arXiv:1307.6174v1 [math.NT] 23 Jul 2013

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 $E(K)[\text{tors}]$ 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, M. Watkins [Wat04] has enumerated all imaginary quadratic fields with class number $h \leq 100$, which would in theory allow us to run our algorithm for all $d \leq 201$ (and for infinitely many other values of d, for instance all prime values).

We implemented our algorithm using the MAGMA programming language 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 $1 \leq d \leq 13$. This list, for each degree d, is described in Section $4.d$.

For $d = 1$ these computations were first done by L. Olson in 1974 [Ols74], whereas for $d = 2$ and 3 they are a special case of work of H. Zimmer and his collaborators over a ten year period from the late 1980s to the late 1990s [MSZ89], [FSWZ90], [PWZ97]. We believe that our results are new for $4 \leq d \leq 13$.

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. Alex Rice, James Stankewicz, Nathan Walters and Ben Wyser 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. Special thanks go to Jon Carlson, who offered use of his MAGMA server and invaluable support with coding in MAGMA. Thanks also go to Andrew Sutherland, whose interest in this project demanded that this paper be polished into publishable form.

Date: July 24, 2013.

1.2. **Connections to prior work.** According to the celebrated **uniform boundedness theorem** of L. Merel [Mer96], 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, B. Mazur proved uniform boundedness for $d = 1$ (i.e., for elliptic curves $E_{/\mathbf{Q}}$) [Maz77]. Moreover, Mazur gave a complete classification of the possible torsion subgroups:

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

Work of Kamienny [Kam86], [Kam92] and of Kenku and Momose [KM88] gives the following result when K is a quadratic number field:

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

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 [MSZ89], Müller, Stroher and Zimmer proved that in the case of integral j-invariant, if K is a quadratic number field then

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

In [PWZ97] Pethö, Weis and Zimmer showed that if E has integral j-invariant and K is a cubic number field then

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

Here we study elliptic curves with complex multiplication. Such curves form a subclass of curves with integral j-invariant [Sil94, Theorem. II.6.4], so our results are subsumed by the above results for $d \leq 3$; 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 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 $N \geq 4$).

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. See for instance [MSZ89], §3. □

We will call the equation (1) the *Kubert normal form* of E, and our notation for a curve in Kubert 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 normal forms, depending on which torsion point we choose to send to $(0,0)$.

2.2. **Modular curves.** The affine modular curve $Y_1(N)$ for $N \geq 4$ 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 $N \geq 4$; that is, points over various number fields which correspond to CM elliptic curves with an N-torsion point(the $Y_1(N)$ for $1 \leq N \leq 3$ are coarse moduli spaces and so will only give us the information we desire over an algebraically closed field). Kubert normal form gives a down-to-earth way of constructing a defining equation for $Y_1(N)$, namely: consider b and c as arbitrary unknowns, and impose the condition that $(0,0)$ is an N-torsion point on $E(b,c)$. This gives a polynomial equation $f_N(b,c) = 0$ that b and c must satisfy. We consider three small examples.

Example 1. : $N = 4$. On $E(b,c)$ we have

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

and so the condition that the origin is a 4-torsion point is that $c = 0$. We could also have noted that $2(0,0) = (b, bc)$, which is a 2-torsion point if and only if $bc = 0$.

Example 2. : $N = 5$. On $E(b,c)$ we have

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

and so the condition that the origin is a 5-torsion point is that $b - c = 0$. We could also have set $2(0,0) = (b, bc)$ equal to $-3(0,0) = (c, c^2)$.

Example 3. : $N = 7$. Set $A = b - c - c^2$. On $E(b,c)$ we have

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

and so the condition that the origin is a 7-torsion point is that $b^2 - bc - c^3 = 0$. We could also have set $4(0,0) = \left(\frac{b(b-c)}{c^2}, \frac{b^2(c^2+c-b)}{c^3} \right)$ equal to $-3(0,0) = (c, c^2)$.

The increasing complexity of the expressions in the examples illustrates the fact that computing this elliptic curve addition, and thus the set of defining polynomials $f_N(b,c)$, becomes a computational bottleneck as N increases.

In general, $(0,0)$ will be an N-torsion point if and only if $\lfloor (N-1)/2 \rfloor (0,0)$ and $-\lceil (N+1)/2 \rceil (0,0)$ are equal. When N is odd, it suffices to compare x-coordinates of these points, as it is impossible that $\lceil (N+1)/2 \rceil (0,0) = \lfloor (N-1)/2 \rfloor (0,0)$. When N is even but not equal to 2, we can either check the x-coordinates or set the y-coordinate of $(N/2)(0,0)$ equal to 0.

It should be noted that even for $N \geq 4$ the equation $f_N(b,c) = 0$ is not the defining equation for $Y_1(N)$ as $[N]P = 0$ implies only that P is a torsion point of order d for some $d|N$. However a simple Moebius 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 Andrew Sutherland [Sut12].

Example 4. : 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. We have null conditions $0 = 0$ for both 1 and 2 while $f_3(b,c) = b$. Thus by Möbius inversion, the equation for $Y_1(6)$ in the (b,c)-plane is $b - c - c^2$. The zero set of this equation will be smooth. For higher N, $Y_1(N)$ is not naturally a plane curve and so there will often be singularities in this plane model.

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 (see e.g. [Cox89]).

Theorem 2.2. *(Heilbronn, 1934)* [Hei34] *For any positive integer d, there are only finitely many imaginary quadratic fields with class number d.*

Corollary 2.3. *For any positive integer d, there are only finitely many imaginary quadratic orders $\mathcal{O}$ such that $h(\mathcal{O}) \leq d$.*

Proof. Suppose $\mathcal{O}$ is an order of conductor f in an imaginary quadratic field K of discriminant D_0. Then Gauss's class number formula [Cox89, Thm 7.24] relates $h(\mathcal{O})$ to $h(K) = h(\mathcal{O}_K)$ where $\mathcal{O}_K$ is the ring of integers of K:

$$h(\mathcal{O}) = h(K) f \frac{w(\mathcal{O})}{w(\mathcal{O}_K)} \prod_{p|f} \left(1 - \frac{1}{p}\left(\frac{D_0}{p}\right)\right), \tag{3}$$

where $w(R)$ denotes the number of roots of unity in the ring R (always 2, 4, or 6 in our situation), the product is taken over primes p dividing the conductor, and $\left(\frac{D_0}{p}\right)$ denotes the Kronecker symbol. The right side of (3) is at least $h(K)\varphi(f)/3$, where $\varphi(f)$ denotes the Euler φ function. So if $h(\mathcal{O}) \leq d$, we have $h(K)\varphi(f)/3 \leq d$, which implies that $\varphi(f) \leq 3d$ and $h(K) \leq 3d$. The lists of f and K satisfying these inequalities are finite (the latter by Heilbronn's theorem) and all $\mathcal{O}$ are of the form $\mathbf{Z} + f\mathcal{O}_K$, so the result follows. □

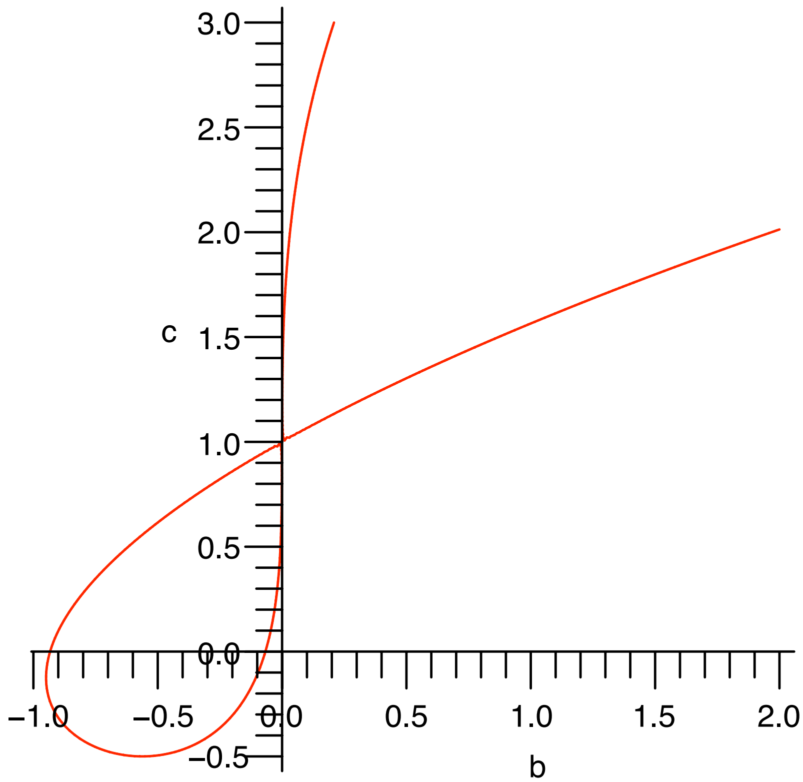

FIGURE 1. The real (b, c) such that $E(b, c)$ has j-invariant 0.

Example 5. : Suppose we wanted to 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

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

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

$$b^2 - bc - c^3 = 0. \tag{5}$$

The real solutions to Equation 4 in the (b, c) affine plane may be seen in Figure 1, and Equation 5 in Figure 2.

The resultant of these two polynomials with respect to c is

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

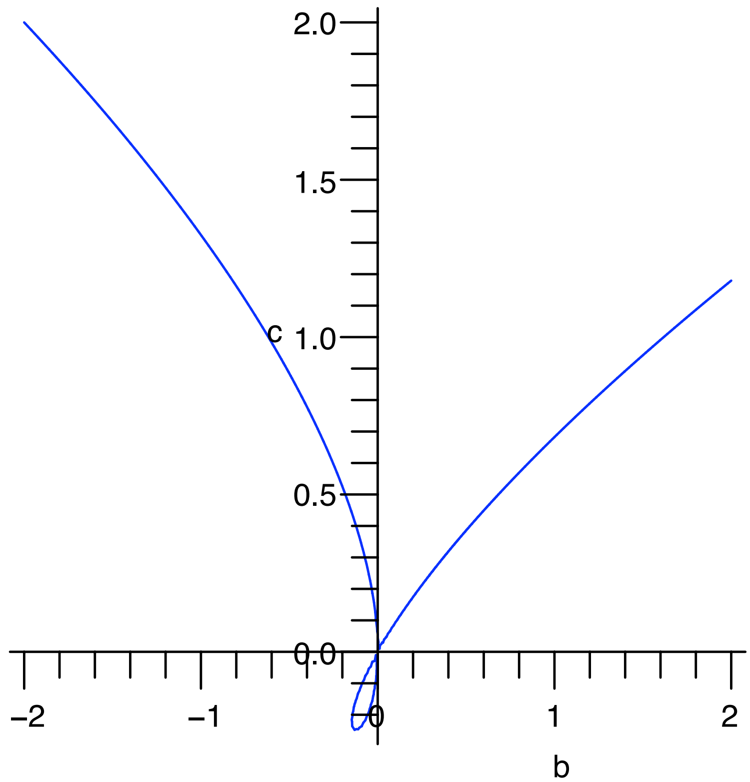

FIGURE 2. The real (b, c) such that $(0, 0)$ is a 7-torsion point on $E(b, c)$.

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

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

the point $(0, 0)$ is a 7-torsion point.[1] Moreover, this curve acquires full 7-torsion over the degree-12 cyclotomic field $\mathbf{Q}(\zeta_{21})$. A result of E. Halberstadt cited in [MS01] shows that if *any* elliptic curve (CM or otherwise) E has full 7-torsion over

[1]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 $y^2 = x^3 - (1296\zeta_3 + 6480)$.

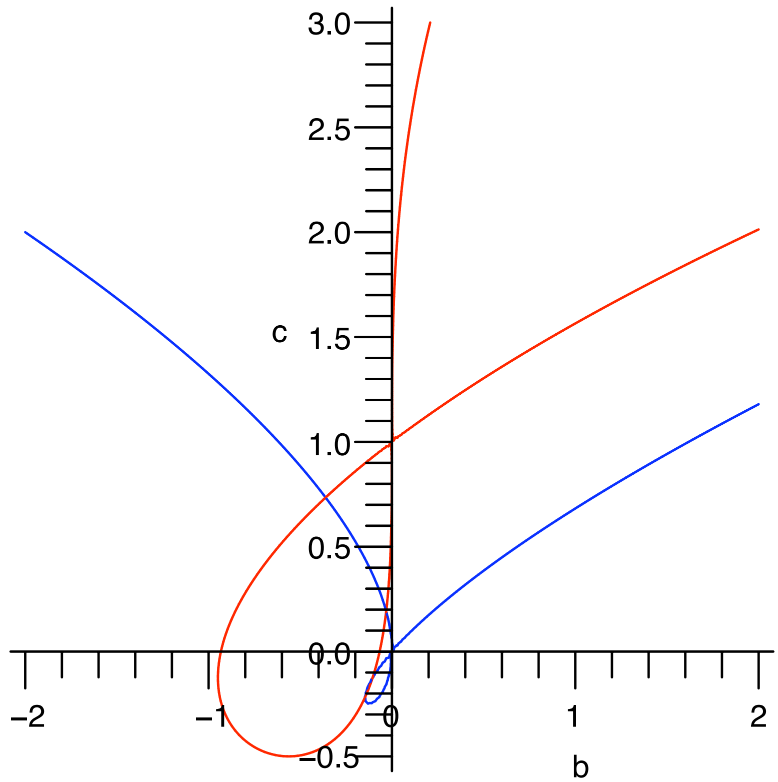

FIGURE 3. The real (b, c) such that $(0, 0)$ is a 7-torsion point on $E(b, c)$ with j-invariant 0.

a number field K, then K strictly contains $\mathbf{Q}(\mu_7)$, and hence has $[K : \mathbf{Q}] \geq 12$. Thus our example of full 7-torsion attains the least possible number field degree.

We generalize the above construction as follows: Writing $j(b, c) = \dfrac{n_j(b, c)}{d_j(b, c)}$ as the quotient of two polynomials, we see that there is an elliptic curve $E(b, c)$ with j-invariant j_0 and an N-torsion point if and only if (b, c) satisfy the equations

$$n_j(b, c) = j_0 d_j(b, c) \qquad (6)$$
$$f_N(b, c) = 0.$$

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 n-th *division polynomial* [Sil86, 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 n-th 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 Complex Multiplication 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 theorems of Silverberg and Prasad-Yogananda can be used to give an explicit upper bound on N.

Theorem 2.4. *(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 e be the exponent of the torsion subgroup of $E(F)$. Then*

(a) $\varphi(e) \leq w(\mathcal{O})d$
(b) If $K \subseteq F$, then $\varphi(e) \leq w(\mathcal{O})d/2$
(c) If $K \not\subseteq F$, then $\varphi(\#E(F)[\mathrm{tors}]) \leq w(\mathcal{O})d$.

Proof. See [Sbg88], [PY01]. 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 as the *SPY bounds*. Using merely the bound of part (a) and the well-known inequality $\sqrt{N} \leq \phi(N)$ for $N \geq 7$, 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 order of a torsion point on an elliptic curve E over a number field F trivially gives a bound on the size of the torsion subgroup. Namely, if every torsion point in $E(F)$ has order at most N then since $E(\mathbf{C})[\mathrm{tors}] \cong (\mathbf{Q}/\mathbf{Z})^2$ [Sil86, Corollary V.1.1], we have $\#E(F)[\mathrm{tors}] \leq N^2$. 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 [Sil86, §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 $d = h(\mathcal{O})\deg$. The strengthening of the SPY bounds as noted in the proof of Theorem 2.4 implies that if e is the exponent of $E(F)[\mathrm{tors}]$ then $\varphi(e) \leq w(\mathcal{O})\deg$. Note also that if deg is odd then it cannot be that $K \subset F$ and so $\varphi(\#E(F)[\mathrm{tors}]) \leq w(\mathcal{O})\deg$.

If $\deg = 2$ then we may assume that $j \neq 0, 1728$ because the possible groups in that case have already been determined [MSZ89]. Thus $w(\mathcal{O}) = 2$, hence either $E(F)[\mathrm{tors}]$ is among the 12 possible torsion subgroups G such that $\varphi(G) \leq 4$ or F

is the compositum of $\mathbf{Q}(j(E))$ with K, otherwise known as the ring class field of $\mathcal{O}$. In the latter case, we have the following.

Theorem 2.5. *(Parish) Let $\mathcal{O}$ be an imaginary quadratic order, j the j-invariant of an elliptic curve with CM by $\mathcal{O}$, $L = \mathbf{Q}(j)$ and K the ring class field of $\mathcal{O}$. Then if E is an elliptic curve defined over K with CM by $\mathcal{O}$ then $E(K)[\mathrm{tors}]$ 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. [Par89, §VI]. □

Much finer information is available within the actual paper of Parish. Except for $j = 0$ and $\mathbf{Z}/3\mathbf{Z} \oplus \mathbf{Z}/3\mathbf{Z}$, each torsion subgroup G which is possible over a ring class field has $\varphi(\#G) \leq 4$. 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. Finally we note that although we can only say that if $E(F)[\mathrm{tors}] \cong \mathbf{Z}/N\mathbf{Z} \oplus \mathbf{Z}/n\mathbf{Z}$ with $n \mid N$ then $\varphi(n) \mid d$, not deg. We can however determine exactly the intersection of $\mathbf{Q}(\zeta_n)$ with $\mathbf{Q}(j(\mathcal{O}))$.

Consider first that if H denotes the ring class field of $\mathcal{O}$, then the maximal abelian sub-extension G of H over $\mathbf{Q}$ is necessarily multi-quadratic [Cox89, §6]. So too must be G', the intersection of $\mathbf{Q}(j(\mathcal{O}))$ with G. Since any abelian extension must be contained in some $\mathbf{Q}(\zeta_m)$ [Cox89, 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 the theory of conductors of abelian extensions tells us that $K \subset \mathbf{Q}(\zeta_n)$ if and only if $\Delta \mid n$ [Mil08, Example V.3.11]. Finally, it is an easy exercise to determine inductively that if M is a multi-quadratic field extension of degree 2^m, then the number of quadratic sub-extensions is $2^m - 1$.

Function 2.6. *(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 multi-quadratic 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 for which it is possible that $E(F)[\mathrm{tors}] \cong G$.

Function 2.7. *(PossibleGroups) Let d be the degree in question, $\mathcal{O}$ 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 $\deg = \dfrac{d}{h}$.*
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* $\varphi(Nn) \leq 4$.
(4) *If* $\deg > 1$ *is odd then remove* $\mathbf{Z}/N\mathbf{Z} \oplus \mathbf{Z}/n\mathbf{Z}$ *from* L' *unless* $\varphi(Nn) \leq w(\mathcal{O}) \deg$ *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* $\varphi(n) \mid \deg \times \mathsf{CyclotomicIntersectionDegree}(\mathcal{O}, n)$ *(Function 2.6).*
(6) *Return* L'.

In Function 2.7, you will of course get 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, $\varphi(N) \leq \frac{w(\mathcal{O})d}{h(\mathcal{O})} = w(\mathcal{O}) \deg$ by the SPY bounds. We also have another tool for ruling out possible orders of torsion.

Theorem 2.8. *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* $\left(\frac{\cdot}{p}\right)$ *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.*

- *If* $\left(\frac{D}{p}\right) = 1$ *then* $(p-1)h(\mathcal{O}_K) \mid 2dw(\mathcal{O}_K)$.
- *If* $\left(\frac{D}{p}\right) = -1$ *then* $(p^2-1)h(\mathcal{O}_K) \mid 2dw(\mathcal{O}_K)$.

Proof. This was directly proven for $D = D_0$ [CCS13, Theorem 2], and can be extended to the case $p \nmid D$ [CCS13, 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 torsion exponents. For $j = 0$, performing the above procedure takes $\frac{1}{100}$ 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 2.9. *(*$\mathsf{PossibleExponents}$*) 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* $\varphi(N) \leq w(\mathcal{O}) \deg$.
(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 2.8 for* $d = h(\mathcal{O}) \deg$.
(3) *Return* L'.

Note however that this list is still far too large a list to use in Function 2.7. We apply a sieve to this list, using resultants as in Example 5, 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

$\frac{3}{100}$ of one second. 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 69.95 seconds 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 2.10. *(SievedTorsion) Let $\mathcal{O}$ be an imaginary quadratic order and let* $\deg$ *be a positive integer.*

1. *Let $L = \mathsf{PossibleExponents}(\mathcal{O}, \deg)$. (Function 2.9)*
2. *For $N \in \mathsf{PossibleExponents}(\mathcal{O}, \deg)$ such that $N \in L$ and $N \geq 4$:*
   - *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 $\mathcal{O}$.*
   - *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 [GKP10]. 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.

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 6. 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 number field F with CM by $\mathbf{Z}[\zeta_4]$ has a rational 2-torsion point for trivial reasons. 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 5, base extend each of these elliptic curves by roots of their n-th division polynomials and then compute the torsion subgroups of all those elliptic curves. For running time reasons however, 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 [Sch95]. The problem with the method of reduction is that it is significantly more difficult over non-integral extensions, as is often the case with the number fields generated by irreducible factors of our Kubert resultants. 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 2.7. 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 $\mathbf{Q}(\zeta_n) \subset L$. Numerically 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 can not base extend F to L and obtain $E(L)[\text{tors}] \cong G$. Moreover, we have ruled this out without computing any torsion on E.

Example 7. Let $\mathcal{O} = \mathbf{Z}\left[\dfrac{1+3\sqrt{-11}}{2}\right]$, 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.

We now describe the procedure for saying that a group G which could have been produced by Functions 2.9 and 2.7 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 either 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 that resultant 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.*
(3) *If $c_i \notin F_i$ then raise an error.*
(4) *If $[F_i : \mathbf{Q}] \mid d$ then compute the compositum of F_i with $\mathbf{Q}(\zeta_n)$ and let d_i be its degree over $\mathbf{Q}$.*
(5) *If $d_i \mid d$ then let T_i be the torsion subgroup of $E(b_i,c_i)$.*
(6) *If $T_i \cong G$ then Return* False, *$E(b_i, c_imaginaryquadraticorderi)$.*
(7) *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.*
(8) *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 n-th division polynomial of $E(b_i,c_i)$, perform Moebius inversion to obtain a polynomial whose roots are x-coordinates of points of exact order n, and factor that polynomial as $\prod_{j=1}^{m} p_j$.*
(9) *If $Degree(p_j) \mid \frac{d}{[F_i : \mathbf{Q}]}$ then let $L_{i,j}$ be the number field given by p_j, generated over F_i by the x-coordinate a_j. Let $g = y^2 + (a_j(1-c_i)-b_i)y + (b_ia_j^2 - a_j^3)$, 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 $e_j = Degree(p_j)\frac{2}{n_g}$.*
(10) *If $e_j \neq 1$ and $e_j \mid \frac{d}{[F_i : \mathbf{Q}]}$ 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 $M_{i,j}$.*
(11) *If $T_{i,j} \cong G$ then Return* False, *$E(b_i,c_i)_{M_{i,j}}$.*
(12) *If for all i and j any of the "If ..."' statements which begin Steps (2)-(11) are false, then Return* True.

We note that in Step 3.1(3), it is possible that $c_i \notin F_i$ and thus it is necessary to 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 $G \in R$.*
   - *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 seconds 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 hours to complete for a total time of roughly 14 hours. 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:

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

Examples of these are:

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

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

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

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:

$$\left\{ \begin{array}{c} \text{Group: } \mathbf{Z}/5\mathbf{Z} \\ j\text{-invariant} = -32768 \\ b^4 - 4b^3 + 46b^2 + 4b + 1 = 0 \\ E(b,b) \end{array} \right\} \left\{ \begin{array}{c} \text{Group: } \mathbf{Z}/8\mathbf{Z} \\ j\text{-invariant} = 1728 \\ b^4 + 2b^3 + b^2 - b - 1/8 = 0 \\ E\left(b, \frac{8b^3+36b^2+46b+3}{13}\right) \end{array} \right\}$$

$$\left\{ \begin{array}{c} \text{Group: } \mathbf{Z}/12\mathbf{Z} \\ j\text{-invariant} = 0 \\ b^4 - 10b^3 + 24b^2 - 16b - 2 = 0 \\ E\left(b, \frac{-6b^3+52b^2-70b-9}{7}\right) \end{array} \right\} \left\{ \begin{array}{c} \text{Group: } \mathbf{Z}/13\mathbf{Z} \\ j\text{-invariant} = 0 \\ b^4 + 4b^3 + 78b^2 + 13b + 1 = 0 \\ E\left(b, \frac{16b^3+44b^2+1354b+45}{483}\right) \end{array} \right\}$$

$$\left\{ \begin{array}{c} \text{Group: } \mathbf{Z}/21\mathbf{Z} \\ j\text{-invariant} = 0 \\ b^4 - b^3 + 720b^2 + 140b + 7 = 0 \\ E\left(b, \frac{278b^3+408b^2+190606b+11467}{66725}\right) \end{array} \right\}$$

$$\left\{ \begin{array}{c} \text{Group: } \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/8\mathbf{Z} \\ j\text{-invariant} = 287496 \\ b^4 - 4b^3 + 4b^2 - b - 1/8 = 0 \\ E\left(b, 32b^3 - 108b^2 + 58b + 6\right) \end{array} \right\}$$

$$\left\{\begin{array}{c}\text{Group: } \mathbf{Z}/2\mathbf{Z}\oplus\mathbf{Z}/10\mathbf{Z}\\ j\text{-invariant} = 1728\\ b^4 - 2/25b^3 + 36/625b^2 + 14/625b + 1/625 = 0\\ E\left(b, \dfrac{-1250b^3 - 4025b^2 - 322b - 48}{401}\right)\end{array}\right\}$$

$$\left\{\begin{array}{c}\text{Group: } \mathbf{Z}/4\mathbf{Z}\oplus\mathbf{Z}/4\mathbf{Z}\\ j\text{-invariant} = 1728\\ x^4 + 4x^3 + 12x^2 + 16x + 8 = 0\\ E(-1/8, 0)\end{array}\right\} \left\{\begin{array}{c}\text{Group: } \mathbf{Z}/3\mathbf{Z}\oplus\mathbf{Z}/6\mathbf{Z}\\ j\text{-invariant} = 1728\\ \mathbf{Q}(\sqrt{3}, \sqrt{-3})\\ E\left(\dfrac{6\sqrt{3}+10}{3}, \dfrac{2\sqrt{3}+3}{3}\right)\end{array}\right\}$$

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 $\mathbf{Z}/11\mathbf{Z}$.
An example of this is:

$$\left\{\begin{array}{c}\text{Group: } \mathbf{Z}/11\mathbf{Z}\\ j\text{-invariant} = -32768\\ \text{Defining Polynomial: } b^5 + 45b^4 - 433b^3 - 289b^2 - 8b + 1 = 0\\ b = b\\ c = \dfrac{2950b^4 + 119306b^3 - 1856634b^2 + 5957524b + 289453}{2186207}\end{array}\right\}$$

4.6. K is a number field of degree 6.

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

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:

$$\left\{\begin{array}{c}\text{Group: } \mathbf{Z}/18\mathbf{Z}\\ j\text{-invariant} = 8000\\ \text{Defining Polynomial: } b^6 - 18b^5 + 155b^4\\ -118b^3 + 3240b^2 + 540b + 27 = 0\\ b = b\\ c = \dfrac{1}{6690435237}(2005172b^5 - 37017075b^4\end{array}\right.$$

$$\left\{\begin{array}{c}\text{Group: } \mathbf{Z}/19\mathbf{Z}\\ j\text{-invariant} = 0\\ \text{Defining Polynomial: } b^6+4b^5+41b^4+93b^3+84b^2+17b+1=0\\ b=b\\ c=\dfrac{106b^5+354b^4+4192b^3+7386b^2+5394b+277}{1661}\end{array}\right\}$$

$$\left\{\begin{array}{c}\text{Group: } \mathbf{Z}/26\mathbf{Z}\\ j\text{-invariant} = 8000\\ \text{Defining Polynomial: } b^6+18b^5+1078/13b^4\\ +1628/169b^3+51/169b^2+12/169b+1/169=0\\ b=b\\ c=\dfrac{1}{16999170731}(-3574272936b^5-61352538637b^4-242840154310b^3\\ +2175443419890b^2+85260813745b+4153994255)\end{array}\right\}$$

$$\left\{\begin{array}{c}\text{Group: } \mathbf{Z}/2\mathbf{Z}\oplus\mathbf{Z}/14\mathbf{Z}\\ j\text{-invariant} = 0\\ \text{Defining Polynomial: } b^6-3/7b^5+76/49b^4+241/2401b^3\\ -2/2401b^2+11/2401b+1/2401=0\\ b=b\\ c=\dfrac{1}{240822191}(14654777214b^5-44780344442b^4\\ +22132816272b^3+39763194140b^2+671793194b+22826125)\end{array}\right\}$$

$$\left\{\begin{array}{c}\text{Group: } \mathbf{Z}/3\mathbf{Z}\oplus\mathbf{Z}/6\mathbf{Z}\\ j\text{-invariant} = 0\\ \mathbf{Q}(\zeta_3,\sqrt[3]{-16})\\ y^2=x^3+16\end{array}\right\}\left\{\begin{array}{c}\text{Group: } \mathbf{Z}/6\mathbf{Z}\oplus\mathbf{Z}/6\mathbf{Z}\\ j\text{-invariant} = 0\\ \mathbf{Q}(\zeta_3,\sqrt[3]{4})\\ y^2=x^3+1\end{array}\right\}$$

$$\left\{\begin{array}{c}\text{Group: } \mathbf{Z}/3\mathbf{Z}\oplus\mathbf{Z}/9\mathbf{Z}\\ j\text{-invariant} = 0\\ \text{Defining Polynomial: } e^6-240e^5+24480e^4+43008e^3=0\\ +161280e^2+138240e+36864\\ b=\dfrac{1}{228063362304}(-7122425e^5+1540074952e^4-133555802100e^3\\ -4491274738608e^2-4300732140864e-23964768836352)\\ c=\dfrac{1}{228063362304}(1120153e^5-242209498e^4+21004489720e^3\\ +706348450176e^2+676381575168e+3739330026240)\end{array}\right\}$$

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.**

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

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

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

Examples of these are:

$$\left\{ \begin{array}{c} \text{Group: } \mathbf{Z}/15\mathbf{Z}, j\text{-invariant} = 0 \\ b^8 - 3885b^7 - 19310b^6 - 64710b^5 - 51750b^4 \\ -11145b^3 - 1220b^2 - 105b - 5 = 0 \\ c = \dfrac{1}{1151465798079233560499}(-2622158686607063300b^7 \\ +10187004772362629052294b^6 + 50951280435831207398930b^5 \\ +171669236426437124358532b^4 + 142823105844501090588204b^3 \\ +39643541419352999254762b^2 + 7201271716620470774476b \\ +321466513000389488499 \end{array} \right\}$$

$$\left\{ \begin{array}{c} \text{Group: } \mathbf{Z}/16\mathbf{Z}, j\text{-invariant} = 16581375 \\ b^8 + 3260b^7 + 8330333/2b^6 + 6346355/2b^5 \\ +10881927/16b^4 + 223373/8b^3 + 1167/16b^2 - 33/4b + 1/16 = 0 \\ c = \dfrac{1}{20364051589748112932784162322891} \\ (-1380972216163088849084444101232b^7 \\ -4501983073403419125822314505121296b^6 \\ -5752023707864878488387072177532768376b^5 \\ -4438921961643506448798670413717173560b^4 \\ -986165562775714115774914190811460269b^3 \\ -49535192212526996086155989461414039b^2 \\ -617005402241097222854953818586588b \\ +5498482966401242482822007385155) \end{array} \right\}$$

$$\left\{\begin{array}{c}\text{Group: } \mathbf{Z}/20\mathbf{Z}, j\text{-invariant} = 287496\\ b^8 - 96b^7 + 105876b^6 + 9256b^5\\ -1458b^4 - 1064b^3 - 12b^2 + 16b + 1 = 0\\ c = \dfrac{1}{529549704362297372}(-446835896417894454b^7\\ +428253847418114920 5b^6 - 4730240434712834269946b^5\\ -1163749950381195092223b^4 - 1027446073587445756 18b^3\\ +3101302951900789635 1b^2 + 4980463275862769234b\\ +776465646841575723)\end{array}\right\}$$

$$\left\{\begin{array}{c}\text{Group: } \mathbf{Z}/30\mathbf{Z}\\ j^2 + 191025j - 121287375 = 0\\ b^4 + 1/85995(-184j - 3385125)b^3 + 1/1911(85j + 765990)b^2\\ +1/17199(101j + 1262250)b + 1/5733(j + 23850) = 0\\ c = \frac{1}{433507834636695}(11480779j + 2221696301211)b^3 +\\ \frac{1}{2167539173183475}(-2707708966j - 477798032638350)b^2\\ +\frac{1}{111155855 03505}(165904016j + 30184998558300)b\\ +\frac{1}{6669351302103}(7772771j + 735896598093)\end{array}\right\}$$

$$\left\{\begin{array}{c}\text{Group: } \mathbf{Z}/34\mathbf{Z}, j\text{-invariant} = 1728\\ b^8 - 6b^7 + 993b^6 + 3504b^5 + 4193b^4 + 1814b^3 + 347b^2 + 30b + 1 = 0\\ c = \frac{1}{534213525451}(1852239032234b^7 - 1152425882383b^6\\ +184185522148670b^5 + 608153529942499b^4\\ +644341944773261b^3 + 198713200484433b^2\\ +233824737700464b + 928368601016)\end{array}\right\}$$

$$\left\{\begin{array}{c}\text{Group: } \mathbf{Z}/39\mathbf{Z}, j\text{-invariant} = 0\\ b^8 + 221b^7 + 15697b^6 + 41459b^5 + 35053b^4\\ +10868b^3 + 2470b^2 + 299b + 13 = 0\\ c = \frac{1}{442956489298127 13}(23319315878322b^7\\ +51860744126038 98b^6 + 3731946908350507 58b^5\\ +1469928104695587720b^4 + 1666344892152873148b^3\\ +688013868510289682b^2 + 214123053773665212b + 11168740478161621)\end{array}\right\}$$

$$\left\{\begin{array}{c}\text{Group: } \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/12\mathbf{Z}, j\text{-invariant} = 54000\\ b^8 - 332b^7 + 27562b^6 - 257048b^5 - 99776b^4\\ -17732b^3 - 1640b^2 - 80b - 2 = 0\\ c = \frac{1}{126284663045 55057}(-2086075449204 17b^7\\ +692300059219008 37b^6 - 5740442117372611734b^5\\ +528577262212953049 06b^4 + 280159271780984240 41b^3\\ +569437469028697346 4b^2 + 586143239945547874b + 23030568229000201)\end{array}\right\}$$

$$\left\{\begin{array}{c}\text{Group: } \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/16\mathbf{Z}, j\text{-invariant} = -3375\\ b^8 - 33b^7 + 761/2b^6 - 235b^5 + 1887/16b^4\\ -249/16b^3 + 3/16b^2 + 15/16b + 1/16 = 0\\ c = \frac{1}{3391572223957}(13721135984 96b^7\\ -451201882256464b^6 + 516808084796400b^5\\ -261195373119408b^4 + 117651088249434b^3\\ +91111734830 31b^2 - 18840755070 31b - 510707725399)\end{array}\right\}$$

$$\left\{\begin{array}{c}\text{Group: } \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/20\mathbf{Z}, j\text{-invariant} = 1728 \\ b^8 + 4b^7 + 78b^6 + 184b^5 + 1468b^4 - 364b^3 - 30b^2 + 12b + 1 = 0 \\ c = \frac{1}{11646981589}(-6537806628b^7 - 2857210090b^6 \\ -52006254231b^5 - 139379704446b^4 - 1008107445440b^3 \\ -127192859836b^2 + 27070327199b + 1645394497)\end{array}\right\}$$

$$\left\{\begin{array}{c}\text{Group: } \mathbf{Z}/6\mathbf{Z} \oplus \mathbf{Z}/6\mathbf{Z}, j\text{-invariant} = -3375 \\ b^8 + 304/3b^7 + 23386/9b^6 + 43099/27b^5 + 183223/81b^4 \\ +252904/243b^3 + 151552/729b^2 + 40960/2187b + 4096/6561 = 0 \\ c = \frac{1}{580519046835}(3033790362b^7 + 306345084723b^6 \\ +7774232461416b^5 + 2082887589060b^4 + 6247887676866b^3 \\ +8414083888787b^2 + 734171627853b + 5726863693)\end{array}\right\}$$

$$\left\{\begin{array}{c}\text{Group: } \mathbf{Z}/4\mathbf{Z} \oplus \mathbf{Z}/8\mathbf{Z}, j\text{-invariant} = -3375 \\ b^8 - 2b^7 + 33b^6 - 16b^5 + 242b^4 - 250b^3 + 33b^2 + 16b + 1 = 0 \\ c = \frac{1}{76109}(4034b^7 - 3909b^6 + 128507b^5 + 68228b^4 \\ +1032986b^3 + 32647b^2 + 88917b + 772)\end{array}\right\}$$

$$\left\{\begin{array}{c}\text{Group: } \mathbf{Z}/4\mathbf{Z} \oplus \mathbf{Z}/12\mathbf{Z}, j\text{-invariant} = 0 \\ e^8 - 80e^7 + 3968e^6 + 1024e^5 + 618496e^4 + 3080192e^3 \\ +20971520e^2 + 33554432e + 16777216 = 0 \\ b = \frac{1}{144713973760}(7319e^7 - 570256e^6 + 27665088e^5 \\ +79469056e^4 + 4023189504e^3 + 26639728640e^2 + 149433352192e \\ +358896107520) \\ c = \frac{1}{506498908160}(188929e^7 - 15333528e^6 \\ +767208576e^5 - 678629888e^4 + 116840288256e^3 + 435409584128e^2 \\ +3373100695552e + 2030901919744)\end{array}\right\}$$

$$\left\{\begin{array}{c}\text{Group: } \mathbf{Z}/5\mathbf{Z} \oplus \mathbf{Z}/10\mathbf{Z} \\ j\text{-invariant} = 1728 \\ \mathbf{Q}(\zeta_{20}) \\ E(\zeta_4, \zeta_4)\end{array}\right\} \left\{\begin{array}{c}\text{Group: } \mathbf{Z}/5\mathbf{Z} \oplus \mathbf{Z}/5\mathbf{Z} \\ j\text{-invariant} = 0 \\ \mathbf{Q}(\zeta_{15}) \\ b = 4\zeta_{15}^7 + 2\zeta_{15}^6 - 2\zeta_{15}^5 - 2\zeta_{15}^3 + 4\zeta_{15} + 1 \\ E(b, b)\end{array}\right\}$$

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 only subgroups which do not occur over $\mathbf{Q}$ or a number field of degree 2 or 4 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:

$$\left\{\begin{array}{c}
\text{Group: } \mathbf{Z}/18\mathbf{Z}, j\text{-invariant} = 54000 \\
b^9 - 6129b^8 - 1031967b^7 - 73855260b^6 - 67586076b^5 \\
-219295335b^4 - 2548827b^3 - 242757b^2 - 21870b - 729 = 0 \\
c = \frac{1}{4700566705551766200818568755582913}(-104272677786239341651108023 65b^8 \\
+63911142667342151180341810555365b^7 \\
+1074577288840661204536119790828 0770b^6 \\
+76761689241133075591648460351648 5833b^5 \\
+526808571618062707377615803323800630b^4 \\
+11415807260156945881402387975522 6785b^3 \\
+1241208897015887543568625469539623b^2 \\
+6551675185726442677026992442950052b \\
+1640253306721348690914689670 92184)
\end{array}\right\}$$

$$\left\{\begin{array}{c}
\text{Group: } \mathbf{Z}/19\mathbf{Z}, j\text{-invariant} = -884736 \\
b^9 + 2098b^8 + 53258b^7 - 6092115b^6 - 666688b^5 \\
+250505b^4 + 38113b^3 + 1174b^2 - 22b - 1 = 0 \\
\frac{1}{8024981626230394861984690088 59}(87840567102881912214725677400b^8 \\
+18428559816916579268336806597 1702b^7 \\
+467000660842902905091029631230 7950b^6 \\
-53534263860780662895036328006723 7356b^5 \\
-34719049512741939369687685988150594b^4 \\
+230935505785055014880194497748780 38b^3 \\
+23665937746252405797882455487110 94b^2 \\
+9730883111938173940240347665510b \\
-216755676138066032180519336363 3)
\end{array}\right\}$$

$$\left\{\begin{array}{c}
\text{Group: } \mathbf{Z}/27\mathbf{Z}, j\text{-invariant} = -12288000 \\
b^9 + 33372b^8 - 2846223b^7 - 191738790b^6 - 161053353b^5 \\
-12447972b^4 + 711576b^3 + 53298b^2 - 243b - 9 = 0 \\
c = \frac{1}{1008016512960749089655899687227835918576479} \\
(1541064083519671913451978574698665610 52b^8 \\
+51428377535639499981432850180928484135563342b^7 \\
-43866478635913659777570839860922836251508 9226b^6 \\
-29544460334692554847838442277019561880827102774b^5 \\
-24568854312917303262398855054694843657759532050b^4 \\
-170173365397527090440068474105640262173869 3398b^3 \\
+1215738991058862035056843143030701138720418 24b^2 \\
+80110831183633951832300027318511690864325 62b \\
-90296221346489638304161689256684711883625)
\end{array}\right\}$$ [2]

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:

[2] The discriminant of the CM order is -27, showing both the sharpness of the SPY bounds and the need to take a close look at torsion exponents which share a common factor with the conductor of the CM order.

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

Examples of these are:

$$\left\{\begin{array}{c}
\text{Group: } \mathbf{Z}/22\mathbf{Z}, j\text{-invariant} = 16581375 \\
b^{10} - 139812b^9 + 4892541392b^8 - 6917407754b^7 - 76009457b^6 \\
+169892375b^5 + 701485b^4 - 106926b^3 + 8600b^2 - 170b + 1 = 0 \\
c = \frac{1}{7059381764517867553704503022959325928200568 1} \\
(2172278713859069649668413658077867890101 21b^9 \\
-3037106047593499198905350591497581193628276671 5b^8 \\
+10627959777969536271934455945607291226165110400321 36b^7 \\
-137161794900220173358775607286874139450106845084907b^6 \\
-1916185955944683354628360393789820525182772771521 7b^5 \\
+32547962058438072095032073032653033295546538336 75b^4 \\
+1828286495211430523695521342970372636147129039 10b^3 \\
-2102670652666517198695248083618581134310959426 7b^2 \\
+1637966229009849894152758115052790065456427251b \\
-1902735262501729400400698023059399423754 1736)
\end{array}\right\}$$

$$\left\{\begin{array}{c}
\text{Group: } \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/22\mathbf{Z}, j\text{-invariant} = -3375 \\
b^{10} + 30b^9 + 428b^8 + 2984b^7 + 10609b^6 + 18057b^5 \\
+12799b^4 + 2256b^3 + 206b^2 + 16b + 1 = 0 \\
c = \frac{1}{47773237776918533}(296246561277605b^9 + 9105144997291383b^8 \\
+13300607755248075 8b^7 + 968142979105142873b^6 \\
+367110296938441419 7b^5 + 691122358643478089 3b^4 \\
+559976489709517814 0b^3 + 129505422445840909 1b^2 \\
+203076703159407429b + 7172139596310456)
\end{array}\right\}$$

$$\left\{\begin{array}{c}
\text{Group: } \mathbf{Z}/31\mathbf{Z}, j\text{-invariant} = 0 \\
b^{10} + 243b^9 + 21455b^8 + 21653b^7 + 1198b^6 - 4704b^5 \\
-788b^4 + 406b^3 + 184b^2 + 24b + 1 = 0 \\
c = \frac{1}{3515614534593596351 75}(67599075460630484448b^9 \\
+16417681834602691685 66b^8 + 1448180726920290594330 08b^7 \\
+12738029833958639004449 4b^6 - 3373994399969735740716b^5 \\
-353966353952666517725 44b^4 - 8793591487595448360268b^3 \\
+18924950400552678272 44b^2 + 14861609552229996085 04b \\
+85553406426150603045)
\end{array}\right\}$$

$$\left\{\begin{array}{c}
\text{Group: } \mathbf{Z}/50\mathbf{Z}, j\text{-invariant} = 1728 \\
b^{10} + 46b^9 + 3542b^8 - 66774b^7 + 1051394b^6 + 512040b^5 \\
+114767b^4 + 14904b^3 + 1132b^2 + 48b + 1 = 0 \\
c = \frac{1}{272453684519138624803522 9}(1294162541175686087137 2b^9 \\
+601519799406047442583816b^8 + 4612365782310225528894820 5b^7 \\
-84223228364489504530189618 7b^6 + 1318883653627892393646161597 3b^5 \\
+132183745221982654166694775 67b^4 + 3593774249373714067761953161b^3 \\
+481666538990471285555799012b^2 + 408420343501108271665263 03b \\
+136814583217092622407154 8)
\end{array}\right\}$$

4.11. K is a number field of degree 11.

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

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:

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

These are:

$$\left\{ \begin{matrix} \text{Group: } \mathbf{Z}/28\mathbf{Z}, j\text{-invariant} = 0 \\ b^{12} - 70b^{11} + 57097b^{10} + 535620b^9 + 12249536b^8 - 1620616b^7 \\ +797507b^6 + 51824b^5 + 1474b^4 + 2106b^3 + 101b^2 + 6b + 1 \\ c = \dfrac{1}{23872024811371775375250598442490604607378999} \\ (532598859471894663495414002329168671018248b^{11} \\ -37301670240967394939678377444762027524378915b^{10} \\ +304111798400011408578110521327600008267440738 01b^9 \\ +284142913880001900431266312351466257193238358436b^8 \\ +65135248828858613904372954804346221070519177180 65b^7 \\ -11048828879769581458737243477293124537466313573 37b^6 \\ +46033735699529158907137261436034600255411550438 8b^5 \\ +21735145782799918126623351073852826131012593736b^4 \\ -911994662602753614197046908573417999647083019b^3 \\ +1496012057510832826800014329365962138290434143b^2 \\ +107163753866698802836035054301456338827977869b \\ -3817873070757765229249893532738434830161217) \end{matrix} \right\}$$

$$\left\{\begin{array}{c}
\text{Group: } \mathbf{Z}/37\mathbf{Z}, j\text{-invariant} = 0 \\
b^{12} - 200b^{11} + 19892b^{10} + 262359b^9 + 1230725b^8 + 1650343b^7 \\
+1275960b^6 + 589648b^5 + 157549b^4 + 22463b^3 + 1659b^2 + 61b + 1 = 0 \\
c = \dfrac{1}{7113247432899470400315281593639904731} \\
(2593020720576323628268339386498298 8b^{11} \\
-5185506991968186437829731227868928038b^{10} \\
+5156967086816481870641190648504587935 98b^9 \\
+6813671361730131865294675391242357884728b^8 \\
+3205147185261588276690937605604478604578 4b^7 \\
+4343410399119861835551195033540078042263 0b^6 \\
+3392250114954124970075311967870128210897 6b^5 \\
+1608905368888114763060242492418986770195 0b^4 \\
+456756277416694278587525342956634982432 6b^3 \\
+759617107899725093883350935947077523682b^2 \\
+84253749070989087833055370323559842168b \\
+3302315937671629475410367894866337823)
\end{array}\right\}$$

$$\left\{\begin{array}{c}
\text{Group: } \mathbf{Z}/42\mathbf{Z}, j\text{-invariant} = 54000 \\
b^{12} - 7243b^{11} + 13272167b^{10} + 26110117b^9 + 869073943b^8 + 393685522b^7 \\
+71536947b^6 + 6515008b^5 + 318037b^4 + 12027b^3 + 814b^2 + 46b + 1 = 0 \\
c = \dfrac{1}{369732575278279488756865276993469747417780928 5} \\
(2736521893168749681266350229930553851625367534b^{11} \\
-19820869495195126944351615043421348127605747292709b^{10} \\
+36321324210396446554183550462527328019167808344048689b^9 \\
+68246566744731106656314180202093260179298297361989682b^8 \\
+237218189857926876605440773749917793564305659266806420 4b^7 \\
+867981267562042118342645071078886515260414332492365778b^6 \\
+116768220218383935757897497314211192554328099307123221b^5 \\
+676227293968885267622118531591200001250465882706829 2b^4 \\
+192360835346719967265194408987187332355640535514680b^3 \\
+130185556104317602136530598914822600345014638690 15b^2 \\
+10344255011101582424608573912389628947600308112 84b \\
+2516913888194512153646384135961235917234850253 7)
\end{array}\right\}$$

$$\left\{\begin{array}{c}
\text{Group: } \mathbf{Z}/57\mathbf{Z}, j\text{-invariant} = 0 \\
b^{12} + 2552b^{11} + 1661537b^{10} + 4195807b^{9} + 10654654b^{8} + 6530587b^{7} \\
+741924b^{6} + 106438b^{5} + 420280b^{4} + 131385b^{3} + 15865b^{2} + 874b + 19 = 0 \\
c = \frac{1}{126875548388983223500980048069289169781511767 7727} \\
(38422551857405657973082999104123825188058447 8b^{11} \\
+980564080012885839389534968483134961466499392800b^{10} \\
+638457378465963233784361970597324501046551262061064b^{9} \\
+164629816773989358122267681808157109898922702887 2268b^{8} \\
+418425898055837195731768508198429681866401148075 3870b^{7} \\
+273980923329160110279015844664808478775499854999 7604b^{6} \\
+448877750941755421793695205605227698244759316073748b^{5} \\
+795185165579479753873489552837245931832861436638 68b^{4} \\
+171400640762304772892911240385850134181621426680782b^{3} \\
+624174235830101895997889299010822980450733874988 30b^{2} \\
+111051930651927871461339638384681365132015137382 32b \\
+512261790227184935578762797837888190689624673777)
\end{array}\right\}$$

$$\left\{\begin{array}{c}
\text{Group: } \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/12\mathbf{Z} \\
j^{3} + 3491750j^{2} - 5151296875j + 12771880859375 = 0 \\
b^{4} + \dfrac{1}{1466223171875}((-852j^{2} - 2966725625j - 12891668968750)b^{3} \\
+(11857j^{2} + 37915615750j - 43122723015625)b^{2} \\
+(4652j^{2} + 15253429500j - 13092419312500)b \\
+(424j^{2} + 1406719000j - 1314937250000)) = 0 \\
c = \dfrac{1}{500587273757701202187 50} \\
((-264910381085j^{2} - 925682753867471250j - 1005477798946866437500)b^{3} \\
+(3019263627356j^{2} + 10548200420888294375j + 4119936455326059328125)b^{2} \\
+(-5328278283298j^{2} - 18616844723059174875j + 8228238638077495365625 0)b \\
+(-992437476440j^{2} - 3466872412690833000j + 5181944013611890593750))
\end{array}\right\}$$

$$\left\{\begin{array}{c}
\text{Group: } \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/18\mathbf{Z}, j\text{-invariant} = 8000 \\
b^{12} - 16b^{11} + 758/9b^{10} + 3356/27b^{9} + 172555/81b^{8} - 10768/243b^{7} \\
+146590/6561b^{6} + 92408/6561b^{5} + 7102/6561b^{4} - 364/2187b^{3} \\
-178/6561b^{2} + 4/6561b + 1/6561 = 0 \\
b = b \\
c = \frac{1}{2239902257807770123832899737349254922739} \\
(38035128699169365806955113749649975522714 4b^{11} \\
-605854850325468445067868482380246833576031 8b^{10} \\
+316034429798212024909252692311863655035520 97b^{9} \\
+495156473766051000205636714890233709264083 40b^{8} \\
+813840749857538413605608512325949579892442625b^{7} \\
+411675206209557765752346545636290222760051 73b^{6} \\
+128117717050725128881871636480079972682321 58b^{5} \\
+664296359175545233769339938040551540220488 7b^{4} \\
+865396273474862220259518955518263250665643b^{3} \\
+151203382646646552491511180521458275402 22b^{2} \\
-301155407538004424738236772626212889151 4b \\
-346074872378308449110076178990439652852)
\end{array}\right\}$$

$$\left\{\begin{array}{c}
\text{Group: } \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/26\mathbf{Z}, j\text{-invariant} = 0 \\
b^{12} + 4b^{11} + 458/13b^{10} + 14747/169b^{9} + 17919/169b^{8} \\
+170100/2197b^{7} + 1058281/28561b^{6} + 342086/28561b^{5} \\
+74609/28561b^{4} + 10655/28561b^{3} + 945/28561b^{2} \\
+47/28561b + 1/28561 = 0 \\
c = \frac{1}{48321004703591304713}(35161962415661716391302b^{11} \\
+10667157639315887430141 2b^{10} + 112446678548879191439998 4b^{9} \\
+1947374331111889589275106b^{8} + 1486607945852662185296458b^{7} \\
+657103187911027379670564b^{6} + 1891889677002641786009 06b^{5} \\
+32752827529523865493680b^{4} + 5900882946631461627552b^{3} \\
+156737370118333041561 8b^{2} + 33845487693231966262 4b \\
+16843851879867012899)
\end{array}\right\}$$

$$\left\{\begin{array}{c}
\text{Group: } \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/28\mathbf{Z}, j\text{-invariant} = -3375 \\
b^{12} - 167b^{11} + 19508b^{10} + 159065b^{9} + 950655b^{8} + 2182101b^{7} \\
+2262344b^{6} + 1209008b^{5} + 432372b^{4} + 60736b^{3} + 2910b^{2} + 25b + 1 = 0 \\
c = \frac{1}{948255521530529709108781000009297558385 7943} \\
(40641433560653484983938215772951242105450b^{11} \\
-678582144931967356910815470208548344815649 1b^{10} \\
+7926163795340816703976226237147294749319116 64b^{9} \\
+6489941438351230782774859589549303718776949019b^{8} \\
+3884345743433870277023343621284747822267999133 9b^{7} \\
+8992610464478779927007287999511591796854661825 2b^{6} \\
+9482739656578556659065655942022667487633813679 3b^{5} \\
+5218938974666254027293294704803650094772302291 2b^{4} \\
+1924828049533694387076028761296776894366467596 1b^{3} \\
+3071083726604148429189195269376774410841524103b^{2} \\
+216473401818931182446186535746448538990970927b \\
+4722221621603141090557393566016205960407710)
\end{array}\right\}$$

$$\left\{\begin{array}{c}
\text{Group: } \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/42\mathbf{Z}, j\text{-invariant} = 0 \\
b^{12} + 57b^{11} + 2069b^{10} + 17441b^{9} + 83355b^{8} + 185010b^{7} \\
+219017b^{6} + 146034b^{5} + 53209b^{4} + 9159b^{3} + 810b^{2} + 40b + 1 = 0 \\
c = \frac{1}{30404944545810885182436208577} \\
(19653154733960145951105231 6b^{11} + 11195493979264411892923409062b^{10} \\
+40623479266387394598851848328 2b^{9} + 341357590449694523776882895035 0b^{8} \\
+1626152920646488397387647691235 4b^{7} + 357973024025108267622861985880 52b^{6} \\
+4187024097422285391571450348153 0b^{5} + 2777342689884069550498627985306 4b^{4} \\
+104316728897479321734883856718 56b^{3} + 21125753771741737946438081377 18b^{2} \\
+285697307799805246699001927942b + 121332543819790440723098070 53)
\end{array}\right\}$$

$$\left\{\begin{array}{c}
\text{Group: } \mathbf{Z}/7\mathbf{Z} \oplus \mathbf{Z}/7\mathbf{Z} \\
j\text{-invariant} = 0 \\
\mathbf{Q}(\zeta_{21}) \\
E(\zeta_3, -1)
\end{array}\right\}$$

$$\left\{\begin{array}{c}
\text{Group: } \mathbf{Z}/3\mathbf{Z} \oplus \mathbf{Z}/12\mathbf{Z}, j\text{-invariant} = 54000 \\
b^{12} - 162b^{11} + 15036b^{10} - 703972b^9 + 16636092b^8 + 126298608b^7 \\
+275296800b^6 + 35294784b^5 - 2076048b^4 - 310816b^3 + 13632b^2 \\
+2112b + 64 = 0 \\
c = \frac{1}{211909924715110734361527949639043840798837056} \\
(1946575604571025009090011972165666598181 4b^{11} \\
-315400940634239355866667489898173248006821 7b^{10} \\
+292777386991386443412330046160094099350155908b^9 \\
-1371173039154080884729363025568669482944971738 0b^8 \\
+3242270255329352035820246975740759318369801718 08b^7 \\
+2449192710483172198689859358672099218106970786264b^6 \\
+5289469240850984564826484521877830683141898102272b^5 \\
+540884862404922486730892198497067302668842292640b^4 \\
-445417304033085192976434402467984872339696370 88b^3 \\
-310817510595808903219026145109116481503339608 0b^2 \\
+617837826632658395455515477912010485728669568b \\
+196633481006048011740104938925543346727734 40)
\end{array}\right\}$$

$$\left\{\begin{array}{c}
\text{Group: } \mathbf{Z}/3\mathbf{Z} \oplus \mathbf{Z}/18\mathbf{Z}, j\text{-invariant} = 8000 \\
b^{12} + 92b^{11} + 6984b^{10} - 30424b^9 + 130947b^8 - 92984b^7 \\
+204398b^6 - 2520b^5 - 12460b^4 - 688b^3 + 212b^2 + 28b + 1 = 0 \\
c = \frac{1}{36528270329783019387307955772 06} \\
(50832777502574813849751759550b^{11} \\
+4647718781643616244793497982025b^{10} \\
+35235968918324778326425535592526 1b^9 \\
-174816141262398819111964023449012 7b^8 \\
+754995883977748793841064186529442 0b^7 \\
-857864402798689661139905309768506 4b^6 \\
+1336997309646994351889816132321824 9b^5 \\
-632010530069127806508934823117128 9b^4 \\
-75131366068897145872570063861137b^3 \\
+1758008879905025689148714928490 70b^2 \\
+48199389061043193675735121218 09b \\
-102774519090083754112623610249 4)
\end{array}\right\}$$

$$\left\{\begin{array}{c}
\text{Group: } \mathbf{Z}/3\mathbf{Z} \oplus \mathbf{Z}/21\mathbf{Z}, j\text{-invariant} = 0 \\
b^{12} - 2781b^{11} + 2010033b^{10} - 729616b^9 + 3741945b^8 \\
+25751877b^7 + 36262512b^6 + 23434530b^5 + 8576946b^4 \\
+1799672b^3 + 213738b^2 + 13377b + 343 = 0 \\
c = \frac{1}{25253824339506521201521992381784891419452107147333} \\
(49314635767639039312109324722961653004364 2076b^{11} \\
-1371433485023782011417383951482728603429689406190b^{10} \\
+9912222994739495625999501128268926507681079863047 02b^9 \\
-346732932513257049068658266986907629671144213195276b^8 \\
+188568087138486965388501799404395743778082226319 9714b^7 \\
+1267249849112196550451037336282795702997959308573169 6b^6 \\
+1818067585321689007346669344537650835560163540806558 4b^5 \\
+1226695841625934681159860977472241891307481786873224 6b^4 \\
+483557284754304572107094409519728080180483664064199 2b^3 \\
+119365506073159091649275802858529424634188806199191 2b^2 \\
+205050045821568074008045061819855295992344186690302b \\
+9567155735299348341626474269342909721200144879333)
\end{array}\right\}$$

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 $\mathbf{Q}$.

References

[Cla04] P.L. Clark, X. Xarles *Bounds for torsion on abelian varieties with integral moduli*, Canad. J. Math. 60 (2008), no. 3, 532555.

[CCS13] P.L. Clark, B. Cook, J. Stankewicz, *Torsion Points on Elliptic Curves with Complex Multiplication (with an Appendix by Alex Rice)*, Int. J. Number Theory 9 (2013), no. 2, 447479.

[Cox89] D. Cox, *Primes of the form $x^2 + ny^2$. Fermat, class field theory and complex multiplication.* John Wiley & Sons, New York, 1989.

[FSWZ90] 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.

[GKP10] B. Grenet, P. Koiran, and N. Portier. *The Multivariate Resultant Is NP-hard in Any Characteristic*. Mathematical Foundations of Computer Science, LNCS 6281, 477-488, 2010.

[Hei34] H. Heilbronn, *On the Class Number in Imaginary Quadratic Fields.* Quart. J. Math. Oxford Ser. 25, 150-160, 1934.

[Kam86] S. Kamienny, *Torsion points on elliptic curves over all quadratic fields.* Duke Math. J. 53 no. 1 (1986), 157–162.

[Kam92] S. Kamienny, *Torsion points on elliptic curves and q-coefficients of modular forms.* Invent. Math. 109 (1992), no. 2, 221–229.

[KM88] M.A. Kenku and F. Momose, *Torsion points on elliptic curves defined over quadratic fields.* Nagoya Math. J. 109 (1988), 125–149.

[Ku76] D.S. Kubert, *Universal bounds on the torsion of elliptic curves.* Proc. London Math. Soc. (3) **33** (1976), 193–237.

[magma] W. Bosma, J. Cannon, and C. Playoust. *The Magma algebra system. I. The user language.* J. Symbolic Comput., **24**(3-4):235-265, 1997

[Maz77] B. Mazur, *Modular elliptic curves and the Eisenstein ideal*, Publ. Math. Inst. Hautes Etudes Sci. 47 (1977) 33168.

[Mer96] L. Merel, *Bornes pour la torsion des courbes elliptiques sur les corps de nombres.* Invent. Math. 124 (1996), 437-449.

[MS01] L. Merel and W.A. Stein, *The field generated by the points of small prime order on an elliptic curve.* Internat. Math. Res. Notices 2001, no. 20, 1075–1082.

[Mil08] J. Milne, *Class Field Theory*, Version 4, http://jmilne.org/math/.
[MSZ89] 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.
[Ols74] L. Olson, *Points of finite order on elliptic curves with complex multiplication*, Manuscripta math. 14 (1974), 195-205.
[Par03] P. Parent, *No 17-torsion on elliptic curves over cubic number fields*. J. Théor. Nombres Bordeaux 15 (2003), no. 3, 831–838.
[Par89] J.L. Parish, *Rational Torsion in Complex-Multiplication Elliptic Curves*, Journal of Number Theory 33 (1989), 257-265.
[PWZ97] A. Pethö, T. Weis and H. Zimmer, *Torsion groups of elliptic curves with integral j-invariant over gneeral cubic number fields*. Internat. J. Algebra Comput. 7 (1997), 353-413.
[PY01] 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.
[SAGE] *SAGE Mathematical Software*, Version 4.1, http://www.sagemath.org
[Sch95] R. Schoof, *Counting points on elliptic curves over finite fields*. JTNB 7, # 1 (1995), 219–254.
[Sbg88] A. Silverberg, *Torsion points on abelian varieties of CM-type*. Compositio Math. 68 (1988), no. 3, 241–249.
[Sil86] J. Silverman, *The Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics 106, Springer Verlag, 1986.
[Sil94] J. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics 151, Springer-Verlag, 1994.
[Sut12] A. Sutherland, *Constructing elliptic curves over finite fields with prescribed torsion*, Mathematics of Computation 81 (2012), 1131-1147.
[Wat04] M. Watkins, *Class numbers of imaginary quadratic fields*. Math. Comp. 73 (2004), no. 246, 907–938.
[Zim76] H. Zimmer, *Points of finite order on elliptic curves over number fields*. Arch. Math. (Basel) 27 (1976), no. 6, 596–603.