ECM using Edwards curves

Tanja Lange

Department of Mathematics and Computer Science

Technische Universiteit Eindhoven

tanja@hyperelliptic.org

26.09.2009

joint work with Daniel J. Bernstein (UIC), Peter Birkner (TU/e),

and Christiane Peters (TU/e)

The $p-1$ factorization method I

$2^{232792560} - 1$ has prime divisors:

$3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 53, 61, 67, 71, 73, 79, 89, 97, 103, 109, 113, 127, 131, 137, 151, 157, 181, 191, 199,$ etc.

These divisors include

- 70 of the 168 primes $\le 10^3$;
- 156 of the 1229 primes $\le 10^4$;
- 296 of the 9592 primes $\le 10^5$;
- 470 of the 78498 primes $\le 10^6$;
- etc.

The $p-1$ factorization method II

- An odd prime p divides $2^{232792560}-1$ iff order of 2 in $\mathbb{F}_p^*$ divides 232792560.
- Many ways for this to happen: 232792560 has 960 divisors.
- Why so many?

The $p-1$ factorization method II

- An odd prime p divides $2^{232792560}-1$ iff order of 2 in $\mathbb{F}_p^*$ divides 232792560.
- Many ways for this to happen: 232792560 has 960 divisors.
- Why so many?
$232792560 = \text{lcm}(1,2,3,4,5,\ldots,20) = 2^4 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19$.
- This can be used to find divisors of integers n: Compute

$$\gcd(2^{232792560}-1, n)$$

to obtain the product of all factors p_i of n s.t. the order of 2 modulo p_i divides 232792560.
- Computation requires modular exponentiation; use square-and-multiply method.

Example

- Put $n = 8597231219$:
  $2^{27} \bmod n = 134217728$;
  $2^{54} \bmod n = 134217728^2 \bmod n = 935663516$;
  $2^{55} \bmod n = 1871327032$;
  $2^{110} \bmod n = 1871327032^2 \bmod n = 1458876811$; . . . ;
  $2^{232792560} - 1 \bmod n = 5626089344$.
- Finally, $\gcd(5626089344, n) = 991$.
- Main work: 27 squarings mod n.
- Could instead have checked n's divisibility by $2, 3, 5, \ldots$. The 167th trial division would have found divisor 991.
- Not clear which method is better. Dividing by small p is faster than squaring mod n. The $p - 1$ method finds only 70 of the primes ≤ 1000; trial division finds all 168 primes . . . but also needs to store them. Asymptotically better.

Generalizations of $p-1$ method

- So numbers are easy to factor if their factors p_i have smooth $p_i - 1$.
- To construct hard to factor numbers avoid such factors – that's it?

Generalizations of $p - 1$ method

- So numbers are easy to factor if their factors p_i have smooth $p_i - 1$.
- To construct hard to factor numbers avoid such factors – that's it?
- Not quite. William's $p + 1$ method works, when $p_i + 1$ is smooth.
- OK, avoid those, too. Anything else?

Generalizations of $p-1$ method

- So numbers are easy to factor if their factors p_i have smooth $p_i - 1$.
- To construct hard to factor numbers avoid such factors – that's it?
- Not quite. William's $p+1$ method works, when $p_i + 1$ is smooth.
- OK, avoid those, too. Anything else?
- Lenstra's Elliptic Curve Method (ECM) finds p_i, when any number in $[p_i + 1 - 2\sqrt{p_i}, p_i + 1 + 2\sqrt{p_i}]$ is smooth.
- No chance of avoiding this, there are many smooth numbers in this interval ($\supseteq \{$Deuring, Lenstra, McKee$\}$).
- This interval is called the Hasse interval, the group order of an elliptic curve over $\mathbb{F}_{p_i}$ lies in this interval.

Overview of ECM

- Principle: Take a point P on an elliptic curve E over $\mathbb{Z}/n$ and compute $[s]P$ for some very smooth s.
- If the order of P on the curve modulo p_i divides s, the point $[s]P$ is the neutral element.
- Find a suitable $\gcd$ computation.
- Can vary P and s (corresponds to varying base 2 and the exponent in the $p-1$ method).
- E modulo p_i has order in $[p_i + 1 - 2\sqrt{p_i}, p_i + 1 + 2\sqrt{p_i}]$; this may or may not be smooth but we can vary E.
- Curve operations more expensive than in $p-1$ method – but can get much higher probabilities for large p_i.
- Can choose curves that are more likely to have smooth order by picking some with non trivial torsion over $\mathbb{Q}$.

ECM as part of NFS

- Factorization of "hard" numbers uses the Number Field Sieve (NFS) which builds a quadratic relation

$$a^2 \equiv b^2 \bmod n \Rightarrow \gcd(n, a - b) \neq 1$$

  using factorizations of auxiliary numbers (easy to factor).
- ECM is most important "general purpose" algorithm.
- Main computation: $[s]P$ for big s on curve modulo n.
- This can use a prime-by-prime strategy or work with a signed window expansion of the scalar.
- Can choose different representations of elliptic curves; choices influenced by efficiency of computation.
- Standard choice used to be Montgomery representation

$$y^2 = x^3 + Ax^2 + x.$$

Brief summary of Edwards curves

- Published by Edwards in 2007, suggested for cryptographic applications by Bernstein/L. in 2007.
- Curve equation over field k of characteristic 0 or p:

$$x^2 + y^2 = 1 + dx^2y^2,\ d \notin \{0, 1\}.$$

- Addition law
$(x_1, y_1) + (x_2, y_2) = \left(\frac{x_1y_2+y_1x_2}{1+dx_1x_2y_1y_2}, \frac{y_1y_2-x_1x_2}{1-dx_1x_2y_1y_2}\right).$
Neutral element is $(0, 1)$ and $-(x_1, y_1) = (-x_1, y_1)$.
- Singular points at infinity $\Omega_1 = (1 : 0 : 0), \Omega_2 = (0 : 1 : 0)$.
Singularities blow up over (minimally) $k(\sqrt{d})$ giving two points of order 2 over Ω_1 and two points of order 4 over Ω_2 (check by using birational equivalence with Weierstrass curves).

Relationship to elliptic curves

- Every elliptic curve with point of order 4 is birationally equivalent to an Edwards curve.
- Let $P_4 = (u_4, v_4)$ have order 4 and shift u s.t. $2P_4 = (0, 0)$. Then Weierstrass form:

$$v^2 = u^3 + (v_4^2/u_4^2 - 2u_4)u^2 + u_4^2 u.$$

- Define $d = 1 - (4u_4^3/v_4^2)$.
- The coordinates $x = v_4 u/(u_4 v),\ y = (u - u_4)/(u + u_4)$ satisfy

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

- Inverse map $u = u_4(1 + y)/(1 - y),\ v = v_4 u/(u_4 x)$.
- Finitely many exceptional points. Exceptional points have $v(u + u_4) = 0$.
- Addition on Edwards and Weierstrass corresponds.

Exceptional points of the map

- Points with $v(u + u_4) = 0$ on Weierstrass curve map to points at infinity on desingularization of Edwards curve.
- Reminder: $d = 1 - (4u_4^3/v_4^2)$.
- $u = -u_4$ is u-coordinate of a point iff

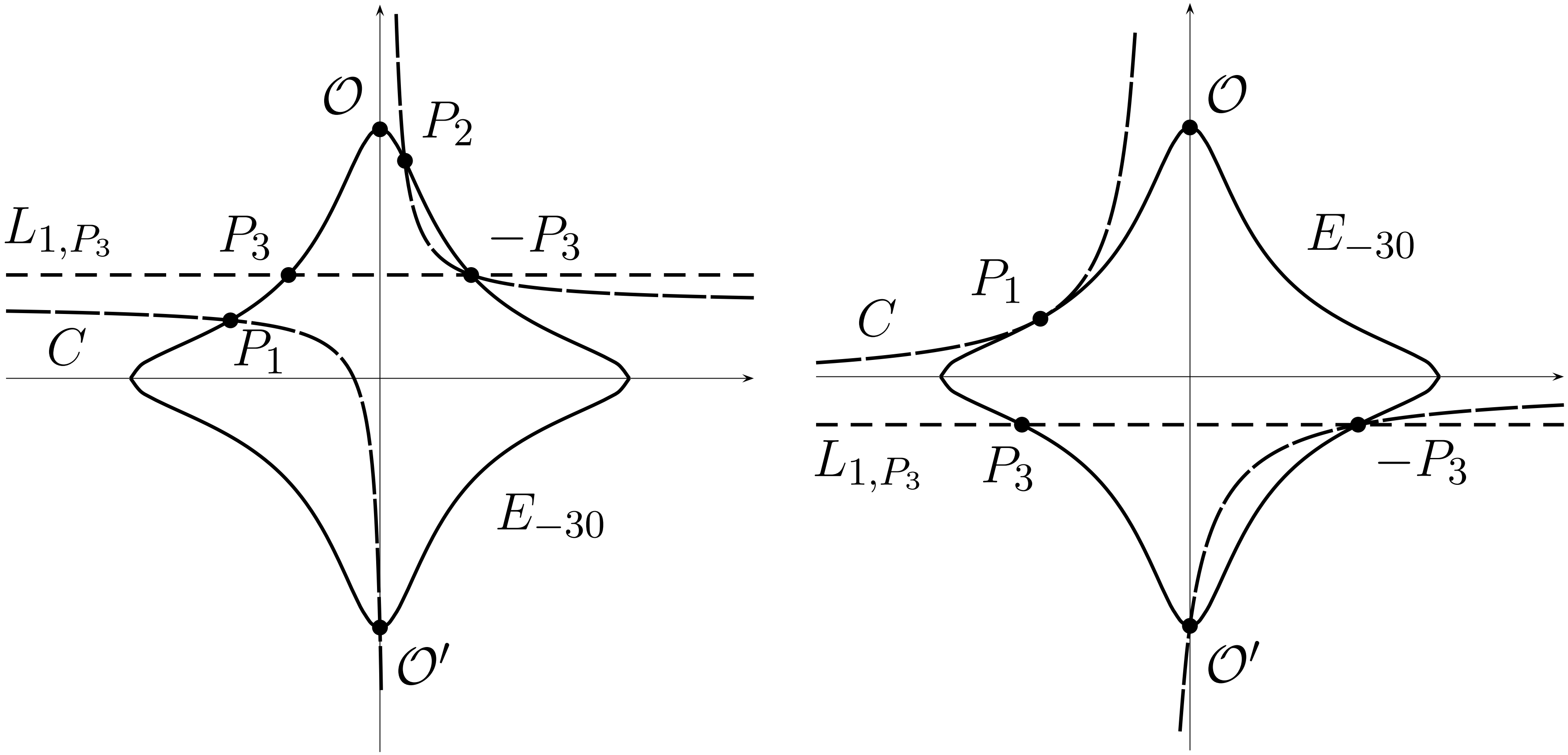
$$\begin{aligned} & (-u_4)^3 + (v_4^2/u_4^2 - 2u_4)(u_4)^2 + u_4^2(u_4) \\ = \ & v_4^2 - 4u_4^3 = v_4^2 d \end{aligned}$$

  is a square, i. e., iff d is a square.
- $v = 0$ corresponds to $(0, 0)$ which maps to $(0, -1)$ on Edwards curve and to solutions of $u^2 + (v_4^2/u_4^2 - 2u_4)u + u_4^2 = 0$. Discriminant is

$$(v_4^2/u_4^2 - 2u_4)^2 - 4u_4^2 = v_4^4 d,$$

  i. e., points defined over K iff d is a square.

Pictures



Addition and doubling over $\mathbb{R}$ for $d < 0$.

Twisted Edwards curves

- Curve equation over field k of characteristic 0 or p:

$$ax^2 + y^2 = 1 + dx^2y^2, \; a, d \neq 0, a \neq d.$$

- Points at infinity:
  - $a = e^2, d = \square$: $(\pm e, 0)$ have order 4, two points of order 2 over Ω_1 and two points of order 4 over Ω_2; subgroup isomorphic to $\mathbb{Z}/2 \times \mathbb{Z}/4$.
  - $a = e^2, d \neq \square$: $(\pm e, 0)$ have order 4, blow-ups of Ω_1, Ω_2 are defined over quadratic extension field, no k-rational points at infinity; subgroup isom. to $\mathbb{Z}/4$.
  - $a \neq \square, d = \square$: two points of order 2 over Ω_1, none over Ω_2; subgroup isom. to $\mathbb{Z}/2 \times \mathbb{Z}/2$.
  - $a \neq \square, d \neq \square, a \cdot d = \square$: two points of order 4 over Ω_2, none over Ω_1; subgroup isom. to $\mathbb{Z}/4$.

Efficient arithmetic on Edwards curves

- "Faster group operations on elliptic curves" by Hisil, Wong, Carter Dawson, mADD = 9M, no multiplication by curve constants.

  $$(x_1, y_1) + (x_2, y_2) = \left(\frac{x_1 y_1 + x_2 y_2}{x_1 x_2 + y_1 y_2}, \frac{x_1 y_1 - x_2 y_2}{x_1 y_2 - y_1 x_2} \right).$$

  These addition formulas are not unified; this is no problem for ECM where one searches for "failures" to the addition law.

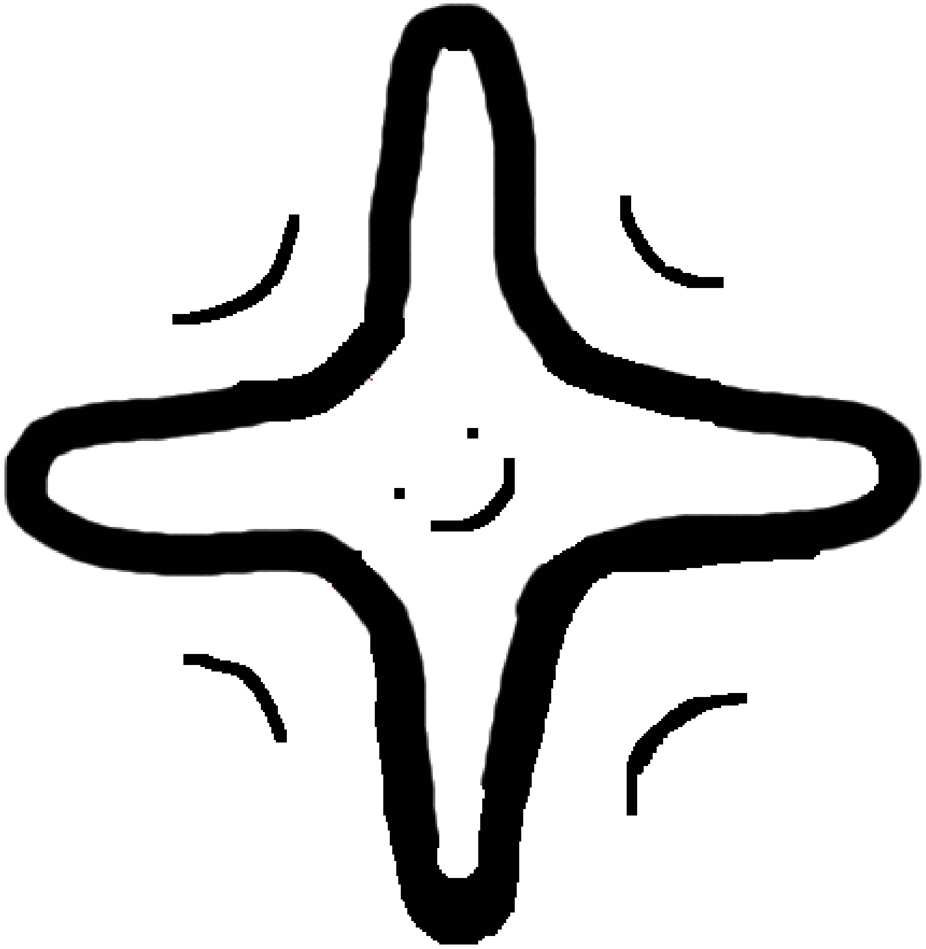
- "Twisted Edwards Curves Revisited" by Hisil, Wong, Carter Dawson, introducing extended Edwards coordinates $(X : Y : Z : T)$ with $T = XY/Z$. Gives ADD=9M (+1D with a for twisted) in general.

Extended Edwards coordinates

- For twisted with $a = -1$ even ADD=8M. Mixed versions save 1M: mADD=7M.
- Doubling is faster: 3M+4S. Per bit of s one doubling is needed.
- Can use signed sliding window method; asymptotically decreases frequency of additions to 0.
- Extended representation is not good for doubling. should be used only for addition; so do main doublings as $2\mathcal{E} \to \mathcal{E}$, last doubling as $2\mathcal{E} \to \mathcal{E}^e$, and $\mathcal{E}^e + \mathcal{E}^e \to \mathcal{E}$ in the scalar multiplication in stage 1. Stage 2 has mostly additions anyway.
- Complete overview of curve shapes, coordinates, addition formulas including faster differential addition than Montgomery at `www.hyperelliptic.org/EFD`.

Design Choices

- Use Edwards curves!



Design Choices

- Use Edwards curves!
- Field arithmetic might make multiplications by small integers faster; this does not generally work in Montgomery representation of integers.
- There are several multiplications by the coordinates of the base point; there are some multiplications by a and in inverted Edwards coordinates by d.
- Can pick small height base point (x_1, y_1), some a and compute d as $d = (ax_1^2 + y_1^2 - 1)/(x_1^2 y_1^2)$. The resulting d has small height, too. Good choices for a are 1 (Edwards) and -1 (particularly fast extended addition).
- Make sure not to choose $(x_1, y_1) \in \{(\pm 1, 0), (0, \pm 1), (\pm c, \pm c)\}$ for any c since these definitely have small order over $\mathbb{Q}$.

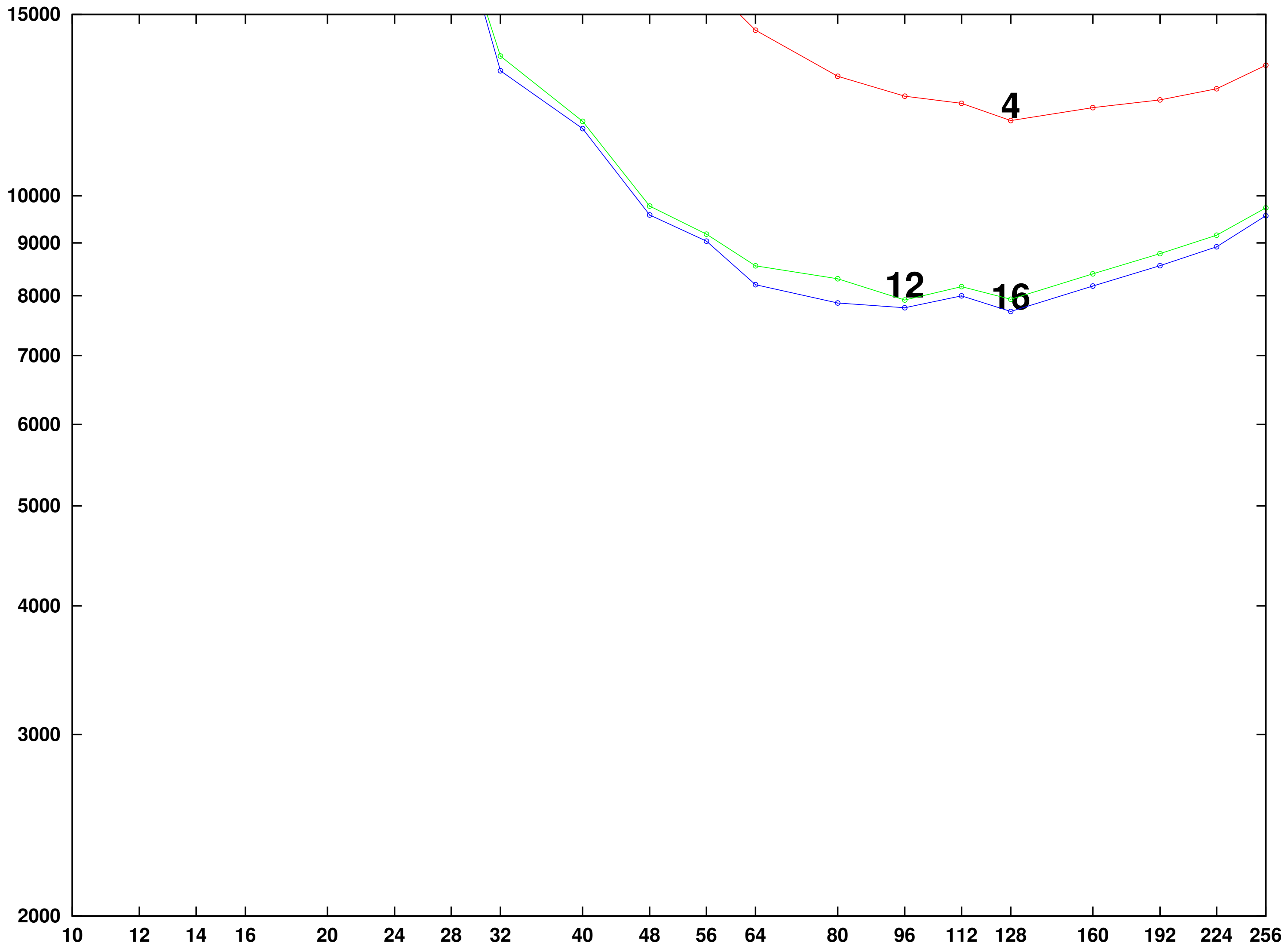
Small order points I

- ECM succeeds in factoring n if $[s]P = (0,1)$ modulo some divisor of n.
- If over $\mathbb{Q}$ the base point P has small order $k|s$ then $[s]P = (0,1)$ modulo all divisors of n, no factorization.
- But: it is interesting to have a large torsion subgroup over $\mathbb{Q}$ to increase the smoothness probability of ord(P).
- Some handwaving:
  - Modulo prime p the number of points on E is in the Hasse interval $[p+1-2\sqrt{p}, p+1+2\sqrt{p}]$.
  - Chance of smooth group order depends on size.
  - If k divides group order the unknown part gets smaller.

Small order points II

- Success rate does go up with size of torsion group.
- Over $\mathbb{Q}$ there are only finitely many points of finite order.
- More precisely: Theorem of Mazur.
  Let $E/\mathbb{Q}$ be an elliptic curve. The torsion subgroup $E_{\text{tors}}(\mathbb{Q})$ of E is isomorphic to one of the following fifteen groups:
  - $\mathbb{Z}/m$ for $m \in \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12\}$,
  - $\mathbb{Z}/2 \times \mathbb{Z}/2m$ for $m \in \{1, 2, 3, 4\}$.
- Search for curves with large torsion subgroup and positive rank, choose base point as a free point.
- Edwards curves have m divisible by 4. For twisted Edwards only $2 \mid m$ guaranteed.

Effect of $\mathbb{Q}$-torsion on cost



Edwards curves with large torsion

- Interesting(=large) choices are $\mathbb{Z}/12$ and $\mathbb{Z}/2 \times \mathbb{Z}/8$. Preprint shows that $\mathbb{Z}/2 \times \mathbb{Z}/6$ does not work for twisted Edwards curves.
- When do curves have a point of order 8? Assume that P_8 doubles to $(1, 0)$.
- $[2](x_8, y_8) = \left(\frac{2x_8y_8}{x_8^2+y_8^2}, \frac{y_8^2-x_8^2}{2-(x_8^2+y_8^2)}\right)$.
- $y_8^2 - x_8^2 = 0 \Rightarrow x_8 = \pm y_8 \Rightarrow x_8^2 + x_8^2 = 1 + dx_8^2x_8^2$, i.e. $d = (2x_8^2 - 1)/x_8^4$.
- Also need that $d = \square$ to have first $\mathbb{Z}/2$ component.
- For $u \notin \{0, -1, -2\}$, $x_8 = (u^2 + 2u + 2)/(u^2 - 2)$ gives square $d = (2x_8^2 - 1)/x_8^4$.

Edwards curves with $\mathbb{Z}/12$

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

- Any Edwards curve with a point of order 3 automatically has $\mathbb{Z}/12$ – and cannot have more.
- Use $(x_1^2+y_1^2)^2-(2y_1)^2=0$ and obtain condition: curve has this structure if there exists a y_6 so that $d=(2y_6+1)/(y_6^3(y_6+2))$ and such that $-(y_6^2+2y_6)$ is a square.
- Points of finite order are then

point	$(0,1)$	$(0,-1)$	$(\pm x_3,y_3)$	$(\pm 1,0)$	$(\pm x_3,-y_3)$	$(\pm y_3,\pm x_3)$
order	1	2	3	4	6	12

Choose other point as basepoint.

Existing constructions

- Two main constructions to obtain large torsion subgroup and a base point that is in the free part.
- Suyama has parameterization that guarantees $\mathbb{Z}/6$ over $\mathbb{Q}$. Modulo any prime the group order is divisible by 4 but not so over $\mathbb{Q}$.
- Have translated this representation to Edwards curves. Height of base point and coefficient does not grow too quickly (linear family of curves).
- Atkin-Morain curves have even larger torsion subgroup $\mathbb{Z}/2 \times \mathbb{Z}/8$ – easy to generate, but the height of the coefficients grows quickly (elliptic family of curves).
- We translated Atkin-Morain to Edwards form.

How to avoid large height coefficients?

- This tuning is only useful if the multiplication implementation notices that size of the factors.
- Use flexibility of twisted Edwards curves and projective coordinates
  - If $d = b/c$, with b, c small, extend both to have $c = e^2$ for some e and $d = b'/(e^2)$. Then the curve is isomorphic to the twisted Edwards curve with $a = e^2$ and $d = b'$ (y unchanged, new x is x/e). All values remain small.
  - Instead of working with $(x_1, y_1) = (r/t, v/w)$ which modulo n would get huge work with projective basepoint $(rw : tv : rw)$ (or divide by gcd).
- Make list of such curves and use in implementations where the field arithmetic caters for multiplication by words.

How to find such curves?

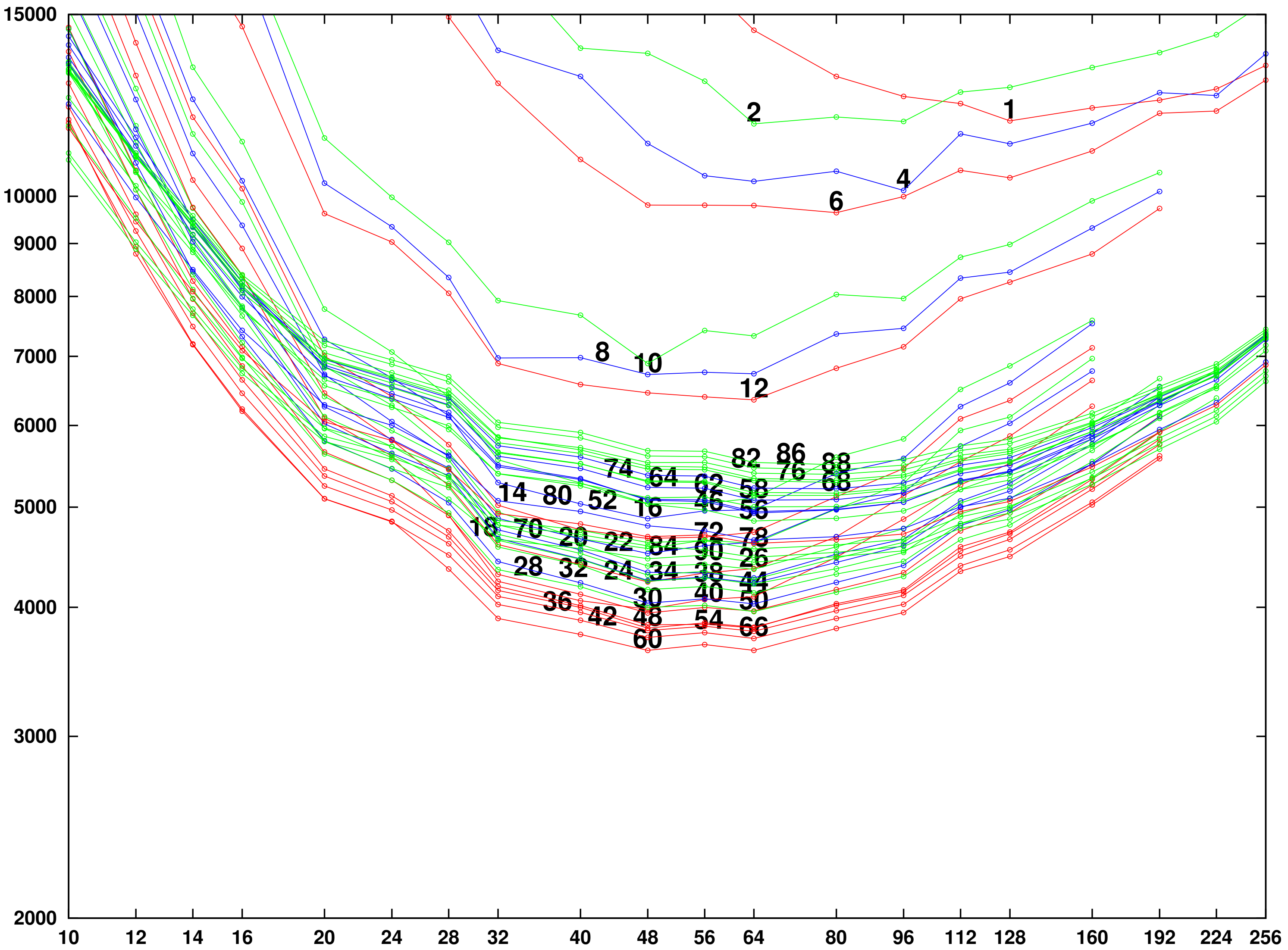
- Want curve with small height coefficient, base point and rank ≥ 1.
- Parametrization: for $u \notin \{0, -1, -2\}$, $x_8 = (u^2 + 2u + 2)/(u^2 - 2)$ gives square $d = (2x_8^2 - 1)/x_8^4$.
- Put $u = a/b$ and search for solutions (a, b, e, f), where (e, f) is a point on the curve but different from all torsion points, i.e. different from $(0, \pm 1), (\pm, 0)$ and $e \neq f$.
- Speed up search by restricting range of u and picking only 1 curve per isomorphism class.
- Computed more than 100 curves with 12 or 16 torsion points.
  `http://cr.yp.to/factorization/goodcurves.html`

The more complete story

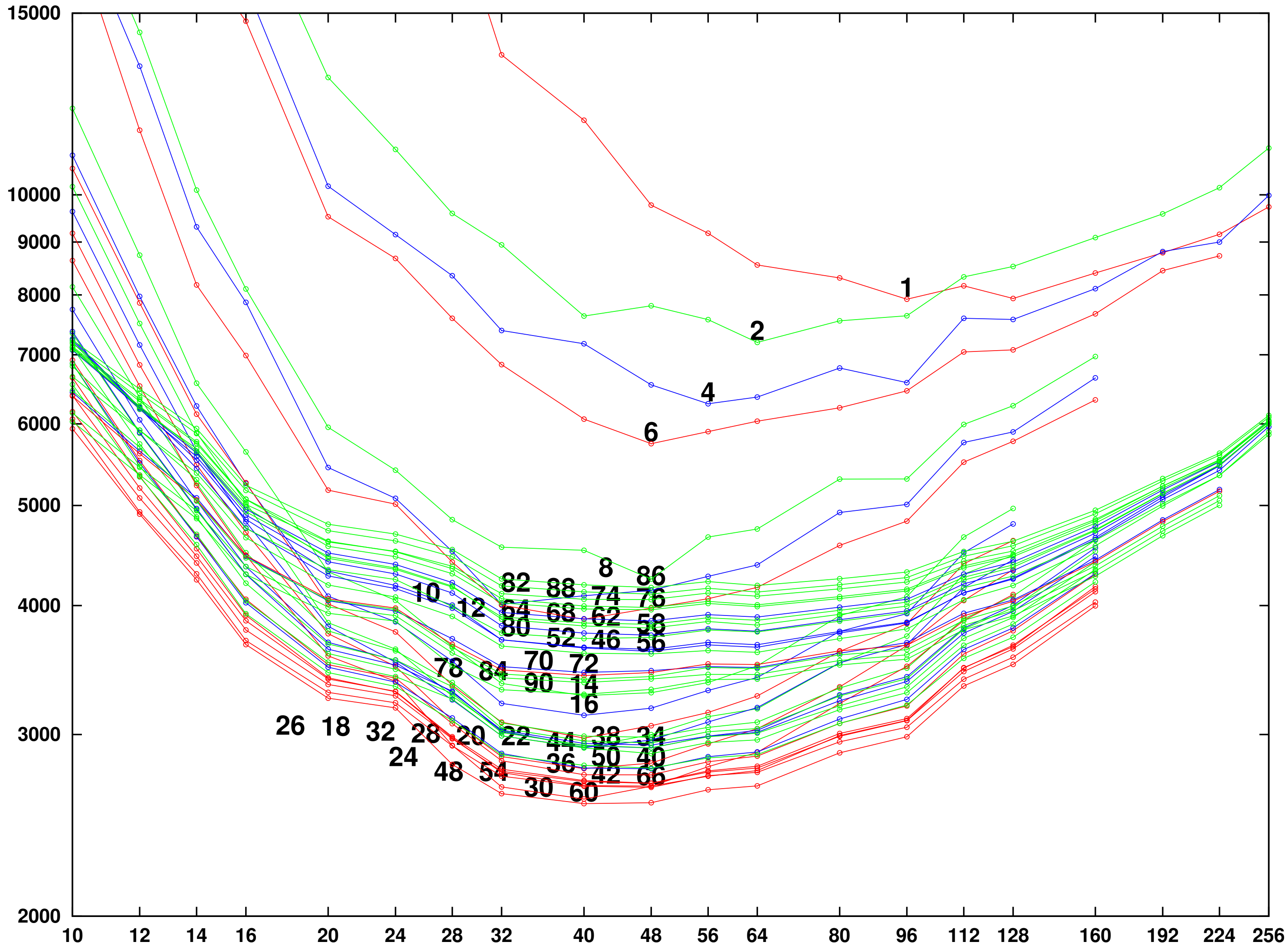
- Initial implementation was based on GMP-ECM; replacing Montgomery curves by Edwards curves in what's described so far (stage 1) saves 8%.
- Higher torsion improved chances by 12 %.
- Do experiments to find good choices of s.
- There is also a second stage which runs through many more primes; need to balance both stages.
- Following pictures show number of multiplications per prime found for different choices of parameters for first and second stage.
- Implementation, preprint (soon to be updated), curves at

  `http://eecm.cr.yp.to/`

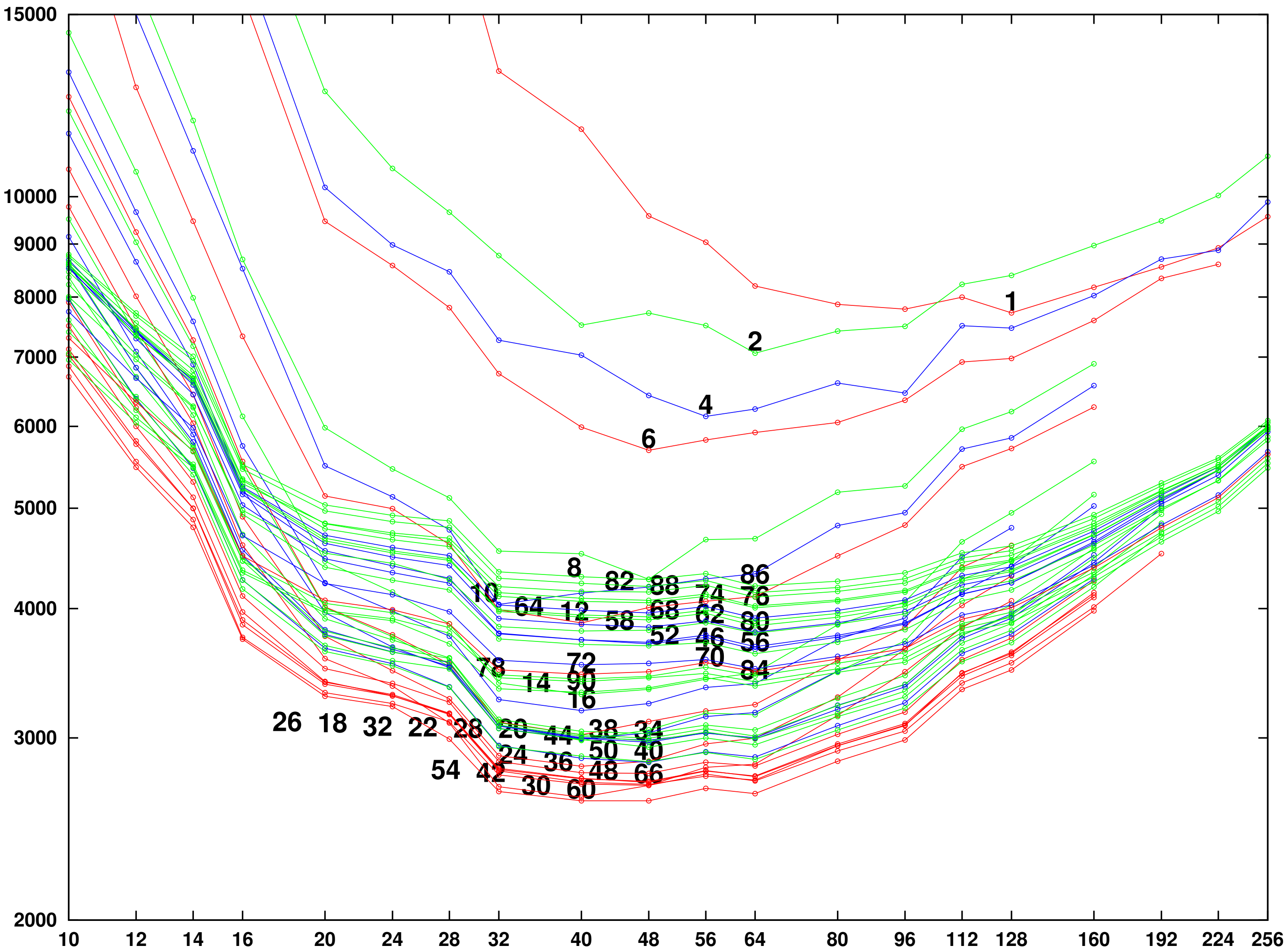
$\mathbb{Z}/4$


15000
10000
9000
8000
7000
6000
5000
4000
3000
2000
10
12
14
16
20
24
28
32
40
48
56
64
80
96
112
128
160
192
224
256
1
2
4
6
8
10
12
14
16
18
20
22
24
26
28
30
32
34
36
38
40
42
44
46
48
50
52
54
56
58
60
62
64
66
68
70
72
74
76
78
80
82
84
86
88
90

$\mathbb{Z}/12$


15000
10000
9000
8000
7000
6000
5000
4000
3000
2000
10 12 14 16 20 24 28 32 40 48 56 64 80 96 112 128 160 192 224 256
1
2
4
6
8 86
82 88 74 76
10 12 64 68 62 58
80 52 46 56
78 84 70 72
90 14
16
26 18 32 28 20 22 44 38 34
24 36 50 40
48 54 42 66
30 60

$\mathbb{Z}/2 \times \mathbb{Z}/8$



http://eecm.cr.yp.to/