Elliptic curve factoring

David, transcribed by Soham

July 2016

Let N be a large (but not huge) number. Goal: find the factorization of N into primes on a classical computer.

1. Bogofactor.
2. Simulate Shor's algorithm.
3. Trial division upto $n-1$.
4. Trial division upto $\sqrt{n}$.
5. Fermat method: try writing $N = x^2 - y^2$ nontrivially.
6. Generalize Fermat to p-th powers.
7. Generalize Fermat by looking at x, y with
$$x^2 - y^2 \equiv 0 \pmod{n}$$
8. Take $x > \sqrt{N}$. If c only has small prime factors, we can assemble a "difference of squares" factorization from such c. As an example, consider (?)

1 Pollard $p-1$ algorithm

$N = pq$. Suppose that $p-1$ is B-smooth, but $q-1$ is not. For any $a \not\equiv 0 \pmod{p}$ or $\pmod{q}$, define

$$M = \prod_{p \leq B} p^{\lfloor \log_p B \rfloor} = \operatorname{lcm}(1, \ldots, B)$$

Now choose a randomly and compute $a^M \equiv 1 \pmod{p}$. Usually, we also have $a^M \not\equiv 1 \pmod{q}$. Then $\gcd(a^M - 1, N)$ will often be a factor of N.

2 Day 2

2.1 Elliptic curves

A set of points in the plane defines an elliptic curve if $y^2 = x^3 + ax^2 + bx + c$. This is called Weierstrass form, and it exists in characteristic not equal to 2. In characteristic not 3, we can change variables further to get $y^2 = x^3 + ax + b$.

How many points does an arbitrary line intersect an elliptic curve E in? Morally, of course, it should be 3, by Bézout's theorem. Nic fixed this in his colloquium by:

- working over $\mathbb{C}$
- using projective coordinates
- counting points with multiplicity

We will, instead, prefer to use a group law on the elliptic curve to fix the first one, because we want to work over finite fields.

Claim: If a line intersects E in two points (with multiplicity), then it intesects in a third point.

This is only true if we are working in some projective space, though. Suppose $y^2 = x^3 + ax^2 + bx + c$. Given $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$, consider the line $y = \lambda x + \nu$ through them.

We get, after using the formula $x_1 + x_2 + x_3 = \lambda^2 - a$, the expression

$$x_3 = \lambda^2 - a - x_1 - x_2$$

where

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1}.$$

This breaks down for $x_2 = x_1$. The line we use in such cases is:

- If $P_1 = P_2$, we just use the tangent line:

$$\lambda = \frac{3x_1^2 + 2a + b}{2y_1}.$$

- For "vertical" lines, we use a point $\mathcal{O}$ at infinity.

2.2 Projectivization

Consider $y^2z = x^3 + ax^2z + bxz^2 + cz^3$. This is homegeneous upto rescaling, and solutions $[x : y : z]$ come up to rescaling. When $z \neq 0$, we can rescale to $[x : y : 1]$. When $[z = 0]$, $x^3 = 0 = x$ so we can rescale to $[0 : 1 : 0]$, which we will use as the identity for the group law.

2.3 The group law

Let $P * Q$ be the third point of intersection of the line through P and Q with E. Then the reflection of $P * Q$ across the x-axis is called $P + Q$.

Theorem 1. This gives us an abelian group structure on the points of the elliptic curve (including $\mathcal{O}$).

Associativity can be brute-forced, or one can look at the (moduli?) space of elliptic curves and use dimension arguments arising from the different expressions
$\mathcal{O}, P, Q, R, P*Q, P*R, Q*R, (P+Q)*R, P*(Q+R)$ C_1, C_2, C_3 cubics, C_1, C_2 intersect in 9 points, if C_3 passes through 8 of those points, then it passes through the 9th one too.

3 Day 2

Question 1. If E is an elliptic curve, how many elements does $E(\mathbb{F}_p)$ have?

$y^2 = x^3 + bx + c$. Heuristically, as x varies, $x^3 + bx + c$ is a square in $\mathbb{F}_p$ half of the time, so we expect $p + 1$ points.

Theorem 2 (Hasse)**.** $|p + 1 - \#E(\mathbb{F}_p)| \leq 2\sqrt{p}$.

Theorem 3 (Sato-Tate)**.** The distribution of the number of points on non-CM elliptic curves varies with a probability distribution that looks like a semicircle.

Definition 1.

$$L_n[a, c] := O(e^{(c+o(1))(\log n)^a (\log\log n)^{1-a}}).$$

In particular, for $a = 0$, we get $(\log n)^{c+o(1)}$, and for $a = 1$, we get $n^{c+o(1)}$.

4 Day 3

Given a curve E, find $\#E(\mathbb{F}_p)$.

1. For each x, determine whether $x^3 + ax + b$ is a square mod p. Each nonzero square contributes 2 points.
2. Pick a random point P on the curve and compute $P, 2P, \cdots$ until you reach $\mathcal{O}$.
3. "Baby step — giant step". Pick a point P and compute

$$P, 2P, 3P, \cdots.$$

Let $Q = -BP$. Now compute

$$Q, 2Q, 3Q, \cdots.$$

There is a point that is on both lists. We get that

$$iP = -jQ = -jBP,$$

so

$$(i + Bj)$$

is a multiple of the order of the group.

4. Let $a = p + 1 - \#E(\mathbb{F}_p)$. We will find $a \pmod{l}$ for lots of small primes l. Once $\pi l > 4\sqrt{l}$, we can use the Chinese remainder theorem to recover a.

   Warmup: Find $a \pmod 2$. 2 divides $\#E(\mathbb{F}_p) \iff x^3 + Ax + B$ has a root α in $\mathbb{F}_p$. We know that any such α has to satisfy $x^p - x$ as well.

   So a root exists iff $\gcd(x^p - x, x^3 + Ax + B) = \gcd(x^p \pmod{x^3 + Ax + B} - x, x^3 + Ax + B) \neq 1$. Modular exponentiation is fast!

Let us generalize to $p \neq 2$.

Definition 2. The *n-torsion* $E[n]$ of E is defined as

$$E \supset E[n] := \{P \in E(\overline{\mathbb{F}_p}) : nP = \mathcal{O}\}.$$

We can try to find $a \pmod{l}$ by studying $E[l]$. In particular, if $E[l](\mathbb{F}_p) \neq 0$ then $l | \#E(\mathbb{F}_p)$.