' unless either ($\mathcal{O} \cong \mathbf{Z}[\zeta_3]$ and $(N, n) = (3, 3)$) or $\varphi(Nn) \leqslant 4$.
(4) If $\deg > 1$ is odd then remove $\mathbf{Z}/n\mathbf{Z} \oplus \mathbf{Z}/N\mathbf{Z}$ from L' unless $\varphi(Nn) \leqslant w(\mathcal{O}) \deg$ and $\varphi(n) \mid d$.
(5) If $\deg > 2$ is even then remove $\mathbf{Z}/n\mathbf{Z} \oplus \mathbf{Z}/N\mathbf{Z}$ from L' unless $\varphi(n) \mid \deg \times$CyclotomicIntersectionDegree$(\mathcal{O}, n)$ (Function 2.9).
(6) Return L'.

In Function 2.10, one gets the best results when the list L is made up of integers N which can be an order of a torsion point on an elliptic curve E with CM by $\mathcal{O}$. Necessarily then, $\varphi(N) \leqslant w(\mathcal{O})d/h(\mathcal{O}) = w(\mathcal{O}) \deg$ by the SPY bounds. We also have another tool for ruling out possible orders of torsion.

THEOREM 2.11. *Let $\mathcal{O}$ be an imaginary quadratic order of discriminant D and let D_0 be the discriminant of the field $K = \mathbf{Q}(\sqrt{D})$, so that $D = f^2 D_0$. If $p \nmid D$ is an odd prime then let $(\cdot/p)$ denote the Legendre symbol at p. If E is an elliptic curve over a number field of degree d with CM by $\mathcal{O}$ with a point of order p then we have the following:*

(a) *if $(D/p) = 1$ then $(p-1)h(\mathcal{O}_K) \mid 2dw(\mathcal{O}_K)$;*
(b) *if $(D/p) = -1$ then $(p^2-1)h(\mathcal{O}_K) \mid 2dw(\mathcal{O}_K)$.*

Proof. This was directly proven for $D = D_0$ [3, Theorem 2], and can be extended to the case $p \nmid D$ [3, Proposition 25]. □

In this way, we can additionally remove large primes from the divisors of possible exponents. Starting from a list of integers up to $w(\mathcal{O}) \deg$, we can then very quickly sieve out impossible

https://doi.org/10.1112/S1461157014000072 Published online by Cambridge University Press

torsion exponents. For $j = 0$, performing the above procedure takes one hundredth of one second to find

$$[2, 3, 4, 5, 6, 7, 8, 9, 10, 12, 13, 14, 15, 16, 18, 20, 21, 24, 26, 28, 30, 36, 42]$$

as a list of possible torsion exponents over a number field of degree 2.

FUNCTION 2.12 (PossibleExponents). Let $\mathcal{O}$ be an imaginary quadratic order and let deg be a positive integer.

(1) Let L be the list of positive integers N such that $\varphi(N) \leqslant w(\mathcal{O}) \deg$.
(2) Let L' be the set of integers $N \in L$ such that if $p \mid N$ is prime then p satisfies the divisibility relations in Theorem 2.11 for $d = h(\mathcal{O}) \deg$.
(3) Return L'.

Note however that this list is still far too large to use in Function 2.10. We apply a sieve to this list, using resultants as in Example 4, where we showed that 7-torsion occurred over a number field of degree 2 for $j = 0$. We note especially that the *Kubert degree sequence* for $j = 0$ and $N = 7$, or the sequence of degrees of irreducible factors of the resultant, is $[2, 6]$. On the other hand, the degree sequence for $j = 0$ and $N = 14$ is $[6, 18]$. Therefore we may eliminate $14, 28$, and 42 from our list of possible torsion exponents because 14-torsion is not possible for $j = 0$ over a number field of degree not divisible by 6. Computing this degree sequence takes 0.03 seconds[†]. If we recursively perform this sieve, it takes 0.24 seconds to find that the torsion exponents which occur for $j = 0$ over a number field of degree 2 are

$$[2, 3, 4, 6, 7].$$

This may seem like a relatively short amount of time to be worried about, but for $j = 0$ and a number field of degree 6 it takes about a minute to find $[2, 3, 4, 6, 7, 9, 14, 19]$ as the list of torsion exponents. For degree 12 it takes over an hour. We describe this process, along with the adjustment we have to make for $\mathcal{O}$ with larger class numbers, in the following function.

FUNCTION 2.13 (SievedTorsion). Let $\mathcal{O}$ be an imaginary quadratic order and let deg be a positive integer.

(1) Let $L =$ PossibleExponents$(\mathcal{O}, \deg)$ (Function 2.12).
(2) For $N \in$ PossibleExponents$(\mathcal{O}, \deg)$ such that $N \in L$ and $N \geqslant 4$:
    (i) let $DegSeq$ be the sequence of integers $Degree(f)h(\mathcal{O})$ where f is an irreducible factor of the resultant corresponding to N-torsion on elliptic curves with CM by $\mathcal{O}$;
    (ii) unless $m \mid h(\mathcal{O}) \deg$ for some $m \in DegSeq$, remove all multiples of N from L.
(3) Return L.

We structure our computation this way to minimize the number of times that we need to compute multivariate resultants. While straightforward and much quicker than computing torsion subgroups of elliptic curves, the computation of multivariate resultants is NP-Hard [**6**]. The memory demands for computing resultants over large degree number fields can also be quite substantial. All told, the longest computation of torsion subgroups occurred in degree 12. Computing the lists of possible torsion subgroups of CM elliptic curves over a number field of degree 12 for each possible quadratic order $\mathcal{O}$ using the above procedure took over 10 hours.

[†]This was computed on a very powerful machine, with four 6-core Xeon processors and 128 GB of memory. These timings are meant to highlight the relative speed of small computations.

https://doi.org/10.1112/S1461157014000072 Published online by Cambridge University Press

3. *Ruling out torsion subgroups of elliptic curves*

Suppose we are given a finite group $G \cong \mathbf{Z}/n\mathbf{Z} \oplus \mathbf{Z}/N\mathbf{Z}$ and we want to test whether it could be a torsion subgroup of an elliptic curve E over a number field F of degree dividing d with CM by an imaginary quadratic order $\mathcal{O}$. If there is such an elliptic curve such that $E(F)[\text{tors}] \cong G$, then we can find $b, c \in F$ such that $E \cong E(b, c)$, where the point $(0, 0)$ is a point of order N. Conversely if we have $b, c \in F$ such that $E(b, c)$ has CM by $\mathcal{O}$ and $(0, 0)$ is a point of order N, it is not necessarily the case that $E(b, c)(F)[\text{tors}] \cong G$. The first and easiest way for this to fail is if $E(b, c)(F)[\text{tors}] \supsetneq G$.

Example 5. The resultant whose roots are the b such that $(0, 0)$ is a 5-torsion point on $E(b, c)$ with CM by $\mathbf{Z}[\zeta_4]$ is

$$(x^2 + 1)^2(x^4 - 18x^3 + 74x^2 + 18x + 1)^2.$$

However, any elliptic curve over a field F of characteristic zero with CM by $\mathbf{Z}[\zeta_4]$ has a Weierstrass equation of the form $y^2 = x^3 + Dx$ [**23**, §X.6] and thus a rational point of order 2. Therefore if we search for $\mathbf{Z}/5\mathbf{Z}$ as a torsion subgroup over a degree 2 field, we find $\mathbf{Z}/10\mathbf{Z}$ as the torsion subgroup of $E(\zeta_4, \zeta_4)$.

It of course may also happen that $G \subsetneq E(F)[\text{tors}]$ and that they have the same exponent. The more typical situation is that $E(F)[\text{tors}] \subset G$. In that case, we have to check to see if there is an extension field L of F of degree still dividing d such that $E(L)[\text{tors}] \cong G$.

To rule this out, there are many options. Of course, we may compute all elliptic curves with CM by $\mathcal{O}$ and with an N-torsion point using the Kubert resultant method of Example 4, base extend each of these elliptic curves by roots of their nth division polynomials and then compute the torsion subgroups of all those elliptic curves. For running time reasons, it is preferable to rule this out before ever computing an elliptic curve or especially a torsion subgroup. Although there are many ways to compute a torsion subgroup of an elliptic curve over a number field, almost all of them involve reducing an elliptic curve modulo various primes in order to take advantage of Schoof's algorithm [**21**]. Unfortunately, irreducible factors of Kubert resultants often have non-integral coefficients, making this process slow or un-supported in some computer algebra systems. Even for computer algebra systems like `magma v2-18.3` with robust support for elliptic curves over number fields given by non-integral polynomials, it can be very time- and memory-consuming to compute torsion subgroups over large degree number fields.

A crucial step is thus a variant of Step (5) of Function 2.10. If $\mathbf{Z}/n\mathbf{Z} \oplus \mathbf{Z}/N\mathbf{Z} \cong E(L)[\text{tors}]$ with $n \mid N$ for some field extension L of F, then we must have $\mathbf{Q}(\zeta_n) \subset L$. We have done almost everything to numerically rule out the possibility that there is some field L of degree dividing d which contains both F and $\mathbf{Q}(\zeta_n)$. Now that we have computed F explicitly via the Kubert resultant, we can compute the compositum of F with $\mathbf{Q}(\zeta_n)$ and its degree over $\mathbf{Q}$. If this degree does not divide d, then we cannot base extend F to L and obtain $E(L)[\text{tors}] \cong G$. Moreover, we have ruled G out without computing any torsion on E.

Example 6. Let $\mathcal{O} = \mathbf{Z}[(1 + 3\sqrt{-11})/2]$, let $d = 12$, and let $G \cong \mathbf{Z}/9\mathbf{Z} \oplus \mathbf{Z}/9\mathbf{Z}$. Since $h(\mathcal{O}) = 2$, the Kubert degree sequence for $\mathcal{O}$ and $N = 9$ is $[6, 12, 54]$. An elliptic curve with CM by $\mathcal{O}$ over the number field defined by the first irreducible factor or a degree two extension thereof cannot have torsion subgroup G by a quick standard computation. Just computing the torsion subgroup over the number field F given by the second irreducible factor ran for several days before quitting due to a lack of memory. While we could not rule out G as a torsion subgroup without computing with F, we found that the compositum of F with $\mathbf{Q}(\zeta_9)$ has degree 36 over $\mathbf{Q}$ and therefore G is not a torsion subgroup of an elliptic curve with CM by $\mathcal{O}$ over a number field of degree 12.

https://doi.org/10.1112/S1461157014000072 Published online by Cambridge University Press

We now describe the procedure for saying that a group G which could have been produced by Functions 2.12 and 2.10 in fact cannot appear as the torsion subgroup of an elliptic curve E with CM by $\mathcal{O}$ over a number field L of degree dividing d. We describe this procedure as a function which returns True if G can be ruled out or False if G can occur, along with an elliptic curve E over a number field L of degree dividing d.

FUNCTION 3.1 (RuledOut). Let $G \cong \mathbf{Z}/n\mathbf{Z} \oplus \mathbf{Z}/N\mathbf{Z}$, let d be a positive integer and let $\mathcal{O}$ be an imaginary quadratic order.

(1) Compute the Kubert resultant whose roots are the $b \in \overline{\mathbf{Q}}$ such that $E(b, c)$ has CM by $\mathcal{O}$ and $(0, 0)$ is a point of exact order N. Factor it as $\prod_{i=1}^{g} f_i$.
(2) If $Degree(f_i)h(\mathcal{O}) \mid d$ then let F_i denote the number field given by f_i, generated over $\mathbf{Q}(j(\mathcal{O}))$ by b_i. Let c_i be the element of F_i (or possibly an extension) such that $E(b_i, c_i)$ is our CM elliptic curve. Compute the compositum of F_i with $\mathbf{Q}(\zeta_n)$ and let d_i be its degree over $\mathbf{Q}$.
(3) If $c_i \notin F_i$ then raise an error.
(4) If $d_i \mid d$ then let T_i be the torsion subgroup of $E(b_i, c_i)$. If $T_i \cong G$ then Return False, $E(b_i, c_i)_{F_i}$.
(5) If $[F_i : \mathbf{Q}] \neq d$ then it may be possible to base extend $E(b_i, c_i)$ to obtain G as a torsion subgroup.
(6) If T_i is a subgroup of G with the same exponent then $T_i \cong \mathbf{Z}/n'\mathbf{Z} \oplus \mathbf{Z}/N\mathbf{Z}$ where $n' \mid n \mid N$. Compute the nth division polynomial of $E(b_i, c_i)$, perform Möbius inversion to obtain a polynomial whose roots are x-coordinates of points of exact order n, and factor that polynomial as $\prod_{j=1}^{m} p_j$.
(7) If $Degree(p_j) \mid d/[F_i : \mathbf{Q}]$ then let $L_{i,j}$ be the number field given by p_j, generated over F_i by the x-coordinate a_j. Let $g = y^2 + (a_j(1 - c_i) - b_i)y + (b_i a_j^2 - a_j^3)$, the polynomial whose roots in $\overline{\mathbf{Q}}$ are the y-coordinates of the points on $E(b_i, c_i)$ with x-coordinate a_j. Let n_g be the number of irreducible factors over $L_{i,j}$ of g and let $e_j = Degree(p_j)(2/n_g)$.
(8) If $e_j \neq 1$ and $e_j \mid d/[F_i : \mathbf{Q}]$ then let $M_{i,j}$ be the field given by the polynomial g. Let $T_{i,j}$ be the torsion subgroup of the base change of $E(b_i, c_i)$ to $M_{i,j}$.
(9) If $T_{i,j} \cong G$ then Return False, $E(b_i, c_i)_{M_{i,j}}$.
(10) If for all possible i and j there is some "If ..."' statement which begins one of Steps (2)–(9) besides Step (3) which is false, then Return True.

We note that in Step 3.1(3), it is possible that $c_i \notin F_i$ and thus we must have an error-raising statement. However, as one may intuit from Figure 3, the probability that two intersection points in the (b, c)-plane have the same b value is zero by the properties of the Zariski topology. We now give an algorithm which produces all torsion subgroups of elliptic curves with CM over a number field of degree d.

ALGORITHM 3.2. Let d be a positive integer and L a list of finite groups which we know to be torsion subgroups of CM elliptic curves over some number field of degree dividing d.

(1) Create an associative array or dictionary A, indexed by imaginary quadratic orders $\mathcal{O}$ such that $h(\mathcal{O}) \mid d$ and either $h(\mathcal{O}) = 1$ or $h(\mathcal{O}) \neq d$. Let the $\mathcal{O}$th entry of A be

$$\mathsf{PossibleGroups}\left(d, \mathcal{O}, \mathsf{SievedTorsion}\left(\mathcal{O}, \frac{d}{h(\mathcal{O})}\right)\right).$$

(2) Let P be the union of all the sets $A(\mathcal{O})$ and let R be $P - L$, the set of groups in P which are not isomorphic to any element of L.
(3) Iterate over $G \in R$.

https://doi.org/10.1112/S1461157014000072 Published online by Cambridge University Press

- If $\mathsf{RuledOut}(G, d, \mathcal{O})$ returns True for all $\mathcal{O}$ such that $G \in A(\mathcal{O})$, move onto the next group.
- If not, append G to L and go to Step (2).

When Algorithm 3.2 is completed, L is the complete list of possible torsion subgroups. If $d = 2$, then Algorithm 3.2 takes 0.87 s to complete when starting with the list given by Zimmer, Müller and Stroher, and rules out only the group $\mathbf{Z}/5\mathbf{Z}$. If $d = 12$, then if we start from Step (2) with a complete list L, the algorithm takes only 3.5 h to complete for a total time of roughly 14 h. Complete records of the ruling out computation may be found on stankewicz.net/torsion.

4. *Isomorphism classes of torsion subgroups of CM elliptic curves E*

4.1. $K = \mathbf{Q}$

$$E(\mathbf{Q})[\text{tors}] \in \{0, \mathbf{Z}/2\mathbf{Z}, \mathbf{Z}/3\mathbf{Z}, \mathbf{Z}/4\mathbf{Z}, \mathbf{Z}/6\mathbf{Z}, \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/2\mathbf{Z}\}.$$

Examples of these are:

Group	Elliptic curve	j-invariant
0	$y^2 = x^3 + 2$	0
$\mathbf{Z}/2\mathbf{Z}$	$y^2 = x^3 - 1$	0
$\mathbf{Z}/3\mathbf{Z}$	$y^2 = x^3 + 16$	0
$\mathbf{Z}/4\mathbf{Z}$	$y^2 = x^3 + 4x$	1728
$\mathbf{Z}/6\mathbf{Z}$	$y^2 = x^3 + 1$	0
$\mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/2\mathbf{Z}$	$y^2 = x^3 - 4x$	1728

4.2. *K is a number field of degree 2*

$$E(K)[\text{tors}] \in \begin{cases} \mathbf{Z}/m\mathbf{Z} & \text{for } m = 1, 2, 3, 4, 6, 7, 10, \\ \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/m\mathbf{Z} & \text{for } m = 2, 4, 6, \\ \text{and} & \mathbf{Z}/3\mathbf{Z} \oplus \mathbf{Z}/3\mathbf{Z}. \end{cases}$$

The only subgroups which do not occur over $\mathbf{Q}$ are:

$$E(K)[\text{tors}] \in \{\mathbf{Z}/7\mathbf{Z}, \mathbf{Z}/10\mathbf{Z}, \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/4\mathbf{Z}, \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/6\mathbf{Z}, \mathbf{Z}/3\mathbf{Z} \oplus \mathbf{Z}/3\mathbf{Z}\}.$$

Examples of these are:

Group	Field extension	Elliptic curve	j-invariant
$\mathbf{Z}/7\mathbf{Z}$	$\mathbf{Q}(\zeta_3)$	$E(\zeta_3, -1)$	0
$\mathbf{Z}/10\mathbf{Z}$	$\mathbf{Q}(\zeta_4)$	$E(\zeta_4, \zeta_4)$	1728
$\mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/4\mathbf{Z}$	$\mathbf{Q}(\zeta_4)$	$y^2 = x^3 + 4x$	1728
$\mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/6\mathbf{Z}$	$\mathbf{Q}(\zeta_3)$	$y^2 = x^3 + 1$	0
$\mathbf{Z}/3\mathbf{Z} \oplus \mathbf{Z}/3\mathbf{Z}$	$\mathbf{Q}(\zeta_3)$	$y^2 = x^3 + 16$	0

4.3. *K is a number field of degree 3*

$$E(K)[\text{tors}] \in \begin{cases} \mathbf{Z}/m\mathbf{Z} & \text{for } m = 1, 2, 3, 4, 6, 9, 14, \\ \text{and} & \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/2\mathbf{Z}. \end{cases}$$

The only subgroups which do not occur over $\mathbf{Q}$ are:

$$E(K)[\text{tors}] \in \{\mathbf{Z}/9\mathbf{Z}, \mathbf{Z}/14\mathbf{Z}\}.$$

https://doi.org/10.1112/S1461157014000072 Published online by Cambridge University Press

Examples of these are:

Group	Defining polynomial	Elliptic curve	j-invariant
$\mathbf{Z}/9\mathbf{Z}$	$b^3 - 99b^2 - 90b - 9$	$E\left(b, \dfrac{-2b^2 + 318b - 75}{753}\right)$	0
$\mathbf{Z}/14\mathbf{Z}$	$b^3 + 5b^2 + 2/7b - 1/49$	$E\left(b, \dfrac{133b^2 + 749b + 54}{167}\right)$	-3375

4.4. *K is a number field of degree 4*

$$E(K)[\text{tors}] \in \begin{cases} \mathbf{Z}/m\mathbf{Z} & \text{for } m = 1, \ldots, 8, 10, 12, 13, 21, \\ \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/m\mathbf{Z} & \text{for } m = 2, 4, 6, 8, 10, \\ \mathbf{Z}/3\mathbf{Z} \oplus \mathbf{Z}/m\mathbf{Z} & \text{for } m = 3, 6, \\ \text{and} & \mathbf{Z}/4\mathbf{Z} \oplus \mathbf{Z}/4\mathbf{Z}. \end{cases}$$

The only subgroups which do not occur over $\mathbf{Q}$ or a number field of degree 2 are:

$$E(K)[\text{tors}] \in \left\{ \begin{array}{c} \mathbf{Z}/5\mathbf{Z}, \mathbf{Z}/8\mathbf{Z}, \mathbf{Z}/12\mathbf{Z}, \mathbf{Z}/13\mathbf{Z}, \mathbf{Z}/21\mathbf{Z}, \\ \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/8\mathbf{Z}, \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/10\mathbf{Z}, \mathbf{Z}/4\mathbf{Z} \oplus \mathbf{Z}/4\mathbf{Z}, \mathbf{Z}/3\mathbf{Z} \oplus \mathbf{Z}/6\mathbf{Z} \end{array} \right\}.$$

Examples of these are:

Group	Field	Elliptic Curve	j
$\mathbf{Z}/5\mathbf{Z}$	$\dfrac{\mathbf{Q}[b]}{(b^4 - 4b^3 + 46b^2 + 4b + 1)}$	$E(b, b)$	-32768
$\mathbf{Z}/8\mathbf{Z}$	$\dfrac{\mathbf{Q}[b]}{(b^4 + 2b^3 + b^2 - b - \frac{1}{8})}$	$E\left(b, \dfrac{8b^3 + 36b^2 + 46b + 3}{13}\right)^{\dagger}$	1728
$\mathbf{Z}/12\mathbf{Z}$	$\dfrac{\mathbf{Q}[b]}{(b^4 - 10b^3 + 24b^2 - 16b - 2)}$	$E\left(b, \dfrac{-6b^3 + 52b^2 - 70b - 9}{7}\right)$	0
$\mathbf{Z}/13\mathbf{Z}$	$\dfrac{\mathbf{Q}[b]}{(b^4 + 4b^3 + 78b^2 + 13b + 1)}$	$E\left(b, \dfrac{16b^3 + 44b^2 + 1354b + 45}{483}\right)$	0
$\mathbf{Z}/21\mathbf{Z}$	$\dfrac{\mathbf{Q}[e]}{(e^4 - e^3 + 2e + 1)}$	$y^2 = x^3 - \begin{pmatrix} 371952e^3 + \\ 3373488e^2 + \\ 3777840e + \\ 1228608 \end{pmatrix}$	0
$\left(\dfrac{\mathbf{Z}/2\mathbf{Z}\oplus}{\mathbf{Z}/8\mathbf{Z}}\right)$	$\dfrac{\mathbf{Q}[b]}{(b^4 - 4b^3 + 4b^2 - b - 1/8)}$	$E(b, 32b^3 - 108b^2 + 58b + 6)$	287496
$\left(\dfrac{\mathbf{Z}/2\mathbf{Z}\oplus}{\mathbf{Z}/10\mathbf{Z}}\right)$	$\dfrac{\mathbf{Q}(\zeta_4)[x]}{(x^2 - \zeta_4 x - \frac{\zeta_4}{2})}$	$E(\zeta_4, \zeta_4)$	1728
$\left(\dfrac{\mathbf{Z}/4\mathbf{Z}\oplus}{\mathbf{Z}/4\mathbf{Z}}\right)$	$\dfrac{\mathbf{Q}[x]}{(x^4 + 1)}$	$E(-1/8, 0)$	1728
$\left(\dfrac{\mathbf{Z}/3\mathbf{Z}\oplus}{\mathbf{Z}/6\mathbf{Z}}\right)$	$\mathbf{Q}(\sqrt{3}, \sqrt{-3})$	$E\left(\dfrac{6\sqrt{3} + 10}{3}, \dfrac{2\sqrt{3} + 3}{3}\right)$	1728

†Although $j(\mathbf{Z}[2i]) = 287496$ and $j(\mathbf{Z}[i]) = 1728$ and so one might reasonably guess two curves over number fields of the same degree with those j-invariants and respective torsion subgroups $\mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/8\mathbf{Z}$ and $\mathbf{Z}/8\mathbf{Z}$ to be rationally isogenous, this is not the case. Indeed the two fields are not isomorphic.

https://doi.org/10.1112/S1461157014000072 Published online by Cambridge University Press

4.5. *K is a number field of degree 5*

$$E(K)[\text{tors}] \in \{0, \mathbf{Z}/2\mathbf{Z}, \mathbf{Z}/3\mathbf{Z}, \mathbf{Z}/4\mathbf{Z}, \mathbf{Z}/6\mathbf{Z}, \mathbf{Z}/11\mathbf{Z}, \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/2\mathbf{Z}\}.$$

The only subgroup which does not occur over $\mathbf{Q}$ is $\mathbf{Z}/11\mathbf{Z}$, which occurs over the maximal real subfield of $\mathbf{Q}(\zeta_{11})$. This occurs for $j = -32768$ in $E(b, c)$ with the following quantities. Hereon, unless otherwise stated, elliptic curves will be given by the values of b and c.

Field extension	b	c
$\dfrac{\mathbf{Q}[e]}{(e^5 - e^4 - 4e^3 + 3e^2 + 3e - 1)}$	$-7e^4 - 2e^3 + 16e^2 - e - 1$	$2e^3 - 4e + 1$

4.6. *K is a number field of degree 6*

$$E(K)[\text{tors}] \in \begin{cases} \mathbf{Z}/m\mathbf{Z} & \text{for } m = 1, 2, 3, 4, 6, 7, 9, 10, 14, 18, 19, 26, \\ \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/m\mathbf{Z} & \text{for } m = 2, 4, 6, 14, \\ \mathbf{Z}/3\mathbf{Z} \oplus \mathbf{Z}/m\mathbf{Z} & \text{for } m = 3, 6, 9, \\ \text{and} & \mathbf{Z}/6\mathbf{Z} \oplus \mathbf{Z}/6\mathbf{Z}. \end{cases}$$

The only subgroups which do not occur over $\mathbf{Q}$ or a number field of degree 2 or 3 are:

$$E(K)[\text{tors}] \in \left\{ \begin{array}{c} \mathbf{Z}/18\mathbf{Z}, \mathbf{Z}/19\mathbf{Z}, \mathbf{Z}/26\mathbf{Z} \\ \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/14\mathbf{Z}, \mathbf{Z}/3\mathbf{Z} \oplus \mathbf{Z}/6\mathbf{Z}, \mathbf{Z}/3\mathbf{Z} \oplus \mathbf{Z}/9\mathbf{Z}, \mathbf{Z}/6\mathbf{Z} \oplus \mathbf{Z}/6\mathbf{Z} \end{array} \right\}.$$

Examples of these are:

Group	$\mathbf{Z}/18\mathbf{Z}$
j, Field	$8000, \mathbf{Q}[e]/(e^6 - 2e^5 + 3e^4 - 2e^3 + 2e^2 + 1)$
b	$\frac{1}{9}(28e^5 - 79e^4 + 86e^3 - 30e^2 + 11e - 31)$
c	$\frac{1}{3}(-8e^5 + 7e^4 - e^3 - 8e^2 - 9e - 5)$

Group	$\mathbf{Z}/19\mathbf{Z}$
j, Field	$0, \mathbf{Q}[e]/(e^6 + e^4 - e^3 - 2e^2 + e + 1)$
b	$2e^5 - e^4 + 2e^3 - 4e^2 + 2$
c	$2e^5 - 2e^4 + 4e^3 - 4e^2 - 2e + 3$

Group	$\mathbf{Z}/26\mathbf{Z}$
j, Field	$1728, \mathbf{Q}[e]/(e^6 - e^4 + 2e^3 - 2e + 1)$
b	$\frac{1}{13}(53e^5 + 6e^4 - 70e^3 + 75e^2 + 5e - 136)$
c	$\frac{1}{13}(-49e^5 - 44e^4 + 14e^3 - 78e^2 - 65e + 46)$

https://doi.org/10.1112/S1461157014000072 Published online by Cambridge University Press

Group	Field extension	Elliptic curve	j
$\left(\frac{\mathbf{Z}/2\mathbf{Z}\oplus}{\mathbf{Z}/14\mathbf{Z}}\right)$	$\frac{\mathbf{Q}(\sqrt{-7})[b]}{(b^3+5b^2+2/7b-1/49)}$	$E\left(b, \frac{133b^2+749b+54}{167}\right)$	-3375
$\left(\frac{\mathbf{Z}/3\mathbf{Z}\oplus}{\mathbf{Z}/6\mathbf{Z}}\right)$	$\mathbf{Q}(\zeta_3, \sqrt[3]{2})$	$y^2=x^3-15x+22$	54000
$\left(\frac{\mathbf{Z}/6\mathbf{Z}\oplus}{\mathbf{Z}/6\mathbf{Z}}\right)$	$\mathbf{Q}(\zeta_3, \sqrt[3]{4})$	$y^2=x^3+1$	0
$\left(\frac{\mathbf{Z}/3\mathbf{Z}\oplus}{\mathbf{Z}/9\mathbf{Z}}\right)$	$\mathbf{Q}(\zeta_9)$	$y^2=x^3+16$	0

4.7. *K is a number field of degree* 7

$$E(K)[\text{tors}] \in \{0, \mathbf{Z}/2\mathbf{Z}, \mathbf{Z}/3\mathbf{Z}, \mathbf{Z}/4\mathbf{Z}, \mathbf{Z}/6\mathbf{Z}, \mathbf{Z}/2\mathbf{Z}\oplus\mathbf{Z}/2\mathbf{Z}\}.$$

No subgroups occur in degree 7 which do not occur over $\mathbf{Q}$.

4.8. *K is a number field of degree* 8

$$E(K)[\text{tors}] \in \begin{cases} \mathbf{Z}/m\mathbf{Z} & \text{for } m=1,\dots,8,10,12,13,\\ & \qquad 15,16,20,21,28,30,34,39,\\ \mathbf{Z}/2\mathbf{Z}\oplus\mathbf{Z}/m\mathbf{Z} & \text{for } m=2,4,6,8,10,12,16,20,\\ \mathbf{Z}/4\mathbf{Z}\oplus\mathbf{Z}/m\mathbf{Z} & m=4,8,12,\\ \mathbf{Z}/m\mathbf{Z}\oplus\mathbf{Z}/m\mathbf{Z} & \text{for } m=3,5,6,\\ \mathbf{Z}/m\mathbf{Z}\oplus\mathbf{Z}/2m\mathbf{Z} & \text{for } m=3,5. \end{cases}$$

The only subgroups which do not occur over $\mathbf{Q}$ or a number field of degree dividing 8 are:

$$E(K)[\text{tors}] \in \left\{ \begin{array}{c} \mathbf{Z}/15\mathbf{Z}, \mathbf{Z}/16\mathbf{Z}, \mathbf{Z}/20\mathbf{Z}, \mathbf{Z}/30\mathbf{Z}, \mathbf{Z}/34\mathbf{Z}, \mathbf{Z}/39\mathbf{Z}\\ \mathbf{Z}/2\mathbf{Z}\oplus\mathbf{Z}/12\mathbf{Z}, \mathbf{Z}/2\mathbf{Z}\oplus\mathbf{Z}/16\mathbf{Z}, \mathbf{Z}/2\mathbf{Z}\oplus\mathbf{Z}/20\mathbf{Z}\\ \mathbf{Z}/6\mathbf{Z}\oplus\mathbf{Z}/6\mathbf{Z}, \mathbf{Z}/4\mathbf{Z}\oplus\mathbf{Z}/8\mathbf{Z}, \mathbf{Z}/4\mathbf{Z}\oplus\mathbf{Z}/12\mathbf{Z}\\ \mathbf{Z}/5\mathbf{Z}\oplus\mathbf{Z}/5\mathbf{Z}, \mathbf{Z}/5\mathbf{Z}\oplus\mathbf{Z}/10\mathbf{Z} \end{array} \right\}.$$

We give examples of these and hereon, unless otherwise stated, their fields of definition will be given only by the defining polynomial over $\mathbf{Q}$.

Group	$\mathbf{Z}/15\mathbf{Z}$
j, Field	$0, e^8-3e^7-2e^6+9e^5-6e^3-2e^2-3e+1=0$
b	$\frac{1}{61}\left(\begin{array}{c}599e^7-303e^6-1758e^5+786e^4\\ +1411e^3+632e^2+755e-307\end{array}\right)$
c	$\frac{1}{61}(-8e^7+68e^6+8e^5-238e^4+28e^3+260e^2+50e-7)$

https://doi.org/10.1112/S1461157014000072 Published online by Cambridge University Press

Group	$\mathbf{Z}/16\mathbf{Z}$
j, Field	$16581375, e^8 - 2e^7 + 6e^6 - 9e^5 + 10e^4 - 8e^3 + 6e^2 - 3e + 1 = 0$
b	$\frac{1}{2}(-16e^7 + 131e^6 - 234e^5 + 268e^4 - 227e^3 + 175e^2 - 90e + 28)$
c	$\frac{1}{2}(-e^7 + 7e^6 - 15e^5 + 16e^4 - 14e^3 + 10e^2 - 6e + 1)$

Group	$\mathbf{Z}/20\mathbf{Z}$
j, Field	$287496, e^8 - 4e^7 + 6e^6 - 8e^4 + 8e^3 - 4e + 2 = 0$
b	$280e^7 - 876e^6 + 873e^5 + 873e^4 - 1553e^3 + 710e^2 + 762e - 487$
c	$-25e^7 + 82e^6 - 88e^5 - 71e^4 + 154e^3 - 77e^2 - 66e + 55$

Group	$\mathbf{Z}/30\mathbf{Z}$
j	$j^2 + 191025j - 121287375 = 0$
Field	$e^8 - 3e^7 - 2e^6 + 9e^5 - 6e^3 - 2e^2 - 3e + 1 = 0$
b	$\frac{1}{61}\begin{pmatrix} -1926e^7 + 7953e^6 - 4967e^5 - 12311e^4 \\ +13878e^3 - 2797e^2 + 7188e - 1853 \end{pmatrix}$
c	$\frac{1}{61}(97e^7 - 367e^6 + 147e^5 + 583e^4 - 492e^3 + 172e^2 - 286e + 62)$

Group	$\mathbf{Z}/34\mathbf{Z}$
j, Field	$1728, e^8 + 4e^7 + 7e^6 + 8e^5 + 8e^4 + 6e^3 + 4e^2 + 2e + 1 = 0$
b	$\frac{1}{17}(-11e^7 - 34e^6 - 38e^5 - 16e^4 - 11e^3 - 11e^2 - e + 3)$
c	$\frac{1}{17}(9e^7 + 31e^6 + 59e^5 + 60e^4 + 50e^3 + 30e^2 + 25e + 6)$

Group	$\mathbf{Z}/39\mathbf{Z}$
j, Field	$0, e^8 - 2e^6 - 3e^5 + 3e^4 + 3e^3 - 2e^2 + 1 = 0$
b	$-12e^7 - 25e^6 + 7e^5 + 82e^4 + 77e^3 - 47e^2 - 95e - 35$
c	$-8e^7 - 4e^6 + 18e^5 + 34e^4 - 14e^3 - 46e^2 + 13$

https://doi.org/10.1112/S1461157014000072 Published online by Cambridge University Press

Group	$\mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/12\mathbf{Z}$
j, Field	$54000, e^8 - 4e^7 + 2e^6 + 8e^5 - 8e^4 + 4e^3 - 16e^2 + 16e - 2 = 0$
b	$\frac{1}{13}\begin{pmatrix} -1083e^7 + 2865e^6 + 1673e^5 - 6205e^4 \\ -5e^3 - 4167e^2 + 11397e - 1570 \end{pmatrix}$
c	$\frac{1}{13}\begin{pmatrix} -306e^7 + 805e^6 + 500e^5 - 1801e^4 \\ +27e^3 - 1218e^2 + 3282e - 453 \end{pmatrix}$

Group	$\mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/16\mathbf{Z}$
j, Field	$-3375, e^8 + 3e^7 + 6e^6 + 8e^5 + 10e^4 + 9e^3 + 6e^2 + 2e + 1 = 0$
b	$\frac{1}{2}(20e^7 + 47e^6 + 79e^5 + 96e^4 + 110e^3 + 89e^2 + 26e + 18)$
c	$\frac{1}{2}(7e^7 + 12e^6 + 22e^5 + 22e^4 + 30e^3 + 17e^2 + 7e + 3)$

Group	$\mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/20\mathbf{Z}$
j, Field	$1728, e^8 - 4e^7 + 6e^6 - 8e^4 + 8e^3 - 4e + 2 = 0$
b	$-5e^7 + 17e^6 - 20e^5 - 12e^4 + 34e^3 - 21e^2 - 15e + 13$
c	$-4e^7 + 13e^6 - 13e^5 - 13e^4 + 24e^3 - 8e^2 - 10e + 7$

Group	$\mathbf{Z}/6\mathbf{Z} \oplus \mathbf{Z}/6\mathbf{Z}$
j, Field	$-3375, e^8 + 3e^7 + 4e^6 + 3e^5 + 3e^4 + 3e^3 + 4e^2 + 3e + 1 = 0$
b	$\frac{1}{15}(132e^7 + 513e^6 + 681e^5 + 267e^4 + 143e^3 + 629e^2 + 602e + 193)$
c	$\frac{1}{15}(-21e^7 - 39e^6 - 3e^5 + 29e^4 - 39e^3 - 32e^2 + 9e + 11)$

Group	$\mathbf{Z}/4\mathbf{Z} \oplus \mathbf{Z}/8\mathbf{Z}$
j, Field	$-3375, e^8 - e^6 - 2e^5 + e^4 + 8e^3 + 12e^2 + 8e + 2 = 0$
b	$\frac{1}{11}(103e^7 - 85e^6 - 43e^5 - 153e^4 + 222e^3 + 655e^2 + 663e + 235)$
c	$\frac{1}{11}(63e^7 - 27e^6 - 64e^5 - 86e^4 + 114e^3 + 452e^2 + 534e + 206)$

https://doi.org/10.1112/S1461157014000072 Published online by Cambridge University Press

Group	$\mathbf{Z}/4\mathbf{Z} \oplus \mathbf{Z}/12\mathbf{Z}$
j, Field	$0, e^8 - 2e^7 + 2e^6 - 2e^5 + 7e^4 - 10e^3 + 8e^2 - 4e + 1 = 0$
b	$\frac{1}{11}(-32e^7 + 66e^6 - 53e^5 + 57e^4 - 220e^3 + 320e^2 - 188e + 115)$
c	$\frac{1}{11}(-28e^7 + 66e^6 - 56e^5 + 54e^4 - 198e^3 + 324e^2 - 214e + 91)$

Group, Field	$\mathbf{Z}/5\mathbf{Z} \oplus \mathbf{Z}/5\mathbf{Z}, \mathbf{Q}(\zeta_{15})$
$j, b = c$	$(0, 4\zeta_{15}^7 + 2\zeta_{15}^6 - 2\zeta_{15}^5 - 2\zeta_{15}^3 + 4\zeta_{15} + 1)$

Group, Field	$\mathbf{Z}/5\mathbf{Z} \oplus \mathbf{Z}/10\mathbf{Z}, \mathbf{Q}(\zeta_{20})$
$j, b = c$	$(1728, \zeta_4)$

4.9. *K is a number field of degree 9*

$$E(K)[\text{tors}] \in \begin{cases} \mathbf{Z}/m\mathbf{Z} & \text{for } m = 1, 2, 3, 4, 6, 9, 14, 18, 19, 27, \\ \text{and} & \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/2\mathbf{Z}. \end{cases}$$

The subgroups which do not occur over $\mathbf{Q}$ or a number field of degree 3 are:

$$E(K)[\text{tors}] \in \{\mathbf{Z}/18\mathbf{Z}, \mathbf{Z}/19\mathbf{Z}, \mathbf{Z}/27\mathbf{Z}\}.$$

Examples of these are:

Group	$\mathbf{Z}/18\mathbf{Z}$
j	54000
Field	$e^9 - 3e^8 + 3e^7 - 6e^6 + 12e^5 - 3e^4 - 15e^3 + 15e^2 - 6e + 1 = 0$
b	$\frac{1}{3}\left(\begin{array}{c} 217e^8 - 235e^7 + 202e^6 - 904e^5 + 841e^4 \\ +971e^3 - 1364e^2 + 617e - 113 \end{array}\right)$
c	$\frac{1}{3}(7e^8 - 8e^7 + 7e^6 - 31e^5 + 32e^4 + 29e^3 - 50e^2 + 25e - 5)$

Group	$\mathbf{Z}/19\mathbf{Z}$
j	-884736
Field	$e^9 - e^8 - 8e^7 + 7e^6 + 21e^5 - 15e^4 - 20e^3 + 10e^2 + 5e - 1 = 0$
b	$-31e^8 + 73e^7 + 112e^6 - 319e^5 - 80e^4 + 397e^3 - 26e^2 - 139e + 22$
c	$(-2e^8 + 16e^6 - 4e^5 - 38e^4 + 14e^3 + 26e^2 - 10e + 1)$

https://doi.org/10.1112/S1461157014000072 Published online by Cambridge University Press

Group[†]	$\mathbf{Z}/27\mathbf{Z}$
j	-12288000
Field	$e^9 - 9e^7 + 27e^5 - 30e^3 + 9e - 1 = 0$
b	$\begin{pmatrix} -4282e^8 - 507e^7 + 38492e^6 + 4523e^5 - 115156e^4 \\ -13456e^3 + 126990e^2 + 14789e - 36852 \end{pmatrix}$
c	$(16e^8 + 2e^7 - 140e^6 - 18e^5 + 410e^4 + 54e^3 - 444e^2 - 58e + 125)$

4.10. *K is a number field of degree* 10

$$E(K)[\text{tors}] \in \begin{cases} \mathbf{Z}/m\mathbf{Z} & \text{for } m = 1, 2, 3, 4, 6, 7, 10, 11, 22, 31, 50, \\ \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/m\mathbf{Z} & \text{for } m = 2, 4, 6, 22, \\ \text{and} & \mathbf{Z}/3\mathbf{Z} \oplus \mathbf{Z}/3\mathbf{Z}. \end{cases}$$

The only subgroups which do not occur over $\mathbf{Q}$ or a number field of degree 2 or 5 are:

$$E(K)[\text{tors}] \in \{\mathbf{Z}/22\mathbf{Z}, \mathbf{Z}/31\mathbf{Z}, \mathbf{Z}/50\mathbf{Z}, \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/22\mathbf{Z}\}.$$

Examples of these are:

Group	$\mathbf{Z}/22\mathbf{Z}$
j	16581375
Field	$e^{10} - e^9 + 2e^8 - 4e^7 + 5e^6 - 3e^5 + 3e^4 - 6e^3 + 7e^2 - 4e + 1 = 0$
b	$\begin{pmatrix} -184243e^9 + 88117e^8 - 299927e^7 + 589670e^6 - 568675e^5 \\ +223462e^4 - 395246e^3 + 908033e^2 - 759722e + 279034 \end{pmatrix}$
c	$\begin{pmatrix} 1905e^9 - 643e^8 + 3210e^7 - 5564e^6 + 5493e^5 \\ -1825e^4 + 4191e^3 - 8721e^2 + 7124e - 2426 \end{pmatrix}$

Group	$\mathbf{Z}/31\mathbf{Z}$
j	0
Field	$e^{10} + 2e^8 - 3e^7 + 3e^6 - 7e^5 + 8e^4 - 7e^3 + 7e^2 - 4e + 1 = 0$
b	$\begin{pmatrix} 43e^9 - 33e^8 + 45e^7 - 222e^6 + 133e^5 \\ -335e^4 + 508e^3 - 326e^2 + 368e - 252 \end{pmatrix}$
c	$\begin{pmatrix} 24e^9 + 10e^8 + 50e^7 - 54e^6 + 44e^5 \\ -148e^4 + 130e^3 - 104e^2 + 122e - 43 \end{pmatrix}$

[†]The discriminant of the CM order is -27 and the SPY bounds are sharp here. Typically when the SPY bounds are sharp, $\gcd(\text{disc}(\mathcal{O}), N) > 1$.

https://doi.org/10.1112/S1461157014000072 Published online by Cambridge University Press

Group	$\mathbf{Z}/50\mathbf{Z}$
j	1728
Field	$e^{10} - 4e^9 + 9e^8 - 14e^7 + 15e^6 - 10e^5 + 3e^4 + 2e^3 - 2e^2 + 1 = 0$
b	$(20e^8 - 59e^7 + 87e^6 - 79e^5 + 31e^4 + 17e^3 - 12e^2 + 4e + 8)$
c	$(e^9 - 6e^8 + 10e^7 - 10e^6 + 7e^5 - e^4 - e^3 - 2e^2 - 2e - 1)$

Group	$\mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/22\mathbf{Z}$
j	-3375
Field	$e^{10} - e^9 + 2e^8 - 4e^7 + 5e^6 - 3e^5 + 3e^4 - 6e^3 + 7e^2 - 4e + 1 = 0$
b	$\begin{pmatrix} -14e^9 + 4e^8 - 22e^7 + 41e^6 - 35e^5 \\ +9e^4 - 30e^3 + 63e^2 - 46e + 10 \end{pmatrix}$
c	$(-6e^9 + 5e^8 - 9e^7 + 23e^6 - 22e^5 + 10e^4 - 13e^3 + 33e^2 - 32e + 11)$

4.11. *K is a number field of degree* 11

$$E(K)[\text{tors}] \in \{0, \mathbf{Z}/2\mathbf{Z}, \mathbf{Z}/3\mathbf{Z}, \mathbf{Z}/4\mathbf{Z}, \mathbf{Z}/6\mathbf{Z}, \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/2\mathbf{Z}\}.$$

No subgroups occur in degree 11 which do not occur over $\mathbf{Q}$.

4.12. *K is a number field of degree* 12

$$E(K)[\text{tors}] \in \begin{cases} \mathbf{Z}/m\mathbf{Z} & \text{for } m = 1, \ldots, 10, 12, 13, 14, \\ & \qquad 18, 19, 21, 26, 37, 42, 57, \\ \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/m\mathbf{Z} & \text{for } m = 2, 4, 6, 8, 10, 12, 14, 18, 26, 28, 42, \\ \mathbf{Z}/3\mathbf{Z} \oplus \mathbf{Z}/m\mathbf{Z} & \text{for } m = 3, 6, 9, 12, 18, 21, \\ \mathbf{Z}/m\mathbf{Z} \oplus \mathbf{Z}/m\mathbf{Z} & \text{for } m = 4, 6, 7. \end{cases}$$

The only subgroups which do not occur over a number field of degree dividing 12 are:

$$E(K)[\text{tors}] \in \begin{cases} \mathbf{Z}/m\mathbf{Z} & \text{for } m = 28, 37, 42, 57, \\ \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/m\mathbf{Z} & \text{for } m = 12, 18, 26, 28, 42, \\ \mathbf{Z}/3\mathbf{Z} \oplus \mathbf{Z}/m\mathbf{Z} & \text{for } m = 12, 18, 21, \\ \text{and} & \mathbf{Z}/7\mathbf{Z} \oplus \mathbf{Z}/7\mathbf{Z}. \end{cases}$$

https://doi.org/10.1112/S1461157014000072 Published online by Cambridge University Press

These are:

Group	$\mathbf{Z}/28\mathbf{Z}$
j	54000
Field	$e^{12} - 4e^{11} + 8e^{10} - 6e^9 - 7e^8 + 20e^7$ $-18e^6 - 4e^5 + 25e^4 - 8e^3 - 6e^2 + 2e + 1 = 0$
b	$\frac{1}{402}\begin{pmatrix} 110e^{11} - 95e^{10} - 24e^9 - 47e^8 - 19e^7 - 232e^6 \\ -119e^5 + 1480e^4 + 369e^3 - 1017e^2 + 149e + 197 \end{pmatrix}$
c	$\frac{1}{402}\begin{pmatrix} 116e^{11} - 423e^{10} + 853e^9 - 655e^8 - 768e^7 + 2238e^6 \\ -1982e^5 - 766e^4 + 2806e^3 - 277e^2 - 441e - 3 \end{pmatrix}$

Group	$\mathbf{Z}/37\mathbf{Z}$
j	0
Field	$e^{12} - 4e^{11} + 11e^{10} - 21e^9 + 32e^8 - 40e^7$ $+45e^6 - 46e^5 + 40e^4 - 26e^3 + 12e^2 - 4e + 1 = 0$
b	$\frac{1}{37}\begin{pmatrix} -196e^{11} + 657e^{10} - 1789e^9 + 3384e^8 - 5292e^7 + 6890e^6 \\ -7695e^5 + 7154e^4 - 4851e^3 + 2221e^2 - 773e + 181 \end{pmatrix}$
c	$\frac{1}{37}\begin{pmatrix} 24e^{11} - 162e^{10} + 432e^9 - 952e^8 + 1462e^7 - 1928e^6 \\ +2090e^5 - 2060e^4 + 1630e^3 - 870e^2 + 294e - 109 \end{pmatrix}$

Group	$\mathbf{Z}/42\mathbf{Z}$[†]
j	54000
Field	$e^{12} - 4e^{11} + 8e^{10} - 11e^9 + 13e^8 - 14e^7$ $+15e^6 - 14e^5 + 7e^4 + 3e^3 - 5e^2 + e + 1 = 0$
b	$\begin{pmatrix} 1416e^{11} - 6140e^{10} + 13362e^9 - 19953e^8 + 24872e^7 - 27802e^6 \\ +30076e^5 - 29333e^4 + 19087e^3 - 1483e^2 - 7097e + 4041 \end{pmatrix}$
c	$\begin{pmatrix} 27e^{11} - 138e^{10} + 342e^9 - 563e^8 + 754e^7 - 896e^6 \\ +1000e^5 - 1038e^4 + 847e^3 - 370e^2 - 7e + 66 \end{pmatrix}$

[†]Note that this elliptic curve is rationally isogenous to the one with $j = 0$ and torsion $\mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/42\mathbf{Z}$.

https://doi.org/10.1112/S1461157014000072 Published online by Cambridge University Press

Group	$\mathbf{Z}/57\mathbf{Z}$
j	0
Field	$e^{12}-2e^{11}+5e^{10}-10e^9+16e^8-22e^7$ $+30e^6-31e^5+28e^4-27e^3+19e^2-7e+1=0$
b	$\begin{pmatrix} 18509e^{11}-25122e^{10}+76123e^9-135966e^8 \\ +207749e^7-272291e^6+378051e^5-328154e^4 \\ +303397e^3-302371e^2+154326e-27788 \end{pmatrix}$
c	$\begin{pmatrix} 128e^{11}-62e^{10}+446e^9-532e^8+876e^7-986e^6 \\ +1542e^5-670e^4+1136e^3-872e^2+18e+71 \end{pmatrix}$

Group	$\mathbf{Z}/2\mathbf{Z}\oplus\mathbf{Z}/12\mathbf{Z}$
j	$j^3+3491750j^2-5151296875j+12771880859375=0$
Field	$e^{12}-4e^{11}+11e^{10}-28e^9+63e^8-114e^7$ $+161e^6-174e^5+141e^4-82e^3+33e^2-8e+1=0$
b	$\frac{1}{8}\begin{pmatrix} 46e^{11}-165e^{10}+327e^9-914e^8+1949e^7-2883e^6 \\ +3279e^5-2583e^4+1240e^3-576e^2+169e-34 \end{pmatrix}$
c	$\frac{1}{8}\begin{pmatrix} 86e^{11}-295e^{10}+760e^9-1947e^8+4217e^7-7168e^6 \\ +9344e^5-9004e^4+6265e^3-2894e^2+769e-103 \end{pmatrix}$

Group	$\mathbf{Z}/2\mathbf{Z}\oplus\mathbf{Z}/18\mathbf{Z}$
j	8000
Field	$e^{12}-4e^{11}+4e^{10}+8e^9-25e^8+24e^7$ $+4e^6-36e^5+46e^4-32e^3+14e^2-4e+1=0$
b	$\frac{1}{369}\begin{pmatrix} -1450e^{11}+3898e^{10}+304e^9-13733e^8+17660e^7-2419e^6 \\ -19740e^5+26634e^4-18553e^3+5681e^2-2148e+155 \end{pmatrix}$
c	$\frac{1}{123}\begin{pmatrix} 1108e^{11}-3354e^{10}+756e^9+10638e^8-17099e^7+6109e^6 \\ +14805e^5-25449e^4+20608e^3-8740e^2+2841e-680 \end{pmatrix}$

https://doi.org/10.1112/S1461157014000072 Published online by Cambridge University Press

Group	$\mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/26\mathbf{Z}$
j	0
Field	$e^{12} - 5e^{11} + 11e^{10} - 9e^9 - 7e^8 + 24e^7$ $-21e^6 + 21e^4 - 25e^3 + 16e^2 - 6e + 1 = 0$
b	$\frac{1}{91}\begin{pmatrix} -781e^{11} + 3351e^{10} - 5753e^9 + 969e^8 + 9554e^7 - 12544e^6 \\ +1862e^5 + 8736e^4 - 11312e^3 + 6330e^2 - 1292e - 19 \end{pmatrix}$
c	$\frac{1}{91}\begin{pmatrix} -198e^{11} + 1336e^{10} - 3552e^9 + 3848e^8 + 1816e^7 - 9198e^6 \\ +8344e^5 + 1134e^4 - 8428e^3 + 8618e^2 - 4202e + 785 \end{pmatrix}$

Group	$\mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/28\mathbf{Z}$
j	-3375
Field	$e^{12} - 4e^{11} + 5e^{10} + 3e^9 - 11e^8 - 3e^7$ $+35e^6 - 47e^5 + 27e^4 - 4e^3 - e^2 - e + 1 = 0$
b	$\frac{1}{43}\begin{pmatrix} 1252e^{11} - 3557e^{10} + 1151e^9 + 6917e^8 - 4746e^7 - 13843e^6 \\ +26751e^5 - 17575e^4 + 2938e^3 + 964e^2 + 523e - 674 \end{pmatrix}$
c	$\frac{1}{43}\begin{pmatrix} 103e^{11} - 501e^{10} + 525e^9 + 659e^8 - 1439e^7 - 1039e^6 \\ +4489e^5 - 4371e^4 + 1157e^3 + 216e^2 - 45e - 219 \end{pmatrix}$

Group	$\mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/42\mathbf{Z}$
j	0
Field	$e^{12} - 4e^{11} + 8e^{10} - 11e^9 + 13e^8 - 14e^7$ $+15e^6 - 14e^5 + 7e^4 + 3e^3 - 5e^2 + e + 1 = 0$
b	$\begin{pmatrix} 17e^{11} - 40e^{10} + 61e^9 - 71e^8 + 82e^7 - 81e^6 \\ +95e^5 - 59e^4 - 12e^3 + 41e^2 - 6e - 7 \end{pmatrix}$
c	$\begin{pmatrix} 6e^{11} - 18e^{10} + 28e^9 - 34e^8 + 38e^7 - 40e^6 \\ +44e^5 - 36e^4 + 20e^2 - 8e - 5 \end{pmatrix}$

https://doi.org/10.1112/S1461157014000072 Published online by Cambridge University Press

Group	$\mathbf{Z}/3\mathbf{Z} \oplus \mathbf{Z}/12\mathbf{Z}$
j	54000
Field	$e^{12} - 3e^{10} - 2e^9 + 12e^8 - 6e^7 - 3e^6$ $-12e^5 + 36e^4 - 38e^3 + 21e^2 - 6e + 1 = 0$
b	$\frac{1}{7843}\begin{pmatrix} -208660e^{11} - 118345e^{10} + 606681e^9 + 844271e^8 \\ -2044930e^7 - 126154e^6 + 712244e^5 + 3124663e^4 \\ -5460349e^3 + 4188689e^2 - 1329972e + 272478 \end{pmatrix}$
c	$\frac{1}{7843}\begin{pmatrix} 55805e^{11} + 25237e^{10} - 174599e^9 - 227269e^8 \\ +578726e^7 + 22958e^6 - 227941e^5 - 894570e^4 \\ +1575065e^3 - 1231382e^2 + 392162e - 82582 \end{pmatrix}$

Group	$\mathbf{Z}/3\mathbf{Z} \oplus \mathbf{Z}/18\mathbf{Z}$
j	8000
Field	$e^{12} - 4e^{11} + 12e^{10} - 24e^9 + 38e^8 - 50e^7$ $+52e^6 - 48e^5 + 36e^4 - 24e^3 + 15e^2 - 6e + 3 = 0$
b	$\frac{1}{53}\begin{pmatrix} -262e^{11} + 1376e^{10} - 4458e^9 + 10137e^8 - 17241e^7 + 23682e^6 \\ -25526e^5 + 22112e^4 - 14766e^3 + 6941e^2 - 2382e + 151 \end{pmatrix}$
c	$\frac{1}{53}\begin{pmatrix} 131e^{11} - 476e^{10} + 1328e^9 - 2339e^8 + 3188e^7 - 3414e^6 \\ +2481e^5 - 1304e^4 + 69e^3 + 319e^2 - 293e + 110 \end{pmatrix}$

Group	$\mathbf{Z}/3\mathbf{Z} \oplus \mathbf{Z}/21\mathbf{Z}$
j	0
Field	$e^{12} - 6e^{11} + 18e^{10} - 35e^9 + 54e^8 - 72e^7$ $+84e^6 - 81e^5 + 66e^4 - 44e^3 + 21e^2 - 6e + 1 = 0$
b	$\frac{1}{49}\begin{pmatrix} -4894e^{11} + 30046e^{10} - 87461e^9 + 154268e^8 \\ -201926e^7 + 235109e^6 - 256228e^5 + 214939e^4 \\ -117237e^3 + 38057e^2 - 7246e + 352 \end{pmatrix}$
c	$\frac{1}{49}\begin{pmatrix} 290e^{11} - 1742e^{10} + 4986e^9 - 8686e^8 + 11366e^7 - 13286e^6 \\ +14434e^5 - 12010e^4 + 6618e^3 - 2248e^2 + 458e - 41 \end{pmatrix}$

https://doi.org/10.1112/S1461157014000072 Published online by Cambridge University Press

Group, Field	$\mathbf{Z}/7\mathbf{Z} \oplus \mathbf{Z}/7\mathbf{Z}, \mathbf{Q}(\zeta_{21})$
(j, b, c)	$(0, \zeta_3, -1)$

4.13. *K is a number field of degree* 13

$$E(K)[\text{tors}] \in \{0, \mathbf{Z}/2\mathbf{Z}, \mathbf{Z}/3\mathbf{Z}, \mathbf{Z}/4\mathbf{Z}, \mathbf{Z}/6\mathbf{Z}, \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/2\mathbf{Z}\}.$$

No subgroups occur in degree 13 which do not occur over $\mathbf{Q}$.

Acknowledgements. This work was begun during a VIGRE research group led by Pete L. Clark and Patrick Corn and attended by Brian Cook, Steve Lane, Alex Rice, James Stankewicz, Nathan Walters, Stephen Winburn and Ben Wyser at the University of Georgia. Special thanks go to Jon Carlson, who offered use of his MAGMA server and invaluable support with coding in MAGMA. Thanks to Bianca Viray for a helpful discussion of the proof of Lemma 2.3. Thanks also go to Andrew Sutherland, whose interest in this project demanded that this paper be polished into publishable form.

References

1. S. Bosch, W. Lütkebohmert and M. Raynaud, *Néron models*, Ergeb. Math. Grenzgeb. (3) 21 (Springer, Berlin, 1990).
2. W. Bosma, J. Cannon and C. Playoust, 'The magma algebra system I: The user language', *J. Symbolic Comput.* 24 (1997) 3–4.
3. P. L. Clark, B. Cook and J. Stankewicz, 'Torsion points on elliptic curves with complex multiplication (with an appendix by Alex Rice)', *Int. J. Number Theory* 9 (2013) no. 2, 447–479.
4. D. Cox, *Primes of the form $x^2 + ny^2$: Fermat, class field theory and complex multiplication* (John Wiley & Sons, New York, 1989).
5. G. Fung, H. Ströher, H. Williams and H. Zimmer, 'Torsion groups of elliptic curves with integral j-invariant over pure cubic fields', *J. Number Theory* 36 (1990) 12–45.
6. B. Grenet, P. Koiran and N. Portier, 'The multivariate resultant is NP-hard in any characteristic', *Mathematical foundations of computer science*, Lecture Notes in Computer Science 6281 (Springer, Berlin, 2010) 477–488.
7. H. Heilbronn, 'On the class number in imaginary quadratic fields', *Q. J. Math.* 25 (1934) 150–160.
8. S. Kamienny, 'Torsion points on elliptic curves over all quadratic fields', *Duke Math. J.* 53 (1986) no. 1, 157–162.
9. S. Kamienny, 'Torsion points on elliptic curves and q-coefficients of modular forms', *Invent. Math.* 109 (1992) no. 2, 221–229.
10. M. A. Kenku and F. Momose, 'Torsion points on elliptic curves defined over quadratic fields', *Nagoya Math. J.* 109 (1988) 125–149.
11. D. S. Kubert, 'Universal bounds on the torsion of elliptic curves', *Proc. Lond. Math. Soc.* 33 (1976) no. 3, 193–237.
12. S. Lang, *Number theory III diophantine geometry*, Encyclopaedia of Mathematical Sciences 60 (Springer, Berlin, 1991).
13. B. Mazur, 'Modular elliptic curves and the Eisenstein ideal', *Publ. Math. Inst. Hautes Études Sci.* 47 (1977) 33–168.
14. L. Merel, 'Bornes pour la torsion des courbes elliptiques sur les corps de nombres', *Invent. Math.* 124 (1996) 437–449.
15. J. Milne, Class field theory, Version 4, http://jmilne.org/math/.
16. H. Müller, H. Ströher and H. Zimmer, 'Torsion groups of elliptic curves with integral j-invariant over quadratic fields', *J. Reine Angew. Math.* 397 (1989) 100–161.
17. L. Olson, 'Points of finite order on elliptic curves with complex multiplication', *Manuscripta Math.* 14 (1974) 195–205.
18. J. L. Parish, 'Rational torsion in complex-multiplication elliptic curves', *J. Number Theory* 33 (1989) 257–265.
19. A. Petho, T. Weis and H. Zimmer, 'Torsion groups of elliptic curves with integral j-invariant over general cubic number fields', *Int. J. Algebra Comput.* 7 (1997) 353–413.
20. D. Prasad and C. S. Yogananda, 'Bounding the torsion in CM elliptic curves', *C. R. Math. Acad. Sci. Soc. R. Can.* 23 (2001) 1–5.

21. R. Schoof, 'Counting points on elliptic curves over finite fields', *J. Théor. Nombres Bordeaux* 7 (1995) no. 1, 219–254.
22. A. Silverberg, 'Torsion points on abelian varieties of CM-type', *Compositio Math.* 68 (1988) no. 3, 241–249.
23. J. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics 106 (Springer, Berlin, 1986).
24. J. Silverman, *Advanced topics in the arithmetic of elliptic curves*, Graduate Texts in Mathematics 151 (Springer, Berlin, 1994).
25. A. Sutherland, 'Constructing elliptic curves over finite fields with prescribed torsion', *Math. Comp.* 81 (2012) 1131–1147.
26. M. Watkins, 'Class numbers of imaginary quadratic fields', *Math. Comp.* 73 (2004) no. 246, 907–938.

Pete L. Clark
University of Georgia
Athens 30602
USA
plclark@gmail.com

Patrick Corn
Virtu Financial
Austin 78746
USA
patrickcorn@gmail.com

Alex Rice
Bucknell University
Lewisburg 17837
USA
arice2386@gmail.com

James Stankewicz
University of Copenhagen
DK-2100 Copenhagen
Denmark
stankewicz@gmail.com

https://doi.org/10.1112/S1461157014000072 Published online by Cambridge University Press