LMS J. Comput. Math. 19 (Special issue A) (2016) 83–99
doi:10.1112/S1461157016000231

JKL-ECM: an implementation of ECM using Hessian curves

Henriette Heer, Gary McGuire and Oisín Robinson

Abstract

We present JKL-ECM, an implementation of the elliptic curve method of integer factorization which uses certain twisted Hessian curves in a family studied by Jeon, Kim and Lee. This implementation takes advantage of torsion subgroup injection for families of elliptic curves over a quartic number field, in addition to the 'small parameter' speedup. We produced thousands of curves with torsion $\mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$ and small parameters in twisted Hessian form, which admit curve arithmetic that is 'almost' as fast as that of twisted Edwards form. This allows JKL-ECM to compete with GMP-ECM for finding large prime factors. Also, JKL-ECM, based on GMP, accepts integers of arbitrary size. We classify the torsion subgroups of Hessian curves over $\mathbb{Q}$ and further examine torsion properties of the curves described by Jeon, Kim and Lee. In addition, the high-performance curves with torsion $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$ of Bernstein *et al.* are completely recovered by the $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$ family of Jeon, Kim and Lee, and hundreds more curves are produced besides, all with small parameters and base points.

1. *Introduction*

The elliptic curve method (ECM) [**17**] for factorization of integers is used for finding 'small' factors of composite integers, which are difficult to factor by other methods.

We wish to investigate the use of Hessian curves, and a particular subclass consisting of curves arising in families described by Jeon, Kim and Lee (JKL) [**15**], in ECM. These curves have a large torsion subgroup over a quartic number field, which yields an improvement to ECM as outlined in [**5**, § 6], for curves over $\mathbb{Q}$, and [**9**, § 5] for curves over quartic number fields (also referred to in [**11**]). In particular, we focus on JKL curves that have torsion subgroup $\mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$ and $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$ over a quartic number field.

We are able to generate a large number of suitable JKL curves with small parameters and positive rank. Specifically, in the $\mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$ case, we are able to generate over 8000 curves in a short time. These curves have a natural representation in twisted Hessian form, and all our curves have a point of infinite order with small height, and small parameters, two things that combine to yield a speedup for scalar multiplication for this class of curves. We present the details in § 3. The larger number of curves facilitates finding large factors and setting records for ECM. In § 4 we study the torsion subgroup of Hessian curves and JKL curves over $\mathbb{Q}$ and over the relevant quartic extension of $\mathbb{Q}$. We present our implementation of ECM using these JKL curves, and compare timings, in § 5.

Along the way we briefly mention JKL curves that have torsion subgroup $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$, but these are not the primary focus of this paper, as in practice they are not generated as quickly as the $\mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$ family. However, we did generate over 700 curves in twisted Edwards form with torsion $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$, and small parameters, and point of infinite order with small

Received 17 February 2016.

2010 Mathematics Subject Classification 11Y05 (primary), 11G05, 14H52 (secondary).

Contributed to the Twelfth Algorithmic Number Theory Symposium (ANTS-XII), Kaiserslautern, Germany, 29 August–2 September 2016.

Research of the second and third authors was supported by the Science Foundation Ireland Grant 13/IA/1914.

height, and surprisingly these include the 25 highest-performance curves found by [5]. These 700 curves can be used directly in EECM-MPFQ.

2. *Elliptic curves*

Let K be any field. The (short) Weierstrass form of an elliptic curve over K is $y^2 = x^3 + ax + b$ where $a, b \in K$.

For an elliptic curve E defined over K we use the notation $E(K)$ for the group of K-rational points, and $E(K)[m]$ denotes the subgroup of m-torsion points.

2.1. *Edwards form*

An *Edwards curve* [12] over K is a curve defined by the equation

$$E_d : x^2 + y^2 = 1 + dx^2y^2,$$

where $d \in K \backslash \{0, 1\}$.

Let $a, d \in K$ be distinct, nonzero elements. The *twisted Edwards curve* [4] is the curve

$$E_{a,d} : ax^2 + y^2 = 1 + dx^2y^2.$$

Every twisted Edwards curve is birationally equivalent to a curve in Weierstrass form.

The identity is (0:1:1) and the inverse of $P = (X{:}Y{:}Z)$ is $-P = (-X{:}Y{:}Z)$.

2.2. *Hessian form*

A *projective twisted Hessian curve* over K has the form

$$H_{a,d} : aX^3 + Y^3 + Z^3 = dXYZ \tag{2.1}$$

and specified point $(0{:}-1{:}1)$, whenever $a, d \in K$, $a(27a - d^3) \neq 0$. A *Hessian* curve is a twisted Hessian curve that has $a = 1$. See [7] for further details on twisted Hessian curves.

One can transform back and forth between Hessian curves and twisted Hessian curves (see [7]). Throughout this paper, all theoretical results will refer to Hessian curves, while the implementation will transform the Hessian curve into a twisted Hessian and work with twisted Hessian curves. This is because retaining two parameters a and d allows both to be small and yields faster arithmetic.

2.3. *The JKL families*

2.3.1. *JKL torsion family* $\mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$. Here we state a theorem of [15] which allows the generation of curves with $\mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$ torsion over the given quartic number field.

THEOREM 2.1. *Let* $K = \mathbb{Q}(\sqrt{-3}, \sqrt{8t^3 + 1})$, *with* $t \in \mathbb{Q}$ *and* $t \neq 0, 1, -\frac{1}{2}$, *and let* E_μ *be an elliptic curve defined by the equation*

$$E_\mu : y^2 = x^3 - 27\mu(\mu^3 + 8)x + 54(\mu^6 - 20\mu^3 - 8)$$

where

$$\mu = \frac{2t^3 + 1}{3t^2}.$$

Then the torsion subgroup of E_μ *over* K *is equal to* $\mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$ *for almost all* t.

https://doi.org/10.1112/S1461157016000231 Published online by Cambridge University Press

We can easily write down the equation for these curves in twisted Hessian form. The parameter μ above is actually already the parameter of the Hessian curve

$$X^3 + Y^3 + Z^3 = 3\mu XYZ$$

We let $d/a = 3\mu$, where $d \in \mathbb{Z}\setminus\{0,1\}, a \in \mathbb{Z}\setminus\{0\}$ are coprime. To get a twisted Hessian curve we simply 'twist' the Hessian curve having parameter d by a to get

$$E_H : aX^3 + Y^3 + Z^3 = dXYZ.$$

To find a point (x, y) on E_H from an affine point (u, v) on E_μ we compute

$$x = \frac{36(\mu^3 - 1) - v}{6(u + 9\mu^2)} - \mu/2,$$
$$y = \frac{v + 36(\mu^3 - 1)}{6(u + 9\mu^2)} - \mu/2.$$

2.3.2. *JKL torsion family* $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$. Here we will also state another theorem of [15], which allows the generation of curves with $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$ torsion over the given quartic number field.

THEOREM 2.2. *Let* $K = \mathbb{Q}(\sqrt{-1}, \sqrt{t^4 - 6t^2 + 1})$ *with* $t \in \mathbb{Q}$, $t \neq 0, \pm 1$ *and let* E_ν *be an elliptic curve defined by the equation*

$$y^2 + xy - (\nu^2 - \tfrac{1}{16})y = x^3 - (\nu^2 - \tfrac{1}{16})x^2, \tag{2.2}$$

where $\nu = (t^4 - 6t^2 + 1)/4(t^2 + 1)^2$ *and* $t \neq 0, \pm 1$. *Then*

$$E_\nu(K)_{\text{tors}} \cong \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}.$$

3. *A speedup*

Bernstein *et al.* [5] provided a new implementation of ECM, named EECM-MPFQ [6], which uses twisted Edwards curves and the MPFQ library for large integer arithmetic. As well as a speedup due to the faster group law formulas of Edwards and twisted Edwards curves (in fact also due to the combined use of extended and projective coordinates), another speedup came from the use of curves with small parameters and point coordinates. To find such curves, Bernstein *et al.* conducted an (enhanced) exhaustive search, taking about a week of computation time on a number of computers. The search yielded 78 curves with torsion $\mathbb{Z}/12\mathbb{Z}$ over $\mathbb{Q}$, and 25 curves with torsion $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$ over $\mathbb{Q}$. However, we discovered that the curves produced by the JKL $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$ and $\mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$ families, by generating curves via the rational parameter t increasing in height, end up with small parameters when converted to twisted Edwards and twisted Hessian form, respectively. Not only this, but our search (using Sage) for a point of infinite order for curves with positive rank yielded base points with small projective coordinates. This perfectly suits an implementation of ECM needing the small parameter speedup. In addition, all 25 of Bernstein *et al.*'s small parameter curves with torsion $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$ over $\mathbb{Q}$ are included in the curves generated by the JKL $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$ family. So in fact Bernstein *et al.*'s high-performance $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$ curves have torsion $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$ over the quartic number field of the JKL construction. We also discovered that many of Bernstein *et al.*'s high-performance $\mathbb{Z}/12\mathbb{Z}$ curves are recovered by the JKL $\mathbb{Z}/24\mathbb{Z}$ family.

https://doi.org/10.1112/S1461157016000231 Published online by Cambridge University Press

For a comparison of our computation against that of Bernstein *et al.*, see Table 1.

We can generate curves very quickly since we have a parameterized family. The curve parameters and base point coordinates tend to slowly increase in height as the height of the curve parameter t is increased, very slowly in the case of the $\mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$ family. This allows the generation of hundreds of $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$ curves, and thousands of $\mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$ curves. In the latter case, not all curves had unique j-invariants, and in fact some were isogenous, but there still remained thousands of unique nonisogenous curves.

The JKL curves with $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$ torsion all have torsion $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$ over $\mathbb{Q}$, see Theorem 4.2. Since they have a point of order 4 over $\mathbb{Q}$ (see Lemma 4.1), they are birationally equivalent over $\mathbb{Q}$ to Edwards curves, and hence to twisted Edwards curves, allowing an immediate improvement to EECM-MPFQ; just augment the list of curves. Indeed, suppose we have a point $P = (r, s)$ of order 4 with $r, s \in \mathbb{Q}$ on the JKL curve with Weierstrass form $E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$. To convert this to twisted Edwards form, compute $v = 1 - 4r^3/s^2$. Then $d = \text{numerator}(v), a = \text{denominator}(v)$ are the parameters of the twisted Edwards curve $E_{a,d} : ax^2 + y^2 = 1 + dx^2y^2$. If we have $Q = (x, y) \in E(\mathbb{Q})$, then $R = (2x/y, (x - a + d)/(x + a - d)) \in E_{a,d}(\mathbb{Q})$.

We conjecture that none of the JKL curves with torsion $\mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$ are isogenous to twisted Edwards curves over $\mathbb{Q}$.

3.1. *Performance of twisted Hessian arithmetic*

Bernstein *et al.*'s combination of twisted Edwards arithmetic, together with the use of extended and projective coordinates, emerged as the winner of the curve arithmetic speed contest among the popular curve forms. In fact Hisil *et al.* in [14] conducted an exhaustive search for fast curve arithmetic formulas, yielding many formulas for the different curve forms, but none faster than is possible with the use of twisted Edwards curves. It may be unlikely that faster formulas exist. However, good use can still be made of the 4800+ curves generated from the JKL $\mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$ family, which have a natural representation in twisted Hessian form, in which case they have small parameters/base points, since twisted Hessian arithmetic is 'almost' as fast as twisted Edwards arithmetic (at least in terms of operation counts). Twisted Edwards doubling in projective coordinates can be done in $3M + 4S + 1a + 6add + 1 * 2$, while addition for the same can be done in $10M + 1S + 1a + 1d + 7add$; see [3]. Here N is the number to be factored, $n = \log(N)$, M denotes multiplication, S denotes squaring, a, d denote multiplication by curve constants, add denotes addition, 2 denotes multiplication by 2, all mod N. In comparison, twisted Hessian doubling in projective coordinates can be done in $7M + 1S + 1d + 7add$, while addition for the same can be done in $12M + 1a + 3add$; see [3]. In the specific context of scalar multiplication of a fixed point, we can effectively reduce addition from $12M + 1a + 3add$ to about $6M + 6m + 1a + 3add$, where m denotes multiplication by a small constant. This is because $6M$ costs $O(n)$ rather than $O(n^2)$ (see below). We can compare this to the method used in EECM-MPFQ, which uses an extended coordinate variant of the addition law presented in [13] costing $9M + 1a$. This is combined with projective doubling, and the total cost in EECM-MPFQ for a double-and-add operation is $(3M + 4S + 1a) + (9M + 1a)$.

TABLE 1. *Resources for generation of small-parameter curves for ECM.*

	#Curves	Type	Torsion	Time	Resources
EECM-MPFQ	25	Edwards	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$	1 week	Several computers
EECM-MPFQ	78	Edwards	$\mathbb{Z}/12\mathbb{Z}$	1 week	Several computers
This work	700	Edwards	$\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$	2 weeks	One desktop computer
This work	4840	Hessian	$\mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$	2 weeks	One desktop computer

https://doi.org/10.1112/S1461157016000231 Published online by Cambridge University Press

Since doublings cannot really take advantage of small coordinates, we cannot apply our idea to twisted Hessian doubling, so our doubling cost remains the same, for a total double-and-add cost of $(7M + 1S + 1d) + (6M + 6m + 1a)$.

The twisted Hessian curve addition law (one of a number of possibilities) is reproduced below so that the idea of this speedup is clear. Note that $(X_1{:}Y_1{:}Z_1)$ is fixed, with small coordinate values, and likewise the curve parameter a is small (d is typically small too, but it is not used in point addition).

We did not implement windowing methods for the stage 1 scalar multiplication, which would have given a slight speedup (see e.g. [8]), but instead we avoid a higher memory cost for stage 1.

We use the following procedure for addition on twisted Hessian curves.

$$\begin{gathered}\text{Input: Points } (X_1{:}Y_1{:}Z_1),\ (X_2{:}Y_2{:}Z_2) \text{ on a twisted Hessian curve } E\\ \text{with equation } aX^3 + Y^3 + Z^3 = dXYZ\\ \text{Output: Point } (X_3{:}Y_3{:}Z_3) = (X_1{:}Y_1{:}Z_1) + (X_2{:}Y_2{:}Z_2) \text{ on } E\end{gathered}$$

$$\begin{gathered}A = X_1 \cdot Z_2, \quad B = Z_1 \cdot Z_2, \quad C = Y_1 \cdot X_2,\\ D = Y_1 \cdot Y_2, \quad E = Z_1 \cdot Y_2, \quad F = a \cdot X_1 \cdot X_2,\\ X_3 = A \cdot B - C \cdot D, \quad Y_3 = D \cdot E - F \cdot A, \quad Z_3 = F \cdot C - B \cdot E.\end{gathered}$$

Since one of the integers involved in calculating A, B, C, D, E, F is small, those multiplications approach $O(n)$ rather than $O(n^2)$, so in effect there are only six multiplications that are $O(n^2)$. The identity is $(0{:}-1{:}1)$ and the inverse of $P = (X{:}Y{:}Z)$ is $-P = (X{:}Z{:}Y)$.

4. *Torsion of JKL and Hessian curves*

In this section we study the torsion points on JKL curves, and Hessian curves (not twisted Hessian). Note that rather than using the addition formulas as stated above, we use the following addition law.

Let $P_1 = (x_1{:}y_1{:}z_1)$, $P_2 = (x_2{:}y_2{:}z_2)$, $P_1 \neq P_2$ and set

$$\begin{aligned}x_3 &= y_1^2 x_2 z_2 - y_2^2 x_1 z_1,\\ y_3 &= x_1^2 y_2 z_2 - x_2^2 y_1 z_1,\\ z_3 &= z_1^2 y_2 x_2 - z_2^2 y_1 x_1.\end{aligned}$$

Then $P_1 + P_2 = (x_3{:}y_3{:}z_3)$.

For doubling we obtain the formula

$$2P_1 = (y_1(z_1^3 - x_1^3){:}x_1(y_1^3 - z_1^3){:}z_1(x_1^3 - y_1^3)).$$

The identity of this addition law is the point $\mathcal{O} = (1{:}-1{:}0)$ at infinity and $-(x{:}y{:}z) = (y{:}x{:}z)$.

A coordinate transformation $x \to z'$, $z \to x'$ sends the curve $H : x^3 + y^3 + z^3 = dxyz$ with specified point $(0{:}-1{:}1)$ and corresponding addition law to the curve $H' : (x')^3 + (y')^3 + (z')^3 = dx'y'z'$ with specified point $(1{:}-1{:}0)$ and addition law defined as above.

4.1. *JKL curves with torsion* $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$

We will study the torsion of the $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$ family of JKL curves. From now on, let K denote the quartic number field $K = \mathbb{Q}(\sqrt{-1}, \sqrt{t^4 - 6t^2 + 1})$ and E_ν the JKL curve $E_\nu : y^2 + xy - (\nu^2 - \frac{1}{16})y = x^3 - (\nu^2 - \frac{1}{16})x^2$ with $\nu = (t^4 - 6t^2 + 1)/4(t^2 + 1)^2$ and $t \neq 0, \pm 1$, $t \in \mathbb{Q}$.

https://doi.org/10.1112/S1461157016000231 Published online by Cambridge University Press

Since $\mathrm{char}(K) = 0$, we can transform E_ν into a short Weierstrass form

$$E_\nu : y^2 = x^3 + px + q \tag{4.1}$$

with

$$p = -\tfrac{1}{3}(\nu^4 + \tfrac{7}{8}\nu^2 + \tfrac{1}{256}) \quad \text{and} \quad q = -\tfrac{2}{27}\nu^6 + \tfrac{11}{72}\nu^4 + \tfrac{11}{1152}\nu^2 - \tfrac{1}{55296},$$

and ν as above.

We use the following lemma to calculate the torsion subgroup of E_ν over $\mathbb{Q}$.

LEMMA 4.1. *Every JKL curve E_ν has at least four points of order 4 defined over $\mathbb{Q}$.*

Proof. Consider the fourth division polynomial:

$$\frac{\psi_4}{y} = 4(x^6 + 5px^4 + 20qx^3 - 5p^2x^2 - 4pqx - 8q^2 - p^3).$$

Inserting p and q from above leads to

$$\begin{aligned}\frac{\psi_4}{y} = {} & \frac{-1}{3057647616}(80\nu^2 - 48x - 1)(16\nu^2 + 48x - 5) \\ & \times (256\nu^4 + 1536\nu^3 + 1536\nu^2 x - 544\nu^2 - 2304\nu x + 2304x^2 + 96\nu + 96x + 1) \\ & \times (256\nu^4 - 1536\nu^3 - 544\nu^2 - 96\nu + 1 + (1536\nu^2 + 2304\nu + 96)x + 2304x^2).\end{aligned}$$

This shows immediately two rational roots, namely

$$x_1 = \tfrac{5}{3}\nu^2 - \tfrac{1}{48} \quad \text{and} \quad x_2 = -\tfrac{1}{3}\nu^2 + \tfrac{5}{48}.$$

Using x_1 and x_2, we can determine the corresponding y-coordinates.

Insert x_1 into $y^2 = x^3 + px + q$ to get

$$y_1^2 = \tfrac{1}{64}(4\nu + 1)^2(4\nu - 1)^2\nu^2 \quad \text{and therefore } y_1 = \pm\tfrac{1}{8}(4\nu + 1)(4\nu - 1)\nu.$$

Similarly, we get

$$y_2 = \pm\tfrac{1}{32}(4\nu + 1)(4\nu - 1)$$

and four points of order 4:

$$\begin{aligned}P_{11} &= (\tfrac{5}{3}\nu^2 - \tfrac{1}{48}, -\tfrac{1}{8}(4\nu + 1)(4\nu - 1)\nu), \\ P_{12} &= (\tfrac{5}{3}\nu^2 - \tfrac{1}{48}, \tfrac{1}{8}(4\nu + 1)(4\nu - 1)\nu), \\ P_{21} &= (-\tfrac{1}{3}\nu^2 + \tfrac{5}{48}, -\tfrac{1}{32}(4\nu + 1)(4\nu - 1)), \\ P_{22} &= (-\tfrac{1}{3}\nu^2 + \tfrac{5}{48}, \tfrac{1}{32}(4\nu + 1)(4\nu - 1))\end{aligned}$$

with clearly rational coefficients. □

THEOREM 4.2. *The torsion subgroup of the JKL curve E_ν over $\mathbb{Q}$ is*

$$E_\nu(\mathbb{Q})_{\mathrm{tors}} = \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}.$$

Proof. Let E_ν/K be a JKL curve. By Lemma 4.1 E_ν has at least four points of order 4. Since $E_\nu(K)_{\mathrm{tors}} = \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$, by Mazur's theorem [**18**] we deduce

$$E_\nu(\mathbb{Q})_{\mathrm{tors}} \in \{\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}, \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}\}.$$

Let $\tilde{P} = (\tilde{x}, \tilde{y})$ with $\tilde{x} = (t^8 + 12t^7 + 20t^6 - 2t^4 - 12t^3 - 4t^2 + 1)/12(t^8 + 4t^6 + 6t^4 + 4t^2 + 1)$ and $\tilde{y} = (t^2 + 2t - 1)(t + 1)^3(t - 1)t^3/2(t^2 + 1)^5$. Straightforward calculations show that $\psi_8(\tilde{P}) = 0$ and $\psi_4(\tilde{P}) \neq 0$. Thus $\tilde{P}$ is a point of order 8 and we can conclude that

$$E(\mathbb{Q})_{\mathrm{tors}} = \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}.$$ □

https://doi.org/10.1112/S1461157016000231 Published online by Cambridge University Press

4.2. *JKL curves with torsion* $\mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$

We consider the JKL curve

$$E_\mu : y^2 = x^3 - 27\mu(\mu^3 + 8)x + 54(\mu^6 - 20\mu^3 - 8)$$

over the quartic number field $K = \mathbb{Q}(\sqrt{-3}, \sqrt{8t^3 + 1})$ for $t \neq 0, 1, -\frac{1}{2}$ and $\mu = (2t^3 + 1)/3t^2$, which has torsion subgroup $\mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$.

By [15], the points of order 2 of E_μ are

$$P_{1,2} = \left(8t^6 + 20t^3 - 1 \pm \frac{3\sqrt{(8t^3+1)^3}}{6t^4}, 0\right) \quad \text{and} \quad P_3 = \left(-\frac{8t^6 + 20t^3 - 1}{3t^4}, 0\right).$$

LEMMA 4.3. *The JKL curve E_μ has exactly one point of order 2 defined over $\mathbb{Q}$.*

Proof. Clearly,

$$P_3 = \left(-\frac{8t^6 + 20t^3 - 1}{3t^4}, 0\right) \in E_\mu(\mathbb{Q}).$$

All we need to show is that $P_{1,2}$ from above are not defined over $\mathbb{Q}$.

We claim that $\sqrt{(8t^3+1)^3} \notin \mathbb{Q}$, which is equivalent to saying that $\sqrt{8t^3+1} \notin \mathbb{Q}$, or that $(2t)^3 + 1$ is not a square in $\mathbb{Q}$. It is well known that the elliptic curve $E : y^2 = x^3 + 1$ defined over $\mathbb{Q}$ has

$$E(\mathbb{Q}) = \{(0, \pm 1), (-1, 0), (2, \pm 3), \mathcal{O}\}.$$

It follows that $(2t)^3 + 1$ is only a square for $t \in \{0, -\frac{1}{2}, 1\}$, which are all not valid values for t. □

LEMMA 4.4. *E_μ has exactly two points of order 3 defined over $\mathbb{Q}$,*

$$P_{1,2} = \left(\frac{1}{3t^4}(2t^3 + 6t^2 + 1)^2, \pm\frac{4}{t^4}(4t^2 - 2t + 1)(t^2 + t + 1)^2\right),$$

and at least two more which are defined over $\mathbb{Q}(\sqrt{-3})$.

Proof. Consider the third division polynomial for elliptic curves in short Weierstrass form $\psi_3 = -(1/9t^{16})(16t^{12} - 96t^{11} + 432t^{10} - 832t^9 + 1152t^8 + 432t^7 - 408t^6 - 72t^5 + 108t^4 + 8t^3 - 12t^2 + (-24t^{10} + 72t^9 + 108t^8 - 24t^7 + 36t^6 - 6t^4)x + 9t^8x^2)(4t^6 + 24t^5 + 36t^4 + 4t^3 + 12t^2 + 1 - 3t^4x)(4t^6 + 4t^3 + 1 + t^4x)$.

We can easily see two roots,

$$x_1 = \frac{4t^6 + 24t^5 + 36t^4 + 4t^3 + 12t^2 + 1}{3t^4} = \frac{(2t^3 + 6t^2 + 1)^2}{3t^4} \in \mathbb{Q}$$

and

$$x_2 = -\frac{4t^6 + 4t^3 + 1}{t^4} \in \mathbb{Q},$$

leading to the points $(x_i, \pm y_i)$, $i = 1, 2$, where

$$y_1^2 = \frac{16}{t^8}(4t^2 - 2t + 1)^2(t^2 + t + 1)^4$$

https://doi.org/10.1112/S1461157016000231 Published online by Cambridge University Press

and

$$y_2^2 = -\frac{16}{27t^{12}}(4t^2-2t+1)^2(t^2+t+1)^4(2t+1)^2(t-1)^4.$$

Thus

$$y_1 = \pm\frac{4}{t^4}(4t^2-2t+1)(t^2+t+1)^2 \in \mathbb{Q},$$
$$y_2 = \pm\frac{4}{9t^6}\sqrt{-3}(4t^2-2t+1)(t^2+t+1)^2(2t+1)(t-1)^2 \in \mathbb{Q}(\sqrt{-3})\backslash\mathbb{Q}.$$

Now consider the quadratic factor of ψ_3. We calculate the roots and obtain

$$\begin{aligned} x_{3,4} &= \frac{1}{3t^4}\left(4t^6-12t^5-18t^4+4t^3-6t^2+1 \pm 6\sqrt{3}\sqrt{-(2t+1)^2(t-1)^4}\cdot t^2\right) \\ &= \frac{1}{3t^4}\left(4t^6-12t^5-18t^4+4t^3-6t^2+1 \pm 6(2t+1)(t-1)^2t^2\sqrt{-3}\right) \end{aligned}$$

which is not in $\mathbb{Q}$. □

Since $E_\mu(K)_{\text{tors}} = \mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$, E_μ cannot have any points of order 4 which are defined over $\mathbb{Q}$ or even K. This also shows that E_μ is not birationally equivalent to a curve in Edwards form.

LEMMA 4.5. *E_μ has two points of order 6 over $\mathbb{Q}$.*

Proof. Consider

$$\psi_6 = \frac{\psi_3}{2y}(\psi_5\psi_2^2 - \psi_1\psi_4^2).$$

Since the roots of ψ_3 are the points of order 3, we can focus on

$$\tilde{\psi_6} = \psi_5\psi_2^2 - \psi_1\psi_4^2.$$

Let $x_1 = (4t^6-24t^5+12t^4-32t^3+24t^2-12t+1)/3t^4 \in \mathbb{Q}$. A straightforward calculation shows $\tilde{\psi_6}(x_1) = 0$ and we get $y_1^2 = (16/t^{10})(4t^2-2t+1)^2(t^2+t+1)^2(t-1)^6$, thus $(x_1, \pm y_1) \in E(\mathbb{Q})[6]$. Since $\psi_3(x_1) \neq 0$, $(x_1 \pm y_1)$ is of order 6. □

With these lemmas, we can now calculate the torsion subgroup of E_μ.

THEOREM 4.6. *Over $\mathbb{Q}$, the JKL curve E_μ has torsion subgroup $\mathbb{Z}/6\mathbb{Z}$ for all μ.*

Proof. From the previous lemmas we already know that $E_\mu(\mathbb{Q})_{\text{tors}}$ has exactly one point of order 2, two of order 3 and at least two points of order 6. Using Mazur's theorem, we can see that

$$E_\mu(\mathbb{Q})_{\text{tors}} \in \{\mathbb{Z}/6\mathbb{Z}, \mathbb{Z}/12\mathbb{Z}, \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}\}.$$

The group cannot be $\mathbb{Z}/12\mathbb{Z}$ because there is no point of order 4 as commented above. Also, $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$ has three points of order 2, while $E_\mu(\mathbb{Q})_{\text{tors}}$ only has one point of order 2 by Lemma 4.3. The only remaining option, therefore, is $E_\mu(\mathbb{Q})_{\text{tors}} = \mathbb{Z}/6\mathbb{Z}$. □

THEOREM 4.7. *Consider the JKL curve E_μ over the quadratic number field $L = \mathbb{Q}(\sqrt{-3})$. Then*

$$E_\mu(L)_{\text{tors}} = \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}.$$

https://doi.org/10.1112/S1461157016000231 Published online by Cambridge University Press

Proof. We already know that $\mathbb{Z}/6\mathbb{Z} \subset E_\mu(L) \subset \mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$. By the theorem of Kamienny, Kenku and Momose (see [16]),

$$E_\mu(L)_{\text{tors}} \in \{\mathbb{Z}/6\mathbb{Z}, \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}, \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}\}.$$

Recall that there are at least four points of order 3 defined over L (see Lemma 4.4). Since both $\mathbb{Z}/6\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$ only have two points of order 3, they cannot be the torsion subgroup of $E_\mu(L)$. Thus $E_\mu(L)_{\text{tors}}$ has to be isomorphic to $\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$. □

THEOREM 4.8. *The torsion subgroup of the JKL curve E_μ over the quadratic number field $L = \mathbb{Q}(\sqrt{8t^3+1})$ is*

$$E_\mu(\mathbb{Q}(\sqrt{8t^3+1}))_{\text{tors}} = \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}.$$

Proof. Analogously to the previous proof, we know that $\mathbb{Z}/6\mathbb{Z} \subset E_\mu(L) \subset \mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$ and again by the Kamienny–Kenku–Momose theorem,

$$E_\mu(L)_{\text{tors}} \in \{\mathbb{Z}/6\mathbb{Z}, \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}, \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}\}.$$

We know that

$$E_\mu(L)[2] = \left\{ \left(8t^6 + 20t^3 - 1 \pm \frac{3\sqrt{(8t^3+1)^3}}{6t^4}, 0\right), \left(-\frac{8t^6+20t^3-1}{3t^4}, 0\right), \mathcal{O} \right\}.$$

Since all points in $E_\mu(L)[2]$ are defined over $L = \mathbb{Q}(\sqrt{8t^3+1})$, $E_\mu(L)_{\text{tors}}$ has three points of order 2. Since $\mathbb{Z}/6\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$ each only have one point of order 2, those two possibilities are ruled out, leaving

$$E_\mu(\mathbb{Q}(\sqrt{8t^3+1}))_{\text{tors}} = \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}.$$ □

4.3. *Torsion points in Hessian and JKL curves*

Some Hessian curves have points of order 2 defined over $\mathbb{Q}$, others do not. Consider, for example, the Hessian curve with parameter $d = -\frac{1}{3}$ and short Weierstrass form

$$E : y^2 = x^3 + \frac{215}{3}x - \frac{10582}{27}.$$

Then $P = (\frac{13}{3}, 0)$ is a point of order 2. On the other hand, the curve

$$E : y^2 = x^3 - 2835x + 9774$$

with parameter $d = 3$ does not have any points of order 2 defined over $\mathbb{Q}$. If P was a point of order 2, then $P = (r, 0)$ where $r \in \mathbb{Q}$ is a root of $f = x^3 - 2835x + 9774$. By the rational root theorem, $r \in \mathbb{Z}$ and r has to divide 9774. One can easily check that no divisor of 9774 is a root of f.

The next theorem classifies the curves with a point of order 2 defined over $\mathbb{Q}$.

THEOREM 4.9. *Let H be a Hessian curve. Then H has a point of order 2 over $\mathbb{Q}$ if and only if $H = E_\mu$ for some JKL curve E_μ as defined above.*

Proof. One direction is clear. If E_μ is a JKL curve, we already know that $E_\mu(\mathbb{Q})_{\text{tors}} = \mathbb{Z}/6\mathbb{Z}$.

Now let $H : x^3 + y^3 + 1 = 3dxy$ be a Hessian curve and $P = (x, y) \in H(\mathbb{Q})$. Then P is a 2-torsion point if and only if

$$2P = \mathcal{O} \Leftrightarrow P = -P \Leftrightarrow x = y.$$

https://doi.org/10.1112/S1461157016000231 Published online by Cambridge University Press

This means that P is a 2-torsion point if and only if

$$2x^3 + 1 = 3dx^2$$

and thus, $d = (2x^3 + 1)/3x^2$ for $x \in \mathbb{Q}$, $x \neq 0$. For $x = 1, -\frac{1}{2}$, we have $d = 1$ and therefore H not smooth. Thus, H is a JKL curve with parameter $d = (2t^3 + 1)/3t^2$ for $t \in \mathbb{Q}\backslash\{0, 1, -\frac{1}{2}\}$ and H is a Hessian curve. □

This classification yields information about the torsion subgroup.

COROLLARY 4.10. *Let H be a Hessian curve. Then $H(\mathbb{Q})_{\text{tors}} = \mathbb{Z}/6\mathbb{Z}$ if and only if $H = E_\mu$ for μ of the form $\mu = (2t^3 + 1)/3t^2$, $t \in \mathbb{Q}\backslash\{0, 1, -\frac{1}{2}\}$.*

Proof. If $H = E_\mu$, we showed in Theorem 4.6, that $H(\mathbb{Q})_{\text{tors}} = \mathbb{Z}/6\mathbb{Z}$. On the other hand, if $H(\mathbb{Q})_{\text{tors}} = \mathbb{Z}/6\mathbb{Z}$, then $H(\mathbb{Q})$ has to have a point of order 2 and, by Theorem 4.9, H has to be a JKL curve. □

In order to calculate the torsion subgroup of Hessian curves, which are not JKL curves, we need the following lemma. Note that for $H_d : x^3 + y^3 + z^3 = dxyz$ in projective Hessian form, the points of order 3 are $P_1 = (0{:}{-}1{:}1)$ and $P_2 = ({-}1{:}0{:}1)$.

LEMMA 4.11. *Over $\mathbb{Q}$, a curve H_d in Hessian form does not have any point of order 9.*

Proof. Let $P = (x{:}y{:}z)$ be a point of order 9. Then $3P = (x_3{:}y_3{:}z_3)$ has to be a point of order 3 and thus $3P = (0{:}1{:}1)$ or $3P = ({-}1{:}0{:}1)$. We obtain

$$\begin{aligned} x_3 &= -(x^6y^2 - x^3y^5 - x^3y^2z^3 + y^5z^3 - x^2z^3)z, \\ y_3 &= (x^5y^3 - x^2y^6 - x^5z^3 + x^2y^3z^3 - x^3y^2 + y^2z^3)z, \\ z_3 &= -(x^3y^3 - x^3z^3 - y^3z^3 + z^6 - x^3 + y^3)xyz, \end{aligned}$$

with $(x_3{:}y_3{:}z_3) \in \{(0{:}1{:}1), ({-}1{:}0{:}1)\}$.

Note, that if $P = (x{:}y{:}z)$ is of order 9, then $xyz \neq 0$, because if $xyz = 0$, then $z_3 = 0$, which is a contradiction to $(x_3{:}y_3{:}z_3) \in \{(0{:}1{:}1), ({-}1{:}0{:}1)\}$.

We start with points $(x{:}y{:}z)$ of order 9 such that $3(x{:}y{:}z) = (0{:}1{:}1)$. Since $xyz \neq 0$ and $(x{:}y{:}z) = (kx{:}ky{:}kz)$ for any $k \in \mathbb{Q}\backslash\{0\}$, we can set $x = 1$. This leads to the following system of equations:

$$\begin{aligned} -y^2 - y^5 - y^2z^3 + y^5z^3 - z^3 &= 0, \\ (y^3 - y^6 - z^3 + y^3z^3 - y^2 + y^2z^3)z &= 1, \\ -(y^3 - z^3 - y^3z^3 + z^6 - 1 + y^3)yz &= 1. \end{aligned}$$

Subtracting the last equation from the second yields

$$-(yz^3 + y^3 - y - 1)(y^3 - z^3 - y)z = 0.$$

Since $z \neq 0$, we have two different cases.

Case 1: $z^3 = y^3 - y$. This changes the first equation to $(y^6 - y^5 - 2y^3 + 2y^2 - 2y + 1)(y + 1)y = 0$. If $y = -1$, then $z^3 = y^3 - y = 0$ and thus $z = 0$, which is a contradiction. Also y cannot be zero, leaving $y^6 - y^5 - 2y^3 + 2y^2 - 2y + 1 = 0$ as the only possibility. According to the rational root theorem, for any root $p/q \in \mathbb{Q}$, both p and q have to be ± 1. If $y = 1$, then $y^6 - y^5 - 2y^3 + 2y^2 - 2y + 1 = -1 \neq 0$, so $y = 1$ is not a root and we have already seen that $y = -1$ cannot be a solution.

https://doi.org/10.1112/S1461157016000231 Published online by Cambridge University Press

Case 2: $z^3 = (-y^3 + y + 1)/y$. Inserting this into the first equation leads to $y^8 - 2y^5 + y^3 - y^2 + y + 1 = 0$. By the rational root theorem, the only rational roots would be $p/q = \pm 1$, which both lead to a contradiction.

Thus, there is no rational point $(x{:}y{:}z) \in E(\mathbb{Q})$, such that $3(x{:}y{:}z) = (0{:}1{:}1)$.

Next, we will examine the points $P = (x{:}y{:}z)$ such that $3P = (-1{:}0{:}1)$. As above, we set $x = 1$ and obtain the following system of equations:

$$\begin{aligned} -(y^5z^3 - y^5 - y^2z^3 - z^3 + y^2)z &= -1, \\ -y^6 + y^3z^3 + y^2z^3 + y^3 - z^3 - y^2 &= 0, \\ (y^3z^3 - z^6 - 2y^3 + z^3 + 1)yz &= 1. \end{aligned}$$

The second equation implies

$$z^3 = \frac{y^6 - y^3 + y^2}{y^3 + y^2 - 1}.$$

Note, that $y^3 + y^2 - 1 \neq 0$ for all $y \in \mathbb{Q}$. We add the first equation to the last one, substitute z^3 by $(y^6 - y^3 + y^2)/(y^3 + y^2 - 1)$ and obtain $y^{13} + y^{12} - y^{11} - 4y^{10} - 2y^9 + 4y^8 + 6y^7 - 5y^5 - 5y^4 + y^3 + 2y^2 + 2y - 1 = 0$. Using the rational root theorem once more, we can see that the equation does not have rational roots and we cannot find a simultaneous solution for all three equations above. □

Now we know the torsion subgroup of Hessian curves.

Corollary 4.12. *Let H be a Hessian curve, but not a JKL curve. Then*

$$H(\mathbb{Q})_{\text{tors}} = \mathbb{Z}/3\mathbb{Z}.$$

Proof. We know that H has exactly two points of order 3 defined over $\mathbb{Q}$ and by assumption H does not have a point of order 2. By Mazur's theorem, this rules out all torsion subgroups but $\mathbb{Z}/3\mathbb{Z}$ and $\mathbb{Z}/9\mathbb{Z}$. By Lemma 4.11 we conclude that $H(\mathbb{Q})_{\text{tors}} = \mathbb{Z}/3\mathbb{Z}$. □

In summary, if H is a Hessian curve, then

$$H(\mathbb{Q})_{\text{tors}} = \begin{cases} \mathbb{Z}/6\mathbb{Z}, & H = E_\mu \text{ for } E_\mu \text{ a JKL curve,} \\ \mathbb{Z}/3\mathbb{Z} & \text{otherwise.} \end{cases}$$

5. *Implementation and timings*

The primary motivation for the implementation was to see if the torsion/small parameter improvements would lead to an implementation that was competitive with either GMP-ECM [21] or EECM-MPFQ. To this end, a choice had to be made as to the eventual application: record setting (which requires targeting integers of arbitrary size) or cofactoring for the number field sieve. The former was desired for JKL-ECM. To target integers of arbitrary size, GNU-MP was used as a multi-precision library (MPFQ is limited to inputs of at most nine words of 64 bits, with a corresponding maximum input size of around 174 digits). Finally, one aim of this work was to test an implementation on the Fionn cluster at the Irish Centre for High-End Computing.

5.1. *Stage* 2

The original algorithm described in [17], now called 'stage 1' of ECM, has seen the subsequent development of 'stage 2'. Where stage 1 allows for all primes in the group order up to a size B_1,

https://doi.org/10.1112/S1461157016000231 Published online by Cambridge University Press

stage 2 allows a single larger prime in the group order factorization between B_1 and some larger bound B_2. Stage 1 computes the residue

$$Q = [S]P$$

for a point P on the elliptic curve. If Q has order between B_1 and B_2 then computing

$$[p]Q$$

for all $B_1 < p \leqslant B_2$ should yield one $[p]Q$ which is the identity. In this naive approach, we must compute $O(B_2)$ extra multiples. An implementation of ECM which includes an optimized stage 2 in practice significantly increases the chances of finding larger primes, even though the asymptotic complexity of the overall algorithm is unchanged (thus it is a logarithmic factor improvement).

There are different approaches to implementing the core idea of stage 2. In fact, our JKL-ECM includes an implementation of the 'FFT continuation' [19], so called because it translates the function of stage 2 into the calculation of a very large integer product, where it is faster to carry out the multiplication via a convolution computed via forward and backward FFT [20]. Luckily, GMP (which JKL-ECM uses for multi-precision arithmetic) handles this automatically once the integers in the product exceed a calibrated threshold, so it was not necessary to write (and optimize) FFT-based convolution. It is the saving induced by FFT multiplication, together with a 'baby-step, giant-step' idea which reduces the required computation to square-root size, which attains the increased likelihood of success of stage 2 without incurring too much extra cost. This makes the FFT continuation indispensable in practice. The memory required by the FFT continuation grows as $B_2 \log(B_2)$ (involving various kinds of in-memory product trees, which have logarithmic depth), placing a practical limit on the value of B_2 that may be used. For more on the ideas that go into stage 2, see additionally [1, 2, 22]. Our implementation was standard, except for a technicality that arises when using twisted Hessian curves in stage 2. We had to use the rational map $\psi(X{:}Y{:}Z) = X^2/(YZ)$; see [5, § 5.2].

5.2. *Using the torsion improvement*

To make full use of the torsion improvement possible with the use of the JKL families, it is necessary to ensure that the torsion subgroup over a given quartic extension of $\mathbb{Q}$ injects into the elliptic curve group over the associated finite field for the prime factor we are attempting to find. This can be at least partially prescribed by choosing numbers of a special form as input. For example, the JKL $\mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$ family is defined over the biquadratic number field $K = \mathbb{Q}(\sqrt{-3}, \sqrt{8t^4+1})$, with $t \in \mathbb{Q}$ and $t \neq 0, 1, -\frac{1}{2}$. To achieve full torsion injection (for example, to ensure that $36 | \#E(\mathbb{F}_p)$ for a prime factor p of N), it is necessary that both $\sqrt{-3}$ and $\sqrt{8t^4+1}$ exist in $\mathbb{F}_p$. We can prescribe the existence of $\sqrt{-3}$ in $\mathbb{F}_p$ by choosing to factor numbers of the form $N = x^2 + 3y^2$, since then $\sqrt{-3} \equiv x/y \mod p$ for any $p | N$ (see, for example, [10], and also [9], where this idea is put to use). We do not have as much control over the other quadratic irrationality ($\sqrt{8t^4+1}$) but we can at least ensure a minimum divisor of $\#E(\mathbb{F}_p)$. If -3 is a quadratic residue in $\mathbb{F}_p$, and $8t^4+1$ is not, then the torsion is actually $\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$ (for primes of good reduction). If $8t^4+1$ is a quadratic residue as well, then the torsion is $\mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$. So if -3 at least is a quadratic residue, then we have a guaranteed factor of at least 18 dividing $\#E(\mathbb{F}_p)$ for any p dividing the number, with roughly a 50% chance that 36 divides $\#E(\mathbb{F}_p)$. Both are larger than anything possible over $\mathbb{Q}$. The case of the $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$ family is similar.

https://doi.org/10.1112/S1461157016000231 Published online by Cambridge University Press

5.3. *Results*

The largest prime factor found was the 57 digit prime factor

$$675047857067159607640250455245491501526526277140638512677$$

of the 248 digit number

$$(5^{228} + 3 \cdot 197^{110})/227812$$

using the twisted Hessian curve

$$aX^3 + Y^3 + Z^3 = dXYZ$$

where $d = 26511$, $a = 231136413353$. The factorization of the group order of the elliptic curve over $\mathbb{F}_p$, with p equal to the above prime, is

$$2 \cdot 3^2 \cdot 58211 \cdot 73757 \cdot 824039 \cdot 13582747 \cdot 17027609 \cdot 74341063 \cdot 99190781 \cdot 6215336273.$$

The stage 1 bound used was 110 000 000 and the effective stage 2 bound used was 1 151 280 345 600. Note that only 1152 curves were run at these bounds to find the factor, far fewer than the 17 899 recommended for t55. In addition, another (slightly smaller) 57-digit factor was found in a different run. Several 56-digit factors were found, in addition to several more factors with 50+ digits smaller than this. Many smaller factors with 40+ digits were found.

5.4. *Speed*

Some timings were obtained for stage 1 using both twisted Edwards and twisted Hessian curves on Fionn. The tests were repeated with the same numbers and bounds, using GMP-ECM. See Tables A.1–A.3. Both the implementation and GMP-ECM were compiled to use GMP 6.0.0a.

We remark at this stage that no assembly language/intrinsics at all were written for JKL-ECM. The performance is purely based on calling the mpz_t class of functions in GNU-MP via C++, so there are significant potential performance gains by making use of SSE/AVX, etc. The lack of assembly optimization is likely the main reason for the slightly slower timings.

5.5. *Effectiveness*

Effectiveness is where our implementation already has an edge over GMP-ECM. Although a slight improvement, the implementation empirically finds more primes for a given bound. Since this was effectively already shown for a $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$ curve vs GMP-ECM in [**5**, Figures 9.1 and 9.2], here we show statistics for a $\mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$ curve vs a typical GMP-ECM curve (a Suyama curve with $\sigma = 4007218240$), and where a random sample of primes congruent to $1 \bmod 3$ are chosen, so that at least torsion $\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$ injects into the elliptic curve group order over $\mathbb{F}_p$ for the implementation. See Figures A.1 and A.2.

6. *Conclusion*

A new implementation of ECM using twisted Edwards and twisted Hessian curve arithmetic and taking advantage of higher torsion over small-degree number fields in certain families of curves is presented. We outline relevant theory regarding Hessian and twisted Hessian curves, in addition to presenting some new results, including a classification of Hessian curve torsion over $\mathbb{Q}$. Our software includes an implementation of the stage 2 FFT continuation, and makes use of a large number of precomputed curves having small parameters, which leads to faster curve arithmetic. The implementation was tested on some numbers of a special form, yielding a 57-digit factor for the effort expended.

https://doi.org/10.1112/S1461157016000231 Published online by Cambridge University Press

Appendix

TABLE A.1. *Stage* 1 *timings on Fionn for twisted Edwards curves for JKL-ECM. Note that double-and-add costs* $(3M + 4S + 1a) + (10M + 1S + 1a)$.

	Cost (milliseconds) for given B_1				
Digits	1e6	3e6	11e6	43e6	110e6
50	2 710	7 910	29 000	113 510	290 400
100	4 240	12 610	46 230	180 860	461 850
150	5 490	16 460	60 380	235 710	602 830
200	7 600	22 800	83 620	326 900	837 200
250	9 850	29 640	108 470	423 850	1084 710
300	12 480	37 560	137 260	537 380	1372 780
350	15 930	47 840	175 250	685 370	1752 690
400	18 920	56 750	207 980	812 300	2082 030

TABLE A.2. *Stage* 1 *timings on Fionn for twisted Hessian curves for JKL-ECM. Note that double-and-add costs* $(7M + 1S + 1d) + (6M + 6m + 1a)$.

	Cost (milliseconds) for given B_1				
Digits	1e6	3e6	11e6	43e6	110e6
50	2 530	7 450	27 330	106 810	273 540
100	4 010	12 040	43 970	171 700	439 180
150	5 250	15 710	57 400	223 740	572 200
200	7 420	22 190	81 380	318 230	814 310
250	9 480	28 410	104 160	406 480	1040 190
300	12 420	37 240	136 520	533 650	1365 220
350	15 970	47 800	175 250	684 990	1751 310
400	18 910	56 620	207 970	811 700	2077 680

TABLE A.3. *Stage* 1 *timings on Fionn for GMP-ECM* 6.4.4, *compiled with GMP* 6.0.0a.

	Cost (milliseconds) for given B_1				
Digits	1e6	3e6	11e6	43e6	110e6
50	896	2 632	9 684	39 058	96 942
100	1 764	5 364	20 037	77 160	201 052
150	2 784	8 288	30 493	119 583	306 243
200	4 564	13 848	50 527	197 932	507 123
250	5 892	17 813	65 244	255 771	655 116
300	7 812	23 373	86 037	336 997	863 873
350	10 228	30 777	113 115	443 391	1140 639
400	16 269	48 967	179 751	705 448	1806 532

https://doi.org/10.1112/S1461157016000231 Published online by Cambridge University Press

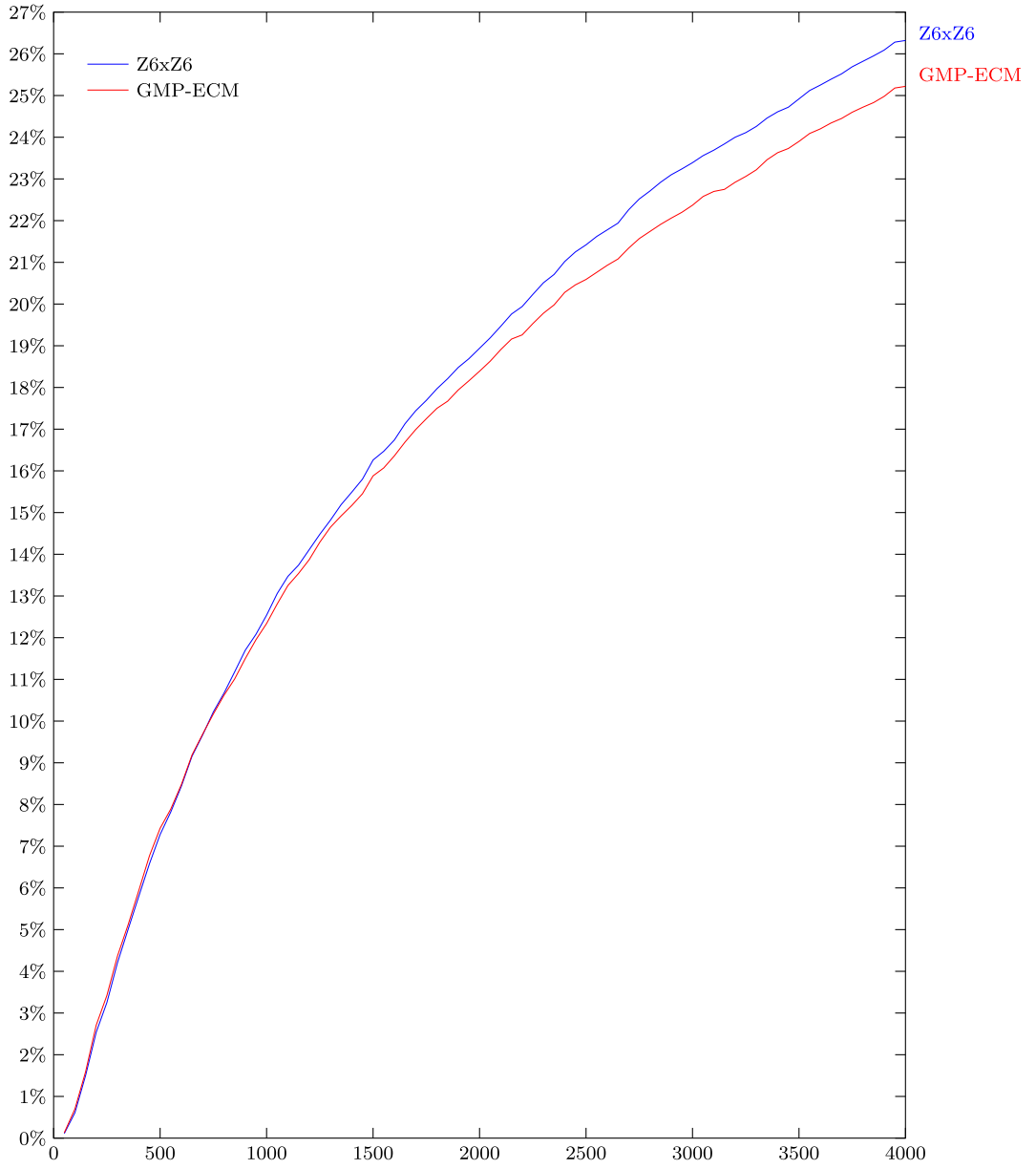

FIGURE A.1. *For a sample of* 65 536 30*-bit primes* $\equiv 1 \bmod 3$*, success probability of stage* 1 *of ECM for the implementation using the Jeon–Kim–Lee* $\mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$ *curve with* $(d, a) = (123, 125)$*, and GMP-ECM using the Suyama curve with* $\sigma = 4007218240$*. The horizontal axis is the stage* 1 *bound used* (*sampled at intervals of* 50).

https://doi.org/10.1112/S1461157016000231 Published online by Cambridge University Press

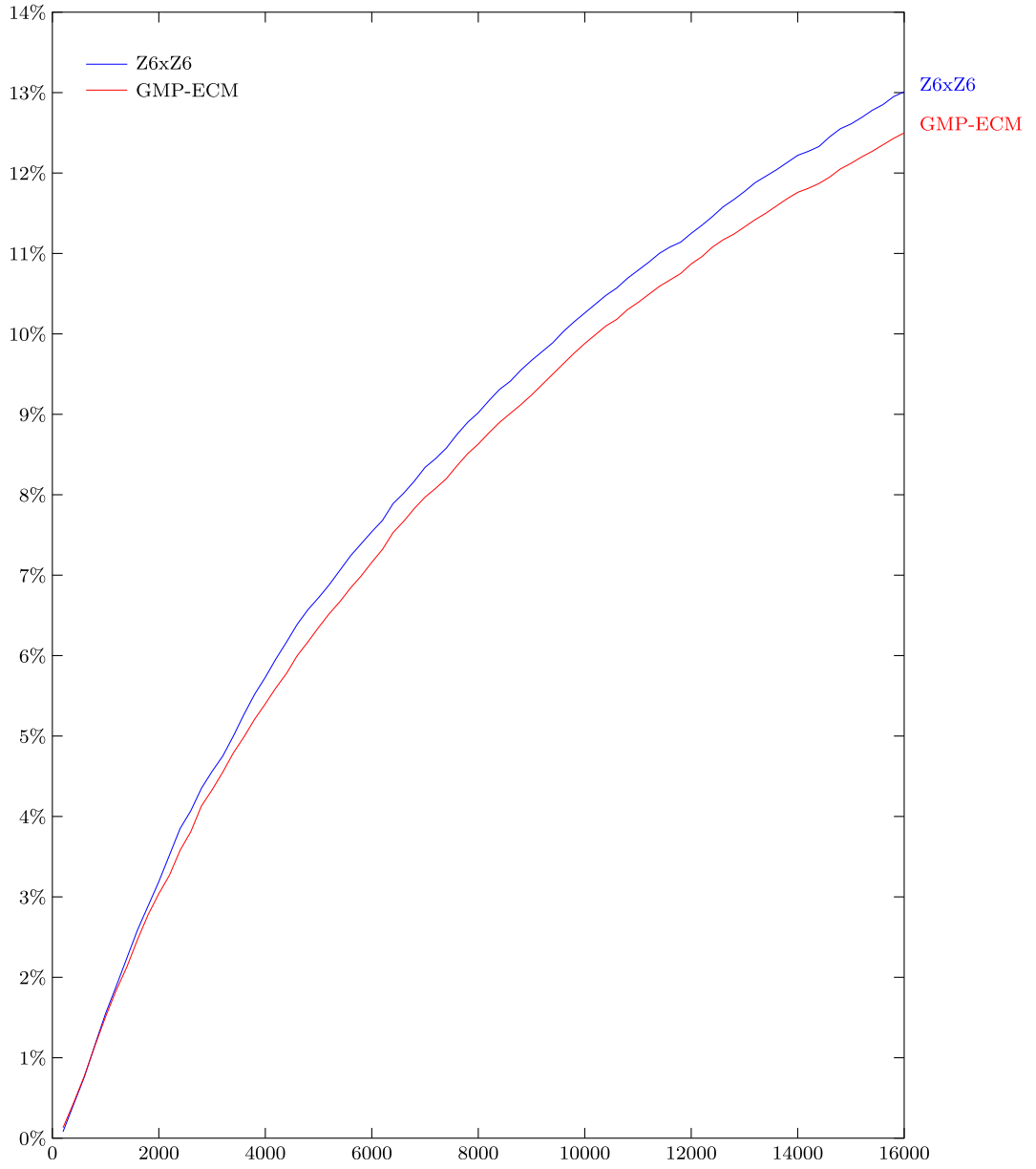

FIGURE A.2. *For a sample of* 65 536 40*-bit primes* $\equiv 1 \bmod 3$*, success probability of stage* 1 *of ECM for the implementation using the Jeon–Kim–Lee* $\mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$ *curve with* $(d, a) = (123, 125)$*, and GMP-ECM using the Suyama curve with* $\sigma = 4007218240$*. The horizontal axis is the stage* 1 *bound used (sampled at intervals of* 200*).*

https://doi.org/10.1112/S1461157016000231 Published online by Cambridge University Press

References

1. D. J. Bernstein, 'Scaled remainder trees', URL: http://cr.yp.to/papers.html#scaledmod. Note: draft, 2004.
2. D. J. Bernstein, 'Fast multiplication and its applications', *Publ. Math. Inst. Hautes Études Sci.* 44 (2008) 325–384.
3. D. J. Bernstein, 'Explicit-formulas database', 2016, http://www.hyperelliptic.org/EFD/.
4. D. J. Bernstein, P. Birkner, M. Joye, T. Lange and C. Peters, 'Twisted Edwards curves', *Progress in cryptology – AFRICACRYPT 2008*, Lecture Notes in Computer Science 5023 (Springer, Berlin, 2008) 389–405.
5. D. J. Bernstein, P. Birkner, T. Lange and C. Peters, 'ECM using Edwards curves', *Math. Comp.* 82 (2013) 1139–1179.
6. D. J. Bernstein, P. Birkner, T. Lange and C. Peters, 'EECM-MPFQ', 2016, http://eecm.cr.yp.to/mpfq.html.
7. D. J. Bernstein, C. Chuengsatiansup, D. Kohel and T. Lange, 'Twisted Hessian curves', 2015, https://eprint.iacr.org/2015/781.pdf.
8. D. J. Bernstein and T. Lange, 'Analysis and optimization of elliptic-curve single-scalar multiplication', *Finite fields and applications*, Contemporary Mathematics 461 (American Mathematical Society, Providence, RI, 2008) 1–19.
9. É. Brier and C. Clavier, 'New families of ECM curves for Cunningham numbers', *Algorithmic number theory: 9th international symposium, ANTS-IX*, Lecture Notes in Computer Science 6197 (Springer, Berlin, 2010) 96–109.
10. D. A. Cox, *Primes of the form $x^2 + ny^2$*, 2nd edn (John Wiley & Sons, Hoboken, NJ, 2013).
11. 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 (2012) 193–203.
12. H. M. Edwards, 'A normal form for elliptic curves', *Bull. Amer. Math. Soc. (N.S.)* 44 (2007) 393–422.
13. H. Hışıl, K. K.-H. Wong, G. Carter and E. Dawson, 'Twisted Edwards curves revisited', *ASIACRYPT, 2008*, Lecture Notes in Computer Science 5350 (Springer, Berlin, Heidelberg, 2008).
14. H. Hışıl, K. K.-H. Wong, G. Carter and E. Dawson, 'An exploration of affine group laws for elliptic curves', *J. Math. Cryptol.* 5 (2011) 1–50.
15. D. Jeon, C. H. Kim and Y. Lee, 'Families of elliptic curves over quartic number fields with prescribed torsion subgroups', *Math. Comp.* 80 (2011) 2395–2410.
16. M. A. Kenku and F. Momose, 'Torsion points on elliptic curves defined over quadratic fields', *Nagoya Math. J.* 109 (1988) 125–149.
17. H. W. Lenstra Jr, 'Factoring integers with elliptic curves', *Ann. of Math.* (2) 126 (1987) 649–673.
18. B. Mazur, 'Modular curves and the Eisenstein ideal', *Publ. Math. Inst. Hautes Études Sci.* (1977) 33–186.
19. P. L. Montgomery, 'An FFT extension of the elliptic curve method of factorization', PhD Thesis, University of California, Los Angeles, ProQuest LLC, Ann Arbor, MI, 1992.
20. A. Schönhage and V. Strassen, 'Schnelle Multiplikation grosser Zahlen', *Computing (Arch. Elektron. Rechnen)* 7 (1971) 281–292.
21. P. Zimmermann *et al.*, 'GMP-ECM', 2016, http://ecm.gforge.inria.fr/.
22. P. Zimmermann and B. Dodson, '20 years of ECM', *Algorithmic number theory: 7th international symposium, ANTS-VII*, Lecture Notes in Computer Science 4076 (eds F. Hess, S. Pauli and M. E. Pohst; Springer, Berlin, 2006) 525–542.

Henriette Heer
Faculty of Mathematics
Technical University of Kaiserslautern
PO Box 3049
D-67653 Kaiserslautern
Germany

heer@rhrk.uni-kl.de

Oisín Robinson
School of Mathematics and Statistics
University College Dublin
Dublin 4
Ireland

oisin.robinson@ucdconnect.ie

Gary McGuire
School of Mathematics and Statistics
University College Dublin
Dublin 4
Ireland

gary.mcguire@ucd.ie

https://doi.org/10.1112/S1461157016000231 Published online by Cambridge University Press