COMPUTATION ON ELLIPTIC CURVES WITH COMPLEX MULTIPLICATION

PETE L. CLARK, PATRICK CORN, STEPHEN LANE, ALEX RICE,
JAMES STANKEWICZ, NATHAN WALTERS, STEPHEN WINBURN, AND BEN WYSER

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 an algorithm and to report on some cases of its successful implementation. The input is a positive integer d. The desired output is the complete (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 must either incorporate or import an effective solution to Gauss' class number problem. That is, we require 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 have implemented our algorithm using the MAGMA programming language and run it on a pair of Unix servers in the University of Georgia Department of Mathematics. At this time we are able to report successful termination of the algorithm for $1 \leq d \leq 11$ and $d = 13$, together with many partial results for $d = 12$. The output of the program for 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 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.

1.2. **Connections to prior work.** According to the celebrated **uniform boundedness theorem** of L. Merel [Mer96], for any fixed $d \in \mathbf{Z}^+$, the supremum of the size of all rational torsion subgroups of all elliptic curves defined over all number fields of degree d is finite.

Date: November 18, 2009.

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:

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

We remark that this corresponds precisely to the list of modular curves $X_1(N, M)$ of genus zero, so is in a sense the minimal conceivable answer.

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

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

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. The best result in this direction is due to Parent, who has shown that the largest prime divisor of $\#E(K)[\text{tors}]$, as E ranges over all elliptic curves defined over cubic number fields K, is 13 [Par03].

Further results come from focusing on particular classes of elliptic curves. Over a period of many years, H. Zimmer and his collaborators worked on the case of elliptic curves with j-invariant in the ring of algebraic integers. In [MSZ89] Müller-Stroher-Zimmer proved that in the case of integral j-invariant, if $[K : \mathbf{Q}] = 2$, then

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

In [PWZ97] Pethö-Weis-Zimmer showed that if E has integral j-invariant and $[K : \mathbf{Q}] = 3$, then

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

Here we study elliptic curves with complex multiplication. Such curves form a subclass of curves with integral j-invariant [Sil94, Thm. 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 3. 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 an N-torsion point 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: $N = 4$**.** 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 $c = 0$. Here we could also have noted that $2(0,0) = (b, bc)$, which is a 2-torsion point if and only if $bc = 0$.

Example: $N = 5$**.** 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 $b - c = 0$. Here we could also have set $2(0,0) = (b, bc)$ equal to $-3(0,0) = (c, c^2)$.

Example: $N = 7$**.** On $E(b,c)$ we have $[7](0,0) =$

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

and so the condition that the origin is a 7-torsion point is that $b^2 - bc - c^3 = 0$. Here 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 defining polynomials $f_N(b,c)$, is the most computationally taxing part of the algorithm for large values of N.

In general, $(0,0)$ will be an N-torsion point if and only if $\lfloor N/2 \rfloor (0,0)$ and $-\lceil N/2 \rceil (0,0)$ are equal. When N is odd, it suffices to compare x-coordinates of these points, as it is impossible that $\lfloor N/2 \rfloor (0,0) = \lceil N/2 \rceil (0,0)$. When N is even, it suffices to set the y-coordinate of $(N/2)(0,0)$ equal to 0.

As we are essentially building an affine model for $Y_1(N)$ for various N, it is natural to consider the map $Y_1(NN') \to Y_1(N')$ sending the point (E,P) to (E,NP), and the map $Y_1(N) \to Y_1(NN')$ sending (E,P) to (E,P). These bear on our work in two ways. First, we will often use the obvious fact that if there are no CM points on $Y_1(N')$ over a certain field, then there are no CM points on $Y_1(NN')$ over that field. Second, if (E,P) is a point on $Y_1(NN')$, it may be that P is an N-torsion point. For precision and efficiency of computation, it is advantageous to recognize when this is the case. We do this by considering the irreducible component of $Y_1(N)$ of points (E,P) where P is not n-torsion for any proper divisor n of N. We give details in the following description of the algorithm.

3. Description of the algorithm

Let $d \leq 100$ be a positive integer. In this section, we describe our algorithm, whose output is a list of all possible abelian groups that occur as torsion subgroups of CM elliptic curves over number fields of degree $\leq d$ (together with one example of a curve with each possible torsion subgroup). At the end of the section, we give a summary of the algorithm in its entirety.

3.1. The finite list of 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 3.1. *(Heilbronn, 1934)* [Hei34] *For any positive integer d, there are only finitely many imaginary quadratic fields with class number d.*

Definition 3.2. *We will call an order in some imaginary quadratic field an* imaginary order.

Corollary 3.3. *For any positive integer d, there are only finitely many imaginary 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:

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

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. □

Our algorithm begins with Watkins' list of discriminants of imaginary quadratic fields of class number at most d (since $d \leq 100$); we then use the Corollary to restrict our attention to a finite number of imaginary orders. MAGMA computes their class numbers explicitly, and we tabulate the orders (in order of discriminant) whose class numbers divide d. The function `HilbertClassPolynomial` in MAGMA then computes the (minimal polynomial of the) j-invariant corresponding to a given discriminant.

3.2. **Possible torsion.** Let E be an elliptic curve over a number field F. 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 3.4. *(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 $K \nsubseteq F$, then $\varphi(\#E(F)[\text{tors}]) \leq w(\mathcal{O})d$.

Proof. See [Sbg88], [PY01]. □

Remark 2. 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 $w(\mathcal{O})^2d^2$. The SPY bounds also lead us to expect that the largest torsion subgroups occur when $w(\mathcal{O})$ is largest, namely when $j = 0, 1728$.

So, given a degree d, there are finite, effectively computable lists of

- the possible orders N of points on CM elliptic curves over a degree-d number field
- the discriminants D of the imaginary orders that arise as endomorphism rings of CM elliptic curves over a degree-d number field

Next we describe a program which takes each pair (N, D) and determines whether there is a CM elliptic curve over a degree-d number field corresponding to the pair. We can solve the classification problem completely for a given d by forming the finite lists above and simply iterating this program over every pair (N, D) on the lists.

3.3. **Fixed N and D.** Suppose we are given an integer $N \geq 4$ and a CM discriminant D together with a positive integer d such that $h(D)|d$. How do we decide whether there is some degree-d number field over which the corresponding CM elliptic curve has an N-torsion point, and if so, how do we find that field?

The CM discriminant D corresponds to a CM j-invariant j_0. Writing

$$j(b,c) = \frac{n_j(b,c)}{d_j(b,c)}$$

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

$$\begin{aligned} n_j(b,c) &= j_0 d_j(b,c) \\ f_N(b,c) &= 0 \end{aligned} \tag{4}$$

We are interested in points of low degree on the intersection of these two affine curves. The *resultant* of the polynomials $n_j(b,c) - j_0 d_j(b,c)$ and $f_N(b,c)$ is a polynomial $R_{N,j_0}(b)$ whose roots are precisely the b-coordinates of the points in the intersection. Given j_0 and N, we compute this resultant and factor it over $\mathbf{Q}(j_0)$.

If N is not prime, we repeat this for all divisors $n \geq 3$ of N, giving resultants $R_{n,j_0}(b)$ for all such divisors. Let $\mathcal{R}_{n,j_0}(b)$ be the factor of $R_{n,j_0}(b)$ whose roots correspond to elliptic curves for which the point $(0,0)$ has *order* n. We wish to compute $\mathcal{R}_{N,j_0}(b)$. But since $R_{N,j_0}(b) = \prod_{\substack{n \geq 3 \\ n|N}} \mathcal{R}_{n,j_0}(b)$, we can use Möbius inversion to find

$$\mathcal{R}_{N,j_0}(b) = \prod_{\substack{n \geq 3 \\ n|N}} R_{n,j_0}(b)^{\mu(N/n)}. \tag{5}$$

Note that $R_{3,j_0}(b) = b^{12}$ for all j_0, and $b = 0$ corresponds to a singular curve. In practice we can ignore powers of b in the expressions on the right side of (5).

We search for factors g of $\mathcal{R}_{N,j_0}(b)$ whose degree is such that adjoining a root β of g to $\mathbf{Q}(j_0)$ gives a number field of absolute degree dividing d.

Given a root β of g as above, we find the greatest common divisor of the univariate polynomials $n_j(\beta,c) - j_0 d_j(\beta,c)$ and $f_N(\beta,c)$. Since β is the b-coordinate of a point on the intersection, we know this gcd is nonconstant. We expect, in fact, that it is of the form $c - \gamma$ for some $\gamma \in \mathbf{Q}(j_0,\beta)$. (In fact, this has been the case in every example we have computed; at any rate it seems unlikely that there will be two different points on the intersection with the same b-coordinate.) In this case $E(\beta,\gamma)$ is an elliptic curve with an N-torsion point over the field $\mathbf{Q}(j_0,\beta)$.

Notice that this elementary method at the heart of the algorithm, solving the system of equations (4), works equally well on any fixed pair (j_0, N). The CM hypothesis is not necessary here–we could run the same resultant computations for any fixed triple (j_0, d, N). (Of course, if we give up the CM hypothesis, the number of admissible j-invariants is no longer restricted, and the number of admissible values of N is restricted only by the bounds of Merel[Mer96].)

Example: $N = 7$, $D = -3$. The corresponding CM j-invariant is 0. The two affine curves are

$$\begin{aligned} 16b^2 + 8b(1-c)(c+2) + (1-c)^4 &= 0 \\ b^2 - bc - c^3 &= 0 \end{aligned}$$

The resultant is

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

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 $\mathbf{Q}(\zeta)$. 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. (The interested 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

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

As a final remark, over the degree-12 cyclotomic field $\mathbf{Q}(\zeta_{21})$, this curve acquires full 7-torsion, and is in fact the lowest-degree example of a CM elliptic curve with full 7-torsion.

As we have previously noted, when we consider a fixed d and run over the list of CM j-invariants of degree $\leq d$, we expect to get the largest values of N for the smallest-degree j-invariants–that is, the 13 integral j-invariants corresponding to orders of class number 1. In fact we have the following theorem guaranteeing that the *largest*-degree j-invariants need not be considered:

Theorem 3.5. *(Parish) Let E/F be an elliptic curve with CM by an imaginary quadratic order $\mathcal{O}$, and suppose that $h(\mathcal{O}) = [F\colon \mathbf{Q}]$. Then $E(F)[tors]$ has order 1, 2, 3, 4, or 6.*

Proof. [Pari89]. □

So in our searches, we need only consider j-invariants of degree strictly less than d.

Once we have identified a curve $E(\beta, \gamma)$ with an N-torsion point, MAGMA can compute the full torsion subgroup of E. Combining these groups with the groups we have found for smaller values of d, we obtain a complete list of torsion subgroups for a given d. Note that we have a complete list even though our algorithm does not detect $0, \mathbf{Z}/2\mathbf{Z}, \mathbf{Z}/3\mathbf{Z}, \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/2\mathbf{Z}$ or $\mathbf{Z}/3\mathbf{Z} \oplus \mathbf{Z}/3\mathbf{Z}$ because the first three occur over $\mathbf{Q}$, while $\mathbf{Z}/3\mathbf{Z} \oplus \mathbf{Z}/3\mathbf{Z}$ can only occur in fields containing ζ_3 (hence with even degree) as a consequence of the Weil pairing ([Sil86, §III.8]). On the other hand, the CM elliptic curve $x^3 + y^3 = z^3$ has full 3-torsion over $\mathbf{Q}(\zeta_3)$, so $\mathbf{Z}/3\mathbf{Z} \oplus \mathbf{Z}/3\mathbf{Z}$ occurs as a subgroup of some CM elliptic curve defined over a number field of degree d if and only if d is even.

3.4. **Summary of the algorithm.** Here is a summary of the algorithm from start to finish. Our input is a positive integer $d \leq 100$, and our output is the finite list of abelian groups which appear as torsion subgroups of CM elliptic curves over number fields of degree d.

Step 1: Compute the finite list of discriminants D of imaginary quadratic orders $\mathcal{O}$ whose class numbers properly divide d. List the j-invariants of the corresponding $\mathcal{O}$-CM elliptic curves.

Step 2: For each imaginary order $\mathcal{O}$ on the list in the previous step, list the values of N up to $\frac{w(\mathcal{O})^2 d^2}{h(\mathcal{O})^2}$. Hence generate a finite list of pairs (N, D) (or equivalently, (N, j_0)) such that an elliptic curve with CM by the imaginary order with discriminant D (equivalently: with j-invariant j_0) may have an N-torsion point over a degree d number field.

Step 3: For each ordered pair (N, j_0) in the above list, compute the polynomial $\mathcal{R}_{N,j_0}(b)$ and factor it over $\mathbf{Q}(j_0)$. If there is no root β such that $\mathbf{Q}(j_0, \beta)$ has degree dividing d, STOP and repeat Step 3 for the next ordered pair on the list.

Step 4: Given a root β such that $\mathbf{Q}(j_0, \beta)$ has degree dividing d, compute the gcd of $n_j(\beta, c) - j_0 d_j(\beta, c)$ and $f_N(\beta, c)$. The roots γ of this gcd give curves $E(\beta, \gamma)$ with an N-torsion point; if the degree of $\mathbf{Q}(j_0, \beta, \gamma)$ is less than or equal to d, add this curve to the list of curves with an N-torsion point over a field of degree dividing d. Repeat Step 3 for the next ordered pair on the list. If the list is exhausted, go to Step 5.

Step 5: Compute the torsion subgroups of the curves on the list from Step 4. ♠♠♠ FIXME! [Jim: here should be a discussion of the 2- and 3-division polynomial issues, looking for full N-torsion, etc...it would be very nice if you could furnish some examples of the various phenomena that occur.]

4. Isomorphism classes of Torsion Subgroups of CM elliptic curves E

4.1. $K = \mathbf{Q}$.

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

4.2. K is a number field of degree 2.

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

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

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

4.3. K is a number field of degree 3.

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

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

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

4.4. K is a number field of degree 4.

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

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

$$E(K)[\text{tors}] \cong \{\mathbf{Z}/5\mathbf{Z}, \mathbf{Z}/8\mathbf{Z}, \mathbf{Z}/12\mathbf{Z}, \mathbf{Z}/13\mathbf{Z}, \mathbf{Z}/21\mathbf{Z}, \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/8\mathbf{Z}, \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/10\mathbf{Z}\}.$$

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

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

The only subgroup which does not occur over $\mathbf{Q}$ is $\mathbf{Z}/11\mathbf{Z}$.

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

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

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

$$E(K)[\text{tors}] \cong \{\mathbf{Z}/18\mathbf{Z}, \mathbf{Z}/19\mathbf{Z}, \mathbf{Z}/26\mathbf{Z}, \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/14\mathbf{Z}\}.$$

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

References

[Cla04] P.L. Clark, *Bounds for torsion on abelian varieties with integral moduli*, 2004 preprint.

[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.

[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.

[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.

[Pari89] 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.

[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.

[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.