Chapitre 1

Rappels sur les corps finis

Les corps finis sont très utilisés en théorie des nombres, cryptographie, codage et codes correcteurs...
Nous rappelons dans ce chapitre les éléments essentiels de la théorie des corps finis.Pour les preuves des résultats, on pourra consulter les ouvrages de référence sur le sujet tels que [7],[6],[10],[11],[16],[26].

1.1 Caractéristique

Définition 1. *On appelle caractéristique d'un anneau A l'entier n tel que $n\mathbb{Z}$ soit le noyau du morphisme de groupes additifs suivant :*

$$\varphi : \left| \begin{array}{ccc} \mathbb{Z} & \longrightarrow & A \\ m & \longmapsto & \underbrace{1_A + 1_A + ... + 1_A}_{m} \end{array} \right.$$

Si l'anneau A est fini, n est nécessairement non-nul.
On montre que si A est intègre, n est nécessairement un nombre premier.

Proposition 1. *Un corps fini K a pour caractéristique un nombre premier p.*
Il contient en conséquence un sous-corps isomorphe à $\mathbb{F}_p$=$\mathbb{Z}/p\mathbb{Z}$.
Le corps K peut être vu comme un espace vectoriel sur $\mathbb{F}_p$, son cardinal est une puissance de p. [11 p 169]

Remarque 1. *Soit L une extension finie d'un corps K. On note $[L : K]$ la dimension de L en tant que K-espace vectoriel.*

Proposition 2. *Soit $K \rightarrow L \rightarrow M$ une tour d'extensions finies.On a :*

$$[M : K] = [M : L][L : K].[11p169]$$

Théorème 1. *(Wedderburn). Tout corps fini est commutatif. [11 p 170]*

1.2 Construction des corps finis

Un corps de cardinal premier étant égal à son sous-corps premier, il s'ensuit que tous les corps de cardinal premier p sont isomorphes à $\mathbb{F}_p$.

Proposition 3. *Soit p un nombre premier.*
Soit P un polynôme irréductible de $\mathbb{F}_p[X]$. Alors l'anneau quotient $K = \mathbb{F}_p[X]/(P)$ peut être muni d'une structure de corps commutatif, de cardinal p^{degP}.[16p5]

1.3 Le groupe multiplicatif

Nous arrivons à la propriété essentielle de structure des groupes multiplicatifs des corps finis.

Proposition 4. *Tout sous-groupe fini du groupe multiplicatif d'un corps est cyclique. [16 p 1]*

Proposition 5. *(Frobenius)*
1. Soit K un corps fini de cardinal $q = p^s$. Soit $x \in K$, alors $x^q = x$.
2. Soit L une extension de degré n de K. L'application :

$$\sigma : \left| \begin{array}{ccc} L & \longrightarrow & L \\ x & \longmapsto & x^q \end{array} \right.$$

est un automorphisme de corps fixant K.De plus, $\sigma^n = Id_L$.
σ est qppelée l'automorphisme de Frobenius. [11 p171]

Lemme 1. *Soit K une extention de degré n d'un corps F de cardinal q . Alors il existe un polynôme P tel que K est isomorphe à $F[X]/(P)$. [7 p9],[16 p6]*

Remarque 2. *Deux corps finis de même cardinal sont nécessairement isomorphes.*

1.4 Nombre de polynômes irréductibles sur $\mathbb{F}_p$

Proposition 6. *Le polynôme $X^{q^n} - X \in \mathbb{F}_q[X]$ est le produit de tous les polynômes irréductibles de $\mathbb{F}_q[X]$ de degré divisant n. [7 P9],[11],[16 P9]*

Définition 2. *.(Fonction de Möbius). On note μ l'application telle que $\mu : \mathbb{N}^* \to \mathbb{N}$ définie par :*

$$\begin{cases} \mu(1) = 1 \\ \mu(n) = 0 \text{ ; s'il existe un indice i tel que } \alpha_i \geq 2 \\ \mu(n) = (-1)^k \text{ ; sinon} \end{cases}$$

où $n = p_1^{\alpha_1} p_2^{\alpha_2} ... p_k^{\alpha_k}$ représente la décomposition en facteurs premiers de n avec $\alpha_i \geq 1$ pour tout i . μ est appelée fonction de Möebius.
Cette fonction μ vérifie la propriète suivante :

Proposition 7. *(Formule de Möebius)*
1. $\forall\ m,n \in \mathbb{N}^*$ *; m et n premiers entre eux* $\Rightarrow \mu(nm)=\mu(n)\mu(m)$
2. Si f et g sont deux fonctions de $\mathbb{N}^*$ *dans* $\mathbb{C}$ *telles que :*

$$\forall n \in \mathbb{N}^* \ ; f(n)=\sum_{d|n} g(d)$$

alors g s'obtient à partir de f par la formule suivante :

$$\forall n \in \mathbb{N}^* \ ; g(n)=\sum_{d|n} f(d)\mu(\frac{n}{d}) \quad \texttt{[11 p 173]}$$

Proposition 8. *(Formule d'inversion de Möebius)*
1) ***Version additive*** *:*
Si (G,+) est un groupe additif, et si f et g sont des fonctions de $\mathbb{N}$ *dans G, alors*

$$g(n)=\sum_{d|n} f(d) \Longleftrightarrow f(n)=\sum_{d|n} g(d)\mu(\frac{n}{d})$$

2) ***Version multiplicative*** *:*
Si (G,.) est un groupe multiplicatif, et si f et g sont des fonctions de $\mathbb{N}$ *dans G, alors*

$$g(n)=\prod_{d|n} f(d) \Longleftrightarrow f(n)=\prod_{d|n} g(d)^{\mu(\frac{n}{d})}. \quad \texttt{[7 p9]}$$

Proposition 9. *Si* $I_q(n)$ *désigne le nombre de polynômes irréductibles unitaires de degré n sur* $\mathbb{F}_q$*, pour n* $\in \mathbb{N}^*$ *On a :*
1. $q^n=\sum_{d|n} dI_q(d)$
2. $I_q(n)=\frac{1}{n}\sum_{d|n} q^d\mu(\frac{n}{d})$ *. [7 p9],[16 p5]*

Définition 3. *Soit* $P(X)=X^n-\sum_{k=1}^{n} a_{n-k}X^{n-k}$ *un polynôme à coefficients dans K . La matrice M d'ordre n définit par :*

$$M=\begin{bmatrix} 0 & 1 & 0 & \dots & \dots & 0 \\ \vdots & \ddots & \ddots & \ddots & & \vdots \\ \vdots & & \ddots & \ddots & \ddots & \vdots \\ \vdots & & & \ddots & \ddots & 0 \\ 0 & \dots & \dots & \dots & 0 & 1 \\ a_0 & a_1 & a_2 & \dots & a_{n-2} & a_{n-1} \end{bmatrix}$$

est appelée matrice compagnon du polynôme P, (ou selon certains ouvrages, sa transposée).

1.5 Représentation des éléments d'un corps fini

Soit $\mathbb{F}_q$ le corps fini à q éléments. Il y a plusieurs manières de représenter les éléments du corps $\mathbb{F}_q$.

1.5.1 Représentation polynomiale

Si $q = p^d$ alors il existe un polynôme irréductible unitaire P de degré d sur $\mathbb{F}_q$ tel que :

$$\mathbb{F}_q \approx \mathbb{F}_p[X]/(P)$$

Donc, si α racine de P alors :

$$\mathbb{F}_q = \mathbb{F}_p[\alpha]$$

1.5.2 Représentation multiplicative

Soit α une racine primitive de P.Alors :

$$\mathbb{F}_q = \{0, 1, \alpha, \alpha^2, ..., \alpha^{q-2}\}$$

1.5.3 Représentation matricielle

Soit C la matrice compagnon associée à P. Alors :

$$\mathbb{F}_q = \mathbb{F}_p[C]$$

1.5.4 Représentation en base p

Les éléments de $\mathbb{F}_q$ $(q = p^d)$ peuvent être représentés comme une chaîne de chiffres en base p ; chaque élément u sera noté $[u_{d-1}u_{d-2}.....u_1u_0]_p$.

1.5.5 Exemple

Soit sur $\mathbb{F}_3$ le polynôme irréductible $P(X) = X^2 + X + 2$.
La matrice compagnon associée à P est $C = \begin{pmatrix} 0 & 1 \\ 1 & 2 \end{pmatrix}$.
La représentation matricielle de $\mathbb{F}_3$ est :

$$\mathbb{F}_3 = \{0, I, 2I, C, 2C, C + I, C + 2I, 2C + I, 2C + 2C\}.[17]$$

1.5.6 Exemple de Table Logarithmique

Tout élément non nul de $\mathbb{F}_{16}$ *est une puissance de* α*, où* α *est une racine primitive du polynôme irréductible sur* $\mathbb{F}_{16}$ *donné par :*$P(X) = X^4 + X + 1$
$\alpha = 0010$:

i	*Code* α^i
0	*0001*
1	*0010*
2	*0100*
3	*1000*
4	*0011*
5	*0110*
6	*1100*
7	*1011*
8	*0101*
9	*1010*
10	*0111*
11	*1110*
12	*1111*
13	*1101*
14	*1001*
15	*0001*

Si on pose $log_\alpha \beta = k$ *alors* $\beta = \alpha^k$*, nous construisons la table suivante :*

$log_\alpha \beta = k$	β
	0000
0	*0001*
1	*0010*
2	*0100*
3	*1000*
4	*0011*
5	*0110*
6	*1100*
7	*1011*
8	*0101*
9	*1010*
10	*0111*
11	*1110*
12	*1111*
13	*1101*
14	*1001*

Pour calculer [1100].[1110], nous regardons dans la table logarithmique $log_\alpha[1100] = 6$ *et* $log_\alpha[1110] = 11$ *; on a :*

$$[1100].[1110] = \alpha^{17} = \alpha^2 = [0100]$$

.

Chapitre 2

Courbe Elliptique

2.1 Définition D'une Courbe Elliptique

Définition 4. *Une courbe elliptique E (définie sur un corps K), notée E(K), est une courbe projective non singulière de genre 1 qui possède un point K-rationnel* Ω .
Toute courbe elliptique E(K) est donnée par l'équation de Weierstrass :

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3$$

où $a_i \in K$ *; i=1,2,3,4,6 .*
On utilisant les coordonnées homogènes $(x = \frac{X}{Z}; y = \frac{Y}{Z})$*, on obtient avec ces nouvelles coordonnées une équation de la forme :*

$$(*)y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

Le point $\Omega[0, 1, 0]$ *est le point à l'infini. [10],[17],[22],[25]*
Schéma de la courbe elliptique d'équation :

$$y^2 = x^3 + 45x + 76$$

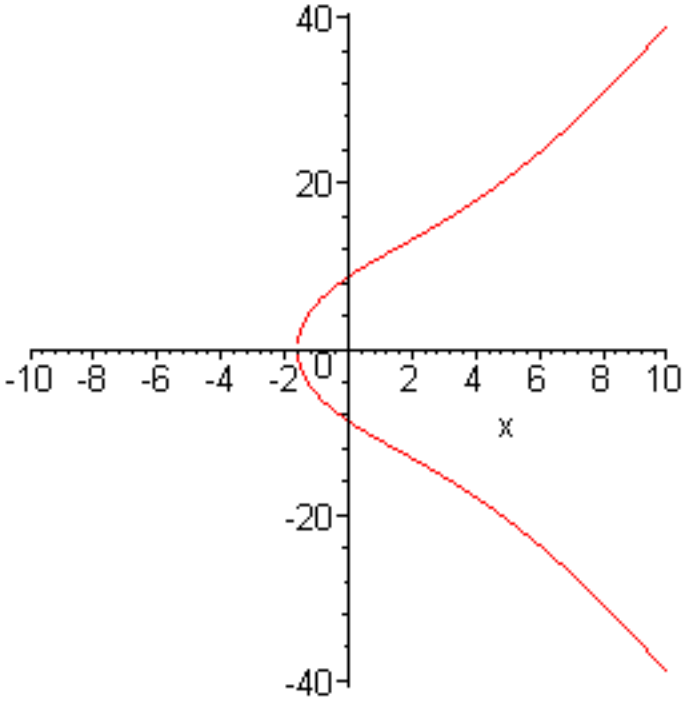
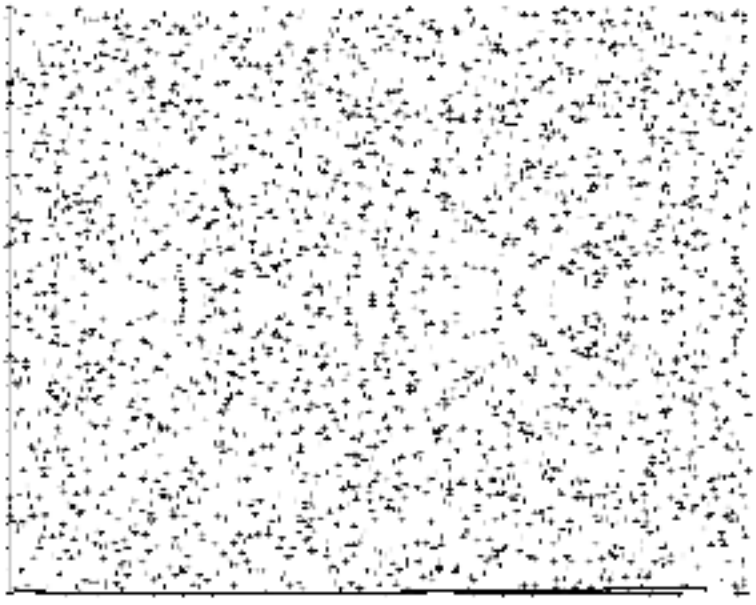


Schéma d'une courbe elliptique sur $\mathbb{Z}/P\mathbb{Z}$ ***:***



Exemple 1. *Soit la courbe elliptique E d'équation* $E : y^2 = x^3 - 4x^2 + 16$.
Alors : $E(\mathbb{Q}) = \{\Omega, (0;4), (0;-4), (4;4), (4;-4)\}$.
Cependant, $E(\mathbb{Q}(\sqrt{-2}))$ *contient un nombre infini de points.*
Donc le nombre de points de E(K) dépend du corps K.

Notations 1. $b_2 = a_1^2 + 4a_2$
$b_4 = 2a_4 + a_1a_3$
$b_6 = a_3^2 + 4a_6$
$b_8 = a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2$
$c_4 = b_2^2 - 24b_4$
$\triangle = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6$
Si $\triangle \neq 0$ *alors on pose* $j = \dfrac{c_4^3}{\triangle}$

Proposition 10. *Une courbe E d'équation* $(*)$ *est non-singulière si et seulement si* $\triangle \neq 0$*, dans ce cas j est appelé le j-invariant de E, on le note j(E).*
$\triangle$ *est appelé le discriminant de E.*

Remarque 3. *Dans le cas où* $a_1 = a_3 = a_2 = 0$ *; on a :* $\triangle = -2^4(27a_6^2 + 4a_4^3)$

Exemple 2. *(*$p = 2; p = 3$*)*

p	$j(E)$	E	$\triangle$	$j(E)$
2	*0*	$y^2 + cy = x^3 + ax + b$	c^4	*0*
2	$\neq 0$	$y^2 + xy = x^3 + ax^2 + b$	a	$\frac{1}{a}$
3	*0*	$y^2 = x^3 + ax + b$	$-a^3$	*0*
3	$\neq$ *0*	$y^2 = x^3 + ax^2 + b$	$-a^3b$	$\frac{-a^3}{b}$

2.2 Loi de groupe explicite

Soit la courbe elliptique E d'équation de Weierstrass (E) :

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3$$

Proposition 11. *Soient* $M(x_1, y_1)$,$N(x_2, y_2)$*et* $R(x_3, y_3)$ *trois points de la courbe* (E) *tels que R=N+M. Alors :*
1) $R = \Omega$ *pour* $x_1 = x_2$ *et* $y_2 = -y_1 - a_1x_1 - a_3$
2) $x_3 = t^2 + a_1t - a_2 - x_1 - x_2$ *et* $y_3 = -(t + a_1)x_3 - s - a_3$ *avec :*

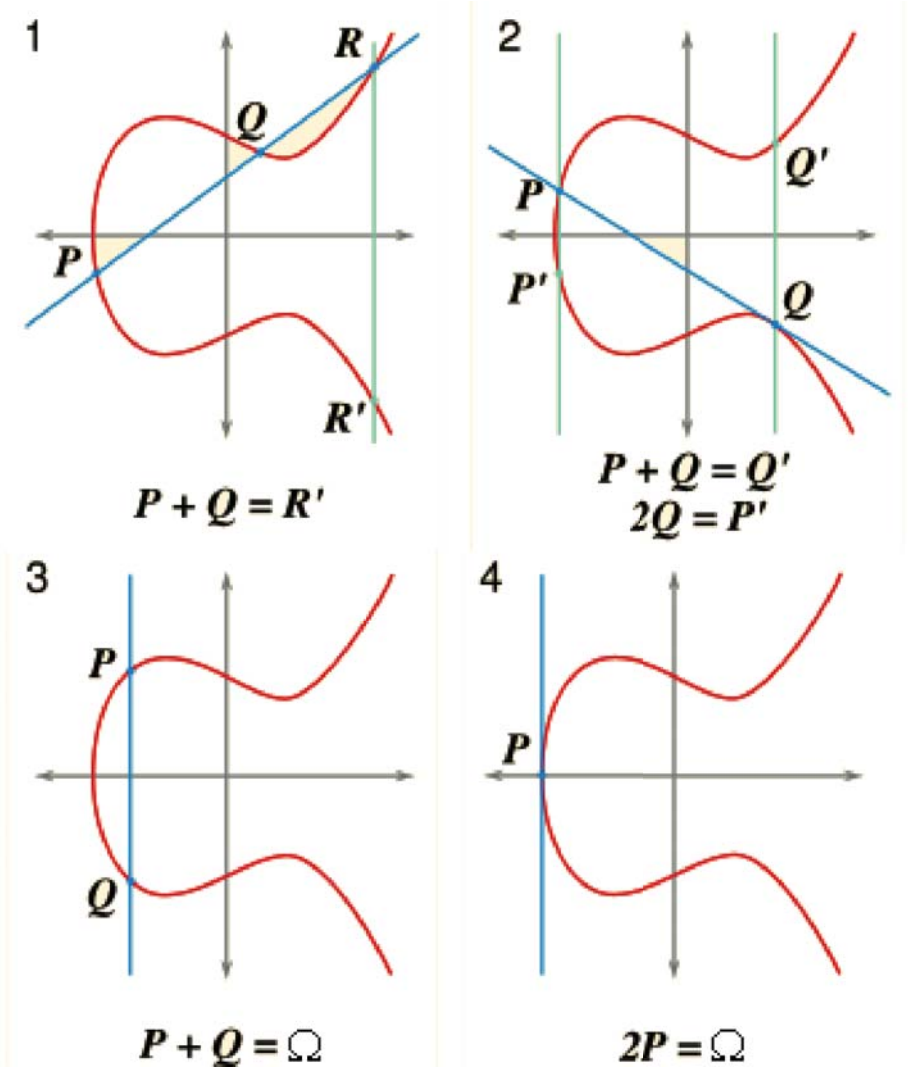
$$t = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1}; \texttt{si } M \neq N \\ \frac{3x_1^2 + 2a_1x_1 + a_4 - a_1y_1}{2y_1 + a_1x_1 + a_3}; \texttt{si } M = N \end{cases}$$

$$s = \begin{cases} \frac{y_1x_2 - y_2x_1}{x_2 - x_1}; \texttt{si } M \neq N \\ \frac{-x_1^3 + a_4x_1 + 2a_6 - a_3y_1}{2y_1 + a_1x_1 + a_3}; \texttt{si } M = N \end{cases}$$

La droite (MN) est d'équation $Y = tX + s$*.[17 p48],[22 p6]*

Démonstration: Soit $R = -S$.
Si S(x, y) alors R$(x, -y - a_1x - a_3)$.
Il suffit de trouver le troixième point S d'intersection de la droite (MN) avec la courbe (E), S vérifie $R + S = \Omega$.
Donc $R = -S$, d'où le résultat. ■

Schéma de la somme de deux points d'une courbe elliptique :



Remarque 4. *La proposition 2 définit une loi additive commutative sur le groupe E(K), dont Ω joue le rôle de l'élément neutre. On dit que les courbes elliptiques sont des variétés abéliennes de dimension un .*

2.3 Isogénie

Définition 5. *(Isogénie)*
Soient E et $E^{'}$ deux courbes elliptiques. Une isogénie entre E et $E^{'}$ est un morphisme non nul $\phi : E \to E^{'}$ satisfaisant $\phi(\Omega) = \Omega^{'}$.
Les courbes E et $E^{'}$ sont dites isogènes s'il existe une isogénie entre elles.

Exemple 3. *Soit E une courbe elliptique.*

Pour chaque $m \in \mathbb{Z} - \{0\}$, l'application multiplication par m est définie par :

$$[m]: \left| \begin{array}{ccc} E & \longrightarrow & E \\ P & \longmapsto & mP \end{array} \right.$$

est une isogénie.
Si $m > 0$, alors $mP = \underbrace{P + P + ... + P}_{m}$.
Si $m < 0$, alors $mP = -m(-P)$.

Définition 6. *Soit $E(K)$ une courbe elliptique et soit $Q \in E(K)$.*
L'application translation par Q est définie par :

$$\tau_Q : \left| \begin{array}{ccc} E & \longrightarrow & E \\ P & \longmapsto & P+Q \end{array} \right.$$

Remarque 5. *L'application τ_Q est un automorphisme de E d'inverse τ_{-Q}, mais elle n'est pas une isogénie sauf pour $Q = \Omega$.*

Proposition 12. *Tout morphisme φ entre les courbes elliptiques E et E' peut s'écrire comme une composition d'une isogénie et d'une translation. [25 p5]*

Démonstration: Soit

$$\varphi : E \to E'$$

un morphisme entre les courbes elliptiques E et E' .
Alors, l'application

$$\phi = \tau_{-\varphi(\Omega)} o \varphi$$

est une isogénie entre E et E' car $\phi(\Omega) = \Omega'$.
Le morphisme φ peut donc s'écrire :

$$\varphi = \tau_{\varphi(\Omega)} o \phi$$

■

Remarque 6. *Si ϕ est une isogénie de E dans E', alors c'est un homomorphisme de groupe de $(E, +)$ dans $(E', +)$.*

Définition 7. *Le noyau d'une isogénie $\phi : E \to E'$ est donc un sous-groupe fini de E. On appelle degré de ϕ l'orde de $Ker\phi$.*

Notation 1. *Si E une courbe elliptique définie sur K, on notera $E(m)$ le noyau de $[m]$ défini sur $\overline{K}$: la clôture algébrique de K.*

Définition 8. *(Isogénie Duale)*
Soit $\phi : E \to E'$ une isogénie de degré m. Alors il existe une unique isogénie $\widehat{\phi} : E' \to E$ telle que $\widehat{\phi} \circ \phi = [m]_{E'}$. On l'appelle isogénie duale de ϕ.

Théorème 2. *Deux courbes elliptiques sont isogènes sur $\mathbb{F}_q$ si et seulement si elles ont même nombre de points. [22 p13]*

Théorème 3. *Deux courbes elliptiques sont isomorphes si et seulement si elles ont le même j-invariant. [22 p14]*

Théorème 4. *Soit $E(K)$ une courbe elliptique sur le corps fini $K = \mathbb{F}_q$. Alors le groupe $(E(K), +)$ est ou bien cyclique, ou bien isomorphe à $\mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z}$ avec $n_2 \mid (n_1 \wedge p-1)$ et caractK $= p$. [22 p14]*

Théorème 5. *(Hasse)*
Soit p un nombre premier. Si $E(\mathbb{F}_p)$ est une courbe elliptique de cardinalité t définie sur le corps fini $\mathbb{F}_p$ alors :

$$\mid p+1-t \mid \leq 2\sqrt{p}$$

On trouvera une démonstration de ce théorème dans [22 p8],[25 p9]

Remarque 7. *Deuring a montré que pour tout entier premier p, pour tout entier t compris entre $p+1-2\sqrt{p}$ et $p+1+2\sqrt{p}$, il existe une courbe elliptique $E(\mathbb{F}_p)$ de cardinal t.*

2.4 Exemple

Soit E la courbe elliptique sur $\mathbb{Z}_7$ d'équation :

$$y^2 = x^3 + 3x + 2$$

on a :

$$E = \{\Omega, [0,3], [0,4], [2,3], [2,4], [4,1], [4,6], [5,3], [5,4]\}$$

Soit la courbe elliptique $E(\mathbb{F}_8)$ d'équation :

$$y^2 + y = x^3 + 1$$

On a :

$E' = \{\Omega', [1,0], [1,1], [\alpha, \alpha^2], [\alpha, \alpha^2+1], [\alpha^2, \alpha^2+\alpha], [\alpha^2, \alpha^2+\alpha+1], [\alpha^2+\alpha, \alpha], [\alpha^2+\alpha, \alpha+1]\}$.

E et E' sont isogènes.

Définition 9. *Soit la courbe elliptique $E(\mathbb{F}_p)$ d'équation de Weierstrass*

$$(E) : Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6.$$

Alors, si t_i, $1 \leq i \leq 7$ sont des nombres rationnels de dénominateurs premiers avec p, la courbe $E(\mathbb{Q})$ définie par :

$$(1+pt_1)Y^2+(a_1+pt_2)XY+(a_3+pt_3)Y = (1+pt_4)X^3+(a_2+pt_5)X^2+(a_4+pt_6)X+a_6+pt_7$$

vérifie :

$$E(\mathbb{Q}) \equiv E(\mathbb{F}_p) \ \texttt{mod p}.$$

$E(\mathbb{F}_p)$ est dite plongée dans $E(\mathbb{Q})$. [3]

Remarque 8. *Si on veut plonger un point $P(x, y)$ de $E(\mathbb{F}_p)$ dans un point $Q(u, v)$ de $E(\mathbb{Q})$. On écrit $Q[r, s, t]$ dans le projectif avec : $r = x + px^{'}$; $s = y + py^{'}$; $t = 1 + pt^{'}$ puis, on détermine $x^{'}$; $y^{'}$; $t^{'}$ tel que $Q[r, s, t]$ soit un point de $E(\mathbb{Q})$.*

2.5 Accouplement de Weil

Soit ξ_l le groupe des racines l^{ieme} de l'unité . L'accouplement e_l de Weil est défini par [13],[25] :

$$e_l : E[l] \times E[l] \longrightarrow \xi_l$$

a) bilinéaire :

$$e_l(P + Q, R) = e_l(P, R)e_l(Q, R)$$
$$e_l(P, Q + R) = e_l(P, Q)e_l(P, R)$$

b) alternée :

$$e_l(P, P) = 1$$
$$e_l(P, Q) = e_l(Q, P)^{-1}$$

c) invariance par l'action de Galois, pour tout $\sigma \in Gal(\overline{\mathbb{Q}}/\mathbb{Q})$:

$$e_l(P, Q)^{\sigma} = e_l(P^{\sigma}, Q^{\sigma})$$

Soit $E(\mathbb{Q})$ une courbe elliptique sur $\mathbb{Q}$, $E(l) = ker[l]$ est un sous-groupe de $E(\overline{\mathbb{Q}})$. On a l'automrphisme p_l^E définie par :

$$\begin{array}{ccccccc} p_l^E : Gal(\overline{\mathbb{Q}}/\mathbb{Q}) & \longrightarrow & Aut(E(l)) & & & & \\ \sigma & \longmapsto & \sigma_E : & E(n) & \longrightarrow & E(n) \\ & & & P & \longmapsto & P^{\sigma} \end{array}$$

Proposition 13. $E(l) \simeq (\mathbb{Z}/l\mathbb{Z})^2$.

Démonstration: Losque la courbe E est considérée sur le corps $\mathbb{C}$, $E(\mathbb{C}) \simeq \mathbb{C}/L$ où L est un réseau [25 p23] :

$$L = \mathbb{Z}w_1 + \mathbb{Z}w_2.$$

L'isomorphisme entre $(\mathbb{Z}/l\mathbb{Z})^2$ et $E(l)$ est alors donné par :

$$(a, b) \longmapsto \frac{a}{l}w_1 + \frac{b}{l}w_2$$

Exemple 4. *Soit la courbe elliptique E d'équation : $y^2 = x^3 - x^2 + x - 1$*
On a :

$$E(2) = \{\Omega, (1, 0), (i, 0), (-i, 0)\}$$

On pose $P = (1, 0)$; $Q = (i, 0)$, on a $\{P, Q\}$ est une base de $E(2)$.
Soit $\sigma \in Gal(\mathbb{Q}(i)/\mathbb{Q})$.On a :

$$Gal(\mathbb{Q}(i)/\mathbb{Q}) = \{\sigma_0, \sigma_1\}$$

$$P^{\sigma_1} = (1^{\sigma_1}, 0^{\sigma_1}) = P$$

$$Q^{\sigma_1} = (i^{\sigma_1}, 0^{\sigma_1}) = (-i, 0) = P + Q$$

et donc :

$$\sigma_0 \longrightarrow \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$\sigma_1 \longrightarrow \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

d'où, $p_2^E : Gal(\mathbb{Q}(i)/\mathbb{Q}) \longrightarrow Aut(E(2))$

$$p_2^E(\sigma_0) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}; p_2^E(\sigma_1) = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

Chapitre 3

Logarithme discret et cryptographie

3.1 Fonction à sens unique

Définition 10. *Une fonction $f : X \to Y$, est dite à sens unique si :*
1) $\forall x \in X$, $f(x)$ est calculable en temps polynomial.
2) Pour presque tout $y \in Im(f)$, il est infaisable de façon calculatoire de trouver $x \in X$ tel que $f(x) = y$. [6p51]

Définition 11. *Une fonction $f : X \to Y$, est dite à sens unique avec trappe si :*
1) f est à sens unique.
2) Connaissant une information supplémentaire appelée trappe, le calcul pour tout $y \in Im(f)$, de $x \in X$ tel que $f(x) = y$ est réalisable en temps polynomial. [6p53]

3.2 Exemple

3.2.1 L'exponentiation modulaire

L'exponentiation modulaire, appelée aussi exponentielle discrète, est une fonction à sens unique est définie par :

$$f: \left| \begin{array}{ccc} \mathbb{Z}_p^\star & \longrightarrow & \mathbb{Z}_p^\star \\ x & \longmapsto & \alpha^x \end{array} \right.$$

où α est choisi de préférence primitif pour que f soit bijective.
Tous les algorithmes connus pour inverser cette fonction, nécessitent un temps de calcul non polynomial en $log(p)$. [6p53]

3.2.2 L'application f_P

Soit E une courbe elliptique. Pour chaque $P \in E$ d'orde q, l'application f_P est une fonction à sens unique est définie par :

$$f_P : \left| \begin{array}{ccc} \mathbb{Z}_q^\star & \longrightarrow & < P > \\ m & \longmapsto & mP \end{array} \right.$$

Il est praticable de calculer $Q = f_P(m)$, mais étant donné $Q \in < P >$ il est deficile de trouver m tel que $Q = f_P(m)$.

3.3 Cryptographie

La cryptographie moderne, fondée sur les fonctions à sens unique, a trente ans. Nous nous accordons en effet à identifier sa date de naissance à la parution du célèbre article de Whitfeld Diffie et Martin Hellman en 1976 (New Directions in Cryptography). Cet article annonçait les idées fondamentales de chiffrement à clé publique et de signature éléctronique qui ont incontestablement structuré la recherche qui a suivi, ces trente années ont été riches en découvertes, innovations, et progrès techniques dont certains étaient décisifs. L' un des hauts faits de la courte histoire de la cryptographie mathématique dite moderne est la mise au point du premier système à clé publique RSA, puis la cryptographie elliptique , Diffie et Hellman ont proposé une solution élégante permettant à deux individus d'échanger une information secrète, c'est le cryptosystéme de Diffie et Hellman.

Définition 12. *Un système cryptographique est la donnée d'un 5-uplet (P,C,K,E,D)vérifiant :*

1) P est un ensemble fini de blocs de texte clairs possibles.

2) C est un ensemble fini de blocs de texte chiffrés possibles.

3) K que l'on appelle espace des clefs est un ensemble fini de clefs possibles.

4) $\forall k \in K$, $\exists$ une fonction de chiffrement e_k et une fonction de déchiffrement d_k avec :

$$e_k : \left| \begin{array}{ccc} P & \longrightarrow & C \\ m & \longmapsto & e_k(m)=c \end{array} \right.$$

$$d_k : \left| \begin{array}{ccc} C & \longrightarrow & P \\ c & \longmapsto & d_k(c)=m \end{array} \right.$$

Et $d_k \circ e_k(m) = m$; $\forall m$ texte clair de P. [2]

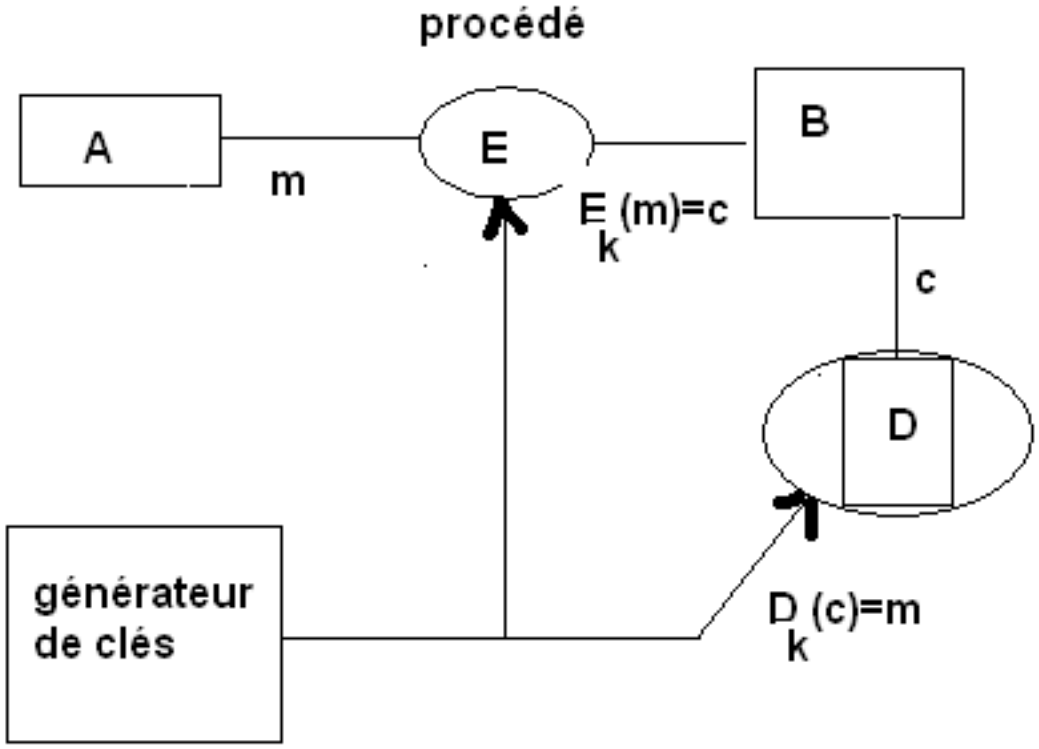


schéma classique d'un cryptosystéme

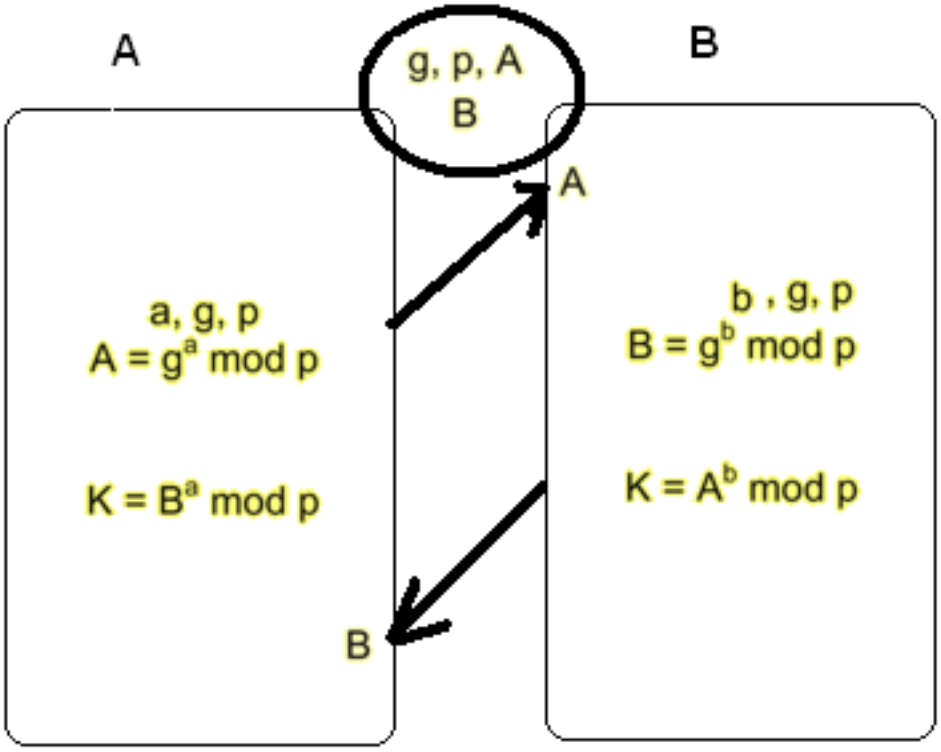
3.3.1 Principe de Diffie-Hellman

Soient deux entités A et B qui veulent échanger de l'information entre elles sans qu'aucune autre personne n'ait la possibilité de s'emparer de leur message.

Version multiplicative :

Un groupe cyclique public G est fixé ainsi qu'un générateur public g de ce groupe.
A et B vont construire une clé commune k, pour cela A choisit un entier n plus petit que l'ordre de G, de même B choisit un entier m plus petit que l'ordre de G.
A calcule g^n *et le transmet à B qui calcule* g^m *et le transmet à A.*
En fin, A et B calculent leur clé secrète $k = g^{nm}$.

Schéma multiplicatif :



Définition 13. *On se donne un groupe G noté multiplicativement et g un élément de G. Soit f_1 l'homomorphisme de groupes défini par :*

$$f_1 : \left| \begin{array}{ccc} \mathbb{Z} & \longrightarrow & G \\ m & \longmapsto & g^m \end{array} \right.$$

Cette applicatiom induit un isomorphisme f de $\mathbb{Z}/ord(g)\mathbb{Z}$ dans $< g >$.
Le morphisme réciproque f^{-1} est appelé logarithme discret en base g. [20p7]

Notation 2.

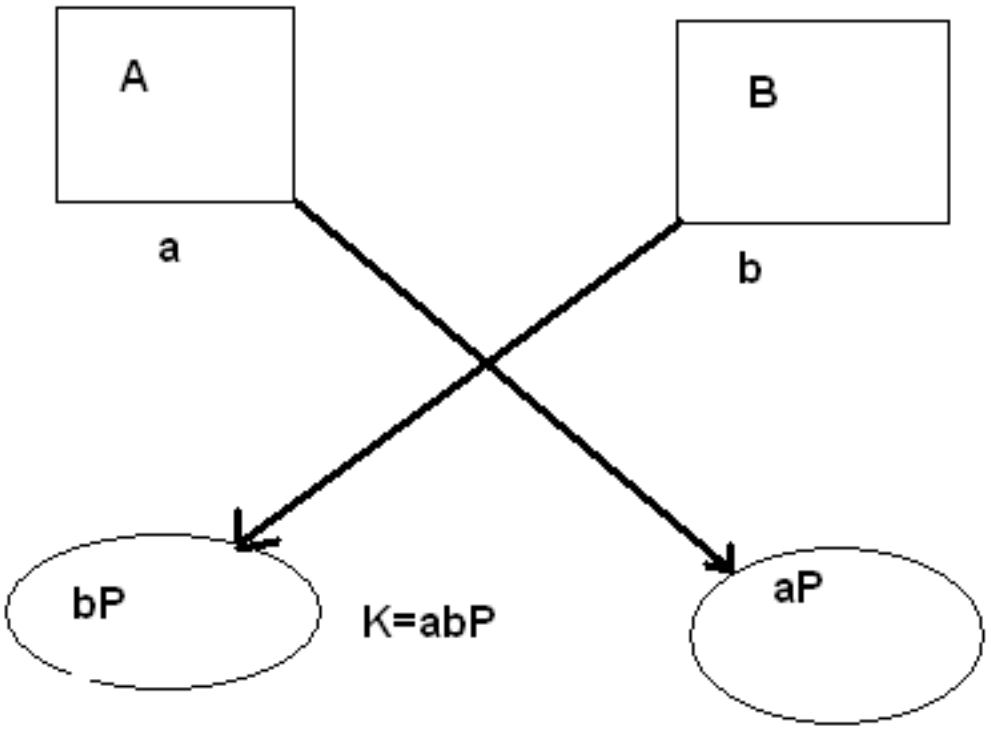
$$s = g^m \Leftrightarrow m = log_g s$$

Version additive :

Une courbe elliptique E est choisie publiquement, ainsi q'un point P de cette courbe.
A choisit un entier n plus petit que l'ordre de $< P >$ de même B choisit un entier

m plus petit que l'ordre de $< P >$.
A calcule nP et le transmet à B qui calcule mP et le transmet à A.
En fin, A et B calculent leur clé secrète $K = nmP$.

Schéma additif :



Remarque 9. *La fonction réciproque de f_P est appelée logarithme discret.*

Notation 3.

$$Q = mP \Leftrightarrow m = log_P Q$$

Remarque 10. *La sécurité du systéme Diffie-Hellman est calculatoire.*
Elle repose sur deux hypothèses :
1) la puissance du calcul de l'opposant.
2) Il n'est pas possible de résoudre le problème du logarithme discret dans un temps polynomial, d'où le choix du groupe G (Groupe générique).

Groupe générique :

Définition 14. *Pour un groupe fini G de cardinal n, on fait les hypothèses minimales suivantes : On suppose qu'il existe un entier $\alpha \geq 0$ tel que :*
1) Les éléments de G sont représentés de façon unique sur $O((logn)^{\alpha})$ bits.
2) Les opérateurs dans le groupe se calculent en $O((logn)^{\alpha})$.
3) Le cardinal du G est connu.
Un tel groupe est dit groupe générique.[11p19]

3.3.2 Principe d'ElGamal Tahar

Version multiplicative :

Soit p un nombre premier trés grand, dit nombre premier cryptographique, tel que le problème du logarithme discret dans $\mathbb{Z}_p^{\star}$ soit difficile à déterminer.
Soit α un élément primitif.
$\mathcal{P} = \mathbb{Z}_p^{\star}$ l'espace des textes clairs.
$\mathcal{C} = \mathbb{Z}_p^{\star} \times \mathbb{Z}_p^{\star}$ l'espace des textes chifrés.
$\mathcal{K} = \{(p, \alpha, \beta, s)/\beta = \alpha^s[p]\}$ l'espace des biclefs clé publique $(p; \alpha; \beta)$, clé sucrète (s).
Pour $K = (p, \alpha, \beta, s)$ et pour un nombre aléatoire secret $l \in \{0, 1, 2....., p-1\}$ on définit :
i) La fonction de chiffrement $e_K(m, l) = (c_1, c_2)$ où $c_1 = \alpha^l[p]$ et $c_2 = m.\beta^l[p]$
ii)La fonction de déchiffrement $d_K(c_1, c_2) = c_2.c_1^{-s} = m[p]$

Remarque 11. *L'opération de chiffrement dans le système d'ElGamal est probabiliste puisque le texte chiffré dépend à la fois du message clair m et de la valeur aléatoire l choisie par l'entité A (l'expéditeur). Le chiffrement d' ElGamal fonctionne comme suit : Le texte clair m est masqué en le multipliant par β^l ce qui donne une partie c_2 du texte chiffré . La valeur donne une deuxième partie du texte chiffré ainsi (c_1, c_2) est transmis au destinataire B qui est le seul à connaître $s = log_{\alpha}\beta$, qui est la clé privée, B peut calculer facilement β^l à partir de α^l, il suffit de calculer $\beta^l = \alpha^{ls}$, ensuite il peut retirer le masque du message m en divisant c_2 par c_1^s.*

Version additive :

Soit P un Point rationnel d'ordre n d'une courbe elliptique $E(\mathbb{F}_q)$ et R un autre point de $E(\mathbb{F}_q)$.
Le cryptosystème d'ElGamal s'adapte également à ce type de problèmes. Les paramètres sont :
1) $\mathcal{K} = (P, a, R)$ avec $R = aP$.
2) On prend $l \in \{0, 1, 2....., n-1\}$ au hasard, la fonction de chiffrement est :

$$e_{\mathcal{K}}(X) = (Y, Z)$$

avec

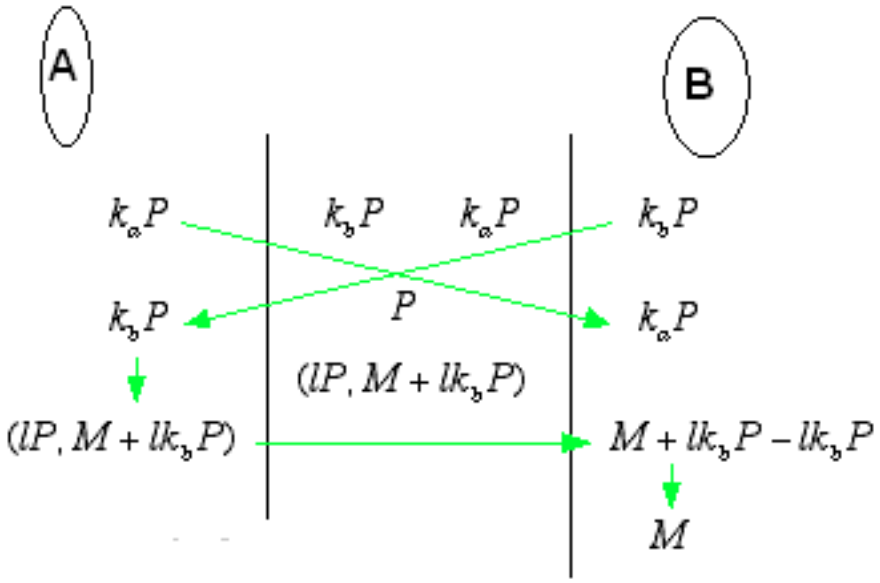
$$Y = lP$$

$$Z = lR + X$$

3) La fonction de déchiffrement est :

$$d_{\mathcal{K}}(Y, Z) = Z - aY$$

Schéma additif *:*



Remarque 12. *En pratique cet algorithme n'est pas utilisé car le codage des messages dans les points rationnels d'une courbe elliptique n'est pas commode, les messages codés sont quatre fois plus longs que les messages en clair .*
On utilise le cryptosystème de Menezes et Vanstone [4] :
1) Espace des clairs : $\mathbb{F}_q^* \times \mathbb{F}_q^*$
2) Espace des chiffrés : $E(K) \times \mathbb{F}_q^* \times \mathbb{F}_q^*$
3) Les paramètres sont $\mathcal{K} = (P, a, R)$ *avec* $R = aP$, $l \in \{0, 1, 2....., n-1\}$ *au hasard et* $n = ord(P)$
4) Pour un message $X = (x_1, x_2)$*, la fonction de chiffrement est :*

$$e_{\mathcal{K}}(X) = (W, y_1, y_2)$$

avec

$$W = lP$$

$$(c_1, c_2) = lR$$

$$y_1 = c_1 x_1$$
$$y_2 = c_2 x_2$$

5) La fonction de déchiffrement est :

$$d_{\mathcal{K}}(W, y_1, y_2) = (z_1, z_2)$$
$$(d_1, d_2) = aW$$
$$z_1 = d_1^{-1} y_1$$
$$z_2 = d_2^{-1} y_2$$

La clé publique est alors constituée de la courbe E et du triplet (n, P, R), tandis que la clé secrète est a.

3.4 Choix de la courbe

Remarque 13. *Il existe des cas de courbes elliptiques pour lesquelles le problème du logarithme discret est considéré comme trivial.Ces courbes sont à éviter.*
Soit E une courbe elliptique sur $\mathbb{F}_q$.
On pose card$(E) = q + 1 - t$, avec $|t| \leq 2\sqrt{q}$
-Si $t = 0$ alors le problème du logarithme discret dans E peut être réduit à $\mathbb{F}_q^*$.
-Si $t = 1$ alors le problème du logarithme discret dans E peut être réduit à $\mathbb{F}_q$.
-Les courbes super-singulières.

Définition 15. *Une courbe elliptique E définie sur $\mathbb{F}_q$ où $q = p^m$ est dite super-singulière si p divise t .*
On montre que les seules valeurs de q^2 sont 0,q,2q,3q et 4q.[1],[4],[23]
On peut connaître la structure du groupe $E(\mathbb{F}_q)$ et le degré de l'extension $\mathbb{F}_{q^k}$ du corps de base $\mathbb{F}_q$ (voir le tableau suivant) :
***Classification des courbes super-singulières** :[1],[4],[23]*

Classe de E	*t*	*Structure du groupe*	*k*
1	*0*	*Cyclique*	*2*
2	*1*	$Z_{\frac{(q+1)}{2}} \oplus \mathbb{Z}_2$	*2*
3	$\pm\sqrt{q}$	*Cyclique*	*3*
4	$\pm\sqrt{2q}$	*Cyclique*	*4*
5	$\pm\sqrt{3q}$	*Cyclique*	*6*
6	$\pm 2\sqrt{q}$	$Z_{\sqrt{q}\pm 1} \oplus \mathbb{Z}_{\sqrt{q}\pm 1}$	*1*

Théorème 6. *(Menezes-Okamoto-Vanstone) :*
Si E est une courbe elliptique super-singulière définie sur $\mathbb{F}_q$, il est possible de réduire le problème du logarithme discret dans E au problème du logarithme discret dans une extension $\mathbb{F}_{q^k}$ de $\mathbb{F}_q$, avec $k \leq 6$, en temps polynomial.
Pour la démonstration de ce théorème on peut consulter .[1]

Exemple 5. *Soit E la courbe elliptique sur $\mathbb{Z}_7$ d'équation :*

$$y^2 = x^3 + 3x + 2$$

on a

$$E = \{\Omega, [0,3], [0,4], [2,3], [2,4], [4,1], [4,6], [5,3], [5,4]\}$$

Table d'addition du groupe *E :*

$+$	Ω	*[0,3]*	*[0,4]*	*[2,3]*	*[2,4]*	*[4,1]*	*[4,6]*	*[5,3]*	*[5,4]*
Ω	Ω	*[0,3]*	*[0,4]*	*[2,3]*	*[2,4]*	*[4,1]*	*[4,6]*	*[5,3]*	*[5,4]*
[0,3]	*[0,3]*	*[2,3]*	Ω	*[5,4]*	*[0,4]*	*[5,3]*	*[4,1]*	*[2,4]*	*[4,6]*
[0,4]	*[0,4]*	Ω	*[2,4]*	*[0,3]*	*[5,3]*	*[4,6]*	*[5,4]*	*[4,1]*	*[2,3]*
[2,3]	*[2,3]*	*[5,4]*	*[0,3]*	*[4,6]*	Ω	*[2,4]*	*[5,3]*	*[0,4]*	*[4,1]*
[2,4]	*[2,4]*	*[0,4]*	*[5,3]*	Ω	*[4,1]*	*[5,4]*	*[2,3]*	*[4,6]*	*[0,3]*
[4,1]	*[4,1]*	*[5,3]*	*[4,6]*	*[2,4]*	*[5,4]*	*[0,3]*	Ω	*[2,3]*	*[0,4]*
[4,6]	*[4,6]*	*[4,1]*	*[5,4]*	*[5,3]*	*[2,3]*	Ω	*[0,4]*	*[0,3]*	*[2,4]*
[5,3]	*[5,3]*	*[2,4]*	*[4,1]*	*[0,4]*	*[4,6]*	*[2,3]*	*[0,3]*	*[5,4]*	Ω
[5,4]	*[5,4]*	*[4,6]*	*[2,3]*	*[4,1]*	*[0,3]*	*[0,4]*	*[2,4]*	Ω	*[5,3]*

Table des multiples des points de *E, mP* ***pour*** *$2 \leq m \leq 9$:*

P	*2P*	*3P*	*4P*	*5P*	*6P*	*7P*	*8P*	*9P*
[5,4]	*[5,3]*	Ω	*[5,4]*	*[5,3]*	Ω	*[5,4]*	*[5,3]*	Ω
[5,3]	*[5,4]*	Ω	*[5,3]*	*[5,4]*	Ω	*[5,3]*	*[5,4]*	Ω
[0,3]	*[2,3]*	*[5,4]*	*[4,6]*	*[4,1]*	*[5,3]*	*[2,4]*	*[0,4]*	Ω
[2,4]	*[4,1]*	*[5,4]*	*[0,3]*	*[0,4]*	*[5,3]*	*[4,6]*	*[2,3]*	Ω
[2,3]	*[4,6]*	*[5,3]*	*[0,4]*	*[0,3]*	*[5,4]*	*[4,1]*	*[2,4]*	Ω
[0,4]	*[2,4]*	*[5,3]*	*[4,1]*	*[4,6]*	*[5,4]*	*[2,3]*	*[0,3]*	Ω
[4,6]	*[0,4]*	*[5,4]*	*[2,4]*	*[2,3]*	*[5,3]*	*[0,3]*	*[4,1]*	Ω
[4,1]	*[0,3]*	*[5,3]*	*[2,3]*	*[2,4]*	*[5,4]*	*[0,4]*	*[4,6]*	Ω

On a :

$$E[9] = \{\Omega, [0,3], [0,4], [2,3], [2,4], [4,1], [4,6]\}$$

$$E[3] = \{\Omega, [5,3], [5,4]\}$$

$$\forall i \in \{1,2,4,5,6,7,8\}, E[i] = \{\Omega\}$$

Soit $P = [0,3]$, on pose $Q = 5P = [4,1]$, donc $log_P Q = 5$

Cryptosystème d'ElGamal *:*

$card(E) = 9$;soit $P = [0,3]$, l'orde de P est 9.

P est un générateur du groupe E.

1)$\mathcal{K} = (P, 5, R)$ avec $R = 5P = [4,1]$.

2) On prend $l \in \{0,1,2.....,8\}$ au hasard $l = 3$, la fonction de chiffrement est :

$$e_{\mathcal{K}}(X) = (Y, Z)$$

avec

$$Y = lP = 3P = [5, 4]$$
$$Z = lR + X = 3R + X = [5, 3] + X$$

3) La fonction de déchiffrement est :

$$d_{\mathcal{K}}(Y, Z) = Z - aY = [5, 3] + X - [5, 3] = X$$

***Cryptosystème de Menezes et Vanstone** :*
1) Espace des clairs :$\mathbb{Z}_7^* \times \mathbb{Z}_7^*$
2) Espace des chiffrés :$E \times \mathbb{Z}_7^* \times \mathbb{Z}_7^*$
3) Les paramètres sont $\mathcal{K} = (P, 5, R)$ *avec* $R = 5P = [4, 1]$, $l \in \{0, 1, 2....., 8\}$ *au hasard,* $l = 3$
4) Pour un message $X = (x_1, x_2)$*, la fonction de chiffrement est :*

$$e_{\mathcal{K}}(X) = (W, y_1, y_2)$$

avec

$$W = 3P = [5, 4]$$
$$(c_1, c_2) = 3R = [5, 3]$$
$$y_1 = 5x_1$$
$$y_2 = 3x_2$$

5) La fonction de déchiffrement est :

$$d_{\mathcal{K}}(W, y_1, y_2) = (z_1, z_2)$$
$$(d_1, d_2) = 5W = [5, 3]$$
$$z_1 = 5^{-1}y_1 = x_1$$
$$z_2 = 3^{-1}y_2 = x_2$$

Exemple 6. *Soit la courbe elliptique* $E(\mathbb{F}_8)$ *d'équation :*

$$y^2 + y = x^3 + 1$$

E contient 9 points :$\Omega; P_1[1, 0]; P_2[1, 1]; P_3[\alpha, \alpha^2]; P_4[\alpha, \alpha^2 + 1]$;
$P_5[\alpha^2, \alpha^2 + \alpha]; P_6[\alpha^2, \alpha^2 + \alpha + 1]; P_7[\alpha^2 + \alpha, \alpha]; P_8[\alpha^2 + \alpha, \alpha + 1]$.

Table d'addition du groupe E *:*

$+$	Ω	P_1	P_2	P_3	P_4	P_5	P_6	P_7	P_8
Ω	Ω	P_1	P_2	P_3	P_4	P_5	P_6	P_7	P_8
P_1	P_1	P_2	Ω	P_5	P_8	P_7	P_4	P_3	P_6
P_2	P_2	Ω	P_1	P_7	P_6	P_3	P_8	P_5	P_4
P_3	P_3	P_5	P_7	P_8	Ω	P_6	P_2	P_4	P_1
P_4	P_4	P_8	P_6	Ω	P_7	P_1	P_5	P_2	P_3
P_5	P_5	P_7	P_3	P_6	P_1	P_4	Ω	P_8	P_2
P_6	P_6	P_4	P_8	P_2	P_5	Ω	P_3	P_7	P_1
P_7	P_7	P_3	P_5	P_4	P_2	P_8	P_1	P_6	Ω
P_8	P_8	P_6	P_4	P_1	P_3	P_2	P_7	Ω	P_5

Table des multiples des points de E, mP ***pour*** $2 \leq m \leq 9$ *:*

Les Points P_i	$2P_i$	$3P_i$	$4P_i$	$5P_i$	$6P_i$	$7P_i$	$8P_i$	$9P_i$
P_1	P_2	Ω	P_1	P_2	Ω	P_1	P_2	Ω
P_2	P_1	Ω	P_2	P_1	Ω	P_2	P_1	Ω
P_3	P_8	P_1	P_5	P_6	P_2	P_7	P_4	Ω
P_4	P_7	P_2	P_6	P_5	P_1	P_8	P_3	Ω
P_5	P_4	P_1	P_7	P_8	P_2	P_3	P_6	Ω
P_6	P_3	P_2	P_8	P_7	P_1	P_4	P_5	Ω
P_7	P_6	P_1	P_3	P_4	P_2	P_5	P_8	Ω
P_8	P_5	P_2	P_4	P_3	P_1	P_6	P_7	Ω

On a :

$$E[9] = \{\Omega, P_3, P_4, P_5, P_6, P_7, P_8\}$$

$$E[3] = \{\Omega, P_1, P_2\}$$

$$\forall i \in \{1, 2, 4, 5, 6, 7, 8\}, E[i] = \{\Omega\}$$

Soit $P = P_3$*, on pose* $Q = 7P_3 = P_7$*, donc* $log_P Q = 7$

Cryptosystème d'ElGamal *:*

$card(E) = 9$ *;soit* $P = P_3$*, l'orde de* P *est 9.*

P *est un générateur du groupe* E*.*

1)$\mathcal{K} = (P, 7, R)$ *avec* $R = 7P = P_7$*.*

2) On prend $l \in \{0, 1, 2.....,8\}$ *au hasard* $l = 4$*, la fonction de chiffrement est :*

$$e_{\mathcal{K}}(X) = (Y, Z)$$

avec

$$Y = lP = 4P = P_5$$

$$Z = lR + X = 4R + X = P_3 + X$$

3) La fonction de déchiffrement est :

$$d_{\mathcal{K}}(Y,Z) = Z - aY = P_3 + X - P_3 = X$$

Cryptosystème de Menezes et Vanstone *:*
1) Espace des clairs : $\mathbb{F}_8^* \times \mathbb{F}_8^*$
2) Espace des chiffrés : $E \times \mathbb{F}_8^* \times \mathbb{F}_8^*$
3) Les paramètres sont $\mathcal{K} = (P, 7, R)$ *avec* $R = 7P = P_7$, $l \in \{0, 1, 2.....,8\}$ *au hasard,* $l = 4$
4) Pour un message $X = (x_1, x_2)$*, la fonction de chiffrement est :*

$$e_{\mathcal{K}}(X) = (W, y_1, y_2)$$

avec

$$W = 4P = P_5$$
$$(c_1, c_2) = 4R = [\alpha, \alpha^2]$$
$$y_1 = \alpha x_1$$
$$y_2 = \alpha^2 x_2$$

5) La fonction de déchiffrement est :

$$d_{\mathcal{K}}(W, y_1, y_2) = (z_1, z_2)$$
$$(d_1, d_2) = 7W = [\alpha, \alpha^2]$$
$$z_1 = (\alpha)^{-1} y_1 = x_1$$
$$z_2 = (\alpha^2)^{-1} y_2 = x_2$$

Bibliographie

[1] *A.Menezes,T.Okamoto,S.Vanstone :Reducing elliptic curve logarithms to logarithms in a field,in proceedings of the twenty third annual ACM symposium on theory of computing,p.80-89,ACM Press,1991.*

[2] *Abdelhak Azhari :Cryptographie mathématique et sécurité de l'information (DESA du FST Fés 2005-2007).*

[3] *Abderrahmame Nitaj :Le problème du logarithme discret elliptique Index et Xedni.*

[4] *Annie chateau :Courbes Elliptiques et cryptographies*

[5] *Antoine Joux Reynald Lercier :Algorithmes pour résoudre le problème du logarithme discret dans les corps finis.*

[6] *Barre Magalie :Travaux d'études et de recherches :Cryptographie.*

[7] *Dany-Jack Mercien :Corps finis.*

[8] *E. Thomé. Computation of discrete logarithms in GL(2^{607})Dans C. Boyd et E. Dawson, éditeurs, Advances in Cryptology ASIACRYPT 2001. Lecture Notes in Comput. Sci., volume 2248, pages 107,124. Springer Verlag, 2001. Proc. 7th International Conference on the Theory and Applications of Cryptology and Information Security, Dec. 9 ,13, 2001, Gold Coast, Queensland, Australia.*

[9] *E.Thomé : Discrete logarithms in GL(2^{607}).*

[10] *Emmanuel Peyre :Corps finis et courbes elliptiques.*

[11] *Emmanuel Thomé :Algorithmes de calcul de logarithmes discrets dans les corps finis.*

[12] *Eugène Malek : Matrices de compagnon généralisées, séminaire Théorie des nombres, tomes 5(1963-1964), exp.n° 17, p.1-17.*

[13] *J. H. Silverman. The arithmetic of elliptic curves. Grad. Texts in Math., volume 106.Springer Verlag, 1986 .*

[14] *Jean-Marc Couveignes : Quelques Mathématiques de la cryptographie à clés publiques.*

[15] *Johammes A.Buchmann :Introduction to cryptography.*

[16] *M.E.Charkani :Conpléments sur les corps finis.*

[17] Marc Joye :Introduction élémentaire à la théorie des courbes elliptiques.

[18] Ndiaye Elhadji Oumar :Etude du problème du logarithme discret dans $GL(p^3)$.

[19] Neal Kobliz :A course in number theory and cryptography.

[20] Nicolas Gürel :Conception de cryptosystèmes à base de courbes algébriques.

[21] S.Pohlig et M.E.Hellman :An improved algorithm for cmputing logarithms over GF(p) and cryptographic significa.

[22] Samuel MIMRAM : TIPE- Courbes elliptiques et factorisation (version détaillée).

[23] Silverman,Joseph H,Suzuki,Joe :Elliptic curve discrete logarithms and the index calculs,in advances in cryptology ;Berlin springer lect note 1514 (1998),5-40.

[24] Steve Gury-Nicolas Rémond :Cryptologie, Elgamal d'àprés Diffie-Hellman.

[25] Steve Thiboutot :Courbes elliptiques, représentations galoisiennes et l'équation :$x^2 + y^3 = z^5$.

[26] Steven Roman :Coding and information theory.

[27] Wells, Albert L.Jun.,A polynomial form for logarithms modulo a prime, IEEE Trans . Inf. Theory 30 (1984) ; 845-846.