CHARLES UNIVERSITY PRAGUE

faculty of mathematics and physics

**Tomáš Sladovník**

Department of algebra

# British elevator II

## Algorithm

Fall school of algebra 2016

- Elliptic curve
- Expansion around $\mathcal{O}$
- Group $E_n$
- Algorithm

### Definition

Let $G$ be a group and for given $a, b \in G$ is the discrete logarithm problem (DLP) defined as solving an equation

$$a^x = b$$

with the variable $x$.

### Example

Let $p$ be a prime number.

- $G$ is group $(\mathbb{Z}_p, *, ^{-1}, 1)$ then DLP is in general difficult to solve.
- $G$ is group $(\mathbb{Z}_p, +, -, 0)$ then DLP is simple.

### Definition (Projective space)

Let $K$ be a field and $n \in \mathbb{N}$. The projective $n$-space over $K$, denoted by $\mathbb{P}^n(K)$, is the set of nonzero vectors in $K^{n+1}$.

$$\mathbb{P}^n(K) = \{\langle v \rangle | v \in K^{n+1} \setminus \{0\}\}$$

For nonzero vectors $(x_0, ..., x_n), (y_0, ..., y_n)$ from $K^{n+1}$:

$$(x_0, ..., x_n) \sim (y_0, ..., y_n) \Leftrightarrow \exists \lambda \in K^* : (y_0, ..., y_n) = (\lambda x_0, ..., \lambda x_n).$$

Class of equivalence given by the element $(x_0, ..., x_n)$ will be denoted by $(x_0 : ... : x_n)$.

**Definition (Weierstrass normal form)**

Let $K$ be a field of characteristics different from 2, 3 and $a_i \in K$ then a cubic curve

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

is in the Weierstrass normal form.

With a change of variable $y$ to $y - \frac{(a_1x+a_3)^2}{2}$, we obtain $y^2 = f(x)$, where $f(x)$ is a cubic polynomial in $x$, which can be changed to the form $x^3 + Ax + B$.

**Definition (Weierstrass minimal form)**

Let $K$ be a field of characteristics different from 2,3 and $A, B \in K$ then cubic curve

$$E : y^2 = x^3 + Ax + B.$$

is in the Weierstrass minimal form.

From now on let assume, for simplification, that an elliptic curve is in Weierstrass minimal form.

**Definition (Elliptic curve)**

The set of points on an elliptic curve over field $K$, denoted by $E(K)$, is the set of solutions of the homogenous cubic equation

$$F(x, y, z) = x^3 + Axz^2 + Bz^3 - y^2 z,$$

which is given by the cubic equation in Weierstrass (minimal) form $y^2 = x^3 + Ax + B$ in $\mathbb{P}^2(K)$. The solutions of $F(x, y, z)$ are points $(x : y : 1)$, where $(x, y)$ is a solution of original cubic equation and the point at infinity $\mathcal{O} = (0 : 1 : 0)$.

When we talk about elliptic curve in Weierstrass form we mean homogenous curve in $\mathbb{P}^2(K)$ with a point in infinity $\mathcal{O}$.

**Definition (Non-singular elliptic curve)**

Let $E(K)$ be an elliptic curve defined over field $K$ in form

$$E : y^2 = x^3 + Ax + B,$$

where $A, B \in K$. We call an elliptic curve nonsingular if and only if it's discriminant

$$\Delta = -16(4A^3 + 27B^2) \neq 0.$$

When we talk about elliptic curve we mean non-singular elliptic curve.

**Definition (Group law on elliptic curve)**

Let $K$ be a field and $E$ be an elliptic curve defied over $K$. Let $Q, P, R \in E(K)$ and $PQ$ is a line which connects $P, Q$ then the group law on an elliptic curve is defined by an equation

$$\sum_{R \in PQ \cap E(\mathbb{Z}_p)} i(R, PQ, E)R = \mathcal{O},$$

where $i(R, PQ, E)$ is an intersection multiplicity.

Let $K$ be a field and $E : y^2 = x^3 + Ax + B$ be an elliptic curve over field $K$. Let $P, Q \in E(K)$ and

$$P \neq Q, P \neq \mathcal{O}, Q \neq \mathcal{O}, \text{ where } P = (x_1, y_1) \text{ a } Q = (x_2, y_2) \text{ then}$$

$$\mathcal{O} + \mathcal{O} = \mathcal{O}$$

$$P + (-P) = \mathcal{O},$$

$$P + \mathcal{O} = \mathcal{O} + P = P.$$

In Weierstrass minimal form it holds, that $-P = (x_1, -y_1)$.
Define functions $x, y : K \times K \to K$ as $x(P) = x_1$ a $y(P) = y_1$.

Computing $2P$:

$$\lambda = \frac{3x_1^2 + A}{2y_1}, \text{ where } y_1 \neq 0$$

$$x(2P) = \lambda^2 - 2x_1$$

$$\beta = y_1 - \lambda x_1$$

$$y(2P) = -(\lambda x(2P) + \beta)$$

Computing $P + Q$:

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

$$x(P + Q) = \lambda^2 - x_1 - x_2$$

$$\beta = y_1 - \lambda x_1$$

$$y(P + Q) = -(\lambda x(P + Q) + \beta)$$

**Theorem**

*Let $K$ be a field and $E$ be an elliptic curve over field $K$. The points on an elliptic curve $E(K)$ with the group law form an abelian group*

$$(E(K), +, -, \mathcal{O}).$$

Until the end of chapter elliptic curves let $p$ be a prime number different from 2, 3 and $E$ be an elliptic curve defined over $\mathbb{Z}_p$.

**Theorem (Hasse)**

$|(p+1) - |E(\mathbb{Z}_p)|| < 2\sqrt{p}$.

**Theorem (Deurini)**

*$m \in (p+1-2\sqrt{p}, p+1+2\sqrt{p})$ then $\exists A, B \in \mathbb{Z}_p$: $4a^3 + 27b^2 \neq 0$ and $|E_{A,B}(\mathbb{Z}_p)| = m$.*

**Theorem**

*Group $E(\mathbb{Z}_p)$ is either cyclic or $E(\mathbb{Z}_p) \cong \mathbb{Z}_{d_1} \times \mathbb{Z}_{d_2}$, where $d1|d2$ and $d1|p-1$.*

**Definition (The trace of Frobenius)**

The trace of Frobenius, denoted by $t$, is defined as

$$t = p + 1 - |E(\mathbb{Z}_p)|.$$

**Corollary**

*If $t = 1$ then*

$$E(\mathbb{Z}_p) \cong (\mathbb{Z}_p, +, -, 0).$$

Using substitution $z = -\frac{x}{y}$ and $w = -\frac{1}{y}$, in other words $x = \frac{z}{w}$ and $y = -\frac{1}{w}$. The $\mathcal{O}$ is now at $(0, 0)$, because $(x : y : z) \mapsto (x : z : -y)$ and the curve has transformed to the form

$$w = z^3 + Azw^2 + Bw^3 = f(z, w),$$

$$w(z) = f(z, w(z))$$

$$w = z^3 + Azw^2 + Bw^3 =$$

$$= z^3 + Az(z^3 + Azw^2 + Bw^3)^2 + B(z^3 + Azw^2 + Bw^3)^3 = ... =$$

$$= z^3 + Az^7 + Bz^9 + A^2z^{11} + ...$$

**Theorem**

*This procedure gives us a power series*

$$w(z) = z^3(1 + Az^4 + Bz^6 + A^2z^8 + \dots).$$

*Moreover $w(z)$ is unique power series, which satisfies*

$$w(z) = f(z, w(z)).$$

$x(z) = \frac{z}{w(z)} = \frac{1}{z^2} - Az^2 + \dots$ and $y(z) = -\frac{1}{w(z)} = -\frac{1}{z^3} + Az\dots$

$$z = -\frac{x(z)}{y(z)}$$

Let $p$ be a prime number different from 2 and 3. Denote $\mathbb{Q}_p$ as field of $p$-adic numbers and $\hat{\mathbb{Z}}_p$ as ring of $p$-adic integers. Let $E$ be an elliptic curve over $\mathbb{Q}_p$ with $A, B \in \mathbb{Z}_p$. In minimal Weierstrass form holds $P = (x, y) \in E(\mathbb{Q}_p) : -P = (x, -y)$.

$$\lambda = \lambda(z_1, z_2) = \frac{w_2 - w_1}{z_2 - z_1} = \sum_{n=3}^{\infty} A_{n-3} \frac{z_2^n - z_1^n}{z_2 - z_1} \in \mathbb{Z}[A, B][[z_1, z_2]]$$

**Theorem**

*With this procedure we can construct the formal group law.*

**Definition (Formal group associated to an elliptic curve)**

For an elliptic curve $E(\mathbb{Q}_p)$ define an associated formal group, denoted by $\hat{E}(p\hat{\mathbb{Z}}_p)$, with the formal group law

$$i(z) = -\frac{x(z)}{-y(z)} = \frac{x(z)}{y(z)} \in \mathbb{Z}[A, B][[z]],$$

$$F(z_1, z_2) = z_1 + z_2 + z_1 z_2(\ldots) \in \mathbb{Z}[A, B][[z_1, z_2]].$$

Constant elements of $F$ are equal to zero.

**Corollary**

$$\hat{E}(p\hat{\mathbb{Z}}_p) \cong p\mathbb{Z}_p$$

**Definition (Sets $E_n$)**

Let $E(\mathbb{Q}_p)$ be a set of points on an elliptic curve $E$ over a field of $p$-adic numbers and $n \in \mathbb{N}$ then

$$E_n(\mathbb{Q}_p) = \{P \in E(\mathbb{Q}_p) : \upsilon_p(x(P)) \leqslant -2n\} \cup \{\mathcal{O}\},$$

where $P = (x_P : y_P : z_P)$ and $x(P) = x_P$.

For nonsingular curve $E_0(\mathbb{Q}_p) = E(\mathbb{Q}_p)$.

**Theorem**

*For all $n \in \mathbb{N}$: $E_n(\mathbb{Q}_p)$ is a subgroup of $E(\mathbb{Q}_p)$.*

### Definition (Reduction modulo $p$)

Reduction modulo $p$ is defined as the mapping

$$\begin{array}{rcl} \pi : \widehat{\mathbb{Z}}_p & \to & \mathbb{Z}_p \\ x_0 + x_1 p + x_2 p^2 + \ldots & \mapsto & x_0, \end{array}$$

where $\widehat{\mathbb{Z}}_p$ is the set of $p$-adic integers.

### Definition (Reduction modulo $p$ of point $P \in \mathbb{P}^2(\mathbb{Q}_p)$)

Let $P \in \mathbb{P}^2(\mathbb{Q}_p)$, $P = (x : y : z)$ such that $x, y, z \in \widehat{\mathbb{Z}}_p$ and at least one coordinate does not belong to $p\widehat{\mathbb{Z}}_p$, then reduction modulo $p$ of point $P$, denoted by $\tilde{P}$, is defined as

$$\pi(P) = (\pi(x) : \pi(y) : \pi(z)) \in \mathbb{P}^2(\mathbb{Z}_p).$$

Let $P = (x : y : 1) \in E(\mathbb{Q}_p)$ and $A, B \in \mathbb{Z}_p$, if $A, B \neq 0$ then $\upsilon(A) = 0$, $\upsilon(B) = 0$. If $x, y \in \widehat{\mathbb{Z}}_p$ then $\pi(P) = (\pi(x) : \pi(y) : 1) \in E(\mathbb{Z}_p)$.
Let $\upsilon(x) < 0$.

$$\upsilon(y^2) = \upsilon(x^3 + Ax + B)$$

$$\upsilon(y) = \frac{\upsilon\left(x^3 + Ax + B\right)}{2}$$

$$\upsilon(y) = \frac{3}{2}\upsilon(x) < 0.$$

From definition we obtain that $\upsilon(x)$ is even.

$$\upsilon(x) = -2n \;\&\; \upsilon(y) = -3n, \text{ where } n \in \mathbb{N}.$$

$$P \in \mathbb{P}^2(\mathbb{Q}_p) \text{ so } (x, y, 1) \sim (p^{3n}x, p^{3n}y, p^{3n})$$

$$\pi(P) = \pi(p^{3n}x, p^{3n}y, p^{3n}) = (0, y_{-3n}, 0) \sim (0, 1, 0) = \mathcal{O}.$$

$$\tilde{P} = \begin{cases} \mathcal{O}, & \text{iff } \upsilon(x) < 0, \\ (\pi(x) : \pi(y) : 1) & \text{otherwise.} \end{cases}$$

**Theorem**

*For all $n \in \mathbb{N}$: $E_n(\mathbb{Q}_p)/E_{n+1}(\mathbb{Q}_p) \cong \mathbb{Z}_p^+$.*

$$E_n(\mathbb{Q}_p)/E_{n+1}(\mathbb{Q}_p) \cong \hat{E}(p^n\widehat{\mathbb{Z}}_p)/\hat{E}(p^{n+1}\widehat{\mathbb{Z}}_p) \cong p^n\widehat{\mathbb{Z}}_p/p^{n+1}\widehat{\mathbb{Z}}_p \cong \mathbb{Z}_p^+.$$

Let $p$ be a prime number, $E$ be a non-singular cyclic elliptic curve in Weierstrass minimal form defined over field $\mathbb{Z}_p$, where $|E(\mathbb{Z}_p)| = p$. Let $P, Q \in E(\mathbb{Z}_p)$ and $P = [m]Q$, where $m \in \mathbb{N}$ and $[m]Q$ means $m \in \mathbb{N}$ times $Q$.

For input $p, E, P, Q$ we want to output a solution for DLP, $m$.

First of all we use, using Hensel's lemma, "British elevator"(lift) and lift up (once will be enough) y-coordinates of points $P, Q$ to $E(\mathbb{Q}_p)$. Let $\overline{y} = y + py_1$ then

$$x^3 + Ax + B - (y + py_1)^2 \equiv 0 \mod p^2,$$
$$2pyy_1 \equiv x^3 + Ax + B - y^2 \mod p^2.$$
$$y_1 \equiv \frac{x^3+Ax+B-y^2}{2y} \mod p.$$

**Theorem**

*For $Q \in E_n(\mathbb{Q}_p)$ and $n \geqslant 0$ mapping*

$$[p] : Q \mapsto [p]Q$$

*is mapping from $E_n(\mathbb{Q}_p)$ to $E_{n+1}(\mathbb{Q}_p)$.*

**Definition ($\psi$)**

Let $Q \in E_1(\mathbb{Q}_p)$ then define mapping $E_1(\mathbb{Q}_p) \to p\mathbb{Z}_p$,
$\psi_p((x, y)) \equiv -\frac{x}{y} + p^2\widehat{\mathbb{Z}}_p$.

**Example (Algorithm)**

Input: $\mathbb{Z}_{1019}$

$$E : y^2 = x^3 + 373x + 837$$
$$\tilde{P} = (293, 914), \tilde{Q} = (794, 329)$$
$$\text{and } [m]\tilde{P} = \tilde{Q}$$

Algorithm: We find the following lifts of these points to $E(\mathbb{Q}_{1019})$

$$P = (293, 914 + 308 * 1019), \; Q = (794, 329 + 561 * 1019.)$$

Those points belong to $E(\widehat{\mathbb{Z}}_p / p^2 \widehat{\mathbb{Z}}_p)$.

## Example (Algorithm)

Using the square and multiply algorithm we count 1019 multiple of lift points
$[1019]P = (867 * 1019^{-2} + 309 * 1019^{-1}, 950 * 1019^{-3} + 16 * 1019^{-2})$,
$[1019]Q = (210 * 1019^{-2} + 952 * 1019^{-1}, 300 * 1019^{-3} + 17 * 1019^{-2})$,
$[1019]P, [1019]Q \in E_1(\mathbb{Q}_{1019})$.
Now we compute image in $\mathbb{Z}_{1019}$
$\psi_{1019}([1019]P) = 367 * 1019 \mod 1019^2$,
$\psi_{1019}([1019]Q) = 305 * 1019 \mod 1019^2$,
and so

$$m = \frac{305}{367} \mod 1019 = 123.$$

# Questions?

Thank you for your attention!