ECM using Edwards curves

Daniel J. Bernstein[1], Peter Birkner[2], Tanja Lange[2], and Christiane Peters[2]

[1] Department of Computer Science (MC 152)
University of Illinois at Chicago, Chicago, IL 60607–7053, USA
djb@cr.yp.to
[2] Department of Mathematics and Computer Science
Technische Universiteit Eindhoven, P.O. Box 513, 5600 MB Eindhoven, Netherlands
tanja@hyperelliptic.org

Abstract. This paper introduces GMP-EECM, a fast implementation of the elliptic-curve method of factoring integers. GMP-EECM is based on, but faster and more effective than, the well-known GMP-ECM software. The main changes are as follows: (1) use Edwards curves instead of Montgomery curves; (2) use twisted inverted Edwards coordinates; (3) use signed-sliding-window addition chains; (4) batch primes to increase the window size; (5) choose curves with small parameters a, d, X_1, Y_1, Z_1; (6) choose curves with larger torsion.

Keywords: factorization, ECM, elliptic-curve method, curve selection, Edwards coordinates, inverted Edwards coordinates, twisted Edwards curves.

1 Introduction

Factorization of integers is one of the most studied problems in algorithmic number theory and cryptology. One of the best factorization methods available is the Elliptic-Curve Method (ECM), introduced by Hendrik W. Lenstra, Jr., in [17] twenty years ago. ECM plays an important role in factoring the "random" integers of interest to number theorists: it is not as fast as trial division and Pollard's rho method for finding tiny prime factors but it is the method of choice for finding medium-size prime factors. ECM also plays an important role in factoring the "hard" integers of interest to cryptologists: those integers are attacked by sieving methods, which use ECM to find large prime factors of auxiliary integers. ECM can also be used directly to find "large" prime factors; the current record, reported in [27], was the discovery by Dodson of a 222-bit factor of the 1266-bit number $10^{381} + 1$.

* Permanent ID of this document: cb39208064693232e4751ec8f3494c43. Date of this document: 2009.01.20. This work has been supported in part by the European Commission through the ICT Programme under Contract ICT–2007–216676 ECRYPT-II, and in part by the National Science Foundation under grant ITR–0716498. This work was carried out while the first author was visiting Technische Universiteit Eindhoven.

Implementations of ECM are available in most computer-algebra packages and have been the subject of countless papers. The state-of-the-art implementation is GMP-ECM, described in detail in the paper [26] by Zimmermann and Dodson.

We have built a faster program, which we call GMP-EECM, by adding various improvements to GMP-ECM. We thank Zimmermann et al. for making their software freely available! In this paper we present the background and initial speed results for GMP-EECM.

1.1. Representations of elliptic curves. Elliptic curves can be expressed in many forms, and elliptic-curve computations can be carried out in many ways. Two fast options reigned supreme for twenty years of elliptic-curve factoring, elliptic-curve primality proving, and elliptic-curve cryptography:

- Short Weierstrass curves $y^2 = x^3 + a_4x + a_6$, with Jacobian coordinates $(X : Y : Z)$ representing $(X/Z^2, Y/Z^3)$, were the representation of choice for most computations.
- Montgomery curves $By^2 = x^3 + Ax^2 + x$, with Montgomery coordinates $(X : Z)$ representing two points $(X/Z, \pm\cdots)$, were the representation of choice for single-scalar multiplication, and in particular for stage 1 of ECM.

The picture changed in 2007 with the advent of Edwards curves. A sequence of papers [5, 2, 6, 7] showed that, for cryptographic applications, Edwards curves involve significantly fewer multiplications than short Weierstrass curves in Jacobian coordinates, and — for sufficiently large scalar multiplications — fewer multiplications than Montgomery curves in Montgomery coordinates. Note that larger scalars benefit from larger windows, reducing the number of additions per bit for Edwards coordinates but not for Montgomery coordinates.

1.2. Contributions of this paper. In this paper we analyze the impact of Edwards curves on ECM, not just in multiplication counts but also in real-world software speeds. Section 2 reviews Edwards curves, twisted Edwards curves, Edwards coordinates, and inverted Edwards coordinates; GMP-EECM uses twisted inverted Edwards coordinates. Section 3 explains exactly how GMP-EECM uses Edwards curves. Our announcement of GMP-EECM in January 2008 marked the first time that Edwards curves had been demonstrated to achieve software speed records.

A large portion of this paper is devoted to explaining which curves we used in GMP-EECM. Curves having 12 or 16 torsion points over $\mathbf{Q}$ are guaranteed to have 12 or 16 as divisors of their group orders modulo primes (of good reduction), improving the smoothness chance of the group orders and thus improving the success chance of ECM. We show how to use analogous improvements for Edwards curves; even better, we find new curves with large torsion group, small curve parameters, and small non-torsion points.

Section 4 explains how to construct Edwards curves having torsion group $\mathbf{Z}/12\mathbf{Z}$ or $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/8\mathbf{Z}$ over $\mathbf{Q}$; the symmetry of Edwards curves simplifies the constructions. Section 4 also shows that twisted Edwards curves cannot have torsion group $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/6\mathbf{Z}$ over $\mathbf{Q}$. Section 5, adapting a construction of Atkin

and Morain from [1] to the Edwards context, explains how to construct an infinite family of Edwards curves having torsion group $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/8\mathbf{Z}$ and (as required for ECM) an explicit non-torsion point. Section 6 describes how we found better choices of Edwards curves to use in GMP-EECM; each of these curves has torsion group $\mathbf{Z}/12\mathbf{Z}$ or $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/8\mathbf{Z}$, an explicit non-torsion point, and small (i.e., fast) parameters.

Acknowledgements. Thanks to Paul Zimmermann for his detailed comments and suggestions.

2 Edwards curves, twisted Edwards curves, Edwards coordinates, and inverted Edwards coordinates

Edwards in [12] introduced a new normal form of elliptic curves. He showed that every elliptic curve over a field k with $2 \neq 0$ can be written in this normal form over an extension of k. To reduce the need for extensions we use the slightly generalized form of Edwards curves introduced in [5].

An Edwards curve, at the level of generality of [5], is given by an equation of the form $x^2 + y^2 = 1 + dx^2y^2$, for some number $d \notin \{0, 1\}$. The addition law on an Edwards curve is given by

$$(x_1, y_1), (x_2, y_2) \mapsto \left(\frac{x_1y_2 + y_1x_2}{1 + dx_1x_2y_1y_2}, \frac{y_1y_2 - x_1x_2}{1 - dx_1x_2y_1y_2} \right).$$

The addition law is strongly unified; i.e., the same formulas can also be used for doubling. The point $(0, 1)$ is the neutral element of the addition law. The negative of a point $P = (x_1, y_1)$ can be computed by reflecting the x-coordinate across the y-axis: $-P = (-x_1, y_1)$. If d is not a square then the addition law is complete; i.e., the addition law holds for all inputs.

The point $(0, -1)$ has order 2. The points $(1, 0)$ and $(-1, 0)$ have order 4. There are two singular points at infinity. Resolving both singularities yields two further points of order 2 and two points of order 4 whose minimal field of definition is $k(\sqrt{d})$. Therefore, there are 3 k-rational points of order 2 if and only if d is a square.

2.1. Standard (projective) Edwards coordinates. A point in affine coordinates on an Edwards curve is given by a pair (x_1, y_1). To avoid inversions in the addition formulas one usually homogenizes the curve equation. This leads to the equation $(X^2 + Y^2)Z^2 = Z^4 + dX^2Y^2$. A point $(X_1 : Y_1 : Z_1)$ that satisfies this equation corresponds to the affine point $(X_1/Z_1, Y_1/Z_1)$ if $Z_1 \neq 0$. The neutral element in projective coordinates is $(0 : 1 : 1)$.

Inversion-free formulas for addition and doubling in homogenized form were introduced in [5]. A general addition in Edwards coordinates takes $10\mathbf{M} + 1\mathbf{S} + 1\mathbf{D} + 7\mathbf{a}$; i.e., 10 field multiplications, 1 field squaring, 1 multiplication by the curve parameter d, and 7 field additions. A doubling takes $3\mathbf{M} + 4\mathbf{S} + 6\mathbf{a}$.

For a collection of explicit formulas and operation counts for elliptic curves in various representations we refer to the Explicit-Formulas Database [4].

2.2. Inverted Edwards coordinates. We next review another representation of points on Edwards curves: inverted Edwards coordinates, introduced in [6]. A projective point $(X_1 : Y_1 : Z_1)$ in inverted Edwards coordinates corresponds to the affine point $(Z_1/X_1, Z_1/Y_1)$. The addition of two points in inverted Edwards coordinates costs only $9\mathbf{M} + 1\mathbf{S} + 1\mathbf{D} + 7\mathbf{a}$, which is a speedup of $1\mathbf{M}$ compared to standard Edwards coordinates. However, a doubling costs $3\mathbf{M}+4\mathbf{S}+1\mathbf{D}+6\mathbf{a}$, and is thus more expensive than in standard Edwards coordinates by $1\mathbf{D}$.

2.3. Twisted Edwards curves. We now review a generalized form of Edwards curves that we introduced in [3] with Joye. The *twisted Edwards curve* $\mathrm{E}_{\mathrm{E},a,d}$ is given by

$$\mathrm{E}_{\mathrm{E},a,d} : ax^2 + y^2 = 1 + dx^2y^2,$$

where a, d are distinct nonzero elements of k.

If $a\bar{d} = \bar{a}d$ then the two curves $\mathrm{E}_{\mathrm{E},a,d}$ and $\mathrm{E}_{\mathrm{E},\bar{a},\bar{d}}$ are quadratic twists. If additionally $\bar{a}/a$ is a square in k, the curves are even isomorphic, where an isomorphism is given by $(x, y) \mapsto (\bar{x}, \bar{y}) = (\sqrt{(a/\bar{a})}x, y)$.

The addition law on the twisted Edwards curve is given by

$$(x_1, y_1) + (x_2, y_2) = \left(\frac{x_1y_2 + y_1x_2}{1 + dx_1x_2y_1y_2}, \frac{y_1y_2 - ax_1x_2}{1 - dx_1x_2y_1y_2}\right).$$

The neutral element and negation are unchanged. See [3] for explicit formulas for group operations on twisted Edwards curves.

For the purpose of this paper the twisted form is interesting since we will find and use curves over $\mathbf{Q}$ with coefficients d of small height, i.e., small numerator and denominator. The smallest integer congruent to d modulo n will usually have as many bits as n, so multiplications by d, as they appear in the addition and doubling formulas of inverted Edwards coordinates, are costly while multiplications by the numerator and denominator separately are cheap.

Additional benefits of twisted Edwards curves were pointed out recently by Hisil, Wong, Carter, and Dawson in [14] but have not yet been integrated into GMP-EECM and are not discussed further in this paper.

2.4. Addition with small parameters. In ECM we save time not only from small parameters a, d but also from small base points for scalar multiplication.

Let $P_2 = (x_2, y_2)$ be a rational point on the Edwards curve $\mathrm{E}_{\mathrm{E},1,\bar{d}}$, and write $\bar{d}$ in the form d/a, where a is a square. The point $(x_2/\sqrt{a}, y_2)$ is then on the isomorphic curve $\mathrm{E}_{\mathrm{E},a,d}$. Let Z_2 be the least common multiple of the numerators of $x_2/\sqrt{a}$ and y_2 and define integers X_2 and Y_2 so that $(Z_2/X_2, Z_2/Y_2) = (x_2/\sqrt{a}, y_2)$. If (x_2, y_2) has small height and if $\sqrt{a}$ is small then the absolute values of X_2, Y_2 and Z_2 are small as well, so multiplications by X_2 etc. are easy.

Additions involving such a point $(X_2 : Y_2 : Z_2)$ need only $5\mathbf{M}+1\mathbf{S}+6\mathbf{D}+6\mathbf{a}$, where the $6\mathbf{D}$ are 1 multiplication by each of a, $2d$, X_2, Y_2, $X_2 + Y_2$, and Z_2.

3 Using Edwards curves in ECM stage 1

This section discusses "stage 1" of ECM. It begins by reviewing the general idea of stage 1 and the state-of-the-art strategies used in GMP-ECM to perform the

elliptic-curve computations in stage 1. It then analyzes the speedups obtained from using Edwards curves.

There are also some elliptic-curve operations in "stage 2" of ECM. We plan to convert those operations to Edwards coordinates, and we expect even larger relative speedups for those operations than in stage 1. However, those operations are typically a small part of the stage-2 time, and stage 2 is typically a small part of the overall ECM time, so our main concern is stage 1.

3.1. Overview of stage 1. "Stage 1" of ECM tries to factor a positive integer n as follows. Choose an elliptic curve E defined over $\mathbf{Q}$. Choose a rational function $\varphi : E \to \mathbf{Q}$ that has a pole at the neutral element of E; for example choose φ as the Weierstrass x-coordinate. Choose a non-torsion element $P \in E(\mathbf{Q})$. Choose a positive integer s with many small prime factors. Choose a sequence of additions, subtractions, multiplications, and divisions that, if carried out over $\mathbf{Q}$, would compute $\varphi([s]P)$, where $[s]P$ denotes the sth multiple of P in $E(\mathbf{Q})$. Compute $\varphi([s]P)$ modulo n by carrying out this sequence of additions, subtractions, multiplications, and divisions modulo n. Hope for an impossible division modulo n. An attempt to divide by a nonzero nonunit modulo n immediately reveals a factor of n; an attempt to divide by 0 modulo n is not quite as informative but usually allows a factor of n to be obtained without much extra work.

If n has a prime divisor q such that $[s]P$ is the neutral element of $E(\mathbf{Z}/q\mathbf{Z})$ then the stage-1 ECM computation will involve an impossible division modulo n, usually revealing a factor of n. This occurs, in particular, whenever s is a multiple of the group size $\#E(\mathbf{Z}/q\mathbf{Z})$. As E varies randomly, $\#E(\mathbf{Z}/q\mathbf{Z})$ varies randomly (with some subtleties in its distribution; see, e.g., [15]) in the Hasse interval $[q - 2\sqrt{q} + 1, q + 2\sqrt{q} + 1]$. What makes ECM useful is that a surprisingly small s, allowing a surprisingly fast computation of $[s]P$, is a multiple of a surprisingly large percentage of the integers in the Hasse interval, and is a multiple of the order of P modulo q with (conjecturally) an even larger probability.

For example, one could try to factor n as follows. Choose the curve $E : y^2 = x^3 - 2$, the Weierstrass x-coordinate as φ, the point $(x, y) = (3, 5)$, and the integer $s = 420$. Choose the following strategy to compute the x-coordinate of $[420](3, 5)$: use the standard affine-coordinate doubling formulas to compute $[2](3, 5)$, then $[4](3, 5)$, then $[8](3, 5)$; use the standard affine-coordinate addition formulas to compute $[12](3, 5)$; continue similarly through $[2](3, 5)$, $[4](3, 5)$, $[8](3, 5)$, $[12](3, 5)$, $[24](3, 5)$, $[48](3, 5)$, $[96](3, 5)$, $[192](3, 5)$, $[384](3, 5)$, $[408](3, 5)$, $[420](3, 5)$. Carry out these computations modulo n, hoping for a division by a nonzero nonunit modulo n.

The denominator of the x-coordinate of $[420](3, 5)$ in $E(\mathbf{Q})$ has many small prime factors: 2, 3, 5, 7, 11, 19, 29, 31, 41, 43, 59, 67, 71, 83, 89, 109, 163, 179, 181, 211, 223, 241, 269, 283, 383, 409, 419, 433, 523, 739, 769, 811, 839, etc. If n shares any of these prime factors then the computation of $[420](3, 5)$ will encounter an impossible division modulo n. To verify the presence of (e.g.) the primes 769, 811, and 839 one can observe that $[420](3, 5)$ is the neutral element in each of the groups $E(\mathbf{Z}/769\mathbf{Z})$, $E(\mathbf{Z}/811\mathbf{Z})$, $E(\mathbf{Z}/839\mathbf{Z})$; the order of $(3, 5)$

turns out to be 7, 42, 35 respectively. Note that the group orders are 819, 756, and 840, none of which divide 420.

3.2. The standard choice of s. Pollard in [20, page 527] suggested choosing s as "the product of all the primes $p_i \leq L$ each to some power $c_i \geq 1$. There is some freedom in the choice of the c_i but the smallest primes should certainly occur to some power higher than the first."

Pollard's prime bound "L" is now called B_1. One possibility is to choose, for each prime $\pi \leq B_1$, the largest power of π in the interval $[1, n + 2\sqrt{n} + 1]$. Then $[s]P$ is the neutral element in $E(\mathbf{Z}/q\mathbf{Z})$ if and only if the order of P is "B_1-smooth", i.e., if and only if the order has no prime divisors larger than B_1. This possibility is theoretically pleasing but clearly suboptimal.

Brent in [10, Section 5] said that "in practice we choose" the largest power of π in the interval $[1, B_1]$ "because this significantly reduces the cost of a trial without significantly reducing the probability of success." GMP-ECM uses the same strategy; see [26, page 529].

3.3. The standard prime-by-prime strategy. Pollard in [20, page 527] said that one "can choose between using the primes p_i in succession or computing P in advance and performing a single power operation." Pollard's "P" is s in the notation of this paper.

As far as we know, all ECM implementations use the first strategy, working with one prime at a time. Brent in [10, Section 5] wrote "Actually, E [i.e., s in the notation of this paper] is not computed. Instead ... repeated operations of the form $P := P^k$ [i.e., $[k]P$ in the notation of this paper], where k ... is a prime power." Montgomery in [18, page 249] wrote "It is unnecessary to compute R [i.e., s in the notation of this paper] explicitly." Zimmermann and Dodson in [26, page 529] wrote "That big product is not computed as such" and presented the prime-by-prime loop used in GMP-ECM.

3.4. The standard elliptic-curve coordinate system. Chudnovsky and Chudnovsky in [11] wrote "The crucial problem becomes the choice of the model of an algebraic group variety, where computations mod p are the least time consuming." They presented explicit formulas for computations on several different shapes of elliptic curves.

Montgomery in [18, Section 10.3.1] introduced what are now called "Montgomery coordinates": a point (x_1, y_1) on the elliptic curve $By^2 = x^3 + Ax^2 + x$ is represented as a pair $(X_1 : Z_1)$ such that $X_1/Z_1 = x_1$. This representation does not distinguish (x_1, y_1) from $(x_1, -y_1)$, so it does not allow addition, but it does allow "differential addition," i.e., computation of $P+Q$ given $P, Q, P-Q$. In particular, Montgomery presented explicit formulas to compute $P, [2k]P, [(2k+1)]P$ from $P, [k]P, [k+1]P$ using $6\mathbf{M} + 4\mathbf{S} + 1\mathbf{D}$, or $5\mathbf{M} + 4\mathbf{S} + 1\mathbf{D}$ if P is given with $Z_1 = 1$, or $4\mathbf{M} + 4\mathbf{S} + 1\mathbf{D}$ if P is a very small point such as $(X_1 : Z_1) = (3, 5)$. One can find earlier formulas for the same computation in [11, formula (4.19)], but Montgomery's formulas are faster.

As far as we know, all subsequent ECM implementations have used Montgomery coordinates. In particular, GMP-ECM uses Montgomery coordinates for

stage 1, with "PRAC," a particular differential addition chain introduced by Montgomery. Zimmermann and Dodson in [26, page 532, Figure 2] report a total cost of 2193683 differential additions to multiply an elliptic-curve point by $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdots 999983 \approx 2^{1440508.1677}$ in Montgomery coordinates. By adding a few counters to the source code of GMP-ECM 6.1.3 (the current version of GMP-ECM at the time when GMP-EECM was announced) we observed that GMP-ECM's stage 1, with $B_1 = 10^6$ and hence $s \approx 2^{1442098.6271}$, used 12982280 multiplications modulo n for 2196070 elliptic-curve additions, of which only 194155 were doublings.

3.5. Speedups in GMP-EECM. GMP-EECM breaks with stage-1 tradition in three ways:

- GMP-EECM uses twisted Edwards curves $ax^2+y^2 = 1+dx^2y^2$ with inverted Edwards coordinates with $\varphi = 1/x$ whereas GMP-ECM uses Montgomery curves with Montgomery coordinates.
- GMP-EECM handles the prime factors π of s in batches, whereas GMP-ECM handles each prime factor separately. GMP-EECM computes the product t of a batch, replaces P with $[t]P$, and then moves on to the next batch. We do not insist on batching *all* of the primes together (although we have done this in all computations so far); the cost of the multiplications to compute t should be balanced against the time saved by larger t. Note, however, that for small P there is no reason that $[t]P$ should be small, so the advantage of a small base point holds for only the first batch.
- GMP-EECM uses "signed sliding window" addition chains. These chains compute $P \mapsto [t]P$ using only 1 doubling and ϵ additions for each bit of t. Here ϵ converges to 0 as t increases in length; this is why a larger t saves time. The savings are amplified by the fact that an addition is somewhat more expensive than a doubling. Note that these chains are not compatible with Montgomery coordinates; they are shorter than any differential addition chain can be.

GMP-EECM follows tradition in its choice of s. We have considered, but not yet analyzed or implemented, other choices of s; in particular, we comment that allowing prime powers in the larger interval $[1, B_1^{1.5}]$ would have negligible extra cost.

To understand the potential speedup here one can simply count multiplications. GMP-ECM uses approximately 9 multiplications for each bit of s, as illustrated by the example with $B_1 = 10^6$ above.

Doubling in Edwards coordinates uses only 7 multiplications; addition in Edwards coordinates uses 12 multiplications but occurs for only a fraction ϵ of the bits of s. The total multiplication count $7 + 12\epsilon$ is below 9 for $\epsilon < 1/6$.

Of course, reality is more complicated than a multiplication count. One disadvantage of Edwards coordinates is the cost of computing products of batches of prime factors of s — although these products can be saved and reused in a series of ECM computations. One advantage of Edwards coordinates is that a larger fraction of the multiplications are squarings and multiplications by curve

constants. Using inverted Edwards coordinates on twisted Edwards curves (as in GMP-EECM) has many more multiplications by curve constants, but this is a good tradeoff when the parameters are small.

3.6. A numerical example. We provided $n = (5^{367}+1)/(2\cdot 3\cdot 73219364069)$ as input to GMP-ECM 6.1.3, with stage-1 bound $B_1 = 16384$, on an Intel Pentium M (6b8) running at 800MHz. Stage 1 used 210299 multiplications modulo n and consumed a total of 2448 milliseconds.

We then provided the same input to our new GMP-EECM software. We used the same stage-1 bound and the same s, but we used our new curve $x^2 + y^2 = 1 + 161^2x^2y^2/289^2$ (see Section 6) in inverted twisted Edwards coordinates, with width-6 signed sliding windows. Stage 1 used only 195111 multiplications modulo n, consumed only 2276 milliseconds, and printed the (previously known) prime 70057995652034894429. We inspected the point order and found that it has largest prime factor 9103 and second-largest prime factor 2459.

Because GMP-EECM is very new we have not yet tried to use it to find record-setting factorizations.

4 Edwards curves with large torsion

Mazur's theorem [22] says that the torsion group $E_{\mathrm{tor}}(\mathbf{Q})$ of any elliptic curve E is isomorphic to one of the following 15 finite groups:

$$E_{\mathrm{tor}}(\mathbf{Q}) \cong \begin{cases} \mathbf{Z}/m\mathbf{Z}, & m = 1,2,3,4,5,6,7,8,9,10,12, \\ \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2m\mathbf{Z}, & m = 1,2,3,4. \end{cases}$$

Any elliptic curve in Edwards form has a point of order 4. It follows that the torsion group of an Edwards curve is isomorphic to either $\mathbf{Z}/4\mathbf{Z}$, $\mathbf{Z}/8\mathbf{Z}$, $\mathbf{Z}/12\mathbf{Z}$, $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/4\mathbf{Z}$, or $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/8\mathbf{Z}$.

The most interesting cases for ECM are $\mathbf{Z}/12\mathbf{Z}$ and $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/8\mathbf{Z}$, since they force the group orders of E modulo primes p (of good reduction) to be divisible by 12 and 16, respectively. In this section we show which conditions an Edwards curve $x^2 + y^2 = 1 + dx^2y^2$ over $\mathbf{Q}$ must satisfy to have torsion group isomorphic to $\mathbf{Z}/12\mathbf{Z}$ or $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/8\mathbf{Z}$. We give parameterizations for both cases.

One could hope to force divisibility by 12 in a different way, namely by finding a twisted Edwards curve with $\mathbf{Q}$-torsion group isomorphic to $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/6\mathbf{Z}$. A twisted Edwards curve does not need to have a point of order 4. However, at the end of this section we show that there is no twisted Edwards curve with $\mathbf{Q}$-torsion group isomorphic to $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/6\mathbf{Z}$.

4.1. Doubling and tripling on Edwards curves. We use doubling and tripling formulas for Edwards curves, given in [2] and [5], to find points of order 8 and 12.

The double of a point (x_1, y_1) on $x^2 + y^2 = 1 + dx^2y^2$ is

$$[2](x_1, y_1) = \left(\frac{2x_1y_1}{x_1^2 + y_1^2}, \frac{y_1^2 - x_1^2}{2 - (x_1^2 + y_1^2)} \right), \tag{1}$$

while the triple is

$$[3](x_1,y_1)=\left(\frac{(x_1^2+y_1^2)^2-(2y_1)^2}{4(x_1^2-1)x_1^2-(x_1^2-y_1^2)^2}x_1,\frac{(x_1^2+y_1^2)^2-(2x_1)^2}{-4(y_1^2-1)y_1^2+(x_1^2-y_1^2)^2}y_1\right). \tag{2}$$

4.2. Torsion group $\mathbf{Z}/2\mathbf{Z}\times\mathbf{Z}/8\mathbf{Z}$. Theorem 4.3 states a genus-0 cover of the set of Edwards curves over $\mathbf{Q}$ with torsion group $\mathbf{Z}/2\mathbf{Z}\times\mathbf{Z}/8\mathbf{Z}$. Theorem 4.4 identifies all the points of order 8 on such curves. Theorem 4.5 states a rational cover and identifies the degree of the cover.

Theorem 4.3. *The torsion group of an Edwards curve $x^2+y^2=1+dx^2y^2$ over $\mathbf{Q}$ is isomorphic to $\mathbf{Z}/2\mathbf{Z}\times\mathbf{Z}/8\mathbf{Z}$ if and only if d is a square and there exists a rational number $x_8\notin\{0,\pm1\}$ satisfying $(2x_8^2-1)/x_8^4=d$.*

Proof. Assume that the torsion group is isomorphic to $\mathbf{Z}/2\mathbf{Z}\times\mathbf{Z}/8\mathbf{Z}$. The point $(1,0)$ has order 4, so there must be a point (x_8,y_8) on the curve with $[2](x_8,y_8)=(1,0)$. This implies $y_8^2-x_8^2=0$ by Formula (1), and then the curve equation $x_8^2+y_8^2=1+dx_8^2y_8^2$ implies $2x_8^2=1+dx_8^4$. In particular, $x_8\notin\{0,\pm1\}$ since $d\neq1$, and therefore $d=(2x_8^2-1)/x_8^4$. Furthermore, the torsion group has three points of order 2 and so d must be a square.

Conversely, assume that d is a square and that $d=(2x_8^2-1)/x_8^4$. Then the curve (after desingularization) has three points of order 2, and it also has the point (x_8,x_8) of order 8. The torsion group thus contains a copy of $\mathbf{Z}/2\mathbf{Z}\times\mathbf{Z}/8\mathbf{Z}$. By Mazur's theorem the torsion group cannot be larger. □

Theorem 4.4. *Assume that $d\in\mathbf{Q}\setminus\{0,1\}$ is a square, and that $x_8\in\mathbf{Q}\setminus\{0,\pm1\}$ satisfies $(2x_8^2-1)/x_8^4=d$. Then the set of 8 points*

$$\left\{(\pm x_8,\pm x_8),\left(\pm1/(x_8\sqrt{d}),\pm1/(x_8\sqrt{d})\right)\right\},$$

where the signs are taken independently, is exactly the set of points of order 8 on the Edwards curve $x^2+y^2=1+dx^2y^2$ over $\mathbf{Q}$.

Proof. We will show that these 8 points are distinct points of order 8 on the curve. The torsion group of the curve is isomorphic to $\mathbf{Z}/2\mathbf{Z}\times\mathbf{Z}/8\mathbf{Z}$ by Theorem 4.3, so it has exactly 8 elements of order 8, which must be exactly these points.

To see that the 8 points are distinct, suppose that $x_8=\pm1/(x_8\sqrt{d})$. Then $\sqrt{d}x_8^2=\pm1$ so $dx_8^4=1$ so $2x_8^2=2$ so $x_8^2=1$, contradiction.

To see that the points $(\pm x_8,\pm x_8)$ are on the curve, use the equation $2x_8^2-1=dx_8^4$. To see that the points $\left(\pm1/(x_8\sqrt{d}),\pm1/(x_8\sqrt{d})\right)$ are on the curve, observe that

$$1+d\frac{1}{(\pm x_8\sqrt{d})^2}\frac{1}{(\pm x_8\sqrt{d})^2}=\frac{1+dx_8^4}{dx_8^4}=\frac{2x_8^2}{dx_8^4}=\frac{2}{(\pm x_8\sqrt{d})^2},$$

again using the equation $2x_8^2-1=dx_8^4$.

To see that all the points have order 8, observe that $[2](x_1,\pm x_1)=(\pm1,0)$ by Formula (1), and that $(\pm1,0)$ has order 4. □

Theorem 4.5. *If $u \in \mathbf{Q}\setminus\{0,-1,-2\}$ then the Edwards curve $x^2+y^2 = 1+dx^2y^2$ over $\mathbf{Q}$, where*

$$x_8 = \frac{u^2+2u+2}{u^2-2}, \qquad d = \frac{2x_8^2-1}{x_8^4},$$

has $P_8 = (x_8, x_8)$ as a point of order 8 and has torsion group isomorphic to $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/8\mathbf{Z}$.

Conversely, every Edwards curve over $\mathbf{Q}$ with torsion group isomorphic to $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/8\mathbf{Z}$ is expressible in this way.

The parameters u, $2/u$, $-2(u+1)/(u+2)$, $-(2+u)/(1+u)$, $-(u+2)$, $-2/(u+2)$, $-u/(u+1)$, and $-2(u+1)/u$ give the same value of d and they are the only values giving this d.

Proof. By Theorem 4.3 the necessary and sufficient condition for $E_{\mathrm{tor}}(\mathbf{Q}) \cong \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/8\mathbf{Z}$ is that there exists $x_8 \notin \{0, \pm 1\}$ satisfying $(2x_8^2-1)/x_8^4 = d$ and that d is a square; i.e., that $2x_8^2-1$ is a square.

The equation $2x_8^2 - 1 = r^2$ has 4 trivial solutions $(1,1), (1,-1), (-1,1)$, and $(-1,-1)$. These tuples violate the condition $x_8 \notin \{0,\pm 1\}$. There are no other solutions to $2x_8^2 - 1 = r^2$ that violate the condition on x_8.

We parameterize $r^2 = 2x_8^2 - 1$ by intersecting it with lines through $(1,-1)$; i.e., the lines given by $r = ux_8 - u - 1$.

$$\begin{aligned} 0 &= (ux_8 - u - 1)^2 - 2x_8^2 + 1 = (u^2-2)x_8^2 - 2u(u+1)x_8 + (u+1)^2 + 1 \\ &= (u^2-2)(x_8 - 1)(x_8 - (u^2+2u+2)/(u^2-2)). \end{aligned}$$

A new solution to $r^2 = 2x_8^2 - 1$ in terms of u is given by $(x_8, r) = ((u^2+2u^2+2)/(u^2-2), (u^2+4u+2)/(u^2-2))$, where the value for r is computed using the line.

This parameterization cannot find $(1,1)$, but this solution is excluded anyway. The solutions $(1,-1)$, $(-1,1)$, and $(-1,-1)$ are found for $u=-2$, $u=-1$, and $u=0$, respectively. So $u \in \mathbf{Q} \setminus \{0,-1,-2\}$ gives a complete parameterization of all Edwards curves with $E_{\mathrm{tor}}(\mathbf{Q}) \cong \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/8\mathbf{Z}$.

The identity

$$\begin{aligned} &(d(u) - d(v))(((u+1)^2+1)((v+1)^2+1))^4 \\ &\quad = 16(u-v)(uv-2)((u+2)v + 2(u+1))(u+2+(u+1)v) \\ &\qquad \cdot (u+v+2)((u+2)v+2)(u+(u+1)v)(uv+2(u+1)) \end{aligned}$$

immediately shows that if v is any of the listed values $u, 2/u, \ldots$ then $d(v) = d(u)$. Conversely, if v is not one of those values then none of the factors $u-v, uv-2, \ldots$ are 0 so $d(v) \neq d(u)$. □

4.6. Torsion group Z/12Z. Theorem 4.7 states a genus-0 cover of the set of Edwards curves over $\mathbf{Q}$ with torsion group $\mathbf{Z}/12\mathbf{Z}$. Theorem 4.8 identifies all the points of order 12 on such curves. Theorem 4.9 states a rational cover.

Theorem 4.7. *The torsion group of an Edwards curve $x^2 + y^2 = 1 + dx^2y^2$ over $\mathbf{Q}$ is isomorphic to $\mathbf{Z}/12\mathbf{Z}$ if and only if there exists a rational number $y_6 \notin \{-2, -1/2, 0, \pm 1\}$ satisfying $(2y_6+1)/(y_6^3(y_6+2)) = d$ and such that $-(y_6^2+2y_6)$ is a square.*

Proof. Rational points of order 3 or 6 are exactly the points (x_6, y_6) for which the x coordinate of $[3](x_6, y_6)$ is 0. By formula (2) these are exactly the points for which $(x_6^2 + y_6^2)^2 = (2y_6)^2$. If this holds for one (x_6, y_6) then it also holds for $(\pm x_6, \pm y_6)$, where the signs are taken independently. Up to signs this means that $x_6^2 + y_6^2 = -2y_6$. If the curve has such a point then d must satisfy the equation $x_6^2 + y_6^2 = 1 + dx_6^2y_6^2$, i.e., $-2y_6 = 1 + d(-2y_6 - y_6^2)y_6^2$. For $y_6 \notin \{-2, -1/2, 0, \pm 1\}$ the value $d = (2y_6 + 1)/(y_6^3(y_6 + 2))$ is defined and not equal to 0 or 1.

For this d we get a point of order 3 or 6 exactly if $x_6^2 = -(y_6^2 + 2y_6)$ has a rational solution.

Since each Edwards curve has a point of order 4 the torsion group must contain a copy of $\mathbf{Z}/12\mathbf{Z}$; by Mazur's theorem the torsion group cannot be larger. □

Theorem 4.8. *Let $x^2 + y^2 = 1 + dx^2y^2$ be an Edwards curve over $\mathbf{Q}$ with $E_{tor}(\mathbf{Q}) \cong \mathbf{Z}/12\mathbf{Z}$ and let $P_3 = (x_3, y_3)$ be a point of order 3 on the curve.*

The 12 torsion points on the curve and their respective orders are as follows:

point	$(0,1)$	$(0,-1)$	$(\pm x_3, y_3)$	$(\pm 1, 0)$	$(\pm x_3, -y_3)$	$(\pm y_3, \pm x_3)$
order	1	2	3	4	6	12

Proof. The points of order 6 are obtained as $(\pm x_3, y_3) + (0, -1)$, the points of order 12 by adding $(\pm 1, 0)$ to the points of order 3 and 6. □

Theorem 4.9. *If $u \in \mathbf{Q} \setminus \{0, \pm 1\}$ then the Edwards curve $x^2 + y^2 = 1 + dx^2y^2$ over $\mathbf{Q}$, where*

$$x_3 = \frac{u^2 - 1}{u^2 + 1}, y_3 = -\frac{(u-1)^2}{u^2+1}, d = \frac{(u^2+1)^3(u^2-4u+1)}{(u-1)^6(u+1)^2}$$

has $P_3 = (x_3, y_3)$ as a point of order 3 and has torsion group isomorphic to $\mathbf{Z}/12\mathbf{Z}$.

Conversely, every Edwards curve over $\mathbf{Q}$ with torsion group isomorphic to $\mathbf{Z}/12\mathbf{Z}$ is expressible in this way.

The parameters u and $1/u$ give the same value of d.

Proof. The points of order 3 are determined by $[2](x_3, y_3) = (-x_3, y_3)$ and $x_3, y_3 \neq 0$. Solving this equation gives $x_3^2 + y_3^2 = -2y_3$, i.e., $x_3^2 + (y_3 + 1)^2 = 1$. Parameterization of the unit circle $r^2 + s^2 = 1$ (with $r = x_3$ and $s = y_3 + 1$) yields $(r, s) = \big((u^2 - 1)/(u^2 + 1), 2u/(u^2 + 1)\big)$ and thus the point $(x_3, y_3) = \big((u^2 - 1)/(u^2 + 1), 2u/(u^2 + 1) - 1\big) = \big((u^2 - 1)/(u^2 + 1), -(u - 1)^2/(u^2 + 1)\big)$.

The parameterization does not find the solution $(r, s) = (1, 0)$, i.e., $(x_3, y_3) = (1, -1)$ which is not a point of order 3. Likewise, $(r, s) = (-1, 0)$ which is found

for $u = 0$ does not lead to a point of order 3. The solutions $(r, s) = (0, \pm 1)$, obtained for $u = \pm 1$ lead to $x_3 = 0$ and are therefore excluded.

The value for d follows from Theorem 4.7. For $u \in \mathbf{Q} \setminus \{0, \pm 1\}$ the value of d is defined and not equal to 0 or 1.

The value of d is invariant under the change $u \leftarrow 1/u$ since

$$\frac{(1+u^2)^3(1-4u+u^2)}{(1-u)^6(1+u)^2} = \frac{(u^2+1)^3(u^2-4u+1)}{(u-1)^6(u+1)^2}.$$

□

Solving the equation $d(u') = d(u)$ for u' in terms of u over the rationals shows that $u \leftarrow 1/u$ is the only rational transformation leaving d invariant that works independently of u.

4.10. Torsion group $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/6\mathbf{Z}$. The following theorem shows that the only way for a twisted Edwards curve to have exactly 12 torsion points is to have torsion group isomorphic to $\mathbf{Z}/12\mathbf{Z}$.

Theorem 4.11. *There exists no twisted Edwards curve over* $\mathbf{Q}$ *with torsion group isomorphic to* $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/6\mathbf{Z}$.

Proof. Every twisted Edwards curve is birationally equivalent to a Montgomery curve; see [3, Section 3]. So it suffices to show that there exists no Montgomery curve over $\mathbf{Q}$ with torsion group isomorphic to $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/6\mathbf{Z}$.

Fix $A, B \in \mathbf{Q}$ and let $\mathrm{E}_{\mathrm{M},A,B} : By^2 = x^3 + Ax^2 + x$ be an elliptic curve over $\mathbf{Q}$ in Montgomery form. Suppose that the torsion group of $\mathrm{E}_{\mathrm{M},A,B}$ is isomorphic to $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/6\mathbf{Z}$.

The subgroup $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$ forces the right-hand side of the curve equation to be equal to $(x-a_1)(x-a_2)x$, where a_1, a_2 are distinct nonzero rational numbers. Then $A = -(a_1 + a_2)$ and $a_2 = 1/a_1$.

The subgroup $\mathbf{Z}/3\mathbf{Z}$ forces an affine point $P_3 = (x_3, y_3)$ of order 3 on the curve; i.e., $[2]P_3 = -P_3 = (x_3, -y_3)$. Using the addition law on $\mathrm{E}_{\mathrm{M},A,B}$ we get $x_3 = B\lambda^2 - 2x_3 - A$, where $\lambda = (3x_3^2 + 2Ax_3 + 1)/(2By_3)$; i.e., $x_3 = (3x_3^2 + 2Ax_3 + 1)^2/(4By_3^2) - 2x_3 - A$. Substitute $By_3^2 = x_3^3 + Ax_3^2 + x_3$ and simplify to see that

$$\frac{3x_3^4 + 6x_3^2 - 1}{4x_3^3} = -A = -(a_1 + 1/a_1).$$

This can be written as $a_1(3x_3^4 + 6x_3^2 - 1) = (a_1^2 + 1)4x_3^3$; i.e., $(x_3 : a_1 : 1)$ is a point on the projective curve

$$C : V(3U^4 + 6U^2Z^2 - Z^4) = (V^2 + Z^2)4U^3.$$

According to Magma [8] this curve has exactly the eight points $(4/3 : 1 : 0)$, $(0 : 1 : 0)$, $(0 : 0 : 1)$, $(1 : 0 : 0)$, $(-1/3 : 1 : 1)$, $(1/3 : -1 : 1)$, $(1 : 1 : 1)$ and $(-1 : -1 : 1)$. Three of the points are at infinity; the other five points give values for x_3 and A such that the corresponding Montgomery curve is singular. Hence the torsion group cannot be isomorphic to $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/6\mathbf{Z}$. □

5 Edwards curves with large torsion and positive rank

Atkin and Morain in [1] found an infinite family of elliptic curves over $\mathbf{Q}$ with torsion group $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/8\mathbf{Z}$ and with explicit non-torsion points. Suyama in [24] had earlier given an infinite sequence of Montgomery curves which have group order divisible by 12 over any prime field, although they do not usually have $\mathbf{Q}$-torsion group $\mathbf{Z}/12\mathbf{Z}$. In this section we translate the Atkin-Morain and Suyama constructions from Weierstrass curves to Edwards curves.

To see the impact of the $\mathbf{Q}$-torsion group we considered Edwards curves with torsion group $\mathbf{Z}/12\mathbf{Z}$ as in Section 4 and computed the group order modulo primes p in the interval $[10^6, 2 \cdot 10^6]$. The average exponents of 2 and 3 in the group order were almost exactly 11/3 and 5/3 respectively. For Suyama curves with torsion group $\mathbf{Z}/6\mathbf{Z}$ the averages were only 10/3 and 5/3, except for a few unusual curves such as $\sigma = 11$ in the notation of Theorem 5.5 below.

5.1. Atkin and Morain's parameterization. The Atkin-Morain family is parameterized by points (s, t) on a particular elliptic curve $T^2 = S^3 - 8S - 32$. Atkin and Morain suggest computing multiples (s, t) of $(12, 40)$, a non-torsion point on this curve. Beware that these points have rapidly increasing height.

Theorem 5.2 (Atkin, Morain). *Let (s, t) be a rational point on the curve $T^2 = S^3 - 8S - 32$. Define $\alpha = ((t + 25)/(s - 9) + 1)^{-1}$, $\beta = 2\alpha(4\alpha+1)/(8\alpha^2-1)$, $c = (2\beta - 1)(\beta - 1)/\beta$, and $b = \beta c$. Then the elliptic curve*

$$E_\alpha : \; Y^2 = X^3 + \frac{((c-1)^2 - 4b)}{4}X^2 + \frac{b(c-1)}{2}X + \frac{b^2}{4}$$

has torsion group isomorphic to $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/8\mathbf{Z}$ and a point with x-coordinate $-(2\beta - 1)/4$.

Theorem 5.3. *Let (s, t) be a rational point on the curve $T^2 = S^3 - 8S - 32$. Define α and β as in Theorem 5.2. Define $d = (2(2\beta - 1)^2 - 1)/(2\beta - 1)^4$. Then the Edwards curve $x^2 + y^2 = 1 + dx^2y^2$ has torsion group isomorphic to $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/8\mathbf{Z}$ and a point (x_1, y_1) with $x_1 = (2\beta - 1)(4\beta - 3)/(6\beta - 5)$ and $y_1 = (2\beta - 1)(t^2 + 50t - 2s^3 + 27s^2 - 104)/(t + 3s - 2)(t + s + 16)$.*

Proof. By construction $x_8 = 2\beta - 1$ satisfies $(2x_8^2 - 1)/x_8^4 = d$. Furthermore

$$d = \frac{(8\alpha^2 - 1)^2(8\alpha^2 + 8\alpha + 1)^2}{(8\alpha^2 + 4\alpha + 1)^4},$$

so d is a square. By Theorem 4.3, the Edwards curve has torsion group isomorphic to $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/8\mathbf{Z}$. Finally, a straightforward calculation shows that $x_1^2 + y_1^2 = 1 + dx_1^2y_1^2$. □

The point with x-coordinate $-(2\beta - 1)/4$ in Theorem 5.2 is generically a non-torsion point. The y-coordinate of the point is not stated explicitly in [1]. The point (x_1, y_1) in Theorem 5.3 is the corresponding point on the Edwards curve.

5.4. Suyama's parameterization. The GMP-ECM package uses a family of elliptic curves in Montgomery form given by Suyama's parameterization (see [26]). We briefly review this parameterization and show how we can obtain a similar result for twisted Edwards curves.

Theorem 5.5 (Suyama). *Let $\sigma > 5$ be an integer. Define*

$$\alpha = \sigma^2 - 5, \quad \beta = 4\sigma, \quad U_0 = \alpha^3, \quad W_0 = \beta^3,$$
$$A = (\beta - \alpha)^3(3\alpha + \beta)/(4\alpha^3\beta) - 2, \quad B = \alpha/W_0.$$

Then the elliptic curve $\mathrm{E}_{\mathrm{M},A,B} : Bv^2 = u^3 + Au^2 + u$ has a $\mathbf{Q}$-torsion subgroup isomorphic to $\mathbf{Z}/6\mathbf{Z}$.

Let $V_0 = (\sigma^2 - 1)(\sigma^2 - 25)(\sigma^4 - 25)$. Then $(u_0, v_0) = (U_0/W_0, V_0/W_0)$ is a point on $\mathrm{E}_{\mathrm{M},A,B}$.

Theorem 5.6. *Let $\sigma > 5$ and $\alpha, \beta, U_0, V_0, W_0$ as in Theorem 5.5. For $a = (\beta-\alpha)^3(3\alpha+\beta)\beta^2/(4\alpha^4)$ and $d = (\beta+\alpha)^3(\beta-3\alpha)\beta^2/(4\alpha^4)$ the twisted Edwards curve $ax^2 + y^2 = 1 + dx^2y^2$ has a point $(x_0, y_0) = (\alpha^3/V_0, (\alpha^3 - \beta^3)/(\alpha^3 + \beta^3))$ and a $\mathbf{Q}$-torsion subgroup isomorphic to $\mathbf{Z}/6\mathbf{Z}$.*

Proof. We showed in [3] that over a non-binary field k every Montgomery curve $\mathrm{E}_{\mathrm{M},A,B} : Bv^2 = u^3 + Au^2 + u$ is birationally equivalent to a twisted Edwards curve $\mathrm{E}_{\mathrm{E},a,d} : ax^2 + y^2 = 1 + dx^2y^2$. The relations between the curve coefficients are $a = (A+2)/B$ and $d = (A-2)/B$ and the map from $\mathrm{E}_{\mathrm{M},A,B}$ to $\mathrm{E}_{\mathrm{E},a,d}$ is given by $(u, v) \mapsto (x, y) = (u/v, (u-1)/(u+1))$. With $A = (\beta-\alpha)^3(3\alpha+\beta)/(4\alpha^3\beta)-2$ and $B = \alpha/\beta^3$ as in Theorem 5.5 we get the desired values for a and d. Mapping the point $(u_0, v_0) = (\alpha^3/\beta^3, V_0/\beta^3)$ to $\mathrm{E}_{\mathrm{E},a,d}$ yields the desired point (x_0, y_0):

$$x_0 = u_0/v_0 = \alpha^3/V_0 \quad \text{and} \quad y_0 = \frac{u_0 - 1}{u_0 + 1} = \frac{\alpha^3 - \beta^3}{\alpha^3 + \beta^3}.$$

□

6 Edwards curves with small parameters, large torsion, and positive rank

One way to save time in computations on generalized Edwards curves is to choose small parameters a, d and small points $(X_1 : Y_1 : Z_1)$; see Section 2.3. Another way to save time is to construct curves of rank at least 1 with large torsion over $\mathbf{Q}$; see Section 5. Unfortunately, essentially all of the curves constructed in Section 5 have large a, d, X_1, Y_1, Z_1.

Our aim in this section is to combine these two time-saving techniques, finding twisted Edwards curves that simultaneously have small parameters a, d, a small non-torsion point $(X_1 : Y_1 : Z_1)$, and large torsion over $\mathbf{Q}$.

Overall we found more than 100 small Edwards curves having small non-torsion points and at least 12 torsion points over $\mathbf{Q}$. Of course, one can easily write down many more small curves if one is willing to sacrifice some torsion.

6.1. Torsion group $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/8\mathbf{Z}$. First we consider the case where the curve has torsion group isomorphic to $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/8\mathbf{Z}$, i.e. there exists a point of order 8 on the curve and d is a square.

Theorem 4.4 states all points of order 8. The other affine points of finite order are $(0, \pm 1)$ and $(\pm 1, 0)$. Any other point (x_1, y_1) on the curve must have infinite order.

Theorem 4.5 gives a complete parameterization of all curves with torsion group isomorphic to $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/8\mathbf{Z}$. Any rational point (u, x_8, d, x_1, y_1) on the surface described by $x_8 = (u^2+2u+2)/(u^2-2)$, $d = (2x_8^2-1)/x_8^4$, and $x_1^2+y_1^2 = 1 + dx_1^2y_1^2$ for $u \in \mathbf{Q} \setminus \{0, -1, -2\}$ gives us a suitable curve for ECM as long as we can ensure that (x_1, y_1) is none of the points of finite order.

We consider only $u > \sqrt{2}$. This does not lose any generality: if $0 < u < \sqrt{2}$ then $2/u > \sqrt{2}$, and $2/u$ produces the same curve by Theorem 4.5; if $u < -2$ then $-(u+2) > 0$, and $-(u+2)$ produces the same curve by Theorem 4.5; if $-2 < u < -1$ then $-2(u+1)/(u+2) > 0$, and $-2(u+1)/(u+2)$ produces the same curve by Theorem 4.5; if $-1 < u < 0$ then $-u/(u+1) > 0$, and $-u/(u+1)$ produces the same curve by Theorem 4.5.

Write u as a/b for positive integers a, b. Expressing x_8 and d in terms of a and b produces the denominator $(a^2+2ab+2b^2)^4$ for d and thus for $dx_1^2y_1^2$. Thus we scale x_1 and y_1 as

$$x_1 = (a^2 + 2ab + 2b^2)/e, y_1 = (a^2 + 2ab + 2b^2)/f.$$

Expressing all variables in a, b, e, f we find that solutions (u, x_8, d, x_1, y_1) correspond to integer solutions a, b, e, f of the $(1, 1, 2, 2)$-weighted-homogeneous equation

$$(e^2 - (a^2 + 2ab + 2b^2)^2)(f^2 - (a^2 + 2ab + 2b^2)^2) = (4ab(a + b)(a + 2b))^2.$$

We found many small solutions to this equation, and thus many of the desired Edwards curves, as follows. We considered a range of positive integers a. For each a we enumerated integers b between 1 and $\lfloor a/\sqrt{2} \rfloor$. For each (a, b) we enumerated all divisors of $(4ab(a+b)(a+2b))^2$, added $(a^2+2ab+2b^2)^2$ to each divisor, and searched for squares.

After about a week of computation on some computers at LORIA, roughly $2 \cdot 10^{16}$ CPU cycles in total, we had inspected more than 10^{14} divisors, found 25 different values of d, and checked that we had 25 different j-invariants.

Here are two examples:

- the solution $(a, b, e, f) = (3, 1, 19, 33)$ produces the order-8 point $(17/7, 17/7)$ and the non-torsion point $(17/19, 17/33)$ on the Edwards curve $x^2 + y^2 = 1 + dx^2y^2$ where $d = 161^2/17^4$;
- the solution $(a, b, e, f) = (24882, 9009, 258492663, 580153002)$ produces the non-torsion point $(86866/18259, 8481/4001)$ on the Edwards curve $x^2+y^2 = 1 + dx^2y^2$ where $d = 5657719^2/3341^4$.

The number of d's below height H appears to grow as roughly $\lg H$. For comparison, the Atkin-Morain procedure discussed in Section 5 generates only about $\sqrt{\lg H}$ examples below height H.

6.2. Torsion group Z/12Z. Writing $u = a/b$ in Theorem 4.9 yields an Edwards parameter d, a non-torsion point (x_1, y_1) and a point (x_3, y_3) of order 3 as follows:

$$d = \frac{(a^2+b^2)^3(a^2-4ab+b^2)}{(a-b)^6(a+b)^2},\ x_3 = \frac{(a^2-b^2)}{(a^2+b^2)},\ y_3 = \frac{-(a-b)^2}{(a^2+b^2)},$$
$$x_1 = \frac{(a^2-b^2)}{e},\ y_1 = \frac{-(a-b)^2}{f}.$$

We have to exclude x_1 from being any of the torsion points stated in Theorem 4.8 and need that $u \in \mathbf{Q} \setminus \{0, \pm 1\}$. Writing $x_1^2 + y_1^2 = 1 + dx_1^2y_1^2$ in terms of a, b, e, f shows that we have to look for points (a, b, e, f) on the surface

$$(e^2 - (a^2-b^2)^2)(f^2 - (a-b)^4) = 16a^3b^3(a^2 - ab + b^2).$$

We found many small solutions as in Section 6.1: for each small (a, b) we enumerated all divisors of $16a^3b^3(a^2 - ab + b^2)$, added $(a^2 - b^2)^2$ to each divisor, and looked for squares.

After about a week of computation on some computers at LORIA we had found 78 different values of d and checked that we had 78 different j-invariants.

Here are two examples:

- the solution $(a, b, e, f) = (3, 2, 23, 7)$ produces the order-3 point $(5/13, -1/13)$ and the non-torsion point $(5/23, -1/7)$ on the Edwards curve $x^2 + y^2 = 1 + dx^2y^2$ where $d = -11 \cdot 13^3/5^2$;
- the solution $(a, b, e, f) = (15180, -7540, 265039550, 161866240)$ produces the non-torsion point $(3471616/5300791, -201640/63229)$ on the Edwards curve $x^2 + y^2 = 1 + dx^2y^2$ where $d = 931391 \cdot 359105^3/140003330048^2$.

References

1. A. O. L. Atkin, Francois Morain, *Finding suitable curves for the elliptic curve method of factorization*, Mathematics of Computation **60** (1993), 399–405. ISSN 0025–5718. MR 93k:11115. URL: `http://www.lix.polytechnique.fr/~morain/Articles/articles.english.html`. Citations in this document: §1.2, §5, §5.1.
2. Daniel J. Bernstein, Peter Birkner, Tanja Lange, Christiane Peters, *Optimizing double-base elliptic-curve single-scalar multiplication*, in Indocrypt 2007 [23] (2007), 167-182. URL: `http://cr.yp.to/papers.html#doublebase`. Citations in this document: §4.1.
3. Daniel J. Bernstein, Peter Birkner, Marc Joye, Tanja Lange, Christiane Peters, *Twisted Edwards Curves*, in Africacrypt [25] (2008), 389–405. URL: `http://eprint.iacr.org/2008/013`. Citations in this document: §2.3, §2.3, §4.10, §5.4.
4. Daniel J. Bernstein, Tanja Lange, *Explicit-formulas database* (2007). URL: `http://hyperelliptic.org/EFD`. Citations in this document: §2.1.
5. Daniel J. Bernstein, Tanja Lange, *Faster addition and doubling on elliptic curves*, in Asiacrypt 2007 [16] (2007), 29–50. URL: `http://cr.yp.to/papers.html#newelliptic`. Citations in this document: §2, §2, §2.1, §4.1.
6. Daniel J. Bernstein, Tanja Lange, *Inverted Edwards coordinates*, in AAECC 2007 [9] (2007), 20–27. URL: `http://cr.yp.to/papers.html#inverted`. Citations in this document: §2.2.

7. Daniel J. Bernstein, Tanja Lange, *Analysis and optimization of elliptic-curve single-scalar multiplication*, in Fq8 [19] (2008), 1–19. URL: http://cr.yp.to/papers.html#efd.
8. Wieb Bosma, John J. Cannon, Catherine Playoust, *The Magma algebra system. I. The user language*, Journal of Symbolic Computation **24** (1997), 235–266. Citations in this document: §4.10.
9. Serdar Boztas, Hsiao-Feng Lu (editors), *Applied algebra, algebraic algorithms and error-correcting codes*, Lecture Notes in Computer Science, 4851, Springer, 2007. See [6].
10. Richard P. Brent, *Some integer factorization algorithms using elliptic curves*, Australian Computer Science Communications **8** (1986), 149–163. ISSN 0157–3055. Citations in this document: §3.2, §3.3. See [24].
11. David V. Chudnovsky, Gregory V. Chudnovsky, *Sequences of numbers generated by addition in formal groups and new primality and factorization tests*, Advances in Applied Mathematics **7** (1986), 385–434. MR 88h:11094. Citations in this document: §3.4, §3.4.
12. Harold M. Edwards, *A normal form for elliptic curves*, Bulletin of the American Mathematical Society **44** (2007), 393–422. URL: http://www.ams.org/bull/2007-44-03/S0273-0979-07-01153-6/home.html. Citations in this document: §2.
13. Florian Hess, Sebastian Pauli, Michael E. Pohst (editors), *Algorithmic Number Theory, 7th International Symposium, ANTS-VII, Berlin, Germany, July 23-28, 2006, Proceedings*, Lecture Notes in Computer Science, 4076, Springer, Berlin, 2006. ISBN 3–540–36075–1. See [26].
14. Huseyin Hisil, Kenneth Koon-Ho Wong, Gary Carter, Ed Dawson, *Twisted Edwards curves revisited*, in Asiacrypt 2008 [21] (2008). URL: http://eprint.iacr.org/2008/522. Citations in this document: §2.3.
15. James McKee, *Subtleties in the distribution of the numbers of points on elliptic curves over a finite prime field*, Journal of the London Mathematical Society **59** (1999), 448–460. URL: http://journals.cambridge.org/action/displayAbstract?fromPage=online&aid=20335. Citations in this document: §3.1.
16. Kaoru Kurosawa (editor), *Advances in cryptology — ASIACRYPT 2007*, Lecture Notes in Computer Science, 4833, Springer, 2007. See [5].
17. Hendrik W. Lenstra, Jr., *Factoring integers with elliptic curves*, Annals of Mathematics **126** (1987), 649–673. ISSN 0003–486X. MR 89g:11125. URL: http://links.jstor.org/sici?sici=0003-486X(198711)2:126:3<649:FIWEC>2.0.CO;2-V. Citations in this document: §1.
18. Peter L. Montgomery, *Speeding the Pollard and elliptic curve methods of factorization*, Mathematics of Computation **48** (1987), 243–264. ISSN 0025–5718. MR 88e:11130. URL: http://links.jstor.org/sici?sici=0025-5718(198701)48:177<243:STPAEC>2.0.CO;2-3. Citations in this document: §3.3, §3.4. See [24].
19. Gary L. Mullen, Daniel Panario, Igor E. Shparlinski (editors), *Finite fields and applications: proceedings of Fq8*, Contemporary Mathematics, 461, American Mathematical Society, 2008. ISBN 978–0–8218–4309–3. See [7].
20. John M. Pollard, *Theorems on factorization and primality testing*, Proceedings of the Cambridge Philosophical Society **76** (1974), 521–528. ISSN 0305–0041. MR 50:6992. URL: http://cr.yp.to/bib/entries.html#1974/pollard. Citations in this document: §3.2, §3.3.
21. Josef Pieprzyk (editor), *Advances in cryptology — ASIACRYPT 2008, 14th international conference on the theory and application of cryptology and information security, Melbourne, Australia, December 7–11, 2008*, Lecture Notes in Computer Science, 5350, 2008. ISBN 978-3-540-89254-0. See [14].

22. Joseph H. Silverman, *The Arithmetic of Elliptic Curves*, GTM, 106, SV, NY, 1886. Citations in this document: §4.
23. Kannan Srinathan, C. Pandu Rangan, Moti Yung (editors), *Indocrypt 2007*, Lecture Notes in Computer Science, 4859, Springer, 2007. See [2].
24. Hiromi Suyama, *Informal preliminary report (8)*, cited in [10] as personal communication and in [18] (1985). Citations in this document: §5.
25. Serge Vaudenay (editor), *Progress in Cryptology — AFRICACRYPT 2008, First International Conference on Cryptology in Africa, Casablanca, Morocco, June 11-14, 2008, proceedings*, Lecture Notes in Computer Science, 5023, Springer, 2008. ISBN 978–3–540–68159–5. See [3].
26. Paul Zimmermann, Bruce Dodson, *20 Years of ECM*, in ANTS VII [13] (2006), 525–542. Citations in this document: §1, §3.2, §3.3, §3.4, §5.4.
27. Paul Zimmermann, *50 largest factors found by ECM*. URL: `http://www.loria.fr/~zimmerma/records/top50.html`. Citations in this document: §1.