Cryptanalytic world records, summer 2014

The elliptic curve method

Dr. Daniel Loebenberger

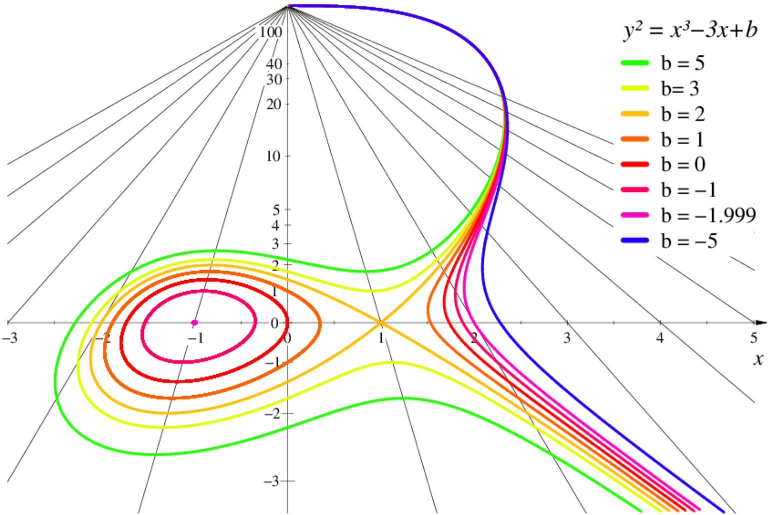
method	year	time
trial division	$-\infty$	$\mathcal{O}^{\sim}\left(2^{n/2}\right)$
Pollard's $p-1$ method	1974	$\mathcal{O}^{\sim}\left(2^{n/4}\right)$
Pollard's ρ method	1975	$\mathcal{O}^{\sim}\left(2^{n/4}\right)$
Pollard's and Strassen's method	1976	$\mathcal{O}^{\sim}\left(2^{n/4}\right)$
Morrison's and Brillhart's continued fractions	1975	$\exp(\mathcal{O}^{\sim}\left(n^{1/2}\right))$
Dixon's random squares, quadratic sieve	1981	$\exp(\mathcal{O}^{\sim}\left(n^{1/2}\right))$
Lenstra's elliptic curves	1987	$\exp(\mathcal{O}^{\sim}\left(n^{1/2}\right))$
number field sieve	1990	$\exp(\mathcal{O}^{\sim}\left(n^{1/3}\right))$
Shor's quantum algorithm	1994	$\mathcal{O}\left(n^{3}\right)$ q.ops.

Pollard's $p-1$ method

Assume the number $N = p \cdot q$ to be factored has the property that $p-1$ is B-smooth. Furthermore, assume you found $e \in \mathbb{Z}$, such that $p-1$ divides e. If we take $a \in \mathbb{Z}_N^\times$, then $a^e = 1 \in \mathbb{Z}_p^\times$. If additionally $a^e \neq 1 \in \mathbb{Z}_q^\times$, we find by computing $\gcd(a^e - 1, N) = p$ a proper factor of N.

The method crucially depends on the nature of the number N to be factored. Now, the *elliptic curve method* modifies this approach: Instead of working in $\mathbb{Z}_N$, we actually work in the group of points of an elliptic curve!

A family of elliptic curves with the point at infinity:



Definition

Let F be a field of characteristic different from 2 and 3, and $a, b \in F$ with $4a^3 + 27b^2 \neq 0$. Then

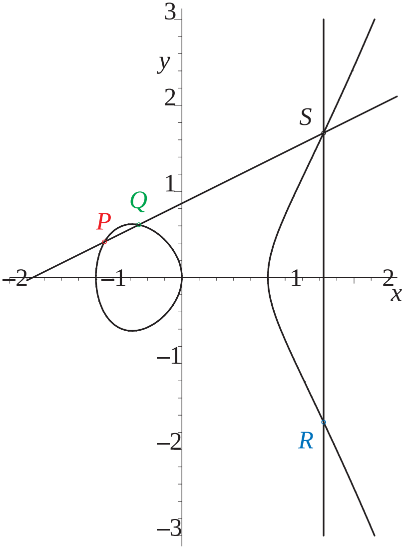
$$E = \{(u, v) \in F^2 : v^2 = u^3 + au + b\} \,\dot{\cup}\, \{\mathcal{O}\} \subseteq F^2 \,\dot{\cup}\, \{\mathcal{O}\}$$

is an *elliptic curve* over F. Here $\mathcal{O}$ denotes the "point at infinity" on E. The *Weierstrass equation* for E is

$$y^2 - (x^3 + ax + b) = 0,$$

E consists of its root (u, v), and a and b are the *Weierstrass coefficients* of E.

Adding two points on the elliptic curve $y^2 = x^3 - x$:



Definition

For $a, b \in \mathbb{Z}_N$ with $\gcd(N, 6) = 1$ and $\gcd(4a^3 + 27b^2, N) = 1$, we call the set

$$E = \{(u, v) \in \mathbb{Z}_N^2 : v^2 = u^3 + au + b\} \,\dot{\cup}\, \{\mathcal{O}\}$$

an *elliptic pseudocurve*.

Algorithm. Elliptic curve method.

Input: An integer $N \geq 2$ with $\gcd(N, 6) = 1$ and N not a perfect power.

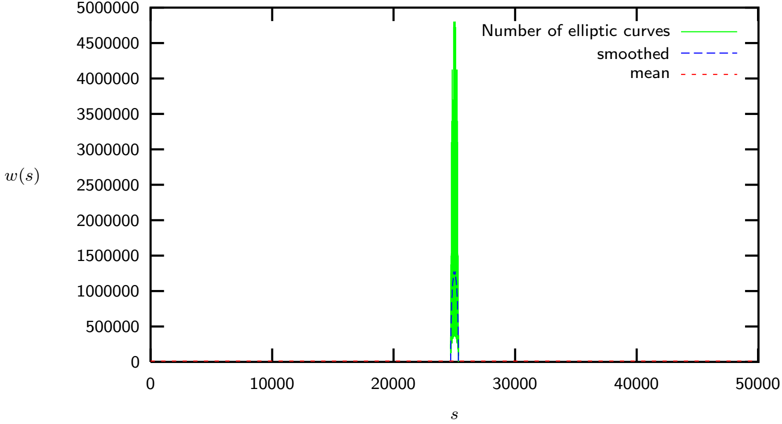
Output: A proper factor of N.

1. Choose the stage-one limit B_1, e.g. $B_1 = 10000$.
2. Repeat 3–5
3. Choose randomly $x, y, a \in \mathbb{Z}_N$.
4. Set $b = (y^2 - x^3 - ax)$ modulo N.
5. Compute $g = \gcd(4a^3 + 27b^2, N)$.
6. While $g = N$.
7. If $g > 1$ return g.
8. Set $P = (x, y)$.
9. Try to compute $Q = kP$ with $k = \prod_{p_i^{a_i} \leq B_1} p_i^{a_i}$.
10. If the computation failed then
11. Return a proper factor of n or start from the beginning.
12. Increment B and start from the beginning.

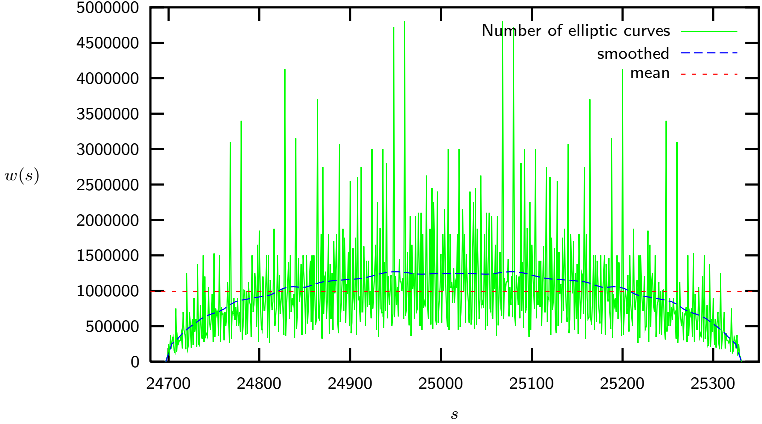
Theorem

Let E be an elliptic curve over the finite field $\mathbb{F}_q$ of characteristic greater than three. Then $\#E \leq 2q + 1$.

The number $w(s)$ of Weierstrass parameters of elliptic curves over $\mathbb{F}_{25\,013}$ with s points:



The number $w(s)$ of Weierstrass parameters of elliptic curves over $\mathbb{F}_{25\,013}$ with s points:



Hasse's bound

If E is an elliptic curve over the finite field $\mathbb{F}_q$, then

$$|\#E - (q+1)| \leq 2\sqrt{q}.$$

Theorem (Lenstra, 1987)

There is a positive constant c such that for every prime $p > 3$ and any set S with $\#S \geq 3$ of integers from the Hasse interval $(p + 1 - 2\sqrt{p}, p + 1 + 2\sqrt{p})$, we have

$$N_1(S) > c \cdot \#S \cdot p^{3/2} / \ln p \text{ and } N_2(S) > c \cdot \#S \cdot p^{5/2} / \ln p.$$

Theorem

On input N, $\gcd(N,6)=1$ not a perfect power with smallest prime factor p, the elliptic curve method runs in an heuristic expected time of

$$\exp((\sqrt{2}+o(1))\sqrt{\ln p \ln\ln p}),$$

when $B_1 = \exp((\sqrt{2}/2+o(1))\sqrt{\ln p \ln\ln p})$.

For ECM there is a a natural second stage. Assume $\#E_{a,b}(\mathbb{F}_p)$ is not B_1-smooth. Then the stage one ECM would always fail to find a factor. But it might be that the group order has just *a single* prime factor exceeding B_1, i.e.

$$\#E_{a,b}(\mathbb{F}_p) = q \cdot \prod_{p_i^{a_i} \leq B_1} p_i^{a_i}$$

for p prime, $q > B_1$. Then, simply going through the subsequent primes beyond B_1 is called *stage 2* of the ECM.

Further improvements:

- Use a special parametrization of the curve, i.e. Montgomery curves.
- Choose special curves whose group order is known to be divisible by 12 or 16.
- Use better arithmetic for large integers.

Theorem (Generalized Montgomery identities)

Given an elliptic curve by $gy^2 = x^3 + cx^2 + ax + b$ and two finite points $P = (x_1, y_1)$, $Q = (x_2, y_2)$ then if $x_1 \neq x_2$ we have

$$x_+ x_- = \frac{(x_1 x_2 - a)^2 - 4b(x_1 + x_2 + c)}{(x_1 - x_2)^2},$$

where $P + Q = (x_+, y_+)$ and $P - Q = (x_-, y_-)$. If $x_1 = x_2$ then

$$x_+ = \frac{(x_1 - a)^2 - 4b(2x_1 + c)}{4(x_1^3 + cx_1^2 + ax_1 + b)}$$

Definition (Differential addition)

Given finite points $P_1 = [X_1 : Y_1 : Z_1]$, $P_2 = [X_2 : Y_2 : Z_2]$ and $P_1 - P_2 = [X_-, Y_-, Z_-]$ on the homogeneous Montgomery curve with $X_- \neq 0$ then for the point $P_1 + P_2 = [X_+ : Y_+ : Z_+]$ we have

$$X_+ = Z_-((X_1X_2 - aZ_1Z_2)^2 - 4b(X_1Z_2 + X_2Z_1 + cZ_1Z_2)Z_1Z_2)$$
$$Z_+ = X_-(X_1Z_2 - X_2Z_1)^2$$

Definition (Differential doubling)

Given $P_1 = [X_1 : Y_1 : Z_1]$ on the homogeneous Montgomery curve then then for the point $2P_1 = [X_+ : Y_+ : Z_+]$ we have

$$X_+ = (X_1 - aZ_1^2)^2 - 4b(2X_1 + cZ_1)Z_1^3$$
$$Z_+ = 4Z_1(X_1 + cX_1^2Z_1 + aX_1Z_1^2 + bZ_1^3)$$

Montgomery curves are given by a cubic $gy^2 = x^3 + cx^2 + ax + b$. Such curves allow particularly nice addition chains:

Algorithm.

Input: A point $P = [X : Z]$, a positive integer k with B bits.
Output: The $[X : Z]$ coordinates of kP.

1. If $n = 0$ then return $\mathcal{O}$.
2. If $n = 1$ then return $[X : Z]$.
3. If $n = 2$ then return double($[X : Z]$).
4. $[U : V] = [X : Z]$, $[T : W] =$ double($[X : Z]$)
5. For j from $B - 2$ downto 0 do [6-7]
6. if $k_j = 1$ then

$$[U : V] = \text{add}([T : W], [U : V], [X : Z])$$
$$[T : W] = \text{double}([T : W])$$

7. else

$$[U : V] = \text{add}([U : V], [T : W], [X : Z])$$
$$[T : W] = \text{double}([U : V])$$

8. if $k_0 = 1$ return add($[U : V], [T : W], [X : Z]$)
9. return double($[U : V]$)

Theorem

Define an elliptic curve by $E_\sigma : y^2 = x^3 + C(\sigma)x^2 + x$ with $C(\sigma) = \frac{(v-u)^3(3u+v)}{4u^3v} - 2$, $u = \sigma^2 - 5$, $v = 4\sigma$ and $\sigma \neq 0, 1, 5$. Then $\#E_\sigma$ is divisible by 12.

Furthermore, either on E (or a twist of it), we have a point with x-coordinate u^3v^{-3} on it.

Thank you!