Edwards Curves and the ECM Factorisation Method

Peter Birkner

Eindhoven University of Technology

Fields Cryptography Retrospective Meeting
12 May 2009

Joint work with Daniel J. Bernstein, Tanja Lange and Christiane Peters

Paper available at http://eprint.iacr.org/2008/016

Outline

1. What is ECM and how does it work?
2. Edwards (and twisted Edwards) curves.
3. How can Edwards curves make ECM faster?

Lenstra's Elliptic Curve Factorisation Method (ECM)

Problem: Find a factor of the composite integer N.

- Let p be a prime factor of N.
- Choose an elliptic curve E over $\mathbb{Q}$ (but reduce $\bmod N$).
- Set $R := \mathrm{lcm}(1, \ldots, B)$ for some smoothness bound B.
- Pick a random point P on E (over $\mathbb{Z}/N\mathbb{Z}$) and compute $Q = [R]P$. In projective coordinates: $Q = (X : Y : Z)$.
- If the order ℓ of P modulo p is B-powersmooth then $\ell \mid R$ and hence Q modulo p is the neutral element $(0 : 1 : 0)$ of E modulo p.

  Thus, the X and Z-coordinates of Q are multiples of p.

  $\Rightarrow$ $\gcd(X, N)$ and $\gcd(Z, N)$ are divisors of N.

Remarks

- Big advantage: We can vary the curve, which increases the chance of finding at least one curve such that P has smooth order modulo p.
- When computing $Q = [R]P$ in affine coordinates, the inversion in $\mathbb{Z}/N\mathbb{Z}$ can fail since $\mathbb{Z}/N\mathbb{Z}$ is not a field. In this case the $\gcd$ of N and the element to be inverted is $\neq 1$.

  $\rightarrow$ Hence we have already found a divisor of N.
- Normally one uses Montgomery curves for ECM. We replace them with Edwards curves since the arithmetic is faster.

Suitable Elliptic Curves for ECM

- For ECM we use elliptic curves over $\mathbb{Q}$ (rank > 0) which have a prescribed torsion subgroup. When reducing those modulo p, we know already some divisors of the group order.

- **Theorem.** Let $E/\mathbb{Q}$ be an elliptic curve and let m be a positive integer such that $\gcd(m, p) = 1$. If E modulo p is non-singular the reduction modulo p

$$E(\mathbb{Q})[m] \to E(\mathbb{F}_p)$$

is injective.

$\Rightarrow$ The order of the m-torsion subgroup divides $\#E(\mathbb{F}_p)$.

In particular this increases the smoothness chance of the group order of $E(\mathbb{F}_p)$.

The Atkin and Morain Construction (1)

- Atkin and Morain give a construction method for elliptic curves over $\mathbb{Q}$ with rank > 0 and torsion subgroup isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$ and a point with infinite order.
- **Advantage:** Infinite family of curves with large torsion and rank 1.
- **Disadvantage:** Large height of the points and parameters slow down the scalar multiplication.

The Atkin and Morain Construction (2)

Example

The curve $E : y^2 = x^3 + 212335199041/4662158400x^2 - 202614718501/22106401080x + 187819091161/419284740484$ has torsion subgroup $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$ and rank 1.

This curve has good reduction at $p = 641$. The group of points on E modulo p is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/336\mathbb{Z}$ and 16 divides $\#E(\mathbb{F}_{641})$ according to the theorem.

Impact of the Size of the Torsion Subgroup

Torsion	Success prob.	
1	0.000862065	25%
6	0.00343531	100%
12	0.00388299	113%
16	0.00393693	115%

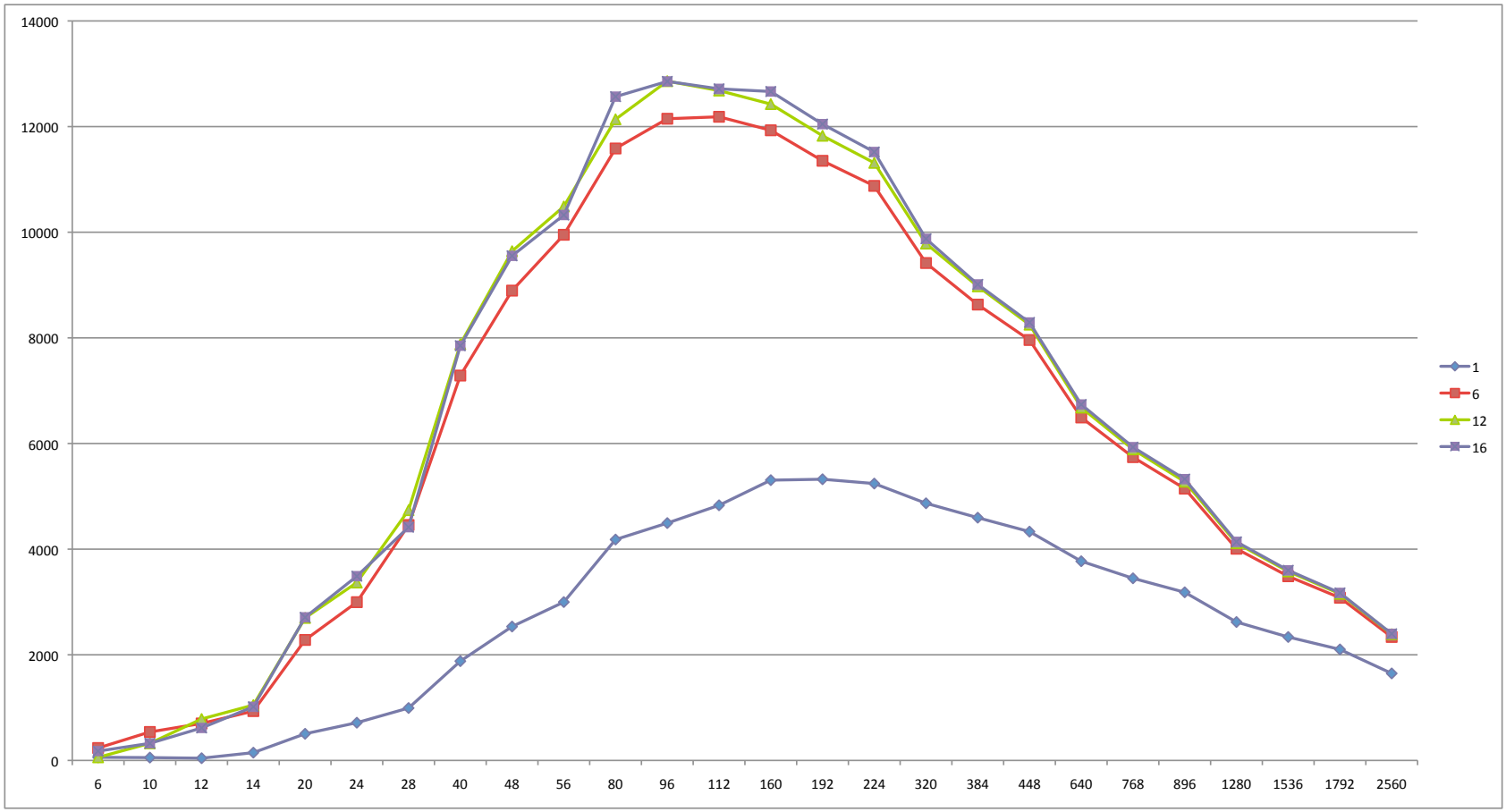
Range: $[2^{27}, 2^{28}]$
$B_1 = B_2 = 64$

Torsion	Success prob.	
1	0.078711	42%
6	0.188585	100%
12	0.197852	105%
16	0.201682	107%

Range: $[2^{19}, 2^{20}]$
$B_1 = B_2 = 128$

- A larger torsion subgroup increases the probability of finding a point of smooth order on the curve modulo p.

Optimal Choice of Smoothness Bound B_1

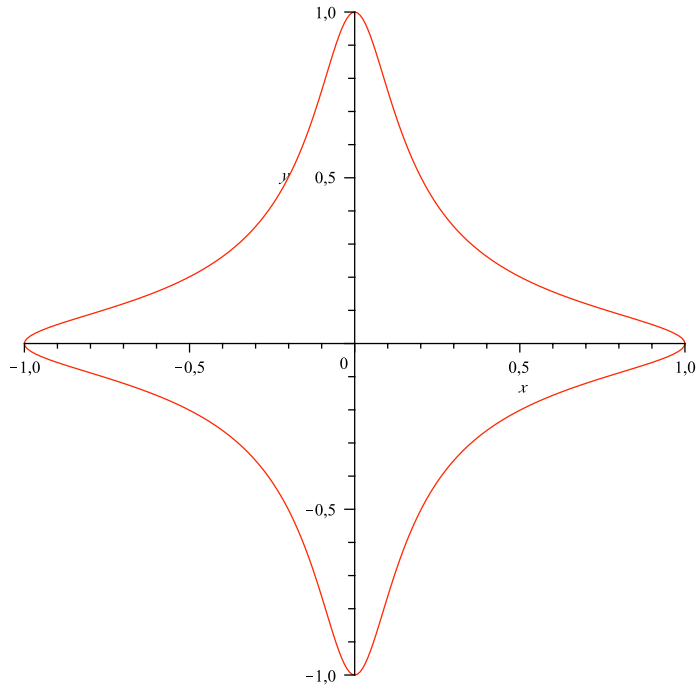


"Normalised" success probability of ECM (20-bit primes) for different values of B_1 and curves with 1, 6, 12 and 16-torsion.

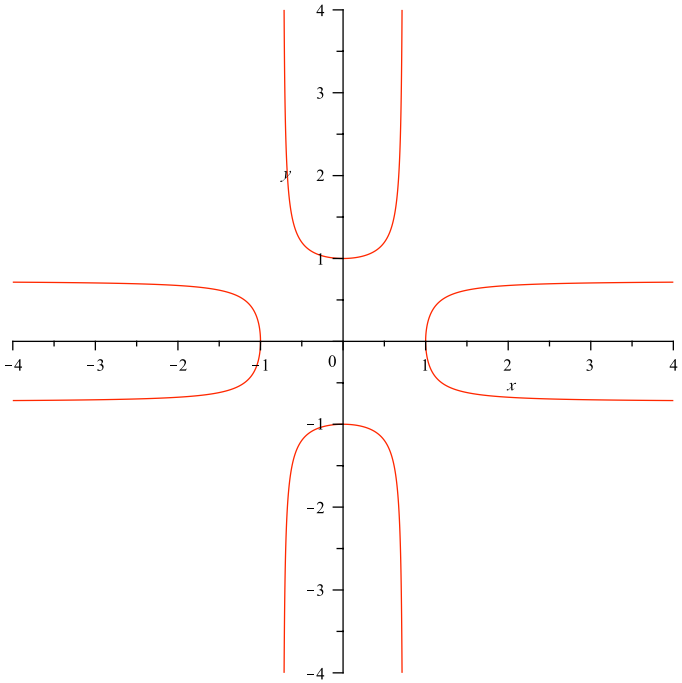
2. Edwards and Twisted Edwards Curves

What is an Edwards Curve?

- Let k be a field with $2 \neq 0$ and $d \in k \setminus \{0, 1\}$.
- An Edwards curve over k is a curve with equation $x^2 + y^2 = 1 + dx^2y^2$.



$d = -70$



$d = 1.9$

Addition Law on Edwards Curves

Addition on the curve $x^2 + y^2 = 1 + dx^2y^2$

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

Doubling formula (addition with $x_1 = x_2$ and $y_1 = y_2$)

$$[2](x_1, y_1) = \left(\frac{2x_1y_1}{1 + dx_1^2y_1^2}, \frac{y_1^2 - x_1^2}{1 - dx_1^2y_1^2} \right)$$

- The neutral element is $(0, 1)$.
- The negative of a point (x, y) is $(-x, y)$.

Twisted Edwards Curves

- Points of order 4 restrict the number of elliptic curves in Edwards form over k.
- Define a twisted Edwards curve by the equation

$$ax^2 + y^2 = 1 + dx^2y^2,$$

  where $a, d \neq 0$ and $a \neq d$.
- Twisted Edwards curves are birationally equivalent to elliptic curves in Montgomery form.
- Every Edwards curve is a twisted Edwards curve ($a = 1$).

Why the Name “twisted”?

- The Edwards curve $E_1 : \bar{x}^2 + \bar{y}^2 = 1 + (d/a)\bar{x}^2\bar{y}^2$

  is isomorphic to the

  Twisted Edwards curve $E_2 : ax^2 + y^2 = 1 + dx^2y^2$

  if a is a square in k $(x = \bar{x}/\sqrt{a}$ and $y = \bar{y})$.

- **In general:** E_1 and E_2 are quadratic twists of each other, i.e. isomorphic over a quadratic extension of k.

3. How can Edwards curves make ECM faster?

ECM using Edwards Curves

- **Theorem of Mazur.** Let $E/\mathbb{Q}$ be an elliptic curve. Then the torsion subgroup $E_{\text{tors}}(\mathbb{Q})$ of E is isomorphic to one of the following fifteen groups:

$$\mathbb{Z}/n\mathbb{Z} \text{ for } n = 1,2,3,4,5,6,7,8,9,10 \text{ or } 12$$

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z} \text{ for } n = 1,2,3,4.$$

- All Edwards curves have two points of order 4.
- For ECM we are interested in large torsion subgroups. By Mazur's theorem the largest choices are $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$, $\mathbb{Z}/12\mathbb{Z}$, and $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$.
- An Edwards curve over $\mathbb{Q}$ with torsion subgroup $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ is not possible. (Also no twisted Edwards curve! See Paper for details.)

Edwards Curves with Torsion Part $\mathbb{Z}/12\mathbb{Z}$

How can we find Edwards curves with prescribed torsion part?

- All Edwards curves have 2 points of order 4, namely $P_4 = (1,0)$ and $P_4' = (-1,0)$.
- We construct a point P_3 of order 3 and obtain a curve with torsion part isomorphic to $\mathbb{Z}/12\mathbb{Z}$ generated by the point $P_{12} = P_3 + P_4$ of order 12.
- We can also ensure that the rank is greater than 0 and determine a point in the non-torsion part which has small height.

Edwards Curves with a Point of Order 3

- Tripling formulas derived from addition law:

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

- For a point P_3 of order 3 we have $[3]P=(0,1)$. (Note, that for a point of order 6 we have $[3]P=(0,-1)$.)

- Thus, the condition is: $\frac{((x_1^2+y_1^2)^2-(2x_1)^2)}{-4(y_1^2-1)y_1^2+(x_1^2-y_1^2)^2}y_1=\pm 1$

- **Theorem.** If $u\in\mathbb{Q}\setminus\{0,\pm 1\}$ and

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

then (x_3,y_3) is a point of order 3 on the Edwards curve given by $x^2+y^2=1+dx^2y^2$.

Edwards Curves with Torsion Part $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$

- If d is a rational square, then we have 2 more points of order 2 on the Edwards curve. If we additionally enforce that the curve has a point of order 8, the torsion group is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$ (due to Mazur).

- We always have 2 points of order 4, namely $(\pm 1, 0)$. For a point P_8 of order 8 we need $[2]P_8 = (\pm 1, 0)$.

  $\rightarrow$ Solve this equation using the doubling formulas.

- We get a parametrisation for this solution: If $u \neq 0, -1, -2$, then $x_8 = (u^2 + 2u + 2)/(u^2 - 2)$ gives $P_8 = (x_8, x_8)$, which has order 8 on the curve given by $d = (2x_8^2 - 1)/x_8^4$.

How to Find Curves with Rank 1?

- Until now we have constructed Edwards curves over $\mathbb{Q}$ with torsion subgroup $\mathbb{Z}/12\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$.
- Which of them have rank > 0?
- For both cases we have a parametrisation: A rational number u gives a curve with the desired torsion subgroup.
- To find a curve with rank 1, put $u = a/b$ and do a exhaustive search for solutions (a, b, e, f), where (e, f) is a point on the curve but different from all torsion points, i.e. different from $\{(0, \pm 1), (\pm 1, 0)\}$ etc. Points of order 8 can be excluded by checking for $e = f$.

  Then the point (e, f) has infinite order over $\mathbb{Q}$.

Summary

Until now we already have

- 100 curves with small parameters and torsion subgroup $\mathbb{Z}/12\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$.
- Complete translation of the Atkin-Morain method to Edwards curves.
- Complete translation of the Suyama construction.
- First experiments showed a speed-up of about 7% + 15%.
- See Cryptology ePrint Archive Report 2008/016 for details.

Thank you for your attention!