JKL-ECM : An Implementation of ECM using Hessian Curves

Henriette Heer, Gary McGuire and Oisín Robinson

ANTS XII

Kaiserslautern

August 2016

Overview

- Elliptic Curve Method (Sketch)
- Torsion Speedup
- The Jeon-Kim-Lee Families
- Edwards/Hessian Curves
- Small Parameters/Hessian Speedup
- Worst-Case Torsion Injection
- Classification
- Implementation/Results
- Conclusion

Elliptic Curve Method (Sketch)

- Say we want to factor $N = p \cdot c$, with p prime, $c > 1$ cofactor.
- Suppose we have an elliptic curve E in Weierstrass form.
- Suppose also that $\#E(\mathbb{F}_p)$ is B-smooth.
- Compute $[B!]P \equiv (X : Y : Z) \ (mod\ N)$, for $P \in E(\mathbb{Z}/N\mathbb{Z})$.
- Then, we can usually recover $p = \gcd(X, N)$.

Torsion Speedup

Theorem ("Torsion Injection")

For an elliptic curve E over a number field K, with torsion subgroup $E(K)_{tors}$, with good reduction mod p, there exists an injective map

$$\tau : E(K)_{tors} \mapsto E(\mathbb{F}_p).$$

In particular, $\#E(K)_{tors} | \#E(\mathbb{F}_p)$*.*

Torsion for Elliptic Curves over $\mathbb{Q}$

Theorem (Mazur's Torsion Theorem, 1977)

For an elliptic curve E over $\mathbb{Q}$, $E(\mathbb{Q})_{tors}$ is isomorphic to one of the following 15 groups:

$$\begin{array}{ll} \mathbb{Z}/m\mathbb{Z} & \textit{for} \;\; 1 \le m \le 12, m \ne 11, \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2m\mathbb{Z} & \textit{for} \;\; 1 \le m \le 4. \end{array}$$

Torsion for Elliptic Curves over $\mathbb{Q}(\sqrt{d})$

Theorem (Kamienny, Kenku, Momose, 1988)

For an elliptic curve E over K, where K is a quadratic number field, $E(K)_{tors}$ is isomorphic to one of the following 26 groups:

$$\begin{array}{ll} \mathbb{Z}/m\mathbb{Z} & \textit{for} \;\; 1 \le m \le 18, m \ne 17, \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2m\mathbb{Z} & \textit{for} \;\; 1 \le m \le 6, \\ \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3m\mathbb{Z} & \textit{for} \;\; m \in \{1, 2\}, \\ \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}. & \end{array}$$

Torsion for Elliptic Curves over K

- For higher degree number fields, fully classifying torsion is an open question.
- Partial results are known in some cases
- For example, for quartic number fields, Jeon, Kim and Lee gave infinite families of elliptic curves with $E(K)_{tors} \cong \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$ or $E(K)_{tors} \cong \mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$
- We use both of these families to improve ECM.

The Jeon-Kim-Lee Families

Theorem (Jeon,Kim,Lee, 2011)

Let $K = \mathbb{Q}(\sqrt{-1}, \sqrt{t^4 - 6t^2 + 1})$, *with* $t \in \mathbb{Q}$ *and* $t \neq 0, \pm 1$, *and let* E *be an elliptic curve defined by the equation*

$$E : y^2 + xy - \left(\nu^2 - \frac{1}{16}\right) y = x^3 - \left(\nu^2 - \frac{1}{16}\right) x^2$$

where

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

Then the torsion subgroup of E *over* K *is equal to* $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$ *for almost all* t.

The Jeon-Kim-Lee Families

Theorem (Jeon,Kim,Lee, 2011)

Let $K = \mathbb{Q}(\sqrt{-3}, \sqrt{8t^4+1})$*, with* $t \in \mathbb{Q}$ *and* $t \neq 0, 1, -\frac{1}{2}$*, and let* E *be an elliptic curve defined by the equation*

$$E : y^2 = x^3 - 27\mu(\mu^3 + 8)x + 54(\mu^6 - 20\mu^3 - 8)$$

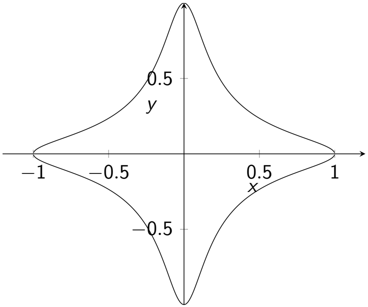
where

$$\mu = \frac{2t^3 + 1}{3t^2}.$$

Then the torsion subgroup of E *over* K *is equal to* $\mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$ *for almost all* t*.*

Edwards Curves

- Any elliptic curve with a point of order 4 over a field K with $2 \neq 0$ can be represented in 'Edwards form' (for $d \in K \setminus \{0, 1\}$)
$$x^2 + y^2 = 1 + dx^2y^2$$



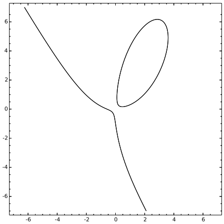
- The curves in the JKL $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$ family have a point of order 4. Therefore they can be represented in Edwards form.

Hessian Curves

- Any elliptic curve with a point of order 3 over a field K can be represented in 'twisted Hessian form'

$$ax^3 + y^3 + 1 = dxy$$

over $\overline{K}$, for $a, d \in K$ with $a(27a - d^3) \neq 0$.



- The curves in the JKL $\mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$ family have a natural representation in Hessian form

$$X^3 + Y^3 + Z^3 = 3\mu XYZ.$$

- Easy to twist this.

Small Parameters

- Suppose $P = (X : Y : Z) \in E(\mathbb{P}^2)$ such that X, Y, Z are small.
- The double-and-add operation will then be faster, since additions re-use P. This speeds up ECM - see ECM using Edwards Curves (2010).
- How do we find such curves?
- Bernstein et al carried out an exhaustive search.
- Since then, the JKL families were described (2011).
- We generated 100s of $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$ curves and 1000s of $\mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$ curves with positive rank using SAGE.
- The curves have small parameters, and base points with small X, Y, Z.

Hessian Speedup?

- Bernstein et al created EECM-MPFQ which uses Edwards curves.
- For its range of application it has unbeaten performance.
- It uses a combination of projective doubling and extended addition.
- Double + add cost (3M + 4S + 1a) + (9M + 1a).

- Hessian projective doubling costs (7M + 1S + 1d).
- Hessian projective addition costs (12M + 1a).
- But base point has small coordinates, so more like (6M + 6m + 1a).
- Double + add cost (7M + 1S + 1d) + (6M + 6m + 1a).

Hessian Curves for ECM

- So Hessian curves are also well-suited to ECM.
- Some questions arise involving the JKL families.
- Strictly, we only get full torsion injection if both quadratic irrationalities of the relevant number field exist in the finite field of interest.

Least Torsion Injection

Theorem (Case $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$, Heer-McGuire-R, 2016)
Over $\mathbb{Q}$, the JKL curve E_ν has torsion subgroup $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$.

- Recall for the E_ν curves the quartic number field is $K = \mathbb{Q}(\sqrt{-1}, \sqrt{t^4 - 6t^2 + 1})$.

Theorem (Case $\mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$, Heer-McGuire-R, 2016)
Over $\mathbb{Q}$, the JKL curve E_μ has torsion subgroup $\mathbb{Z}/6\mathbb{Z}$.

- Recall for the E_μ curves the quartic number field is $K = \mathbb{Q}(\sqrt{-3}, \sqrt{8t^4 + 1})$.

Least Torsion Injection

Theorem (E_μ, $\mathbb{Q}(\sqrt{-3})$, Heer-McGuire-R, 2016)
Consider the JKL curve E_μ over the quadratic number field $L = \mathbb{Q}(\sqrt{-3})$. Then

$$E_\mu(L)_{tors} = \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}.$$

- In particular, this is better than any torsion possible over $\mathbb{Q}$.

Theorem (E_μ, $\mathbb{Q}(\sqrt{8t^3+1})$, Heer-McGuire-R, 2016)
The torsion subgroup of the JKL curve E_μ over the quadratic number field $L = \mathbb{Q}(\sqrt{8t^3+1})$ is

$$E_\mu(L)_{tors} = \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}.$$

Classification

- We might wonder if there exists a family of Hessian Curves with torsion $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$ over $\mathbb{Q}$.
- However, we have

Theorem (Classification of Hessian Curves over $\mathbb{Q}$, Heer-McGuire-R, 2016)

If H is a Hessian curve, then

$$H(\mathbb{Q})_{tors} = \begin{cases} \mathbb{Z}/6\mathbb{Z}, & H = E_\mu \text{ for } E_\mu \text{ a JKL curve} \\ \mathbb{Z}/3\mathbb{Z}, & \text{else.} \end{cases}$$

Implementation

- EECM-MPFQ uses MPFQ to handle large integer arithmetic.
- MPFQ can work with integers up to 9 words of 64 bits, or about 174 digits
- In this range, EECM-MPFQ outperforms the competition.
- GMP-ECM uses Gnu-MP to handle large integer arithmetic.
- It handles integers of arbitrary size.
- JKL-ECM is also based on Gnu-MP, and handles integers of arbitrary size.
- However we did not use assembly/intrinsics etc.
- Thus, we do not outperform GMP-ECM in terms of speed.
- (Although it is close, and the gap narrows with larger inputs).

Implementation

- To have any chance of competing with GMP-ECM, we had to implement stage 2.
- We implemented stage 2 using the FFT continuation
- We programmed this using Kronecker Substitution for polynomial arithmetic.
- Also, we used Bernstein's 'scaled remainder tree' for multipoint evaluation.
- This was done from first principles.
- (Note: We rely on Gnu-MP's fast integer multiplication in the FFT range).

Results

- We tested our implementation on Fionn, a cluster at ICHEC.
- At the time of writing, the largest factor found was a 57 digit factor of $5^{228} + 3 \cdot 197^{110}$. If $n = x^2 + 3y^2$ then $\forall p | n, \sqrt{-3} \in \mathbb{F}_p$.
- The stage 1 bound used was 110e6.
- The effective stage 2 bound used was about 1150e9.
- Since then, we found a 60 digit factor of $271^{128} + 3 \cdot 132^{50}$.
- For this, we used a stage 1 bound of 400e6.
- Curiously, we managed this despite having only 4,840 twisted Hessian curves to work with.
- The recommended number of curves for $t55$ is 17,884 and for $t60$ is 42,057.
- Curve effectiveness thus appears to play a part.

Results

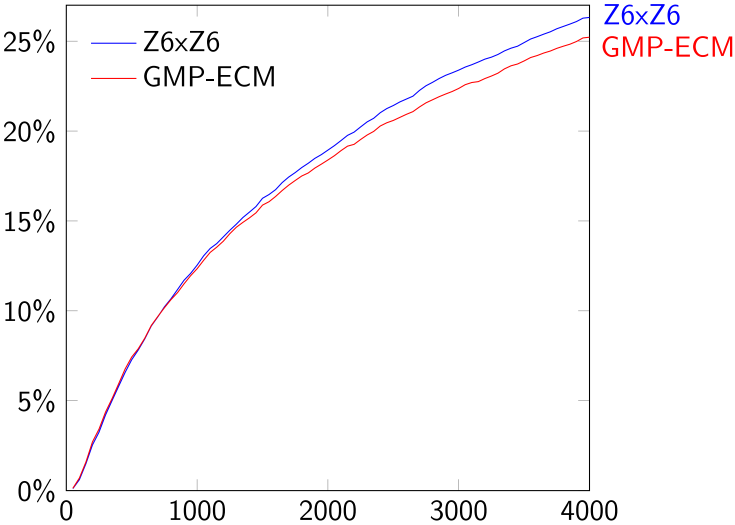


Figure: Stage 1 success probability for a sample of 65536 30-bit primes $\equiv 1 \bmod 3$

Results

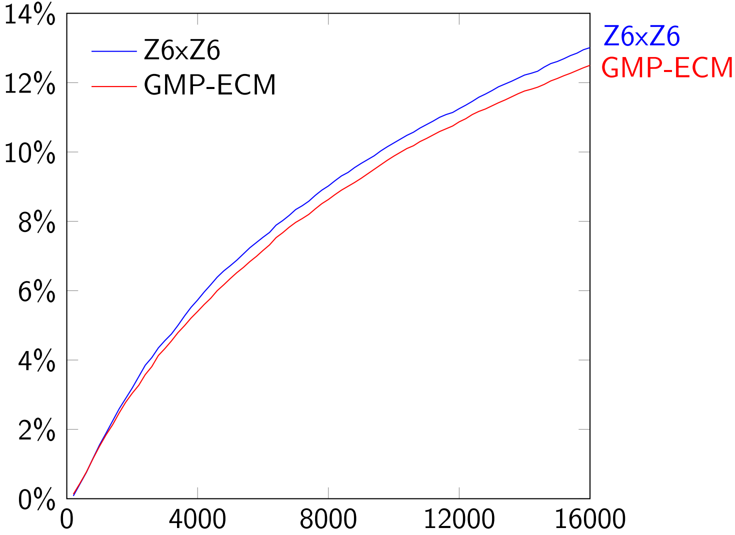


Figure: Stage 1 success probability for a sample of 65536 40-bit primes $\equiv 1 \bmod 3$

Conclusion

- We have presented JKL-ECM, a new implementation of ECM.
- It uses twisted Hessian curves from the JKL $\mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$ family.
- It also has the option of using up to 700 curves from the JKL $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$ family.
- We have also answered some theoretical questions that arise regarding Hessian curves.
- This includes a classification of Hessian curves over $\mathbb{Q}$.
- We will make JKL-ECM available for download.