MPRI – Cours 2.12.2

F. Morain

Lecture III: introduction to elliptic curves

2010/09/28

The slides are available on http://www.lix.polytechnique.fr/Labo/Francois.Morain/MPRI/2010

I. Definition and group law

$\mathbf{K}$ field of characteristic $\neq 2, 3$. Elements of $\mathbf{K}^3 - \{(0,0,0)\}$ are equivalent iff

$$(x_1, y_1, z_1) \sim (x_1', y_1', z_1') \iff \exists\, \lambda \neq 0, x_1 = \lambda x_1', y_1 = \lambda y_1', z_1 = \lambda z_1'.$$

Projective space: $\mathbf{P}^2(\mathbf{K})$ = equivalence classes of $\sim$.

Elliptic curve defined for points in $\mathbf{P}^2(\mathbf{K})$:

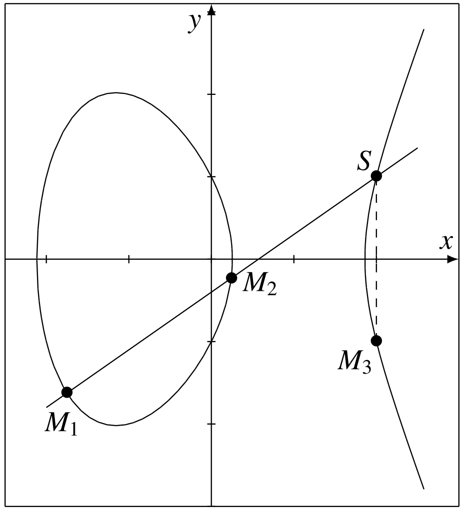
$$Y^2 Z = X^3 + aXZ^2 + bZ^3 \quad (1)$$

with $4a^3 + 27b^2 \neq 0$ (discriminant of E).

Def. $E(\mathbf{K}) = \{(x : y : z)$ satisfying (1)$\}$.

Prop. $E(\mathbf{K}) = \{(0 : 1 : 0)\} \cup \{(x : y : 1)$ satisfying (1)$\}$ = point at infinity $\cup$ affine part.

The group law



$M_3 = M_1 \oplus M_2$

$$\lambda = \begin{cases} (y_1 - y_2)/(x_1 - x_2) \\ (3x_1^2 + a)/(2y_1) \end{cases}$$

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

$$y_3 = \lambda(x_1 - x_3) - y_1$$

$$[k]M = \underbrace{M \oplus \cdots \oplus M}_{k \text{ times}}$$

Rem. Standard equation and group law formulas for any field. Can be improved in many ways, see BS's part.

II. Curves over finite fields

Thm. (Hasse) $\#E(\mathbb{F}_p) = p + 1 - t$, $|t| \leq 2\sqrt{p}$.

Thm. (Deuring) given $|t|$, there exists E s.t. $\#E = p + 1 - t$.

Key advantage: enough groups of cardinality close to p (e.g., primality proving).

Caveat:

- no general formula for $\#E$ except in some special cases, e.g. $E : Y^2 = X^3 + X$ has $p + 1 - 2u$ points when $p = u^2 + v^2$.
- no efficient way for finding E given t except in some special cases (complex multiplication).

Rem. Generalizable to $q = p^n$.

Group structure

Thm. $E(\mathbb{F}_p) \simeq E_1 \times E_2$ of respective ordres m_1 and m_2 s.t. $m_2 \mid p-1$ and $m_2 \mid m_1$.

Prop. (Murty; Vlăduţ) Almost always, $E(\mathbb{F}_p)$ is cyclic.

Consequence:

$$\sqrt{p}-1 < \exp(E(\mathbb{F}_p)) < (\sqrt{p}+1)^2.$$

Thm. (Schoof) For almost all curves $E/\mathbb{Q}$, there exists $C_E > 0$ s.t.

$$\frac{\exp(E(\mathbb{F}_p))}{\sqrt{p}} > C_E \frac{\log p}{(\log\log p)^2}.$$

Computing the cardinality

Invent a method in time:

- $O(p)$:
- $O(p^{1/2})$:
- $O(p^{1/4})$:

Algorithms:

- $g=1$, p large: Schoof (1985). $\tilde{O}((\log p)^5)$, completely practical after improvements by Elkies, Atkin, and implementations by M., Lercier, etc. New recent record (2010/07) A. Sutherland, for $p = 16219299585 \cdot 2^{16612} - 1$ (5000dd), 1378 CPU days AMD Phenom II 3.0 GHz.
- $p=2$: p-adic methods (Satoh, Fouquet/Gaudry/Harley; Mestre). Completely solved.

III. ECDLP

DLP in general resistant on an elliptic curve except

- supersingular curves ($t=0$), due to the MOV reduction;
- anomalous curves ($t=1$).

ECC112b: taken from `http://lacal.epfl.ch/page81774.html`, Bos/Kaihara/Kleinjung/Lenstra/Montgomery (EPFL/Alcatel-Lucent Bell Laboratories/MSR) $p = (2^{128}-3)/(11 * 6949)$, curve secp112r1

- 3.5 months on 200 PS3; 8.5×10^{16} ec additions ($\approx$ 14 full 56-bit DES key searches); started on January 13, 2009, and finished on July 8, 2009.
- half a billion distinguished points using 0.6 Terabyte of disk space.

IV. Maurer & Wolf (1/3)

Thm. Let G have cardinality $p \equiv 3 \bmod 4$ (a prime) and oracle $\mathcal{O}$ which can compute g^{xy} given any pair (g^x, g^y). Suppose we have found $E/\mathbb{F}_p : Y^2 = X^3 + AX + B$ of generator $P_0 = (x_0, y_0)$ whose cardinality m is smooth (hence DLP on E is easy). Then: one can solve the DLP on G.

Proof. What we can compute with $\mathcal{O}$:

- $g^{P(x)}$ for any polynomial $P(x) \in \mathbb{Z}[x]$;
- g^{x^n} using $O(\log n)$ calls;
- $g^{1/x} = g^{x^{p-1}}$;
- $g^{P(x)/Q(x)}$ for any fraction;
- the Legendre symbol (x/p): $g^{(x/p)} = g^{x^{(p-1)/2}}$ and compare to g or g^{-1};
- $g^{\sqrt{x}} = g^{x^{(p+1)/4}}$;
- $(g^{M_{3x}}, g^{M_{3y}})$ s.t. $M_3 = M_1 \oplus M_2$ on E and $M_i = (g^{M_{ix}}, g^{M_{iy}})$.

Maurer & Wolf (2/3)

INPUT: a.

OUTPUT: x s.t. $a = g^x$.

Step 1: find e s.t. $(x+e)^3 + A(x+e) + B$ is a square by computing $(((x+e)^3 + A(x+e) + B)/p)$ using $\mathcal{O}$.

Step 2: compute $g^{\sqrt{(x+e)^3+A(x+e)+B}} = g^y$, say. $P = (x+e, y)$ is a point on E, represented as (g^{x+e}, g^y). There exists k s.t. $P = [k]P_0$.

Step 3: since m is smooth, k is easily found: if $q^\alpha \mid\mid m$, then we can compute $[m/q^\alpha]P = (g^w, g^z)$ using the oracle. Since we know $[m/q^\alpha]P_0$, we can compute all its multiples (u, v) or (g^u, g^v) and compare them to (g^w, g^z) to find $k \bmod q^\alpha$.

Step 4: recover $P = (x+e, y) = [k](x_0, y_0)$ and therefore x.

Maurer & Wolf (3/3)

Complementary remarks:

- Can be generalized to other groups G, other groups E.
- We may concentrate on breaking DL instead of DH (and conversely).