Abstract. This paper improves the price-performance ratio of ECM, the elliptic-curve method of integer factorization. In particular, this paper constructs \( a = -1 \) twisted Edwards curves having \( \mathbb{Q} \)-torsion group \( \mathbb{Z}/2 \times \mathbb{Z}/4, \mathbb{Z}/8 \), or \( \mathbb{Z}/6 \) and having a known non-torsion point; demonstrates that, compared to the curves used in previous ECM implementations, some of the new curves are more effective at finding small primes despite being faster; and precomputes particularly effective curves for several specific sizes of primes.

Keywords: Factorization, ECM, elliptic-curve method, curve selection, Edwards coordinates, twisted Edwards curves, Suyama curves.

1 Introduction

ECM, Lenstra’s elliptic-curve method of integer factorization [11], does not find the secret prime factors of an RSA modulus as quickly as the number-field sieve (NFS) does. However, ECM is an increasingly important tool inside NFS as a method of finding many smaller primes.

This paper proposes a new two-part strategy to choose curves in ECM. We have implemented the strategy as a patch to the state-of-the-art “EECM-MPFQ” software, and demonstrated through extensive computer experiments that the new strategy achieves better ECM price-performance ratios than anything in the previous literature.

1.1. Background: Edwards curves in ECM. Edwards curves were first described by Edwards in [7]. Bernstein and Lange [5] gave inversion-free formulas for addition and doubling, showing that Edwards curves allow faster scalar multiplication than all other known curve shapes.
Edwards curves save time in many applications in cryptography and number theory — provided that the underlying curve is allowed to have a point of order 4. This 4-torsion requirement does not sound troublesome for ECM: the conventional wisdom is that torsion points increase the chance of factorization. This conventional wisdom is based on the heuristic that, for a curve having a torsion group of size \( r \), the group order modulo \( p \) has the same smoothness probability as an integer divisible by \( r \) in the Hasse interval \([p + 1 - 2\sqrt{p}, p + 1 + 2\sqrt{p}]\), or equivalently an integer in \([ (p + 1 - 2\sqrt{p})/r, (p + 1 + 2\sqrt{p})/r ]\), so increasing \( r \) increases the smoothness chance. For more details on this heuristic and the extent to which it holds, see [4, Section 9].

Bernstein, Birkner, Lange, and Peters demonstrated in [4] the speed of Edwards curves inside ECM. The same paper introduced new small-coefficient high-torsion positive-rank Edwards curves and reported measurements of the effectiveness of two representative curves, i.e., the success chance of the curves at finding primes of various sizes. One curve was the smallest-coefficient positive-rank Edwards curve having torsion group isomorphic to \( \mathbb{Z}/12 \); the other, \( \mathbb{Z}/2 \times \mathbb{Z}/8 \). Those curves turned out to be simultaneously faster and more effective than the standard ECM choices described in detail in [17], namely Montgomery curves (specifically Suyama curves) for stage 1 and Weierstrass curves for stage 2.

Twisted Edwards curves \( ax^2 + y^2 = 1 + dx^2y^2 \) were introduced in [3] as a generalization of Edwards curves; they do not necessarily have a point of order 4. For a twisted Edwards curve with \( a = -1 \) and negative \( d \) the affine graph looks like the following:

To visualize the behavior at infinity we map a sphere to \( \mathbb{P}^2(\mathbb{R}) \), rotate the sphere to an angle that makes the relevant points at infinity visible at the same time as \((0,0)\), and then project the front half of the sphere onto a circle. This first picture shows that there is a single point at infinity and that the curve has two different tangent lines at this point — but only the second picture shows the true nature of things: