Parametrizations for Families of ECM-Friendly Curves

Alexandre Gélin

Laboratoire de Mathématiques de Versailles,
UVSQ – CNRS – Université Paris-Saclay

The Elliptic Curve Method (ECM) for integer factorization was introduced in 1985 by H.W. Lenstra and published two years later in [Len87]. It is the asymptotically fastest method that has been published for finding relatively small factors of large composites. Although the number field sieve is the most efficient general algorithm for integer factorization, there are two common use cases for ECM: it is widely used in attempts to find factors of large composites for which no information is available about the sizes of the prime factors (Propper found the largest ECM factor so far, a 274-bit factor of $7^{337}+1$) and it is used for the so-called *cofactoring* step of the number field sieve (where many relatively small composites have to be factored).

Given an odd composite integer N to be factored, ECM performs arithmetic operations on elliptic curves considered to be defined over the finite field $\mathbf{F}_p$ of cardinality p, for an unknown prime divisor p of N. It may find p if the cardinality of at least one of these curves over $\mathbf{F}_p$ is smooth. For this reason, we use curves that are known to have favorable smoothness properties, such as a large torsion group over $\mathbf{Q}$ or a cardinality that is divisible by a fixed factor. Constructions of ECM-friendly curves were published by Suyama [Suy85] (with a slight improvement by Montgomery in [Mon87, Section 10.3.2]), Atkin-Morain [AM93], and generalized by Bernstein *et al.* in [BBL10].

Originally formulated using Weierstrass curves, until around 2008 implementations of ECM mostly used Montgomery's approach from [Mon87]. With the introduction of Edwards curves [Edw07], a number of follow-up papers by Bernstein *et al.* [BBJ+08, BBLP08] ultimately led to "$a=-1$ *twisted Edwards*" curves by Hisil *et al.* [HWCD08] with torsion group isomorphic to $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/4\mathbf{Z}$ as one of the current most efficient ways to implement ECM, as shown by Bernstein *et al.* in [BBL10]. For these curves, Barbulescu *et al.* in [BBB+12] identify three families that all have the same larger smoothness probability and an even better fourth family. In [BBB+12] a parametrization is provided for one of the three equivalent families; the others are only illustrated by — a finite set of — small values found by enumeration. In particular a parametrization of the fourth and best family, which could lead to a better choice of curves for ECM, has

so far not been published. By *parametrization* we mean that an elliptic curve along with a non-torsion point is determined as a function of some parameter: the parameter may be a point on some other elliptic curve or a rational number, thus giving rise to *elliptic* and *rational* parametrizations.

We extend the constructions from [BBB+12] by developing six further rational parametrizations, and use three of them to formulate five new elliptic parametrizations that enable fast generation of curves for all families of curves from [BBB+12]. We conduct the same tests as described in [BBL10] for the family of curves that are, based on their Galois properties, most promising for ECM. With respect to the criteria from [BBL10], usage of this family of curves leads to slightly better performance of ECM than reported before, with no significant fluctuations across curves from this same family. The newly parameterized curves may prove to be most useful for ECM-based cofactoring in the number field sieve.

References

[AM93] A. O. L. Atkin and F. Morain. Finding suitable curves for the elliptic curve method of factorization. *Mathematics of Computation*, 60:399–405, 1993.

[BBB+12] R. Barbulescu, J. W. Bos, C. Bouvier, T. Kleinjung, and P. L. Montgomery. Finding ECM-friendly curves through a study of Galois properties. In *Proceedings of the Tenth Algorithmic Number Theory Symposium*, pages 63–86, 2012.

[BBJ+08] D. J. Bernstein, P. Birkner, M. Joye, T. Lange, and C. Peters. Twisted Edwards curves. In *Progress in Cryptology - AFRICACRYPT 2008, Proceedings*, pages 389–405, 2008.

[BBL10] D. J. Bernstein, P. Birkner, and T. Lange. Starfish on strike. In *Progress in Cryptology - LATINCRYPT 2010, Proceedings*, pages 61–80, 2010.

[BBLP08] D. J. Bernstein, P. Birkner, T. Lange, and C. Peters. ECM using Edwards curves. *Mathematics of Computation*, 82(282):1139–1179, 2013.

[Edw07] H. M. Edwards. A normal form for elliptic curves. *Bulletin of the American Mathematical Society*, 44:393–422, 2007.

[HWCD08] H. Hisil, K. K.-H. Wong, G. Carter, and E. Dawson. Twisted Edwards curves revisited. In *Advances in Cryptology - ASIACRYPT 2008, Proceedings*, pages 326–343, 2008.

[Len87] H. W. Lenstra Jr. Factoring integers with elliptic curves. *Annals of Mathematics*, 126:649–673, 1987.

[Mon87] P. L. Montgomery. Speeding the Pollard and elliptic curve methods of factorization. *Mathematics of Computation*, 48:243–264, 1987.

[Suy85] H. Suyama. Informal preliminary report. (cited in [Mon87]), 1985.