LES COURBES ELLIPTIQUES ET LA CRYPTOGRAPHIE

Zahia TALEB

Encadrant :Abdelmadjid BAYAD

TABLE DE MATIERES

Introduction :

Les courbes elliptiques sont un sujet très à la mode en mathématiques ;
Tout a commencé lorsque Lenstra a découvert un algorithme de factorisation polynomial sur ces structures. Ensuite ,en 1985 , Koblitz et Miller ont proposé d'adopter les protocoles de la cryptographie basés sur les courbes elliptiques .

Ce rapport est organisé comme suit :

Pour aborder le chapitre des courbes elliptiques ,nous avons revu quelques bases nécessaires dans le plan projectif .

Nous verrons qu'à toute courbe elliptique est associé une structure de groupe ;nous montrerons qu'une courbe elliptique est équivalente à une forme particulière :les équations de Weierstrass .

Enfin, la dernier chapitre propose quelques applications liées aux courbes elliptiques.

Chapitre I : Plan projectif

Introduction :

Le plan projectif est un objet qui date de la découverte des lois de la perspective par Léon B. Alberti et Filippo Brunelleschi à la renaissance. C'est une formalisation des points de fuites des parallèles qui se rejoignent pour donner une impression de profondeur de champs sur un tableau ou un dessin. Imaginons un peintre debout dans un paysage et élevons nous très haut au dessus de lui, si je trace des parallèles qu'il voit dans chaque direction du plan, elles semblent se rejoindre à l'infini.

Le plan projectif est un objet mouvant qui peut s'aborder par plusieurs biais.

Le plan projectif est une surface non orientable qui n'est pas représentable (plongeable) dans l'espace à trois dimensions usuel.

I-1/Plan projectif P_2

Définition I-1 :

Soit K un corps ,

Le plan projectif P_2 (K) est l'ensemble des points p = (a,b,c) non nul dans K^3 de sorte que deux points p=(a,b,c) et p'= (a',b',c') sont considérés comme étant des points équivalents si il existe t appartient à k^* tel que (a,b,c) = t (a',b',c').

a, b et c sont appelés les coordonnées homogènes du point p.

plus généralement ,on appelle le n- espace projectif noté P_n (K) l'ensemble des classes d'équivalence des (n+1)uples suivants :

$$P_n(K) = \frac{\left\{(a_0, a_1, \ldots a_n) \in k^{n+1} \mid a_0, a_1, \ldots, a_n \text{ non tous nuls}\right\}}{¿}$$

où $(a_0, a_1, \ldots a_n) \sim (a'_0, a'_1, \ldots a'_n)$ s'il existe t appartient à k^* tel que

$(a_0, a_1, \ldots a_n) = t\ (a'_0, a'_1, \ldots a'_n)$.

Définition I-2 :

le degré d'un monôme d'un polynôme p de l'anneau K [x_1,….x_n] est la somme des exposants des variables x_i apparaissant dans ce monôme.

Le degré de p est le plus grand degré de ses monômes.

Définition I-3 :

Soit p ¿ K [x_1,….x_n] un polynôme de degré d.

P est dit homogène si chacun de ses monômes est de degré d.

Dans toute la suite K [x_1,….x_n]$_d$ désigne l'ensemble des polynômes de degré d homogène.

P est dit irréductible si il ne peut s'écrire comme le produit non trivial de deux polynômes de $K[x_1,\ldots x_n]_d$.

Proposition I-1 :

Soit $p(x_1,\ldots x_n)$ un polynôme à coefficients dans K

P est homogène de degré d >0 si est seulement si pour variable auxiliaire t :

$P(tx_1,\ldots,tx_n) = t^d p(x_1,\ldots,x_n)$

Preuve :

La condition nécessaire est évidente.

Démontrons la condition suffisante.

Ecrivons p comme somme des polynômes homogènes non nuls de degré d_i

$p = p_{d1} + p_{d2} + \ldots + p_{dr}$, $d_1 < d_2 < \ldots < d_r$

$P(tx_1,\ldots,tx_n) = t^d p(x_1,\ldots,x_n)$ implique que

$t^{d1} p_{d1} + t^{d2} p_{d2} + \ldots + t^{dr} p_{dr} = t^d p = t^d p_{d1} + t^d p_{d2} + \ldots + t^d p_{dr}$

donc $t^{di} = t^d \ \forall$ i .

par conséquent, r=1 car $d_1 < d_2 < d_3 < \ldots < d_r$ et $p = p_{d1} = p_d$.

corollaire (formule d'Euler) :

si F ¿ $K[x_1,\ldots x_n]_d$ est un polynôme homogène de degré d défini sur K alors :

$$\sum_{i=1}^{n} X_i \frac{\partial F}{\partial X_i} = d \cdot F$$

Définition I-4 :

Une courbe C de $P_2(K)$ est l'ensemble des points qui satisfait p(x,y,z)=0 où p est un polynôme homogène de degré d.

si d = 1, C est une droite.

Si d = 2, C est une droite.

Si d = 3, C est une cubique.

Remarque :

Le plan usuel (x,y) sur K appelé plan affine est noté $A_2(K)$ est l'ensemble des points (x,y) appartient à $K^{2.}$

si nous introduisons les coordonnées X, Y , Z telles que x = X/Z et y = Y/Z alors à tous point (x,y) de $A_2(K)$ correspond le point (X,Y,Z) de $P_2(K)$.

réciproquement si Z ¿ 0 alors tout points (X,Y,Z) de $P_2(K)$ correspond le point (x,y) de A_2 (K).

le cas Z=0 :

considérons dans $A_2(K)$. deux droites parallèles L : ax+by+c=0 avec (a,b) ¿ (0,0) et L' : a'x+b'y+c = 0 où a' = t .a et b'= t b

dans $P_2(K)$, ces droites s'écrivent :

L : aX+bY+cZ=0 et L' : a'X+b'Y+c'Z=0 .

Ces deux droites s'intersectent en un point pour lequel Z = 0

Ce point est appelé point à l'infini.

Pour cela on peut définir $P_2(K)$ comme suit :

$P_2(K) = A_2(K)$ ¿ {l'ensemble des direction dans $A_2(K)$ }

Définition I-5 :

On dit que L intersecte C d'équation f(X,Y,Z)=0 en p_1 avec un ordre m si $f^{(m)}(p_1)$ ¿ 0

Et si $f^{(l)}(p_1) = 0$ pour l<m quand notera $I(p_1,L,C)=m$

Définition I- 6 :

Un point P d'une courbe C : F(X,Y,Z)=0 est dit singulier si :

$$\frac{\partial F}{\partial X}|_p = \frac{\partial F}{\partial Y}|_p = \frac{\partial F}{\partial Z}|_p = 0$$

si non p est dit non singulier ou simple .

la courbe C est appelé courbe non singulière si tous ses points sont simples.

I-1/Théorème de Bezout

Théorème (faible de Bezout) :

Soit un corps infini K.

Si F ¿ K $[X,Y,Z]_m$ et G ¿ K $[X,Y,Z]_n$ sont deux courbes ayant plus de mn points communs, alors F et G ont un facteur non constant en commun.

Corollaire :

Si F ¿ K $[X,Y,Z]_d$ est une courbe est si L est une droite telles que $\sum_{p\in L} I(P,L,C) > d$, alors L divise C.

Preuve :

Par l'absurde, supposons que L de divise pas C. par le théorème faible de Bezout , nous savons que C est L ont un nombre fini de points communs et , par conséquent $\sum_{p\in L} I(P,L,C)$ est fini. Montons que $\sum_{p\in L} I(P,L,C) \leq d$. Par une transformation projective, nous pouvons supposer que L est la droite à l'infini Z=0 .En faisant éventuellement une translation sur la variable Y,nous pouvons également supposer que tous les points d'intersections ont une coordonnée en Y non nulle.

Notons $P_i = (r_i,1,0)$ les points d'intersections de C(X,1,0) avec L : Z=0.

Comme K est infini , il existe (r,1,0) qui n'appartient pas à C ¿ L et donc, C(X,1,0) est un polynôme non nul.

Ce polynôme a donc au plus d racines comptées avec leur multiplicité.

Par conséquent, la $\sum_{p\in L} I\left(P, L, C\right) \leq d$, ce qui est contraire à l'hypothèse.

CHAPITRE II : COURBES ELLIPTIQUES

Définition II-1 :

Une courbe elliptique est un couple $\left(E, O\right)$ ou E est un cubique irréductible non singulière et $O \in E$ .La courbe elliptique E est définie sur un corps k si E est une courbe sur K et si $O \in E\left(K\right)$.

II-1/ Equations de Weierstrass d'une courbe elliptique .

Théorème 1 (version projective) :

Si E est courbe elliptique définie sur un corps k alors il existe une application

$: E(K) \to P^2(K)$ qui définie un isomorphisme de

$E(K)$ sur une courbe $C(K)$ donnée par l'équation de Weierstrass :

$C: F(X, Y, Z) = Y^2 Z + a_1 XYZ + a_3 YZ^2 - X^2 - a_2 X^2 Z - a_2 XZ^2 - a_6 Z^2 = 0$

ou $a_1, \ldots\ldots, a_6 \in K$ et tel que $(0) = (0,1,0)$

Preuve :

Pour alléger les notations ,nous allons écrire l'équation de Weierstrass en coordonnées non homogène : $x = X/Z$ et $y = Y/Z$

$E = y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6$ et le point à l'infini $0 = (0,1,0)$

Remarquons que 0 est le seul point à l'infini et qu'il n'est pas singulier car

$\frac{\partial F}{\partial Z}(0,1,0) = 1 \neq 0 \cdot$

Nous définissons également les quantités suivantes :

$b_2 = a_1^2 + 4a_2, b_4 = 2a_4 + a_1 a_3, b_6 = a_3^2 + 4a_6$ (Polynôme)

Définition II-2 :

Le discriminant de l'équation de Weierstrass est de la quantité

$= -b_2^2 b_8 - 8b_4^3 - 27b_6^2 + 2b_2 b_4 b_6$ et le j-eme invariant d la courbe elliptique E est la quantité

$$j(E) = \frac{c_4^3}{\qquad\qquad}$$

Corollaire (version affine)simplifiée

Soit K un corps de caractéristique p .Une courbe C définie sur K donnée par l'équation de Weierstrass ^rend alors une forme simplifiée :

1/ Si $p \neq 2$,on remplace y par $y^2 = x^3 + \frac{b_2}{4}x^2 + \frac{b_4}{2}x + \frac{b_6}{4}$.

Si $p \neq 3$,en remplace x par $\left(x - \frac{b_2}{12}\right)$ on obtient : $y^2 = x^3 - \frac{c_4}{48} - \frac{c_6}{864}$

2/ l'invariant de l'équation générale de Weierstrass :

$y + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6$ vaut :

$$j(E) = \frac{a_1^{12}}{\qquad\qquad}$$

si $j(E) = 0$,donc si $a_1 = 0$ alors la substitution x par $\left(x + a_2\right)$ donne

$$y^2 + a_3 y = x^3 + \left(a_2^2 + a_4\right)x + \left(a_2^3 + a_4 a_2 + a_6\right)$$

sinon on remplace (x, y) par $\left(\left(a_1^2 x + \frac{a_3}{a_1}\right), a_1^3 y + \frac{a_1^2 a_4 + a_3^2}{a_1^3}\right)$ pour avoir

$$y^2 + xy = x^3 + \frac{a_1 a_2 a_3}{a_1^3}x^2 + \frac{a_1^4 a_4^2 + a_3^4 + a_1^5 a_3 a_4 + a_1^3 a_3^3 + a_4^4 a_2 a_3^2 + a_5^6 a_6}{a_1^{12}}$$

3/ En (1) ,nous avons montrer que si $p \neq 2$ alors :

$$y^2 = x^2 + a_2 x^2 + a_4 x + a_6$$

l'invariant de cette courbe (en caractéristique 3) vaut :

$$j(E) = \frac{a_2^2}{\qquad\qquad}$$

si $j(E)=0$ alors $a_2=0$ et nous avons l'expression demandée

sinon il suffit de remplacer x par $\left(x+\frac{a_4}{a_2}\right)$ pour obtenir $y^2=x^3+a_2x^2+\frac{2a_2^2a_4^2+a_2^3a_6+a_4^3}{a_2^3}$

Lemme 1 :

Soit un corps K et une courbe E donnée par l'équation de Weierstrass :

$C: f(x,y)=y^2+a_1xy+a_3y-x^3-a_2x^2-a_4x-a_6=0$

dont le discriminant vaut et le j-eme invariant $j(E)$

le changement de variables :

$(x,y)\leftarrow(u^2x+r,u^3y+u^2sx+t)$ avec $r,s,t,u(¿0)\in K$

transforme l'équation précédente en :

$E': f'(x,y)=y^2+a_1'xy+a_3'xy+a_3'y-x^3-a_2'x^2-a_4'x-a_6'=0$

ou les coefficients sont données par :

$$ua_2'=a_1+2s$$
$$u^2a_2'=a_2-sa_1+3r-s^2$$
$$u^3a_3'=a_3+ra_1+2t$$
$$u''a_4'=a_4-sa_3+2ra_2-(t+rs)a_1+3r^2-2st$$

¿
{¿{¿{¿¿¿
¿

de plus

$u^¿$ ^{2} $'=$ ¿ et

$j(E')=j(E)$

Preuve :

Il suffit juste de remplacer x et y par leurs nouvelles expressions pour obtenir les relations dérivées .

Théorème 2 :

Soit K un corps de caractéristique p.Deux courbes données par leurs équations de Weierstrass dont le discriminant est non nul sont isomorphes si et seulement si elles ont le même j-invariant.

Preuve :

$\Rightarrow$) Par le lemme précédent .

$\Leftarrow$) Pour simplifier les calculs ,nous allons supposer que $p \neq 2,3$.

Soient deux courbes E et E' ayant le même j-invariant dont les équations de Weierstrass sont données par :

$E : y^2 = x^3 + a_4 + a_6$

$E' : y^2 = x^3 + a'_4 x + a'_6$

Comme $j(E) = 1728 \dfrac{4a_4^3}{4a_4^3 + 27a_6^2}$ et $4 \dfrac{a_4'^3}{4\ a_4'^3 27 a_6'^2}$ sont égaux alors

$j(E') = 1728$

$a_6^2 a_4'^3 a_4^3 a_6'^2$

cherchons des isomorphismes de la forme $(x, y) \leftarrow (u^2 x, u^3 y)$,

(1)si $a_4 = 0$ alors $a_6 \neq 0$ car ($\neq 0$) donc $a'_4 = 0$

on obtient un isomorphisme en prenant $u=\left(a_6/a_6^{'}\right)^{1/6}$

(2)si $a_6=0$ alors $a_4\neq 0$

donc $a_6^{'}=0$, on obtient un isomorphisme en prenant $u=\left(a_4/a_4^{'}\right)^{1/4}$

(3)si $a_4 a_6\neq 0$ alors $a_4^{'}a_6^{'}\neq 0$ on obtient un isomorphisme en prenant

$u=\left(a_4/a_4^{'}\right)^{1/6}=\left(a_6/a_6^{'}\right)^{1/4}$

Si p=2 ou 3 ,la démonstration se fait de la même manière en prenant les équations de Weierstrass correspondantes ;

Théorème 3 :

Soit C une courbe elliptique donnée par une équation de Weierstrass alors C est non singulière si et seulement si $\neq 0$.

Preuve :

$(\Leftarrow)$ soit l'équation générale de Weierstrass :

$C: f(x,y)=y^2+a_1xy+a_3y-x^3-a_2x^2-a_4x-a_6=0$

Montrons d'abord que le point à l'infini p = (0,1,0) n'est jamais singulier .

Regardons C une courbe de $(P_2)=P_2$.

$F(X,Y,Z)=Y^2Z+a_1XYZ+a_3YZ^2-X^3-a_2X^2Z-a_4XZ^2-a_6Z^3=0$

Comme $\left(\frac{\partial F}{\partial Z}\right)(p)=1\neq 0$ alors p n'est pas singulier de C .

Par l'absurde, supposons que C soit singulière en un point $p_0=(x_0,y_0)$.

Par le changement de variable $(x,y)\leftarrow(x-x_0,y-y_0)$ nous ramenons le point p_0 en (0,0).

Par le lemme précédent , cette transformation ne modifie pas le discriminant (car u = 1).

Nous avons alors $a_6=f$ (0,0) = 0.

$$a_4=\left(\frac{\partial f}{\partial x}\right)(0,0\ )=0$$

et $a_3=\left(\frac{\partial f}{\partial y}\right)(0,0\ )=0$

la courbe C a donc pour équation :

$C: f(x,y)=y^2+a_1xy-x^3-a_2x^2=0$.

Le discriminant de cette équation est égale à zéro .

Ce qui contredit l'hypothèse .

$(\Rightarrow)$ Pour simplifier les calculs , nous allons supposer que $p\neq 2,3$

soit alors la courbe C donnée par l'équation de Weierstrass :

$C: y=x^3+a_4x+a_6$

Si la courbe est singulière en un point $p_0=(x_0,y_0)$ alors :

$2y_0=0\Rightarrow y_0=0$

$3x_0^2+a_4=0\Rightarrow x_0^2=\frac{-a_4}{3}$

or $p_0=(x_0,y_0)$ est un point de courbe ,par conséquent :

$y_0^2=x_0^3+a_4x_0+a_6=\frac{2}{3}a_4x_0+a_6$

Il s'ensuit que

$x_0^2=\frac{9a_6^2}{4a_4^2}=-\frac{a_4}{3}$

$=-16(4a_4^3+27a_6^2)=0$

Si p=2 ou 3,la démonstration se fait de la même façon en prenant les équations de Weierstrass correspondantes .

Définition II-3:

Les trois théorèmes précédents permettent de donner une définition alternative d'une courbe elliptique .

Une courbe elliptique est une courbe isomorphe à la courbe donnée par des équations de Weierstrass ou $\neq 0$ plus le point à l'infini p = (0,1,0).

II-2/Réduction d'une cubique :

Soit K un corps de caractéristique ¿2 .

L'équation projective d'une cubique irréductible non singulière est donnée par f(X,Y,Z) = 0 ou

$$f(X,Y,Z)=s_1X^3+s_2X^2Y+s_3XY^2+s_4Y^3+(s_5X^2+s_6XY+s_7Y^2)Z+(s_8X+s_9Y)Z^2+s_{10}Z^3$$

Cette équation peut être vue comme un polynôme de degré 3 en Z .

$$f(X,Y,Z)=c_0Z^3+c_1(X,Y)Z^2+c_2(X,Y)Z+c_3(X,Y) \ .$$

Soit $p_0=(x_0,y_0,z_0)$ un point de la courbe .

La tangente en p_0 intersecte la courbe en un troisième point unique $p_1=(x_1,y_1,z_1)$.

Cette tangente a pour équation :

$$\frac{\partial f}{\partial X}(x_0,y_0,z_0)X+\frac{\partial f}{\partial Y}(x_0,y_0,z_0)Y+\frac{\partial f}{\partial Z}(x_0,y_0,z_0)Z=0$$

Supposons que $z_1\neq 0$ et faisons un changement de variables (X,Y,Z) $\leftarrow(x-x_1,y-y_1,Z)$.

Les coordonnées du point p_1 deviennent (0,0,1) .

Etant donné que ce point appartient à la tangente ,la dérivée partielle par rapport à Z en p_0 est nulle .

Comme la courbe est non singulière ,en dérivés partielles par rapport à X et à Y en p_0 ne peuvent pas n'annuler simultanément .

Supposons à présent que la dérivée partielle par rapport à Y en p_0 soi non nulle .

Le point $p_1=(0,0,1)$ appartient aussi à la courbe et donc s_{10} = 0 .

Après changement de variables les équations précédentes deviennent :

$$f(X,Y,Z)=s_1X^3+s_2X^2Y+s_3XY^2+s_4Y^3+(s_5X^2+s_6XY+s_7Y^2)Z+(s_8X+s_9Y)Z^2$$

$$f(X,Y,Z)=c_1(X,Y)Z^2+c_2(X,Y)Z+c_3(X,Y)$$

$Y=\quad X\quad$ ou $\qquad\qquad =\dfrac{\frac{\partial f}{\partial X}|P_0}{\frac{\partial F}{\partial Y}|P_0}$

De plus $p_0=(x-x_0,y-y_0,z_0)$ et $p_1=(0,0,1)$.

Chapitre III : Structure de groupe sur une courbe Elliptique

III-1/ règle de la sécante tangente :

Proposition 1 :

Soit C une cubique irréductible non singulière et L une droite définies sur un corps K.

Si C a deux points d'intersection avec la droite L, alors C a trois points d'intersection avec la droite L.

Preuve :

Comme C est irréductible alors C ¿ L a un nombre fini de points.

Soit la droite L : a aX+bY+cZ=0 où par symétrie on suppose que c ¿ 0.

Les points d'intersections de C et de L sont les racines du polynôme :

$P(x,y)=P(X,Y,-\frac{aX+bY}{c})$ ¿ $K[X,Y]_3$

Notons $p_1 = (a_1 , b_1 , c_1)$ et $p_2 = (a_2 , b_2 , c_2)$ les deux points d'intersection de C avec L, alors comme $q(a_1 , b_1)= q(a_2 , b_2) = 0$ il vient que

$q(X,Y)=v(X,Y) \prod_{i=1}^{2} (b_i X - a_i Y)$ où v (X,Y) ¿ $K[X,Y]_1$

le troisième point d'intersection de C avec L est donné par :

$p_3= (a_3 , b_3, -\frac{aa_3+bb_3}{c})$ où (a_3 ,b_3) est l'unique racine de v(X,Y) .

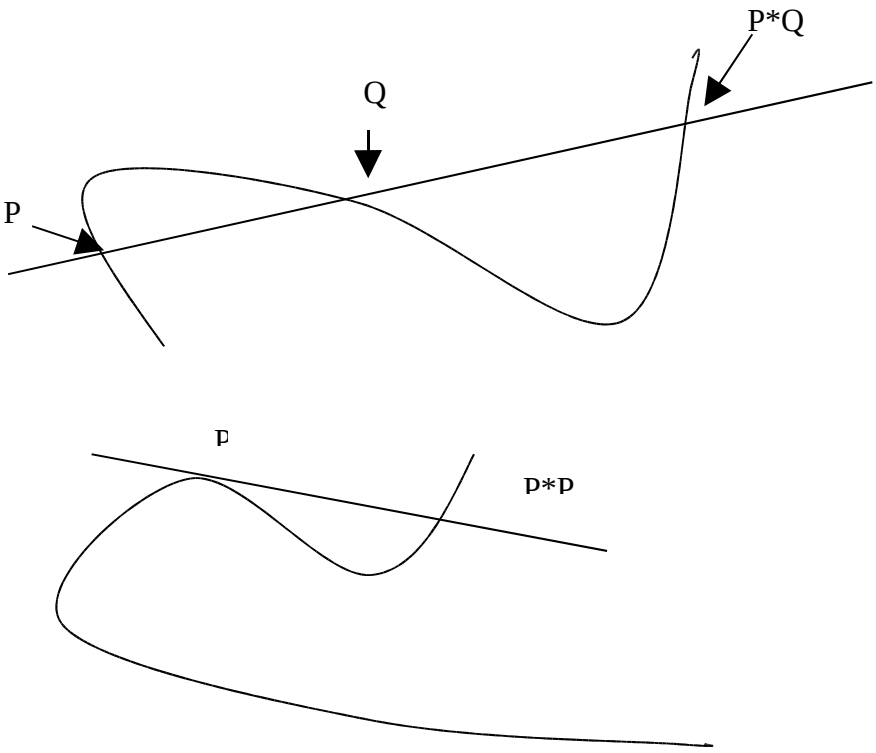
par cette proposition, on peut définir la lois de composition de la sécante tangente :

si P , Q ¿ C(K), alors on définit L = PQ la droite sécante qui passe par P et Q.

par la proposition on sait qu'i existe un troisième point qui passe par C et L.

on le note P*Q.

2- si p ¿ C(k), alors on définit L=PP la droite tangente à C qui passe par P et on sait par la proposition précédente qu'il existe un troisième point appartenant à C ¿ L , on le note P*P.



Règle de la sécante tangente

Théorème 3 :

Soit K un corps infini.

Si(E ,O) est une courbe elliptique définie sur K ,alors l'opérateur :

$P+Q=O*(P*Q)$ définit une structure de groupe commutatif ayant O comme élément neutre.

De plus, si O' est un autre point de (E,O),alors l'opération :

$P+'Q=O'*(P*Q)$ définit une structure de groupe isomorphe au premier.

Preuve :

i)-a)Par la définition de la sécante tangente la commutativité est évidente.

$P+Q=O*(P*Q)=O*(Q*P)=Q+P$

b) O est l'élément neutre car $P+O=O*(P*O)=O+P=P$

c) L'élément symétrique d'un élément Q est définit par :

$-Q=(O*O)*Q$.

En effet,

$-Q+Q=O*(((O*O)*Q)*Q)=O*(O*O)=O+O=O$

Et

$Q+(-Q)=O*(Q*((O*O)*Q))=O*(O*O)=O+O$

d) Il reste à démontrer l'associativité.Calculons :

$$\begin{aligned}P*(Q+R)&=P*(O*(Q*R))\\&=((O*Q)*Q)*(O*(Q*R))\\&=((P*Q)*O)*(Q*(Q*R))\\&=((P*Q)*O)*R\\&=(O*(P*Q))*R\\&=(P+Q)*R\end{aligned}$$

En appliquant O sur les deux membres de l'égalité, nous trouvons : $P+(Q+R)=(P+Q)+R$.

ii) construisant l'application bijective

$$:(E,+)\to(E,+), P\to P-O' ,$$

Alors ;

$$(P+Q)=(P+Q)-O'$$

$$\begin{aligned}&= O*[(O*(P*Q))*((O*O)*O'\\&= O*[(O*(O*O))*((P*Q)*O')]\\&= O*[O*(P+'Q)]\\&=\end{aligned}$$

$$P+'Q= \qquad (P)+' \qquad (Q)$$

l'application est donc un isomorphisme .

III-2/ Théorème de Poincaré :

Soit un corps K .

Si (E,O) est une courbe elliptique définie sur K ;

De plus ,si O' est un autre point de la courbe elliptique, alors l'opération :

$$P+'Q=O*(P*Q)$$

définit une structure de groupe isomorphe au premier .

Démonstration :

Nous savons que si (E,O) est une courbe elliptique définie sur Q ,alors l'opération $P+Q=O*(P*Q)$ définit une structure de groupe .

Nous devons démontrer que ,si (E',O') est une courbe elliptique définit sur F_p ,

l'application modulo q : $E(Q)\to E'(F_P)$

P P' est un homomorphisme de groupe .

Soient P et Q deux points de $E(Q)$ tel que $P+Q=R$.

Notons respectivement L_1, L_2 les droites PQ et $(P*Q)R$; et donc

$E\cap L_1=\{P,Q,P*Q\}$ et $E\cap L_2=\{P*Q,R,O\}$

Construisons l'application bijective :

$$:(E',+)\to(E',+'),P' \qquad P'-O'$$

alors ,par le théorème précédent et comme l'application modulo q est un homomorphisme de $E(Q)$ dans $E'(F_p)$, l'application est donc un isomorphisme .

III-3/ Formules explicites sur l'addition et le doublement des points :

Soit E une courbe elliptique donnée par l'équation de Weierstrass :

$E: f(x,y)=y^2+a_1xy+a_3y-x^3-a_2x^2-a_4x-a_6=0$

Soient $P=(p_1,p_2)$ et $Q=(q_1,q_2)$ deux points de la courbe E .

Addition des points P et Q :

Si $p_1=q_1$ et si $q_2=-p_2-a_1p_1-a_3$ alors

$$P+Q=O$$

Notons $R=(r_1,r_2)$ la somme de P et Q .

Remarquons que R n'est pas le point à l'infini .

Supposons que $q_2\neq-p_2-a_1p_1-a_3$.

si $p_1\neq q_1$,posons :

$$=\frac{q_2-p_2}{q-p_1} \text{ et}$$

$$=p_2- \cdot p_1 .$$

La sécante passante par P et Q a pour équation

$y=$ $\cdot x+$.

En substituons dans l'équation de E , nous obtenons :

$f(x,$ $\cdot x+$ $)=cx^3-c(p_1+q_1+r_1)x^2+c(q_1r_1+p_1q_1+p_1r_1)x-cp_1q_1r_1$

.

b) si $p_1=q_1$, alors P = Q

L'addition de P et Q revient alors à doubler le point P .

Doublement du point P :

Les formules vues ci-dessus restent valables ,

représente dans ce cas le coefficient angulaire de la tangente à la courbe en P :

$$= -\frac{\frac{\partial f}{\partial x}(p_1, p_2)}{\frac{\partial f}{\partial y}(p_1, p_2)} = \frac{3p_1^2 + 2a_2 p_1 + a_4 - a_1 p_2}{2p_2 + a_1 p_1 + a_3} .$$

Chapitre IV : Application des courbes elliptiques

Introduction :

Les courbes elliptiques ont toujours attiré l'attention des mathématiciens ,en particulier depuis le jour ou Andrew Wiles a réussi ,en les utilisant , à démontrer le grand théorème de Fermat .

Les développements qu'elles permettent n'avaient pas échappé dès 1985 à l'attention des personnes s'intéressant à la cryptographie .

Utilisation :

L'intérêt qu'on l'on choisi deux points p_1 et p_2 de la courbe et que l'on trace la droite $\left(p_1 p_2\right)$,celle-ci recoupe la courbe en un troisième point p'_3 .

En prenant p'_3 symétrique de p_3 par rapport à ox .on peut définir une addition des points : $p_1 + p_2 = p_3$.

IV-1/ Théorème de Fermat :

Proposition (petit théorème de Fermat)

Soit p un nombre premier .Tout entier a satisfait :

$a^p \equiv a(\bmod p)$.

de plus si a n'est pas divisible par p alors $a^{p-1} = 1 \ (\bmod p)$.

Preuve :

Considérons d'abord le cas ou p ne divise pas a ,alors $a \in F_p^{\iota}$.

Par conséquent ,nous avons $a^{p-1} \equiv 1 \pmod{p}$.

Si nous multiplions les deux membre par a nous obtenons $a^p \equiv a \pmod{p}$

si p divise a alors $a \equiv 0 \pmod{p}$ .donc c'est trivial .

Ce théorème (Fermat) permet d'introduire la notion ne nombres pseudo premiers.

Définition :

Un nombre est dit pseudo premier en base b est un nombre composé impair n qui se divise pas par b et tel que :

$b^{n-1} = 1 \pmod{n}$

Théorème d'Euler :

Si p un nombre impair alors pour tout nombre x premier avec p,on a :

$x^{(p-1)/2} \equiv 1 \pmod{p}$

Preuve :

On a $x^{p-1} \equiv 1 \pmod{p}$.

Donc $x^{(p-1)/2}$ est une racine de l'équation $x^2 - 1 = 0$ dans le corps F_p .

D'ou $x^{(p-1)/2} \equiv 1 \pmod{p}$ ou $x^{(p-1)/2} \equiv -1 \pmod{p}$.

Montrons que l'ensemble des carrés de F_P^{ι} coïncide avec les $x \in F_P^{\iota}$ tels que :

$x^{(p-1)/2} = 1$.

Si x est un carré de F_P^{ι} , $x = y^2$ alors $x^{(p-1)/2} = y^{p-1} = 1$.

Montrons que seuls les carrés de F_p^{ι} sont tels que $x^{(p-1)/2} = 1$.

Tout d'abord ,il y a exactement (p-1)/2 carrés dans F_P^{ι} .

En effet , $a^2=b^2 \Leftrightarrow a=b$ ou a = -b .

De plus l'application de $F_P^{\times}$ dans $\{1, -1\}$ qui associe x par $x^{(p-1)/2}$ est surjective et est un morphisme de groupe .

Donc le noyau contient (p-1)/ 2 éléments .

IV-2/ Factorisation d'un entier par les courbes elliptiques :

L'exponentielle elliptique s'applique à la cryptographie de façons diverses.

En particulier ,elle donne naissance à un algorithme de factorisation .

Montrons comment utiliser l'exponentielle modulaire pour factoriser . Voici un algorithme probabiliste appelé *algorithme p-1 de Pollard* :

Supposons que l'on souhaite trouver un diviseur non trivial de l'entier n, et que ce dernier admette un facteur premier p assez particulier, en ce sens que p-1 soit suffisamment fiable. Rappelons que ça signifie que tous les facteurs premiers de p-1 sont inférieurs à un certain entier A <<n. Alors on peut affirmer que A ! est un multiple de p-1.

Dans ce cas d'après le petit théorème de Fermat , on a pour tout entier a,

$a^{A!} \equiv 1 \bmod p$

En d'autres termes , $a^{A!}-1$ est un multiple de p .L'idée alors est de choisir au hasard un nombre a, et de calculer $a^{A!}$ mod. .Puis à l'aide de l'algorithme d'Euclide ,le pgcd de n et de $a^{A!}-1$ modulo n qui est un multiple de p .

On s'arrange pour choisir une équation $y^2=x^3+ax+b$ vérifiant $4a^3+27b^2 \neq 0$ sur n'importe quel corps fini F_P ou p / n ; pour cela il suffit de vérifier que $p \gcd(n, 4a^3+27b^2)=1$. Parallèlement , on choisit (x,y) vérifiant l'équation précédente modulo n .En particulier,cela veut dire que si l'on réduisait (x,y) modulo un diviseur p de n , on obtiendrait un point P de la courbe elliptique C associée à l'équation précédente sur F_P .

Ensuite on choisit un entier A d'une taille raisonnable ,et on effectue modulo n le calcul de A ! .P , c'est à dire à l'aide d'une application répétée des formules citées en deuxième chapitre

prises modulo n- on obtient un couple (X,Y) qui , s'il était réduit modulo p, donnerait le point A ! . P de a courbe elliptique C .

IV-3/ Les crypto systèmes basés sur les courbes elliptiques :

Les cryptosystèmes ont fait l'objet d'études intensives, depuis que N.Koblitz et V.Muller ont proposé l'utilisation des courbes elliptiques en cryptographie .

L'intérêt particulier est le fait que ces cryptosystèmes offrent le même niveau de sécurité que d'autres cryptosystèmes largement utilisés pour la signature et l'authentification (comme RSA) ,mais avec des clés de taille inférieure .Ceci les rend très attractifs pour les applications qui nécessitent des ressources très limitées(mémoire,puissance,bande passante….) telles que cartes à puces, téléphonie mobile ou communication par satellite .

La cryptographie à clé publique « le RSA » :

La méthode de cryptographie RSA a été inventé en 1977 par Ron Rivest ,Adi Shamir et Len Adleman .

Le RSA est encore le système cryptographique le plus utilisé de nos jours .

Principe de fonctionnement :

Si Bob souhaite recevoir des messages en utilisant le RSA , il procède de la façon suivante :

Création des clés :

Bob crée 4 nombres p,q,e et d :

* p et q sont deux grands nombres premiers distincts .Leur génération se fait au hasard , en utilisant un algorithme de test de primalité probabiliste.

* e est un entier premier avec le produit (p-1)(q-1).

* d est tel que ed = 1modulo(p-1)(q-1) . Autrement dit, ed-1 est un multiple de (p-1)(q-1).

On peut trouver d à partir de e, p et q ,en utilisant l'algorithme d'Euclide.

Distribution des clés :

Le couple (n,e) constitue la clé publique de Bob .Il la rend disponible par exemple en la mettant dans un annuaire .

Le couple (n,d) constitue sa clé privé .Il la garde secrète.

Envoi du message codé :

Alice veut envoyer un message codé à Bob .Elle le représente sous forme d'un u plusieurs entiers M compris entre 0 et n-1.

Alice possède la clé publique (n,e) de Bob .

Elle calcule $C = M^e$ mod n .C'est ce dernier nombre qu'elle envoie à Bob .

Réception de message codé :

Bob reçoit C et il le calcule grâce à sa clé privée $D = C^d (\mathrm{mod}\, n)$.

D'après le théorème d'Euler, $D = M^{de} = M (\mathrm{mod}\, n)$.

Il a donc reconstitué le message initial.

Les courbes elliptiques et le problème du logarithme discret :

Les courbes elliptiques peuvent être définies sur des corps finis ,et les munir d'une addition à partir de la donnée du point P et de l'entier d,nous pouvons calculer le point Q tel que :

$$Q = dP$$

Le problème inverse ,consistant à trouver d en supposant Pet Q connus(problème dit du logarithme discret sur les courbes elliptiques) est très difficile à le résoudre lorsque la courbe elliptique est définie sur un corps fini .

Implémentation de l'algorithme généralisé de Montgomery :

L'algorithme de Montgomery a été introduit par Montgomery et s'appliquait seulement sur une catégorie spéciale des courbes elliptiques.

Récemment, cette méthode est devenue également applicable aux courbes elliptiques définies sur des corps premiers finis grâce aux formule d'addition et de doublement .

Soit E une courbe elliptique définie sur un corps premier F_p par l'équation suivante :

$y^2 = x^3 + ax + b$.

Les formules d'addition et de doublement des points d'une courbe elliptique définie sur un corps premier ,en se basant sur la technique de Montgomery ,sont données par les propositions suivantes :

Proposition 1:

Soient $P = (x, y)$ et Q = (x',y') deux points de la courbe ,avec $P + Q = (x'', y'')$

La x-coordonnée de P+Q vérifie :

$$x(P+Q) = \frac{-4\,(x+x')+(xx'-a)^2}{x''(x-x')} \ .$$

Si $y \neq 0$, alors la x-coordonnée de 2P vérifie :

$$x(2P) = \frac{(x^2-a)^2 - 8\ dx}{4\,(x^3+ax+b)}$$

La proposition suivante nous donne la formule pour retrouver la y-coordonnée d'un point P à partir de sa x-coordonnée , de la x-coordonnée d'un autre point Q ,et des coordonnées du point P-Q .

Proposition 2 :

Soient $P = (x, y), Q = (x', y')$ deux points de la courbe elliptique avec $P + Q = (x'', y'')$.

Si $y \neq 0$, la y-coordonnée de P vérifie :

$$y(P) = \frac{2b + (a + xx')(x + x") - x'(x" - x)^2}{2y"} .$$

Implémentation en coordonnées projectives standards :

En utilisant les coordonnées projectives standards , le point (X,Y,Z) correspond au point affine $\left(\frac{X}{Z}, \frac{Y}{Z} \right)$.

On garde le point P-Q en coordonnées affines (x,y).

Les formules d'addition , de doublement et de détermination de la y-coordonnée deviennent :

Addition :

$$X" = -4\ bZZ'(XZ' + X'Z) + (XX' - aZZ')^2$$
$$Z" = x(XZ' - X'Z)^2$$

Doublement :

$$X"' = (X^2 - aZ^2)^2 - 8\ bXZ^3$$
$$Z"' = 4Z(X^3 + aX^3 + aXZ^2 + bZ^3)$$

Détermination de la y-coordonnée :

$$y(P) = 2\ bZ^2 Z' + Z'(aZ + xX)(xZ + X) - X'(xZ - X)^2$$
$$Z(P) = 2Z^2 Z' y$$

Ces formules nous ont permis d'obtenir un des algorithme les plus efficaces de multiplication scalaire sur les courbes elliptiques définies sur les corps premiers .

Il est donée comme suit :

Algorithme :

Input : un entier positif k et un point P=(x,y) de la courbe .

Output : $Q = kP$.

1.Si k=0 ou x=0 renvoyer (0,0).

2.Faire $k \leftarrow (k_l \ldots\ldots\ldots k_0)_2$.

3.Faire $X \leftarrow x, Z \leftarrow 1, X' \leftarrow X^2 - aZ^2 - 8\ bXZ^3, Z' \leftarrow 4Z(X^3 + aXZ^2 + bZ^3)$

4.Pour i de i à 0 faire

si $k_i = 1$ alors ECCaddoub(X,Z,X',Z')

sinon ECCaddoub(X',Z,X,Z)

5.Renvoyer Q=ECCrecouv(X,Z,X',Z') .

Conclusion :

Les courbes elliptiques ont un grand avantage ,à savoir si nous adaptons des protocoles cryptographiques sur les courbes elliptiques ,la taille des clés sera de plus en moins plus petite pour une sécurité équivalente et qu'il est possible de travailler sur des corps finis en se basant sur l'addition et le doublement des points d'une courbes elliptique .

Bibliographie

[1] Gilles Zemor : Cours de cryptographie.

[2] Gilles Dubertret : Initiation à la cryptographie.

[3] Neal Koblitz : Introduction to elliptic and moduler forms.

[4] E.Breir ; M .Joye:Weierstrass Elliptic Curve and side –channel Attacks.

[5] Peter L . Montgomery: Speeding the pollard and elliptic curve method of factirisation.

[6] Jean –Marc Couveignes; François Morain : Théorie algorithmique des nombres.