Modular curves over number fields and ECM

François Morain

MODULAR CURVES OVER NUMBER FIELDS AND ECM

F. MORAIN

Abstract. We construct families of elliptic curves defined over number fields and containing torsion groups $\mathbb{Z}/M_1\mathbb{Z} \times \mathbb{Z}/M_2\mathbb{Z}$ where (M_1, M_2) belongs to $\{(1,11)$, $(1,14)$, $(1,15)$, $(2,10)$, $(2,12)$, $(3,9)$, $(4,8)$, $(6,6)\}$ (i.e., when the corresponding modular curve $X_1(M_1, M_2)$ has genus 1). We provide formulae for the curves and give examples of number fields for which the corresponding elliptic curves have non-zero ranks, giving explicit generators using D. Simon's program whenever possible. The reductions of these curves can be used to speed up ECM for factoring numbers with special properties, a typical example being (factors of) Cunningham numbers $b^n - 1$ such that $M_1 \mid n$. We explain how to find points of potentially large orders on the reduction, if we accept to use quadratic twists.

1. Introduction

The Elliptic Curve Method (ECM) is a factoring algorithm which uses properties of elliptic curves over finite fields [46]. Algorithmic improvements were detailed in [49, 50]. It is very efficient to find rather large factors of integers (see the account in [65]). One of the reference implementations for this algorithm is GMP-ECM (see [66]); an alternative using Edwards curves is available at https://eecm.cr.yp.to/.

There is an abundant literature on the choice of curves that seem more efficient than random curves [16, 13, 49, 3], and more recently [9, 25]. Generally, rational curves are used and reduced modulo N. Theoretical results on the efficiency of these curves can be found in [7]. For specific numbers N we want to factor and for which we may know properties of its prime divisors, some algebraic extensions have been considered [14, 56].

The best we can obtain are infinite families of pairs (E, P) where E is defined over some number field K and (large) torsion group (over some extension L/K), together with a point P of infinite order (over $\mathbb{Q}$). Such a point is needed to initialize the computations in ECM. All examples with $K = L = \mathbb{Q}$ have this feature, and some for which $K = \mathbb{Q}$ and L is a quadratic extension.

From a theoretical point of view, we are looking at points on modular curves $X_1(M_1, M_2)$ where M_1 and M_2 are two positive integers and $M_1 \mid M_2$. Of particular interest are the modular curves of genus 0 and 1 that may lead to infinite parametrizations for E, and in some rare cases to families (E, P).

A first result in this work (Section 2.2.2) is to show that we can find an initialization point for ECM without requiring a point of infinite order, if we content ourselves to use twists and some increase in the number of curves to be tried. After recalling known facts about ECM in Section 3, we describe in Section 4 modular curves and give useful formulas for constructing actual elliptic curves from a modular curve, in various forms. In Section 5, we explain how we can use them in ECM for Cunningham numbers, or more generally to numbers for which roots of polynomials modulo N are known. The situation is easier when K is Galois. Algorithms are given in Section 6. There are several problems appearing in the course of this building, namely $\mathbb{Q}$-curves for which only one conjugate can be used in ECM. We add to this some factorizations of numbers of the

Date: January 9, 2023.

The author is on leave from Délégation Générale pour l'Armement.

form $b^n \pm 1$ for $12 < b < 10^4$ (from the tables initially created by Brent, Montgomery and te Riele) obtained with our work.

2. Elliptic curves

2.1. **Over $\mathbb{F}_p$.** The cardinality m of an elliptic curve over a prime field $\mathbb{F}_p$ satisfies Hasse's theorem: $t = m - (p+1)$ where $|t| < 2\sqrt{p}$. Moreover $E(\mathbb{F}_p)$ is either cyclic or the product of at most two groups $E = E_1 \times E_2$ with $m_i = \#E_i$ and $m_1 \mid m_2$, $m_1 \mid p-1$, this latter result being obtained using the Weil pairing.

2.1.1. *Various models of curves.* Various forms of elliptic curves have been considered for ECM, starting from the Weierstrass short model (in affine or projective form):

$$E_W : Y^2 = X^3 + AX + B, 4A^3 + 27B^2 \neq 0. \tag{1}$$

The Montgomery form (introduced in [49])

$$E_{M,m_a,m_b} : m_b Y^2 = X^3 + m_a X^2 + X \tag{2}$$

(where $m_b \neq 0$, $m_a^2 \neq 4$) is well suited for curves having a rational abscissa of a point of order 4, also enjoying a very fast group law algorithm (see [17] for many properties of this form). A similar use can be made of the twisted Edwards form [9]

$$E_{Ed,a,d} : au^2 + v^2 = 1 + du^2v^2. \tag{3}$$

Since we are using elliptic curves with special torsion group, we can contemplate the idea of using Kohel's results [37] which state that there exists a group law more suited to a curve with a given torsion group.

The curve E_{M,m_a,m_b} can be transformed into

$$E_{W,m_a,m_b} : v^2 = u^3 + (m_b^2(1 - m_a^2/3))u + m_b^3(m_a/3)(2(m_a/3)^2 - 1)$$

via $(X, Y) \mapsto (m_b(X + m_a/3), m_b^2 Y)$. We also have transformation to a twisted Edwards form:

$$E_{Ed,a,d} : au^2 + v^2 = 1 + du^2v^2, a = (m_a + 2)/m_b, d = (m_a - 2)/m_b. \tag{4}$$

Last in the list are curves in twisted Hessian form [10]:

$$E_{H,h_a,h_d} : h_a X^3 + Y^3 + Z^3 = h_d XYZ. \tag{5}$$

Curves in this form have a rational point of order 3, and rational 3-torsion when $h_a = 1$.

2.1.2. *Quadratic twists.* We gather results on the quadratic twists for the various forms of curves in the following Proposition. Over $\mathbb{F}_p$, if E has $p + 1 - t$ points, a quadratic twist has cardinality $p + 1 + t$.

Proposition 2.1. *Take λ such that $\left(\frac{\lambda}{p}\right) = -1$.*

i) For a Weierstrass curve $E : Y^2 = X^3 + AX + B \bmod p$, a quadratic twist is given by $\tilde{E} : \lambda Y^2 = X^3 + AX + B \bmod p$.

ii) For a Montgomery curve, $E : m_b Y^2 = X^3 + m_a X^2 + X$ has quadratic twist $\tilde{E} : \lambda m_b Y^2 = X^3 + m_a X^2 + X$.

iii) For a twisted Edwards curve, $E : aX^2 + Y^2 = 1 + dX^2Y^2$, we get $\tilde{E} : \lambda a X^2 + Y^2 = 1 + \lambda d X^2 Y^2$.

For Hessian curves, there are no easy formulas for such twists.

We note the following result that we will use later.

Lemma 2.1. *The curves E and $\tilde{E}$ have the same 2-torsion points.*

Proof: let E be in Weierstrass form. The 2-torsion points of E are characterized by $Y = 0$, i.e., $X^3 + AX + B = 0$, which is the same for $\tilde{E}$. □

2.2. **What happens modulo composite numbers.**

2.2.1. *Reduction.* Let N be a composite integer (to be factored). We use "elliptic curves modulo N" as objects E_N coming from one of the above forms, asking for the discriminant to be invertible modulo N. In this way, if p is a prime factor of N, the reduction of E_N modulo p is an elliptic curve and O_p is the point at infinity. The "group law" on E_N is the same as the group law on E_p, except that when dealing with a point whose reduction modulo p is zero, a divisor of N will generally be revealed. See [46] for more details.

For ECM to work, we need also a "point" $P_N \mod N$, i.e., an element of $E_N(\mathbb{Z}/N\mathbb{Z})$. To simplify the exposition, we call (E_N, P_N) an *elliptic pair.*

2.2.2. *Finding elliptic pairs modulo N.* Finding a point on a curve E boils down to solving a quadratic equation, that is not known to be solvable modulo a composite number without factoring it. This makes the search for points modulo N problematic. In ECM, one can cheat by creating (E_N, P_N) from P_N itself. In the Weierstrass model, choose $P_N = (x_0, y_0)$, A and deduce $B = y_0^2 - x_0^3 - Ax_0$.

Let us state a result that will help us.

Proposition 2.2. *Suppose N is a composite number and p one of its prime factor.*

a) (Weierstrass form) Suppose $E_0 : Y^2 = X^3 + aX + b$. Select some x_0 and let $\lambda \equiv x_0^3 + ax_0 + b \bmod N$. Then $(x_0, 1)$ is a point on $E_\lambda : \lambda Y^2 = X^3 + aX + b \bmod N$.

b) (Montgomery form) Take $E_0 : m_bY^2 = X^3 + m_aX^2 + X$. Choose some x_0 and compute $\lambda = (x_0^3 + m_ax_0^2 + x_0)/m_b \bmod N$. If $\left(\frac{\lambda}{p}\right) = 1$, the point $(x_0, 1)$ is a point on a curve $\tilde{E} : \lambda m_bY^2 = X^3 + m_aX^2 + X$ which is isomorphic to E_0. If λ is a non square modulo p, then $E \bmod p$ will be a twist of $E_0 \bmod p$.

c) (Twisted Edwards form) Start from $E_0 : aX^2 + Y^2 = 1 + dX^2Y^2$. For some random x_0 and y_0, consider $P_1 = (x_0 \neq 0, y_0 \neq \pm 1, 1)$ such that $y_0^2 \neq a/d$. Compute λ such that $(a\lambda)x_0^2 + y_0^2 = 1 + (d\lambda)x_0^2y_0^2$, in other words $\lambda = -(y_0^2 - 1)/(x_0^2(-dy_0^2 + a))$, which defines an Edwards curve E_λ of parameters $(a\lambda, d\lambda)$ with P_1 on it and which is isomorphic to E_0 when $\left(\frac{\lambda}{p}\right) = 1$.

Part a) of the following Proposition originates from [3]. Note also that we cannot deal with Hessian curves, since quadratic twists cannot be described naturally without going back to some other form.

One can use quadratic twists in the following way. Given some elliptic curve E_0 defined modulo N, compute a pair (E, P) modulo N so that P is a point on E_λ, and where $E_\lambda \bmod p$ is isomorphic either to $E_0 \bmod p$ or its twists.The price to pay for this is that cannot really control this twist. Suppose E_0 was designed to have some torsion property. We expect the reduction of E_0 modulo p to keep this torsion property. If $E \bmod p$ is isomorphic to $E_0 \bmod p$, then $E \bmod p$ has the same torsion property. If $E \bmod p$ is isomorphic to a twist of $E_0 \bmod p$, we generally lose the desired property. Therefore, we need to try a few selections of E. In practice, we have the same problem as in the $p + 1$ method of factoring [64], and several curves should be used. Let us explain how it works in practice, depending on the form of the elliptic curve.

By Lemma 2.1, E has the same number of torsion points for all possible choices of λ. This means we do not loose too much when reducing them. Still, ECM will succeed to find p if $E_0 \bmod p$ or its twist has smooth order. To improve the success of the method, we may have to increase the number of curves tried. A phenomenon close to the one that is encountered in the $p + 1$ method [64].

3. How to factor a number with ECM

3.1. **Generalities.** Let N be the integer to factor. Let (E_N, P_N) be an elliptic pair. The point P_N is multiplied on E_N until the reduction of some of its multiple modulo p (for some unknown $p \mid N$)

hits the point O_p. This works if the order of P_p (the reduction of P_N to E_p) is B-smooth for some integer B. Write E_p as the product of two cyclic groups, $E_p^{(1)} \times E_p^{(2)}$ of respective cardinalities m_1 and m_2 with $m_1 \mid m_2$ and $m_1 \mid p-1$. Having m_2 B-smooth will force $\operatorname{ord}(P_p)$ to be B-smooth. It should be noted at this point that ECM requires a lot of curves to attain its theoretical behavior (indeed, a sub-exponential number of such curves). So our ability to generate a lot of curves easily is essential.

3.2. **Good curves for ECM.** A classical choice of E modulo N comes from reducing a curve $\overline{E}$ defined over $\mathbb{Q}$ (or $\overline{\mathbb{Q}}$) modulo N. Early authors and continuators (see also below) introduced the idea to force some torsion group in $E/\mathbb{Q}$ to help the smoothness of $E \bmod p$ for prime p. The practical effect was measured, but not justified from a theoretical point of view. Next section explains this.

There are theoretical as well as practical complications when trying large torsion groups over number fields. Over $\mathbb{Q}$, each group $\mathcal{T}$ appears infinitely often, also with families containing a point of infinite order. Over quadratic fields, we know the list of possible $\mathcal{T}$. Note also that we need to reduce the resulting curves “modulo N”, which is not easy, apart for special numbers as that of the Cunningham project.

Having a good curve is not enough. For ECM to work, we need a point P on E. This point should not have small order. In some cases (e.g., for the elliptic curves obtained from modular curves defined over $\mathbb{Q}$ from Table 1), we have parametrized families $(\overline{E}, \overline{P})$ of a curve and a point of infinite ordre, and we can use the reduction of $\overline{P}$ modulo N as our starting point P. In a more standard situation, we have a good curve $\overline{E}$ and we can find P using Simon's algorithm (see below). Alternatively, we can use Proposition 2.2.

3.3. **Friendly curves for ECM.** A series of papers by Barbulescu *et alii* made a remarkable link with Serre's work on the Galoisian properties of division points on elliptic curves [6, 7]. As a result, a criterion for computing the friendliness of the reduction of $E/\mathbb{Q}$ was developed. High values of it were found, going further than simply having large torsion group [29]. The work was extended to the reduction of a rational curve E over some quadratic field in [8]. It is expected that this will extend to general number fields.

Let $E/\mathbb{Q}$ be an elliptic curve and look at its reduction modulo a prime p of good reduction. For a prime ℓ, define

$$\overline{\mathrm{val}}_\ell(E)) = \sum_{k\geq 1} k \cdot \mathrm{Prob}(\{p \text{ prime s.t. } \mathrm{val}_\ell(\#E(\mathbb{F}_p)) = k\}).$$

A large value of this quantity for many small ℓ's would indicate good smoothness properties of reductions of E. From an experimental point of view, we could approximate this quantity by

$$c_\ell(E) = \lim_{x\to+\infty} \frac{1}{\pi(x)} \sum_{p\leq x} \mathrm{val}_\ell(\#E(\mathbb{F}_p)).$$

In [7], the authors use Galois properties of the ℓ^k torsion points of E to give a precise value for $\overline{\mathrm{val}}_\ell(E))$. By analogy with NFS, they introduce $\alpha(E) = \sum_\ell \alpha_\ell(E)$, with $\alpha_\ell(E) = \log \ell(1/(\ell-1) - \overline{\mathrm{val}}_\ell(E))$. This enables them to write for a prime p of size n,

$$\mathrm{Prob}(\#E(\mathbb{F}_p) \text{ is } B-\text{smooth}) \approx \mathrm{Prob}(m \text{ of size } ne^{\alpha(E)} \text{ is } B-\text{smooth}).$$

They also prove that $|\alpha(E)| < \infty$ and that there is an absolute maximum for $\alpha(E)$, namely $\alpha_0 \approx -0.812$, which explains why ECM is rather successful in finding factors of a number. Also, finding smaller values of α gives very interesting curves for ECM. The results led to new families of curves [8] that gave very good values for α, see also [29].

In the case where E is defined over K, the theory does not exist yet. For a Galois field K of degree d and defining polynomial $M_K(X)$, we propose the following heuristic modification of the function c_ℓ:

$$\tilde{c}_\ell(E/K) = \lim_{x\to+\infty} \frac{1}{\#\Pi_K(x)} \sum_{p\leq x, p\in\Pi_K} \frac{1}{d}\sum_{i=1}^{d} \mathrm{val}_\ell(\#E_{\theta_i}(\mathbb{F}_p))$$

where $\Pi_K = \{p \text{ prime}, (p) \text{ splits in } K\}$, $M_K(X) = \prod_{i=1}^{d}(X-\theta_i) \bmod p$. The reason for this is as follows. Suppose the prime p splits in K. Then $M_K(X) \bmod p$ has d roots. Each root θ_i yields a reduction for E modulo p. Now, we cannot know which curve will be considered in ECM, so that we average the values of the valuation over all curves. Now we replace α_ℓ by

$$\tilde{\alpha}_\ell(E) = \log \ell(1/(\ell-1) - \tilde{c}_\ell(E/K))$$

and similarily replace α by $\tilde{\alpha} = \sum_\ell \tilde{\alpha}_\ell(E)$. A small (negative) value of $\tilde{\alpha}$ should indicate some friendliness of E/K for ECM.

This formula justifies one way to increase $\tilde{c}_\ell(E/K)$: have rational ℓ^k-torsion points for some small ℓ and $k > 0$.

4. Modular curves

Modular curves are associated to congruence groups, in particular the curves $X_0(N)$ parametrize elliptic curves with rational isogenies, the curves $X_1(N)$ those with a point of order N and those of $X_1(M_1, M_2)$ parametrize the curves with a torsion structure $\mathbb{Z}/M_1\mathbb{Z} \times \mathbb{Z}/M_2\mathbb{Z}$. Points with coordinates over a number field L give the coefficients of elliptic curves with coefficients defined over L. In this work we restrict to the case $X_1(M_1, M_2)$ which offers the best examples of ECM-friendly curves with rational coefficients. Since the genus increases rapidly as M_1 and M_2 increase, this method is bound to stop even more rapidly.

4.1. Theoretical results.

Suppose M_1 and M_2 are two integers, $M_1 \geq 1$ and $M_1 \mid M_2$. We abbreviate $X_1(\mathbb{Z}/M_1\mathbb{Z} \times \mathbb{Z}/M_2\mathbb{Z})$ to $X_1(M_1, M_2)$. Of particular interest are curves of genera 0 or 1, since they may lead to infinite families of curves over number fields. Our primary interest are the elliptic curves parametrized by these modular curves, with a special emphasis on curves over $\mathbb{Q}$ or small degree extension. Then it remains to identify which modular curves yield which elliptic curves over which number fields yielding the corresponding torsion subgroup. For instance, elliptic curves coming from $X_1(M_1, M_2)$ have their torsion defined over a field containing $\mathbb{Q}(\zeta_{M_1})$ (see [58, Corollary 8.1.1]).

Let K be a number field and E an elliptic curve defined over K. Also $\mathrm{Tors}(E/K)$ denotes the torsion subgroup of E defined over K. Let L denote a finite algebraic extension of K. We denote by $E(L/K)$ the curve obtained by embedding K trivially into L and $\mathrm{Tors}(E(L/K))$ the group corresponding to the extension. We need results on the possible torsion groups that exist for this case.

By [47], we know that the only possible torsion groups for $E(\mathbb{Q})$ are

$$\left\{ \begin{array}{ll} \mathbb{Z}/M_2\mathbb{Z}; & M_2 = 1, 2, \ldots, 10 \text{ or } 12, \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/M_2\mathbb{Z}; & M_2 = 2, 4, 6, 8. \end{array} \right. \tag{6}$$

Merel [48] and Parent [55] have given explicit bounds for the largest prime power dividing $\#\mathrm{Tors}(E)$ as a function of the degree d of $K/\mathbb{Q}$, so that we can list groups that *may* occur. For the degree 2, this was studied in [33] and proved in [32]. High rank curves have been given in [1, 54] for $d = 2$, [12, 20, 61, 62, 63] for $d = 3$, [21] for $d \in \{5, 6\}$.

4.2. **Curves and equations.** We refer the reader to the site `https://math.mit.edu/~drew/X1mn.html` that gives equations for $X_1(M_1, M_2)$. These equations correct a lot of misprints in the literature (too many to be given here).

Table 1 lists the modular curves of genus 0. Column K indicates the smallest field of definition of E, L the smallest extension of K containing the given torsion. In the last column, we indicate the source for infinite families of curves E/K with positive rank and explicit point of infinite order. We add that Dujella maintains a web site with a lot of information on this topic [22, 23]. The case $\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$ is special, in the sense that infinite families cannot occur (T. A. Fisher, private communication, 2021). Some of the articles present parametrizations in Montgomery or Edwards form.

M_1	M_2	K	L	parametrization	infinite family of elliptic pairs
1	2	$\mathbb{Q}$	$\mathbb{Q}$	[38]	[28, 53, 34, 41]
1	3	$\mathbb{Q}$	$\mathbb{Q}$	[38]	[41, 40]
1	4	$\mathbb{Q}$	$\mathbb{Q}$	[38]	[41, 40]
1	5	$\mathbb{Q}$	$\mathbb{Q}$	[38]	[4, 41, 42, 40]
1	6	$\mathbb{Q}$	$\mathbb{Q}$	[38]	[59, 41, 40, 43]
1	7	$\mathbb{Q}$	$\mathbb{Q}$	[38]	[4, 41, 40, 44, 45]
1	8	$\mathbb{Q}$	$\mathbb{Q}$	[38]	[41, 40, 45, 24]
1	9	$\mathbb{Q}$	$\mathbb{Q}$	[38]	[4, 40]
1	10	$\mathbb{Q}$	$\mathbb{Q}$	[38]	[4, 40]
1	12	$\mathbb{Q}$	$\mathbb{Q}$	[38]	[49, 40]
2	2	$\mathbb{Q}$	$\mathbb{Q}$	[38]	[35, 39, 39, 41, 40]
2	4	$\mathbb{Q}$	$\mathbb{Q}$	[38]	[40, 43]
2	6	$\mathbb{Q}$	$\mathbb{Q}$	[38]	[40, 45, 26, 24]
2	8	$\mathbb{Q}$	$\mathbb{Q}$	[38]	[4, 40]
3	3	$\mathbb{Q}$	$\mathbb{Q}(\zeta_3)$	[56, 14]	[25]
3	6	$\mathbb{Q}$	$\mathbb{Q}(\zeta_3)$	[56, 14]	[14, 25]
4	4	$\mathbb{Q}$	$\mathbb{Q}(\zeta_4)$	[56, 14]	[14]
5	5	$\mathbb{Q}$	$\mathbb{Q}(\zeta_5)$	[36]	none, but infinite family of E

Table 1. Modular curves of genus 0.

The curves $X_1(M_1, M_2)$ of genus 1 are listed in Table 2 as elliptic curves. The last column indicates a reference containing infinite families of number fields for which the rank of the curve is non-zero; we indicate if this stands for quadratic (quad.), cubic or quartic fields. All the curves are

M_1	M_2	$X_1(M_1, M_2)$	parametrization	reference
1	11	$s^2 - s = t^3 - t^2$	[57]	quad. [31], cubic [30]
1	14	$s^2 + st + s = t^3 - t$	[57]	quad. [31], cubic [30]
1	15	$s^2 + st + s = t^3 + t^2$	[57]	quad. [31], cubic [30]
2	10	$s^2 = t^3 + t^2 - t$	[56]	quad. [31], cubic [30]
2	12	$s^2 = t^3 - t^2 + t$	[56]	quad. [31], cubic [30]
3	9	$s^2 = t^3 + 16$	[56, 14]	quartic [31]
4	8	$s^2 = t^3 - t$	[56, 14]	quartic [31]
6	6	$s^2 = t^3 + 1$	[14, 25]	quartic [31]

Table 2. Modular curves of genus 1.

defined over $\mathbb{Q}$, and of rank 0 over $\mathbb{Q}$. Extending these curves to quadratic fields yield examples where the rank is > 0, thus providing us with an infinite family of elliptic curves having given torsion.

We also need parametrizations giving the parameters of the elliptic curves obtained from a point on $X_1(M_1, M_2)$. These form Table 3. We may give these in different formats corresponding to the original article and/or corrected computations in some cases. A pair (a, b) refers to $Y^2 + aXY + bY = X^3 + bX^2$ in Tate normal form; a pair (m_a, m_b) refers to a Montgomery form $m_b Y^2 = X^3 + m_a X^2 + X$. Also, when $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ is a subgroup of the torsion group, putting these in Hessian form can be handy and we give h_d in $X^3 + Y^3 + Z^3 = h_d XYZ$. We did not include the value of the discriminants of the curves since they are too bulky. It is to be understood that we do not consider values of the parameters makinyg the curve singular. Also, some parameters have to be avoided when they cancel the denominator of the formulas.

M_1	M_2	parametrization
1	11	$a = ((t-1)s - t^3 + t^2 + t)/t, b = t(t-1)(s-t)$
1	14	$a = (t^4 - st^3 + (2s-4)t^2 - st + 1)/((t+1)(t^3 - 2t^2 - t + 1))$ $b = (-t^7 + 2t^6 + (2s-1)t^5 - (2s+1)t^4 - 2(s-1)t^3 + (3s-1)t^2 - st)$ $/((t+1)(t^3 - 2t^2 - t + 1))^2$
1	15	$a = ((t^2 - t)s + (t^5 + 5t^4 + 9t^3 + 7t^2 + 4t + 1))/((t+1)^3(t^2 + t + 1))$ $b = (t(t^4 - 2t^2 - t - 1)s + t^3(t+1)(t^3 + 3t^2 + t + 1))/((t+1)^6(t^2 + t + 1))$
2	10	$a = (t^3 + t^2 - 5t - 1)/(t^2 - 4t - 1), b = -t(t-1)(t+1)^3/(t^2 - 4t - 1)^2$
2	12	$a = (2(3t^2 - 1)(t^2 + 1)s + t^6 + 8t^5 - 7t^4 + 8t^3 - t^2 - 1)/((t+s)^3(s - 1 + 2t))$ $b = (t^4 - 1)((t^3 + 2t^2 - t + 2)s + 3t^4 - 3t^3 + 4t^2 - t + 1)/((t+s)^4(s - 1 + 2t)^2)$ $m_a = 1/4s(t^8 - 4t^7 + 4t^6 + 20t^5 - 26t^4 + 20t^3 + 4t^2 - 4t + 1)/(t^3 + 1)/(t-1)^3/t^2$ $m_b = t(6t^6 + (s-2)t^5 + 11st^4 - (14s - 6)t^3 + (16s - 2)t^2 - s(7t - 1)/(t^3 + 1)/(t-1)^3$
3	9	$h_d = ((s - 12)t^3 - 128s)/(8t^3)$
4	8	$m_a = (t^8 + 20t^6 - 26t^4 + 20t^2 + 1)/(4t(t^2 - 1)(t^2 + 1)^2),$ $m_b = (t-1)/(4t(t+1))$
6	6	$h_d = 3(6\zeta_3 t^2 + t^3 + 4)/(t + \zeta_3)/(t - 2\zeta_3)^2$

Table 3. Formulas for building curves from a point (t, s) on $X_1(M_1, M_2)$.

In some cases, Edwards' form is simpler. For $X_1(4, 8)$, we get

Proposition 4.1. *Let (t, s) be a point on $X_1(4, 8)$, i.e., $s^2 = t^3 - t$. Consider the curve E_t in Edwards form*

$$u^2 + v^2 = 1 + d_t u^2 v^2$$

with $d_t = ((t^2 - 2t - 1)/(t^2 + 2t - 1))^4$ and assume $d_t \notin \{0, 1\}$. Then E_t has torsion group containing $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$ over $\mathbb{Q}(t, s)$.

Proof: Compute

$$a = (m_a + 2)/m_b = \left(\frac{(t^2 + 2t - 1)^2}{(t^2 + 1)(t - 1)}\right)^2 = a_0^2, \quad d = (m_a - 2)/m_b = \left(\frac{(t^2 - 2t - 1)^2}{t^2 + 1)(t - 1)}\right)^2.$$

Now write

$$(a_0 u)^2 + v^2 = 1 + \frac{d}{a}(a_0 u)^2 v^2$$

with

$$\frac{d}{a} = \left(\frac{t^2 - 2t - 1}{t^2 + 2t - 1}\right)^4.$$

So we are back to an Edwards form and, as was to be expected, with coefficient being a square. □

In the same vein

Proposition 4.2. *Let* (t, s) *be a point on* $X_1(2, 12)$*, i.e.,* $s^2 = t^3 - t^2 + t$*. Consider the curve* $E_{t,s}$ *in Edwards form*

$$u^2 + v^2 = 1 + d_{t,s}u^2v^2$$

with

$$d_{t,s} = \left(\frac{8st(t+1)(t-1)^3 - t^8 + 4\,t^7 - 4\,t^6 - 20\,t^5 + 26\,t^4 - 20\,t^3 - 4\,t^2 + 4\,t - 1}{(t^2+1)^3\,(t^2 - 4\,t + 1)}\right)^2$$

the value being distinct from 0 and 1. Then $E_{t,s}$ *has torsion group containing* $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$ *over* $\mathbb{Q}(t, s)$*.*

5. Getting roots of some polynomials modulo composite numbers

In this section, we give examples of integers for which we have "natural" roots of known polynomials modulo N. We can end up with a list of roots of polynomials that may correspond to number fields for which elliptic curves with some large torsion group exist. For example, when $a^n = 1 \bmod N$, all prime factors p of N larger than a are $1 \bmod n$, and we may use points on $X_1(M_1, M_2)$ with $M_1 \mid n$.

5.1. Numbers occurring in ECPP.

In the complex multiplication method which is at the heart of the ECPP algorithm [3, 51] we write (a putative) prime p as a norm in some imaginary quadratic field $\mathbb{Q}(\sqrt{-D})$ $(D > 0)$, that is $4p = U^2 + DV^2$ for some rational integers U and V. From this, we deduce that the cardinality of the associated curve E is $m = p + 1 - U$ or $4m = (U-2)^2 + DV^2$. We have either $\gcd(U-2, V) > 1$ or we get a square-root of $-D \bmod m$. Note that a different use of curves with CM was already given in [4].

5.2. When we know roots of unity modulo N.

Suppose we know a solution to $a^\ell \equiv 1 \bmod N$ for some integer ℓ, which happens for Cunningham numbers and generalizations. We can use curves defined over a subfield of $\mathbb{Q}(\zeta_\ell)$ and having interesting torsion groups. Note also that we can find roots of binomial polynomials using $a^{\ell+r} \equiv a^r \bmod N$ leading to use the field $\mathbb{Q}[X]/(X^d - a^r)$ for some $d \mid \ell + r$. This favors small values of a.

To illustrate these ideas, we explain how to find square-roots of some small elements using cyclotomic fields. Combining these square-roots gives us multiquadratic fields and more occasions of using modular curves.

A particular case is for q a prime power, and is inspired by [2] (see also [5]). Assume N is a composite number and that $a > 1$ is an integer of order q modulo N, where q is an odd prime or in $\{4, 8\}$:

$$a^q \equiv 1 \bmod N.$$

Let p be a prime divisor of N. We can assume $a \not\equiv 1 \bmod p$, since otherwise $\gcd(a-1, N)$ would yield a factor of N. If $q = 4$, $b = a^2 \bmod N$ is a squareroot of 1 and if it is different from ± 1, $\gcd(b-1, N)$ factors N, so we may assume that $b \equiv -1 \bmod N$ and a behaves like a fourth root of unity. If $q = 8$, we deduce that $a^4 = -1 = (1/a)^4$ (same reasonning since a^4 is a square-root of 1 modulo N) and $(a \pm 1/a)^2 \equiv \pm 2 \bmod N$.

The integer a behaves as a q-th root of unity. We put $q^* = (-1)^{(q-1)/2}q$ when q is prime and we define $4^* = -4$ and $8^* = 8$ (say). A well-known subfield of $\mathbb{Q}(\zeta_q)$ is $\mathbb{Q}(\sqrt{q^*})$ obtained via period polynomials. Let ζ be a primitive q-th root of unity in $\mathbb{C}$. Define the two periods:

$$\eta_0 = \sum \zeta^{\mathcal{R}}, \eta_1 = \sum \zeta^{\mathcal{N}}$$

where $\mathcal{R}$ runs through the non-zero quadratic residues modulo q, and $\mathcal{N}$ through the non-residues. Then, it is well known (see e.g., [19]) that

$$\eta_0 + \eta_1 = -1, \eta_0 - \eta_1 = 2\eta_0 + 1 = \sqrt{q^*}.$$

Coming back to our problem, we replace ζ by a, and we can compute $\sqrt{q^*}$ modulo N. For example, for $q = 7$, one finds:

$$2(a + a^2 + a^4) + 1 \equiv \sqrt{-7} \bmod p.$$

6. Implementation and results

6.1. **Precomputations.** We use SageMath to look for examples of curves $X_1(M_1, M_2)$ of non-zero rank over some small degree field (say ≤ 4), using D. Simon code (available in SageMath: if E/K is a curve over some number field, the call `E.simon_two_descent()` yields independent generators of E/K – timings may vary). Note that the heights of the candidate curves grow rapidly, making the computations rapidly cumbersome and sometimes taking too much time. See the author's web page [*] for a Magma file containing the required data. In this way, we continue the computations performed on $X_1(2, 10)$ in [60]. The same method can be used for $\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$, and a list of 100 values of the rational parameter was established using Magma.

6.2. **Algorithms.** To simplify the description:

- $\mathcal{D}_L(x)$ is the defining polynomial of L whose elements are noted as polynomials in T;
- $\mathcal{P}_K(x)$ is the defining polynomial of the subfield K or L whose elements are noted as polynomials in T_2; we also need $\mathcal{I}_{L/K} : L \to K$ sending T to T_2;
- $\mathcal{Z}$ is a set of root(s) of $\mathcal{P}_K(x)$ modulo N;
- X_K is some modular curve $X_1(M_1, M_2)/K$ of genus 1, non-zero rank and point of infinite order G_K; $E_\infty(s, t, T)$ and $P_\infty(s, t, T)$ are the formulas for building an elliptic curve over K having torsion $\mathbb{Z}/M_1\mathbb{Z} \times \mathbb{Z}/M_2\mathbb{Z}$ over K, with coefficients as rational fractions obtained from Table 3.

In general, L and K are Galois. Let us give two examples. First, let $L = K = \mathbb{Q}(\sqrt{d})$ be a quadratic extension of $\mathbb{Q}$, with $\mathcal{D}_L(x) = \mathcal{P}_L(x) = x^2 - d$, $\mathcal{I}_{L/K} = \textit{identity}$. Second, let $L = \mathbb{Q}(\zeta_{67})$ with $\mathcal{D}_L(x) = (x^{67} - 1)/(x - 1)$; L has a degree 3 subfield K generated by $\mathcal{P}_K(x) = x^3 + x^2 - 22x + 5$. We find (with Magma) that

$$\mathcal{I}_{L/K}(T) = -(T^{65}+T^{63}+T^{61}+T^{60}+T^{57}+T^{56}+T^{55}+T^{54}+T^{51}+T^{50}+T^{49}+T^{48}+T^{47}+T^{46}+T^{44}$$
$$+T^{41}+T^{39}+T^{38}+T^{37}+T^{36}+T^{35}+T^{34}+T^{33}+T^{32}+T^{31}+T^{30}+T^{29}+T^{28}+T^{26}+T^{23}+T^{21}+T^{20}+T^{19}$$
$$+T^{18} + T^{17} + T^{16} + T^{13} + T^{12} + T^{11} + T^{10} + T^7 + T^6 + T^4 + T^2 + 1).$$

To simplify the exposition, we suppose we dispose of a generic family (E_∞, P_∞), we proceed with Algorithm 1. Note that we assume that all values of (s, t, z) (resp. all σ's) lead to elliptic curves. Were it not the case, we would discard the bad values. The same comment applies to all algorithms below.

Since $X_1(M_1, M_2)$ is defined over $\mathbb{Q}$, any point $P \in X_1(M_1, M_2)$ gives rises to points ${}^\sigma P$ on X_1 when $\sigma \in \mathrm{Aut}(K)$.

[*] http://www.lix.polytechnique.fr/Labo/Francois.Morain/ECM/X1_data.mag

Algorithm 1: Building curves containing a known torsion group over K

```
1  Function ECMTorsion($K, X_K, G_K, z, E_\infty, P_\infty, k_{\max}$)
       Output: A list of elliptic pairs $(E/K, P/K)$ with $E/K$ containing a known torsion
               group
2      $\mathrm{Aut}_K \leftarrow$ automorphisms of $K$
3      for $k \leftarrow 1$ to $k_{\max}$ do
4          $Q_z = (s,t) \leftarrow [k]G_K$ on $X_K$
5          $(E_{k,id}, P_{k,id}) \leftarrow (E_\infty(s,t,z), P_\infty(s,t,z))$
6          for $\sigma \in \mathrm{Aut}_K$ do
7              if ${}^\sigma G_K \neq G_K$ then
8                  $(E_{k,\sigma}, P_{k,\sigma}) \leftarrow ({}^\sigma E_{k,id}, {}^\sigma P_{k,id})$
9          Store non-isomorphic non-isogenous curves $(E_{k,\sigma}, P_{k,\sigma})$ in $\mathcal{L}$
10     return $\mathcal{L}$
```

As an example of isomorphic curves, consider $K = \mathbb{Q}[X]/(X^3 - X^2 - 10X + 8)$, defining a subfield of $\mathbb{Q}(\zeta_{62})$; on $X_1(14)/K$, the point $((T^2 - 3T)/2, T^2 - 4T + 2)$ has infinite order. The corresponding curve with torsion group containing $\mathbb{Z}/14\mathbb{Z}$ (incidentally, it contains $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/14\mathbb{Z}$) has equation $E : Y^2 + aXY + bY = X^3 + bX^2$ with $a = -8T^2 + 2T + 81, b = 140T^2 - 30T - 1424$. One automorphism of K sends T to $-85T^2 - 195T + 206$ and E is sent to $E' : Y^2 + a'XY + b'Y = X^3 + b'X^2$ with $a' = 5T^2 + 11T - 13, b' = -85T^2 - 195T + 206$, which has the same (rational) j-invariant as E and turns out to be isomorphic to E.

Line 7 encompasses the case where G_K would be fixed by σ, thereby giving the same curve $E_{k,\sigma} = E_{k,id}$, not of any use for ECM. It may happen that some of the $E_{k,\sigma}$'s turn out to be isogenous, which is a bad idea for ECM, since their reductions modulo p have the same cardinality. Perhaps we are facing a $\mathbb{Q}$-curve (isogenous to all its conjugates) that must be discarded (or we just keep $E_{k,id}$) for ECM. This occurs for degree 2^i fields (starting with the frequent quadratic cases), or when K is Galois. In all cases, Algorithm QCurveTest of [18] is required (as well as a lot of interesting properties of isogenous curves and extensions of [27]).

The problem with Algorithm 1 is that the height of $[k]G_K$ explodes. We might want to replace it with a computation on X_K mod N; note that this computation modulo N could reveal a factor of N (we perform ECM inside ECM)! But in this way, we would not recognize isogenous curves. The idea is to use small finite prime fields, and opt for a probabilistic approach. If the curves do not have the same cardinality over such a field, then the curves are not isogenous and we keep all of them. A rigorous bound for n (as well as a more precise value for Π) could come from [11] (in particular §5.3 when K is quadratic; see also the GP-script given at `https://lmbp.uca.fr/~billerey/`).

The final algorithm to build curves modulo N is Algorithm 3. In lines 9 and 10, we understand that the σ-action is supposed easy to compute (algebraically) modulo N. If any factor of N is found during the precomputations, we report it and stop.

6.3. **Experiments.**

6.3.1. *A numerical example.* First consider an example for $(M_1, M_2) = (1, 11)$. The modular curve $X_1(11) : s^2 - s = t^3 - t^2$ yield elliptic curves (in Kubert form)

$$Y^2 + aXY + bY = X^3 + bX^2$$

with

$$a = ((t-1)s - t^3 + t^2 + t)/t, \quad b = t(t-1)(s-t).$$

Algorithm 2: Selecting suitable curves

```
Function ECMTorsionIndices($(K, X_K, G_K, E_\infty, k_{\max})$)
    Output: A list of integers $k$ such that the corresponding curves are non-isogenous
    $\mathrm{Aut}_K \leftarrow$ automorphisms of $K$
    Select a set $\Pi = \{p_1, p_2, \dots, p_n\}$ of small splitting primes in $K$, i.e., $p$ such that $\mathcal{P}_K$
      splits completely modulo $p$ and $X_K/p$ is an elliptic curve over $\mathbb{F}_p$; choose a root $z_i$ of
      $\mathcal{P}_K(x) \bmod p_i$
    for $k \leftarrow 1$ to $k_{\max}$ do
        for $i \leftarrow 1$ to $n$ do
            $Q_{z_i} = (s, t) \leftarrow [k]G_K$ on $X_K/p_i$
            $E_{i,k,id} \leftarrow E_\infty(s, t, z_i)$
            for $\sigma \in \mathrm{Aut}_K$ do
                if ${}^\sigma G_K \neq G_K$ then
                    $E_{i,k,\sigma} \leftarrow {}^\sigma E_{i,k,id}$
            if the cardinalities of $E_{i,k,\sigma}$ for all $\sigma$ are distinct then
                Store $k$ in $\mathcal{L}$
                exit the $i$ loop
    return $\mathcal{L}$
```

Algorithm 3: Building curves containing a known torsion group over K

```
Function ECMTorsionN($(N, K, X_K, G_K, \mathcal{Z}, E_\infty, P_\infty, k_{\max})$)
    Output: A list of elliptic pairs $(E/K, P/K)$ with $E/K$ containing a known torsion
            group
    $\mathcal{L} \leftarrow$ECMTorsionIndices$(K, X_K, G_K, E_\infty, k_{\max})$
    $\mathcal{E} \leftarrow \emptyset$
    for $k \in \mathcal{L}$ do
        for $z \in \mathcal{Z}$ do
            $Q_z = (s, t) \leftarrow [k]G_K$ on $X_K \bmod N$
            $(E_{k,id}, P_{k,id}) \leftarrow (E_\infty(s, t, z), P_\infty(s, t, z)) \bmod N$
            for $\sigma \in \mathrm{Aut}_K$ do
                if ${}^\sigma G_K \neq G_K$ then
                    $(E_{k,\sigma}, P_{k,\sigma}) \leftarrow ({}^\sigma E_{k,id}, {}^\sigma P_{k,id}) \bmod N$
            Store $(E_{k,\sigma}, P_{k,\sigma})$ in $\mathcal{E}$
    return $\mathcal{E}$
```

Over $K\langle T\rangle = \mathbb{Q}(\sqrt{6})$, $X_1(11)$ has non-zero rank with point of infinite order $G_K = (18 - 7T : 103 - 42T : 1)$. We compute

k	$[k]G_K = (t, s)$	rank
1	$(18 - 7T, 103 - 42T, 1)$	1

for which $\tilde{\alpha}(E) = -3.178$. This curve can help factoring numbers of the form $b^{6n} \pm 1$.

6.3.2. *Statistics for $\tilde{\alpha}$.* For a choice of curves and parameters k, Table 4 gathers some statistics on our curves using our heuristic function $\tilde{\alpha}$. Some of these values are comparable with those in [8].

M_1, M_2	defining polynomial for K	k	α
$4, 8$	$\Phi_{10}(X)$	1	-4.225
$4, 8$	$X^4 + X^3 + 2X^2 - 4X + 3$	59	-4.178
$4, 8$	$X^2 + 5$	85	-4.150
$2, 12$	$X^4 + X^3 + 2X^2 - 4X + 3$	21	-3.871
$2, 12$	$X^4 + X^3 + 2X^2 - 4X + 3$	10	-3.857
$2, 12$	$X^4 + X^3 + 2X^2 - 4X + 3$	75	-3.857
$2, 12$	$X^4 + X^3 + 2X^2 - 4X + 3$	66	-3.853
$2, 12$	$X^2 + 5$	49	-3.847
11	$\Phi_8(X)$	91	-3.248
11	$\Phi_8(X)$	10	-3.243
11	$\Phi_8(X)$	56	-3.234
11	$\Phi_8(X)$	43	-3.232
11	$X^4 + X^3 + 2X^2 - 4X + 3$	43	-3.231

Table 4. Examples of small values of $\tilde{\alpha}$.

6.4. **Examples of factorizations.** The typical use is in factoring numbers of the form $A^n \pm B^n$, among which we find the Cunningham project [15] and the tables of Brent/Montgomery/te Riele available at `http://myfactors.mooo.com/`. In our program, we use examples obtained from Table 2. We use GMP-ECM as the core ECM factoring program. Our findings are reported in [52] and its updates and consist of more than 100 factors found (at the date of this submission). Let us sketch the preliminary algorithm for factoring $N \mid b^n + s$ (Algorithm 4).

Algorithm 4: Factoring $b^n \pm 1$

```
Function Factoring($b, n, s, N$)
    Input  : $N \mid b^n + s$, $s \in \{\pm 1\}$
    Output: Factor of $N$
    if $s = 1$ then
        $n \leftarrow 2n$
    // Now, $b^n \equiv 1 \bmod N$
    $g \leftarrow \gcd(b^n - 1, N)$
    if $g > 1$ then
        return $g$
    // Compute roots of unity modulo $N$
    for all prime divisors $d$ of $n$ do
        $\zeta_d \leftarrow b^{n/d} \bmod N$
    // Compute square-roots
    for all prime factors $q$ of $n$ do
        compute $\sqrt{q^*} \bmod N$ as explained in Section 5
    Compute all possible $\sqrt{m} \bmod N$ by multiplication of known square-roots
    Use $\zeta_d$ in modular curves $X_1(M_1, M_2)$ with $d \mid M_1$ in ECM, since $p \equiv 1 \bmod d$
    Use $K = \mathbb{Q}(\sqrt{m})$ and corresponding modular curves in ECM
```

6.4.1. *Quadratic examples.* We extract large numbers, forming Table 5 and were obtained on the cluster of our team; the symbol dd denotes the number of decimal digits of N or of p depending on the column.

N factor of (dd)	$p \mid N$	dd	torsion, poly
$90, 136+ (243)$	95029336145694838957824482284328662990992760116961	50	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z}, Z^2+2$
$\langle 2 \rangle \times \langle 2 \cdot 3^3 \cdot 5 \cdot 7 \cdot 17 \cdot 23^2 \cdot 557 \cdot 93169 \cdot 191507 \cdot 211093 \cdot 3555857 \cdot 19430611 \cdot 19286145689 \rangle$			
$59, 148+ (246)$	6153600891183451358288633718234351691755490502156977	52	$\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}, Z^2-37$
$\langle 2^2 \rangle \times \langle 2^4 \cdot 3^4 \cdot 31 \cdot 383 \cdot 659 \cdot 12413 \cdot 44087 \cdot 176261 \cdot 269231 \cdot 4538333 \cdot 5268647 \cdot 244317397 \rangle$			
$74, 145+ (210)$	3242269523406605838609691912552260883503075877086401	52	$\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}, Z^2-5$
$\langle 2^2 \rangle \times \langle 2^3 \cdot 11 \cdot 13 \cdot 53 \cdot 839 \cdot 1427 \cdot 32647 \cdot 658663 \cdot 792277 \cdot 1532647 \cdot 8783009 \cdot 48689154383 \rangle$			
$517, 67- (180)$	43673375920790464063197381024563082702565341226931	50	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}, Z^2-67$
$\langle 2 \rangle \times \langle 2^4 \cdot 3^5 \cdot 11 \cdot 17 \cdot 31^2 \cdot 47 \cdot 40151 \cdot 500389 \cdot 717341 \cdot 761489 \cdot 1183837 \cdot 51181421299 \rangle$			
$69, 145- (196)$	43973740306053298612759811200943577004074844768891	50	$\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}, Z^2-29$
$\langle 2 \rangle \times \langle 2^3 \cdot 5 \cdot 13 \cdot 1381 \cdot 834469 \cdot 1456837 \cdot 3504673 \cdot 29722321 \cdot 37912759 \cdot 6377193661 \rangle$			
$69, 145+ (136)$	2312935912505799788408225250017130492549337428188531	52	$\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}, Z^2-29$
$\langle 2 \rangle \times \langle 2^2 \cdot 11 \cdot 13 \cdot 43 \cdot 66499 \cdot 236681 \cdot 351023 \cdot 1047667 \cdot 3274151 \cdot 18302677 \cdot 135555908207 \rangle$			

Table 5. Some factorizations: each second line contains the group structure

The last two rows contain factorizations illustrate the discussion after Proposition 2.2. The desired torsion group is $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$ but the reduction falls on a twist modulo p. We keep 2-torsion points, and we have luck that the cardinalities of the twists are smooth.

6.4.2. *With a subfield of a cyclotomic field.* Consider $N = (737^{67}+1)/(269 \cdot 5227)$. Since 67 is prime, the situation is slightly more difficult. A 67-th root of unity is $b = 737^2$. The field $\mathbb{Q}(\zeta_{67})$ has a subfield K of degree 3 generated by $f(X) = X^3+X^2-22X+5$. It turns out that $X_1(2, 12)_K$ has rank 1, generated by $P_\infty = (-T^2/3 - T/3 + 28/3 : 7T^2/6 + 7T/8 - 649/24 : 1)$. The curve corresponding to $[21]P_\infty$ on X_1 modulo N is

$$m_a = 556252050226768787427471559967481290265336087385792522658530539830903255633105716 21\backslash$$

$$26394377497799681191808482285866668708887092670840892300135319849910159488826805940581441408611 82001,$$

$$m_b = 1092565450992883745690146579644261206321930585106252648233689673035960992306920171 6\backslash$$

$$40211050246154450721262000915737211314570736437198630487788372189761322680155455564821752482710626384.$$

With $B_1 = 43 \cdot 10^6$ and $B_2 = 240490660426$, GMP-ECM finds the 48 digits prime divisor $p = 870917417466838788698821597667901172952093040299$. We find that $E \bmod p$ has two generators of respective orders

$$n_1 = 2, n_2 = 2^3 \cdot 3 \cdot 5 \cdot 19 \cdot 907 \cdot 5413 \cdot 8807 \cdot 22973 \cdot 553103 \cdot 4764239 \cdot 6769901 \cdot 10778026289.$$

7. Final comments

We have described a possible use of modular curves of genus 1 for building curves with large torsion groups for ECM. Curves of larger genus can only give use sporadic points and no useful family. It remains to be seen how to compute the friendliness of the proposed curves or wait for more curves to appear, as was the case for the rational case.

Acknowledgments

The author would like to thank J. Cremona and T. A. Fisher for discussions on the properties of $X(5)$; R. Barbulescu for sharing his joint work on the friendliness of elliptic curves for ECM; B. Smith and A. Leroux around elliptic curves, isogenies and computations; J. Crombie about his web server for storing factorizations of $b^n \pm 1$ for large b's. I hereby acknowledge the very useful reports of the referees that did a lot to improve this article. During the ANTS meeting, I had interesting questions and discussions with D. Harvey and D. Gordon; thanks to them.

Conflicts of Interest Statement

The author asserts that there are no conflicts of interest.

Data Availability Statement

A file containing data in human readable format is available as `http://www.lix.polytechnique.fr/Labo/Francois.Morain/ECM/X1_data.mag`.

References

[1] J. Aguirre, A. Dujella, M. Jukić Bokun, and J. C. Peral. High rank elliptic curves with prescribed torsion group over quadratic fields. *Period. Math. Hungar.*, 68(2):222–230, 2014.

[2] A. O. L. Atkin. Probabilistic primality testing. In P. Flajolet and P. Zimmermann, editors, *Analysis of Algorithms Seminar I.* INRIA Research Report XXX, 1992. Summary by F. Morain.

[3] A. O. L. Atkin and F. Morain. Elliptic curves and primality proving. *Math. Comp.*, 61(203):29–68, July 1993.

[4] A. O. L. Atkin and F. Morain. Finding suitable curves for the elliptic curve method of factorization. *Math. Comp.*, 60(201):399–405, January 1993.

[5] E. Bach and K. Huber. Note on square roots mod$N$. *IEEE Trans. Inform. Theory*, 45:807–809, 1999.

[6] R. Barbulescu. Familles de courbes adaptées à la factorisation des entiers. Rapport de stage M1, 2009.

[7] R. Barbulescu, J. W. Bos, C. Bouvier, T. Kleinjung, and P. L. Montgomery. Finding ECM-friendly curves through a study of Galois properties. In *ANTS X—Proceedings of the Tenth Algorithmic Number Theory Symposium*, volume 1 of *Open Book Ser.*, pages 63–86. Math. Sci. Publ., Berkeley, CA, 2013.

[8] R. Barbulescu and S. Shinde. A classification of ECM-friendly families using modular curves. *Mathematics of Computation*, September 2021. intégré à la thèse de doctorat de Sudarshan Shinde, Sorbonne Université, 10 juillet 2020.

[9] D. J. Bernstein, P. Birkner, T. Lange, and C. Peters. ECM using Edwards curves. *Math. Comput.*, 82(282):1139–1179, 2013. Follow-up `http://eecm.cr.yp.to/eecm-20111008.pdf`.

[10] D. J. Bernstein, C. Chuengsatiansup, D. Kohel, and T. Lange. Twisted Hessian curves. In K. E. Lauter and F. Rodríguez-Henríquez, editors, *Progress in Cryptology - LATINCRYPT 2015 - 4th International Conference on Cryptology and Information Security in Latin America, Guadalajara, Mexico, August 23-26, 2015, Proceedings*, volume 9230 of *Lecture Notes in Computer Science*, pages 269–294. Springer, 2015.

[11] N. Billerey. Critères d'irréductibilité pour les représentations des courbes elliptiques. *Int. J. Number Theory*, 7(4):1001–1032, 2011.

[12] J. Bosman, P. Bruin, A. Dujella, and F. Najman. Ranks of elliptic curves with prescribed torsion over number fields. *Int. Math. Res. Not. IMRN*, (11):2885–2923, 2014.

[13] R. P. Brent. Some integer factorization algorithms using elliptic curves. *Australian Computer Science Communications*, 8:149–163, 1986.

[14] E. Brier and C. Clavier. New families of ECM curves for Cunningham numbers. In G. Hanrot, F. Morain, and E. Thomé, editors, *Algorithmic Number Theory*, volume 6197 of *Lecture Notes in Comput. Sci.*, pages 96–109. Springer-Verlag, 2010. 9th International Symposium, ANTS-IX, Nancy, France, July 2010, Proceedings.

[15] J. Brillhart, D. H. Lehmer, J. L. Selfridge, B. Tuckerman, and S. S. Wagstaff, Jr. *Factorizations of* $b^n \pm 1,\ b = 2, 3, 5, 6, 7, 10, 11, 12$ *up to high powers.* Number 22 in Contemporary Mathematics. AMS, 2 edition, 1988.

[16] D. V. Chudnovsky and G. V. Chudnovsky. Sequences of numbers generated by addition in formal groups and new primality and factorization tests. *Adv. in Appl. Math.*, 7:385–434, 1986.

[17] C. Costello and B. Smith. Montgomery curves and their arithmetic - the case of large characteristic fields. *J. Cryptogr. Eng.*, 8(3):227–240, 2018.

[18] J. E. Cremona and F. Najman. $\mathbb{Q}$-curves over odd degree number fields. *Res. Number Theory*, 7(4):Paper No. 62, 30, 2021.

[19] H. Davenport. *Multiplicative number theory*, volume 74 of *Graduate Texts in Mathematics*. Springer–Verlag, 2nd edition, 1980.

[20] M. Derickx and F. Najman. Torsion of elliptic curves over cyclic cubic fields. *Math. Comp.*, 88(319):2443–2459, 2019.

[21] M. Derickx and A. V. Sutherland. Torsion subgroups of elliptic curves over quintic and sextic number fields. *Proc. Amer. Math. Soc.*, 145(10):4233–4245, 2017.

[22] A. Dujella. High rank elliptic curves with prescribed torsion. `https://web.math.pmf.unizg.hr/~duje/tors/tors.html`.

[23] A. Dujella. Infinite families of elliptic curves with high rank and prescribed torsion. `https://web.math.pmf.unizg.hr/~duje/tors/generic.html`.

[24] A. Dujella, M. Kazalicki, and J. C. Peral. Elliptic curves with torsion groups $\mathbb{Z}/8\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$. *Revista de la Real Academia de Ciencias Exactas, Fsicas y Naturales. Serie A. Matemticas*, 115(4), Aug 2021.

[25] A. Dujella and F. Najman. Elliptic curves with large torsion and positive rank over number fields of small degree and ECM factorization. *Period. Math. Hungar.*, 65(2):193–203, 2012.

[26] A. Dujella and J. C. Peral. Elliptic curves with torsion group $\mathbb{Z}/8\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$. In *Trends in number theory*, volume 649 of *Contemp. Math.*, pages 47–62. Amer. Math. Soc., Providence, RI, 2015.

[27] N. D. Elkies. On elliptic K-curves. In *Modular curves and abelian varieties*, volume 224 of *Progr. Math.*, pages 81–91. Birkhäuser, Basel, 2004.

[28] S. Fermigier. Exemples de courbes elliptiques de grand rang sur $\mathbf{Q}(t)$ et sur $\mathbf{Q}$ possédant des points d'ordre 2. *C. R. Acad. Sci. Paris Sér. I Math.*, 322(10):949–957, 1996.

[29] A. Gélin, T. Kleinjung, and A. K. Lenstra. Parametrizations for families of ecm-friendly curves. In M. A. Burr, C. K. Yap, and M. S. E. Din, editors, *Proceedings of the 2017 ACM on International Symposium on Symbolic and Algebraic Computation, ISSAC 2017, Kaiserslautern, Germany, July 25-28, 2017*, pages 165–171. ACM, 2017.

[30] D. Jeon, C. H. Kim, and Y. Lee. Families of elliptic curves over cubic number fields with prescribed torsion subgroups. *Math. Comp.*, 80(273):579–591, 2011.

[31] D. Jeon, C. H. Kim, and Y. Lee. Families of elliptic curves over quartic number fields with prescribed torsion subgroups. *Math. Comp.*, 80(276):2395–2410, 2011.

[32] S. Kamienny. Torsion points on elliptic curves and q-coefficients of modular forms. *Invent. Math.*, 109(2):221–229, 1992.

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

[34] S. Kihara. Construction of high-rank elliptic curves with a non-trivial rational point of order 2. *Proc. Japan Acad. Ser. A Math. Sci.*, 73(5):165, 1997.

[35] S. Kihara. On the rank of elliptic curves with three rational points of order 2. II. *Proc. Japan Acad. Ser. A Math. Sci.*, 73(8):151, 1997.

[36] F. Klein. *Vorlesungen über das Ikosaeder und die Auflösung des Gleichungen fünften Grades*. Teubner, Leipzig, 1884.

[37] D. Kohel. Addition law structure of elliptic curves. *J. Number Theory*, 131(5):894–919, 2011.

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

[39] L. Kulesz. Courbes elliptiques de rang ≥ 5 sur $\mathbf{Q}(t)$ avec un groupe de torsion isomorphe à $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$. *C. R. Acad. Sci. Paris Sér. I Math.*, 329(6):503–506, 1999.

[40] L. Kulesz. Families of elliptic curves of high rank with nontrivial torsion group over $\mathbb{Q}$. *Acta Arith.*, 108(4):339–356, 2003.

[41] L. Kulesz and C. Stahlke. Elliptic curves of high rank with nontrivial torsion group over $\mathbb{Q}$. *Experiment. Math.*, 10(3):475–480, 2001.

[42] O. Lecacheux. Rang de courbes elliptiques sur $\mathbf{Q}$ avec un groupe de torsion isomorphe à $\mathbf{Z}/5\mathbf{Z}$. *C. R. Acad. Sci. Paris Sér. I Math.*, 332(1):1–6, 2001.

[43] O. Lecacheux. Rang de courbes elliptiques avec groupe de torsion non trivial. *J. Théor. Nombres Bordeaux*, 15(1):231–247, 2003. Les XXIIèmes Journées Arithmetiques (Lille, 2001).

[44] O. Lecacheux. Rang de familles de courbes elliptiques. *Acta Arith.*, 109(2):131–142, 2003.

[45] O. Lecacheux. Rang de courbes elliptiques dont le groupe de torsion est non trivial. *Ann. Sci. Math. Québec*, 28(1-2):145–151 (2005), 2004.

[46] H. W. Lenstra, Jr. Factoring integers with elliptic curves. *Ann. of Math. (2)*, 126:649–673, 1987.

[47] B. Mazur. Rational points on modular curves. In *Modular forms of one variable V*, volume 601 of *Lecture Notes in Math.*, pages 107–148. Springer Verlag, 1977. Proceedings International Conference, University of Bonn, Sonderforschungsbereich Theoretische Mathematik, July 2-14, 1976.

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

[49] P. L. Montgomery. Speeding the Pollard and elliptic curve methods of factorization. *Math. Comp.*, 48(177):243–264, January 1987.

[50] P. L. Montgomery. *An FFT extension of the Elliptic Curve Method of factorization*. PhD thesis, University of California – Los Angeles, 1992.

[51] F. Morain. Implementing the asymptotically fast version of the elliptic curve primality proving algorithm. *Math. Comp.*, 76:493–505, 2007.

[52] F. Morain. Some factors of numbers of the form $b^n \pm 1$ found using ecm with new classes of curves, 2022.

[53] K. Nagao. Construction of high-rank elliptic curves with a nontrivial torsion point. *Math. Comp.*, 66(217):411–415, 1997.

[54] F. Najman. Some rank records for elliptic curves with prescribed torsion over quadratic fields. *An. Ştiinţ. Univ. "Ovidius" Constanţa, Ser. Mat.*, 22(1):215–219, 2014.

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

[56] F. P. Rabarison. Structure de torsion des courbes elliptiques sur les corps quadratiques. *Acta Arith.*, 144(1):17–52, 2010.

[57] M. A. Reichert. Explicit determination of nontrivial torsion structures of elliptic curves over quadratic number fields. *Math. Comp.*, 46(174):637–658, April 1986.

[58] J. H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Grad. Texts in Math.* Springer, 1986.

[59] H. Suyama. Informal preliminary report (8). 25 Oct 1985.

[60] A. Trbović. Torsion groups of elliptic curves over quadratic fields $\mathbb{Q}(\sqrt{d})$, $0 < d < 100$. *Acta Arith.*, 192(2):141–153, 2020.

[61] J. Wang. On the cyclic torsion of elliptic curves over cubic number fields. *J. Number Theory*, 183:291–308, 2018.

[62] J. Wang. On the cyclic torsion of elliptic curves over cubic number fields (II). *J. Théor. Nombres Bordeaux*, 31(3):663–670, 2019.

[63] J. Wang. On the cyclic torsion of elliptic curves over cubic number fields (iii), 2020.

[64] H. C. Williams. A $p+1$ method of factoring. *Math. Comp.*, 39(159):225–234, July 1982.

[65] P. Zimmermann and B. Dodson. 20 years of ECM. In F. Hess, S. Pauli, and M. Pohst, editors, *Algorithmic Number Theory – ANTS-VII*, volume 4076 of *Lecture Notes in Comput. Sci.*, pages 525–542. Springer-Verlag, 2006.

[66] P. Zimmermann et al. GMP-ECM (elliptic curve method for integer factorization). `https://gforge.inria.fr/projects/ecm/`, 2010.

LIX - Laboratoire d'Informatique de l'École Polytechnique, CNRS, Institut Polytechnique de Paris and GRACE - Inria Saclay–le-de-France, France

Email address: `morain@lix.polytechnique.fr`