Edwards Curves and the ECM Factorisation Method

Peter Birkner

Eindhoven University of Technology

The 12th Workshop on Elliptic Curve Cryptography
22 September 2008

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

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

Outline

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

Pollard's p-1 Method (1)

Problem: Find a prime factor p of the composite integer N.

- **Fermat's little theorem:** $a^{p-1} \equiv 1 \bmod p$, if p prime and a coprime to p.
- We pick a random element $a \in \{2, \ldots, N-1\}$ and fix a smoothness bound B.
- We hope for $p-1$ (or the order of $a \bmod p$) to be B-powersmooth, i.e. all prime powers $\leq B$.
- Set $R := \mathrm{lcm}(1, \ldots, B)$.
- $\mathrm{ord}(a) \bmod p$ is B-powersmooth $\Rightarrow$ R is a multiple of $\mathrm{ord}(a)$. Thus $a^R \equiv a^{k \cdot \mathrm{ord}(a)} \equiv 1 \bmod p \Rightarrow p \,|\, a^R - 1$.

Result: $\gcd(a^R - 1, N)$ is a factor of N.

Pollard's p-1 Method (2)

This method can fail for two reasons:

1. N does not have a prime divisor p and an element a such that $\mathrm{ord}(a) \bmod p$ is B-powersmooth, i.e. $\gcd(a^R - 1, N) = 1$.

   $\rightarrow$ Increase smoothness bound B.

   $\rightarrow$ Or pick a new a.

2. All prime divisors of N are found simultaneously, i.e. $\gcd(a^R - 1, N) = N$.

   $\rightarrow$ Pick another $1 < a < N$ and try again.

   $\rightarrow$ Ensure that $\mathrm{ord}(a)$ is **not** B-powersmooth modulo all primefactors of N at the same time. Decrease smoothness bound B.

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 over Pollard p-1: We can vary the curve, which increases the chance of finding at least one curve such that P has smooth order modulo p.

  Using Pollard p-1 we are restricted to $\mathbb{Z}/p\mathbb{Z}$.

- 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 (1)

- 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 $E(\mathbb{F}_p)$.

Suitable Elliptic Curves for ECM (2)

Summary

- We want curves with large torsion group over $\mathbb{Q}$.
- We need a generator P of the non-torsion part. Then we can reduce $Q = [R]P$ modulo N for many different values of N (smoothness bound fixed).
- For efficient computation of $Q = [R]P$ we like to have cheap additions. Hence P should have small height.

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

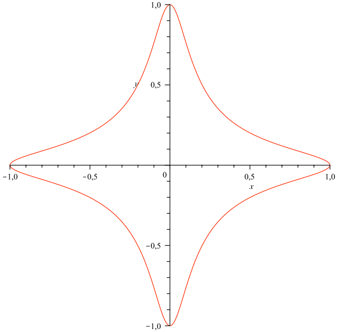
The curve $E : y^2 = x^3 + 212335199041/4662158400x^2 - 202614718501/22106401080x + 187819091161/419284740484$ has torsion subgroup $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$ and rank 1.

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.

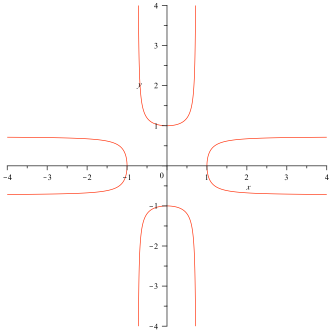
2. Edwards Curves

What is an Edwards curve? (1)

- 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 $x^2 + y^2 = 1 + dx^2y^2$.



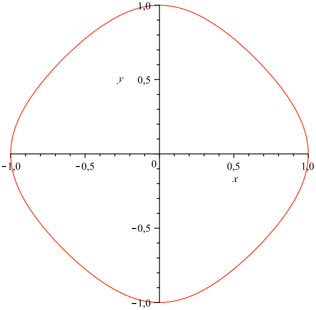
$d = -70$



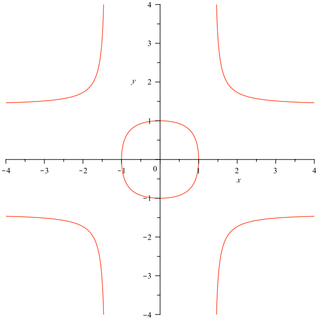
$d = 1.9$

What is an Edwards curve? (2)

- In 2007, Harold M. Edwards introduced a new normal form for elliptic curves.
- Lange and Bernstein slightly generalised this form for use in cryptography, and provided explicit addition and doubling formulas (see Asiacrypt 2007).



$d = -1$



$d = 1/2$

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 $y_1 = y_2$)

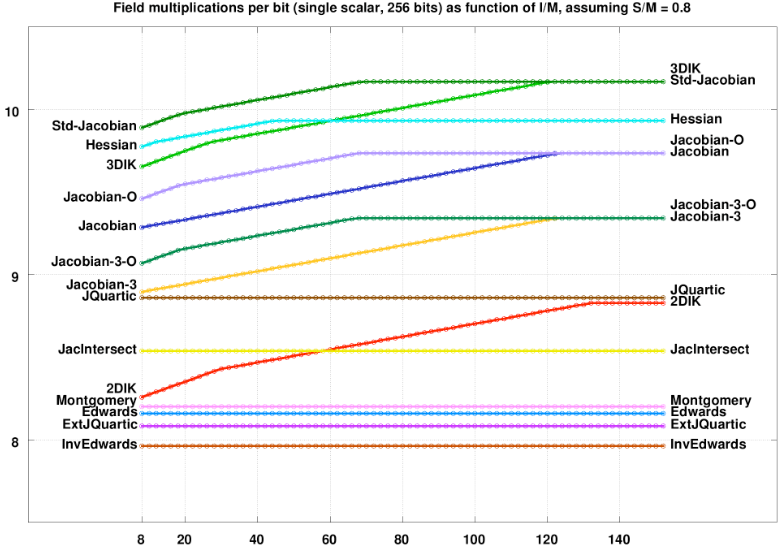
$$[2](x_1, y_1) = \left(\frac{2x_1y_1}{1 + dx_1^2y_1^2}, \frac{y_1^2 - x_1^2}{1 - dx_1^2y_1^2} \right)$$

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

The Edwards Addition Law is Complete

- For d not a square in k, the Edwards addition law is complete, i.e. there are no exceptional cases
- Edwards addition law allows omitting all checks
  - Neutral element is affine point on the curve
  - Addition works to add P and P
  - Addition works to add P and $-P$
  - Addition just works to add P and any Q
- Only complete addition law in the literature

Edwards Curves are Fast!



3. How can Edwards curves make ECM faster?

ECM using Edwards Curves (1)

- We can construct Edwards curves over $\mathbb{Q}$ (rank > 0) with prescribed torsion-part and small parameters, and find a point in the non-torsion subgroup.
- To compute $[R]P$ for ECM we use inverted Edwards coordinates which offer very fast scalar multiplication.
- The point in the non-torsion part has small height. This means that all additions in the scalar multiplication are additions with a small point.
- **Example:** $N = (5^{367} + 1)/(2 \cdot 3 \cdot 73219364069)$
  GMP-ECM: 210299 mults. modulo N in 2448 ms.
  GMP-EECM: 195111 mults. modulo N in 2276 ms.
  $\rightarrow$ Speed-up of 7% in first experiments.

ECM using Edwards Curves (2)

- **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 $\mathbb{Q}$.

Advantages of GMP-EECM over GMP-ECM (1)

- We choose curves with large torsion subgroups (12 or 16 points) and therefore large guaranteed divisors of the order of $\#E$ modulo p. GMP-ECM uses Suyama curves which have a rational torsion group of order 6.
- We choose curves with parameters and non-torsion points of small height (smaller than Atkin-Morain) and our implementation takes this into account by working with projective base points and projective parameters. The GMP-ECM implementation does not make use of small height elements and instead computes every fraction a/b modulo p which means that the numbers get big.

Advantages of GMP-EECM over GMP-ECM (2)

- In inverted Edwards coordinates the cost of a scalar multiplication is $1DBL + \varepsilon ADD$ per bit, where $\varepsilon \to 0$ when the scalar gets large, i.e. asymptotically $3M + 4S + 1D$.

  GMP-ECM uses Montgomery curves. The Montgomery ladder needs $5M + 4S + 1D$ per bit; GMP-ECM uses the PRAC algorithm instead of the latter. It needs an average of $9M$ per bit.

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 %.
- (See Cryptology ePrint Archive Report 2008/016 for details.)

Thank you for your attention!