D34: Méthodes de calcul efficaces et sécurisées

Nicolas Méloni

Master 2: 1er semestre
(2014/2015)

Arithmétique des courbes sur $\mathbb{F}_p$

Rappel

Une courbe elliptique peut être munie d'un structure de groupe commutatif. La somme $R = (x_3, y_3)$ de deux points $P = (x_1, y_1), Q = (x_2, y_2)$ s'obtient comme suit:

- $-P = (x_1, -y_1)$
- $x_3 = \lambda^2 - x_1 - x_2, y_3 = \lambda(x_1 - x_3) - y_1$ où

$$\lambda = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1} \text{ si } P \neq \pm Q \\ \frac{3x_1^2 + a}{2y_1} \text{si} P = Q \end{cases}$$

- L'inversion modulaire étant une opération très couteuse, on cherche un système de représentation des points permettant de l'éviter.

Définition

- On représente un point $P = (x, y)$ par un triplet $(X : Y : Z)$ vérfiant:
$$(X : Y : Z) \sim \left(\frac{X}{Z}, \frac{Y}{Z}\right) \text{ si } Z \neq 0$$
$$(0 : 1 : 0) \sim \mathcal{O}$$
- L'équation de la courbe devient alors:
$$Y^2Z = X^3 + aXZ^2 + bZ^3.$$
- Pour tout $\lambda \neq 0$, on a $(X : Y : Z) \sim (\lambda X : \lambda Y : \lambda Z)$.
- $-(X : Y : Z) = (X : -Y : Z)$.

Formules d'addition de points

- Soient $P_1 = (X_1 : Y_1 : Z_1)$, $P_2 = (X_2 : Y_2 : Z_2)$ et $P_3 = P_1 + P_2 = (X_3 : Y_3 : Z_3)$:

$$
\begin{aligned}
A &= Y_2 Z_1 - Y_1 Z_2, \\
B &= X_2 Z_1 - X_1 Z_2, \\
C &= A^2 Z_1 Z_2 - B^3 - 2B^2 X_1 Z_2, \\
X_3 &= BC, \\
Y_3 &= A(B^2 X_1 Z_2 - C) - B^3 Y_1 Z_2, \\
Z_3 &= B^3 Z_1 Z_2.
\end{aligned}
$$

- Cout total: $12\mathtt{M} + 2\mathtt{S}$

Formules de doublement de point

- Soient $P_1 = (X_1 : Y_1 : Z_1)$, $P_3 = [2]P_1$:

$$A = aZ_1^2 + 3X^2, \quad B = Y_1 Z_1,$$
$$C = X_1 Y_1 B, \qquad D = A^2 - 8C$$

$$X_3 = 2BD,$$
$$Y_3 = A(4C - D) - 8Y_1^2 B^2,$$
$$Z_3 = 8B^3$$

- Cout total: $7\mathtt{M} + 5\mathtt{S}$
- Amélioration: $5\mathtt{M} + 6\mathtt{S}$

Coordonnées Jacobiennes

Définition

- On représente un point $P = (x, y)$ par un triplet $(X : Y : Z)$ vérfiant:
$$(X : Y : Z) \sim \left(\frac{X}{Z^2}, \frac{Y}{Z^3}\right) \text{ si } Z \neq 0$$
$$(0 : 1 : 0) \sim \mathcal{O}$$
- L'équation de la courbe devient alors:
$$Y^2 = X^3 + aXZ^4 + bZ^6.$$
- Pour tout $\lambda \neq 0$, on a $(X : Y : Z) \sim (\lambda^2 X : \lambda^3 Y : \lambda Z)$.
- $-(X : Y : Z) = (X : -Y : Z)$.

Formules d'addition de points

- Soient $P_1 = (X_1 : Y_1 : Z_1)$, $P_2 = (X_2 : Y_2 : Z_2)$ et $P_3 = P_1 + P_2 = (X_3 : Y_3 : Z_3)$:

$$\begin{array}{lll} A = X_1 Z_1^2, & B = X_2 Z_1^2, & C = Y_1 Z_2^3, \\ D = Y_2 Z_1^3, & E = B - A, & F = 2(D - C), \\ G = (2E)^2, & H = EG, & I = AG. \end{array}$$

$$\begin{aligned} X_3 &= F^2 - H - 2I \\ Y_3 &= F(F - X_3) - 2CH, \\ Z_3 &= ((Z_1 + Z_2)^2 - Z_1^2 - Z_2^2)E \end{aligned}$$

- Cout total: $11\mathtt{M} + 5\mathtt{S}$

Formules de doublement de point

- Soient $P_1 = (X_1 : Y_1 : Z_1)$, $P_3 = [2]P_1$:

$$A = X_1 Y_1^2, \quad B = 3(X_1 - Z_1)^2 (X_1 + Z_1)^2$$

$$\begin{aligned} X_3 &= B^2 - 8A, \\ Y_3 &= -8Y_1^4 + B(4A - X_3), \\ Z_3 &= (Y_1 + Z_1)^2 - Y_1^2 - Z_1^2. \end{aligned}$$

- Cout total: $4\mathtt{M} + 6\mathtt{S}$
- Cout total: $1\mathtt{M} + 8\mathtt{S}$

Coordonnées mixtes

- Dans les deux systèmes de coordonnées précédents, un point (x, y) (coordonnées affines) est toujours équivalent au point $(x : y : 1)$.
- La somme d'un point quelconque et d'un point pour lequel $Z = 1$ et en général beaucoup plus efficace (ex: coord. Jac. $7\mathtt{M} + 4\mathtt{S}$).
- Si un point est amené à être réutilisé plusieurs fois lors du multiplication de point, il peut devenir intéressant de le convertir en coordonnées affines.

Coût d'un multiplication de point

Coord.	DBL	ADD	mADD	Dbl-and-Add M/bit
Aff.	2M+2S+I	2M+S+I	-	$3\mathtt{M}+\frac{5}{2}\mathtt{S}+\frac{3}{2}\mathtt{I}$
Proj.	5M+6S	12M+2S	-	11M+7S
Jac.	1M+8S	11M+5S	-	$\frac{13}{2}\mathtt{M}+\frac{21}{2}\mathtt{S}$
mJac.	1M+8S	11M+5S	7M+4S	$\frac{9}{2}\mathtt{M}+10\mathtt{S}$

TableCout moyen d'un multiplication de point en fonction de différents systèmes de coordonnées

Schéma de précalculs

Inversion multiple

- Soient $P_1 = (X_1 : Y_1 : Z_1), \ldots, P_r = (X_r : Y_r : Z_r)$ r points d'un CE.
- On pose $\alpha = (Z_1 Z_2 ... Z_r)^{-1}$.
- L'ensemble des $(Z_i)^{-1} = \alpha \prod_{j \neq i} Z_j$ peut être obtenu pour un cout total de: $\mathtt{I}+3(r-1)\mathtt{M}$

Schéma de précalculs

- On convertit le point $[2]P$ en coordonnées affine,
- on calcule les points $[3]P, \ldots, [2^w - 1]P$,
- on otient les inverses de $Z_3, \ldots, Z_{2^w-1}$ par inversion multiple,
- on convertit les points en coordonnées affine

Double bases chainées

Définition

Soit k un entier positif, on appelle représentation en base double de k toute écriture de k de la forme:

$$k = \sum_{i,j} a_{i,j} 2^i 3^j, \qquad a_{i,j} \in \{0, 1\}.$$

- Calculer une représentation efficace est difficile et couteux en temps de calcul

Double bases chainées

Définition

Soit k un entier positif, on appelle représentation en base double chain'ees de k toute écriture de k de la forme:

$$k = \sum_{i,j} 2^{b_i} 3^{t_i},$$

où (b_i) et (t_i) sont des suites décroissantes.

On peut alors écrire:

$$k = 2^{b_l} 3^{t_l} (2^{u_{l-1}} 3^{v_{l-1}} (\dots (2^{u_1} 3^{u_1} + 1) \cdots + 1) + 1)$$

où $\forall i \in \{1, \dots l-1\}$ $u_i = b_i - b_{i+1}$ et $v_i = t_i - t_{i+1}$.

Algorithm 1 Conversion cDBNS

Require: $k \in \mathbb{N}$

Ensure: $\texttt{cDBNS}(k)$

1: $i \leftarrow 0,$
2: **while** $k \leq 1$ **do**
3: **while** $k \mod 2 = 0$ **do** $k \leftarrow k/2, u_i \leftarrow u_i + 1$
4: **end while**
5: **while** $k \mod 3 = 0$ **do** $k \leftarrow k/3, v_i \leftarrow v_i + 1$
6: **end while**
7: $k \leftarrow k - 1,$
8: $i \leftarrow i + 1$
9: **end while**
10: **return** $((b_{i-1}, t_{i-1}) \dots (b_0, t_0))$ (où $b_j = \sum_{k \leq j} u_k$)

Algorithm 2 Multiplication de Point cBDNS

Require: $P \in E$ et $k = \sum_{i=1}^{l} c_i 2^{b_i} 3^{t_i} \in \mathbb{N}$.
Ensure: $[k]P \in E$.

1: $Q \leftarrow P$
2: **for** $i = 1 \dots l-1$ **do**
3: $\quad u_i \leftarrow b_i - b_{i+1}$, $v_i \leftarrow t_i - t_{i+1}$
4: $\quad Q \leftarrow [3^{v_i}]Q, Q \leftarrow [2^{u_i}]Q$
5: $\quad Q \leftarrow Q + P$
6: **end for**
7: $Q \leftarrow [3^{t_l}]Q$
8: $Q \leftarrow [2^{b_l}]Q$
9: **return** Q

Triplement de point

Formules de triplement de point

- Soient $P_1 = (X_1 : Y_1 : Z_1)$, $P_3 = [3]P_1$:

$$A = Y_1^4, \qquad B = 3X_1^2 + aZ_1^2,$$
$$C = 6((X_1 + Y_1^2)^2 - X_1^2 - Y_1^4) - B^2 \qquad D = 16Y_1^4$$
$$E = (B + C)^2 - B^2 - C^2 - D$$

$$X_3 = 4(X_1C^2 - 4Y_1^2E),$$
$$Y_3 = 8Y_1(E(16Y_1^4 - E) - C^3),$$
$$Z_3 = (Z_1 + C)^2 - Z_1^2 - C^2.$$

- Cout total: $5\mathtt{M} + 10\mathtt{S}$

Courbes de Montgomery

Définition

Soit $E(\mathbb{F}_p)$ une courbe elliptique, on dit que E est une courbe de Montgomery si elle est isomorphe à une courbe de la forme:

$$E_M : By^2 = x^3 + Ax^2 + x.$$

Théorème

Soit $E(\mathbb{F}_p) : y^2 = x^3 + ax + b$ une courbe elliptique, E est une courbe de Montgomery si et seulement si:

1. $x^3 + ax + b$ a au moins une racine α dans $\mathbb{F}_p$,
2. $3\alpha^2 + a$ est un carré dans $\mathbb{F}_p$.

Courbes de Montgomery

Formules d'addition de points

$$\begin{aligned} X_{m+n} &= Z_{m-n}((X_m - Z_m)(X_n + Z_n) + (X_m + Z_m)(X_n - Z_n))^2, \\ Z_{m+n} &= X_{m-n}((X_m - Z_m)(X_n + Z_n) - (X_m + Z_m)(X_n - Z_n))^2. \end{aligned}$$

Formules de doublement

$$\begin{aligned} 4X_nZ_n &= (X_n + Z_n)^2 - (X_n - Z_n)^2, \\ X_{2n} &= (X_n + Z_n)^2(X_n - Z_n)^2, \\ Z_{2n} &= 4X_nZ_n((X_n - Z_n)^2 + ((A+2)/4)(4X_nZ_n)). \end{aligned}$$

- Le triplet (X_i, Y_i, Z_i) représente le point $[i]P$
- Cout: $4\mathtt{M} + 2\mathtt{S}$ pour l'addition et $3\mathtt{M} + 2\mathtt{S}$ pour le doublement

Le triplet (X_i, Y_i, Z_i) représente le point $[i]P$.

Algorithm 3 Echelle de Montgomery

Require: $P \in E$ et $k = (k_{l-1} \dots k_0)_2 \in \mathbb{N}$.
Ensure: $[k]P \in E$.

1: $(P_1, P_2) \leftarrow (\mathcal{O}, P)$
2: **for** $i = l - 1 \dots 0$ **do**
3: **if** $k_i = 0$ **then**
4: $(P_1, P_2) \leftarrow ([2]P_1, P_1 + P_2)$
5: **else**
6: $(P_1, P_2) \leftarrow (P_1 + P_2, [2]P_2)$
7: **end if**
8: **end for**
9: **return** P_1