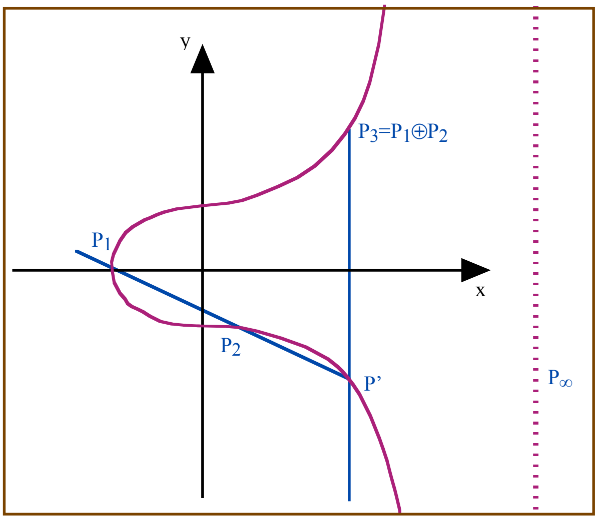
Structure de groupe sur les Courbes elliptiques réelles

http://www.certicom.com/resources/ecc_tutorial/ecc_tutorial.htlm



Définition

Soient (a,b) un couple de réels tels que $4a^3 + 27b^2$!= 0.

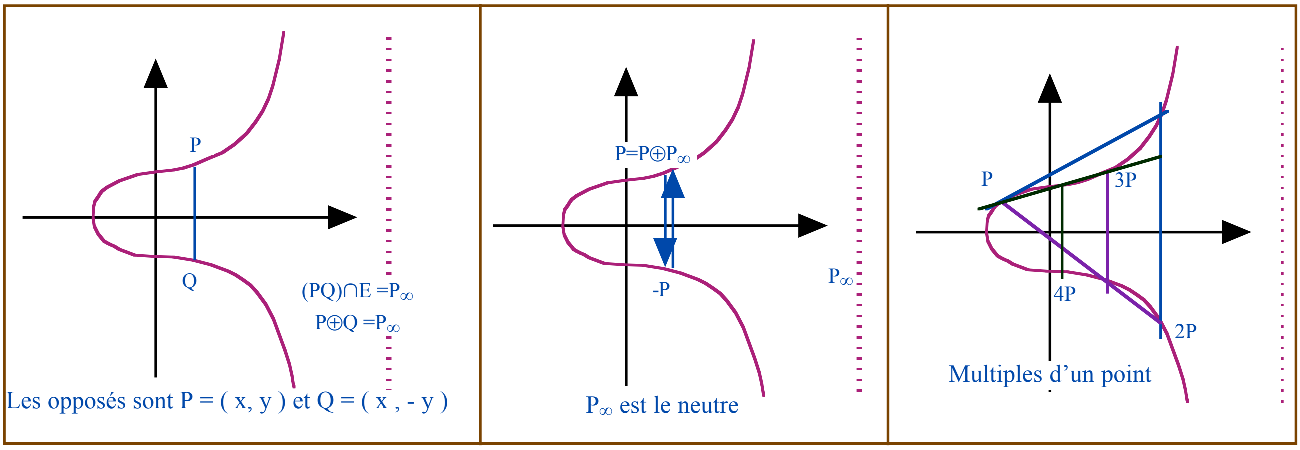
$E_{a,b}$ est la réunion des points (x,y) tq $y^2 = x^3 + ax + b$ et de la direction de la droite (Oy).

La direction de (Oy) s'appelle le point à l'infini, noté P_∞.

L'addition $\oplus$ sur les points de Ea,b se fait selon le schéma ci-contre. Les cas particuliers sont gérés par l'utilisation des tangentes en lieu des sécantes.

Elle munit la courbe elliptique d'une structure de groupe abélien: associativité , élément neutre , existence d'opposé pour tout point, commutativité.

Quelques exemples:



Justifier les résultats suivants

Résultats: $4\ a^3 + 27\ b^2 \neq 0$ (La condition s'impose pour que la courbe soit sans point singulier)

- **Le point à l'infini est élément neutre:** $P_\infty \oplus P = P$
- **Pour P_1 et P_2 distincts, $P_1 \neq P_\infty$, $P_2 \neq P_\infty$**, les coordonnées du point $P_3 = P_1 \oplus P_2$ se calculent par

  Pour $P_i = (x_i , y_i)$,

  $x_3 = \lambda^2 - x_1 - x_2$ et $y_3 = \lambda (x_1 - x_3) - y_1$.

  où λ est la pente de la droite (P_1 P_2) (si $P_1 \neq P_2$)
- **Pour le point $P_{\infty/2}$ d'ordonnée nulle**, à tangente verticale: $P_{\infty/2} \oplus P_{\infty/2} = P_\infty$
- **Pour $P \neq P_\infty$, $P\oplus P$ a pour coordonnées** $x_3' = \lambda^2 - 2x$ et $y_3 = \lambda (x - x_3) - y$ où λ est la pente de la tangente passant en P, i.e $\lambda = (3\ x^2 + a) (2\ y)^{-1}$.

Etude de la suite des multiples d'un point $(nP)_n$.

CNS pour que cette suite converge (passer à la limite dans la formule de récurrence (n+1)P = nP + P)
CNS pour que les sous-suites (2nP) et ((2n+1)P) convergent.
CNS pour que les sous-suites (3nP), ((3n+1)P) et ((3n+2)P) convergent.

Les courbes elliptiques dans un corps fini, et leur structure de groupe

a) Définitions

Soit un corps commutatif F_p contenant un nombre fini d'éléments noté p, p > 3.

Si p est premier F_p est Z/pZ. Autrement, p ne contient qu'un seul nombre premier dans sa décomposition.

On utilise les mêmes définitions et les mêmes règles de calcul sur ce corps fini:

Un groupe elliptique $E_{a,b}(p)$ de F_p est l'ensemble des points d'équation $y^2 = x^3 + a\,x + b$ auquel on adjoint un point à l'infini. La condition $4\,a^3 + 27\,b^2 \neq 0$ s'impose pour que la courbe soit sans point singulier.

La strucutre de groupe s'obtient à partir de l'opération ⊕ suivante:

- **Le point à l'infini est élément neutre:** $P_\infty \oplus P = P$
- **Pour P_1 et P_2 distincts, $P_1 \neq P_\infty$, $P_2 \neq P_\infty$,** les coordonnées du point P_1P_2 se calculent par

  Pour $P_i = (x_i , y_i)$,

  $$x_3 = \lambda^2 - x_1 - x_2 \quad \text{et} \quad y_3 = \lambda\,(x_1 - x_3) - y_1 .$$

  où λ est la pente de la droite $(P_1\ P_2)$ (si $P_1 \neq P_2$)
- **Pour le point $P_{\infty/2}$ d'ordonnée nulle,** à tangente verticale: $P_{\infty/2} \oplus P_{\infty/2} = P_\infty$
- **Pour $P \neq P_\infty$, $P \oplus P$ a pour coordonnées** $x_3' = \lambda^2 - 2x$ et $y_3 = \lambda\,(x - x_3) - y$ où λ est la pente de la tangente passant en P, i.e $\lambda = (3\,x^2 + a)\,(2\,y)^{-1}$.

b) Obtention de la courbe elliptique $E_{a,b}$:

Une méthode rudimentaire pour obtenir le groupe elliptique $E_{a,b}(p)$ de F_p d'équation $y^2 = x^3 + a\,x + b$. est de réaliser une double boucle:

```
Calcul des éléments du groupe elliptique Ea,b d'équation y² = x³ + a x +b

 • Boucle: ( x de 0 à p-1 )
    • Boucle ( y de 0 à p-1 )
         • Si y² = x³ + a x +b compléter Ea,b avec (x,y)
    • FinBoucle
 • FinBoucle
```

Programmer cette double boucle

Le groupe elliptique $E = E_{1,1}$ ($y^2 = x^3 + x + 1$) dans le plan $F_{37} \times F_{37}$ contient les points (vous ne les trouverez pas dans cet ordre avec l'algorithme de la double boucle)

x	30	14	2	21	33	36	17	28	27	29	6	35	10	13	1	9
y	13	24	14	25	28	31	26	22	29	31	36	18	7	18	22	6
x	31	24	19	0	11	26	8	25	8	26	11	0	19	24	31	9
y	36	14	16	36	23	18	15	0	22	19	14	1	21	23	1	31
x	1	13	10	35	6	29	27	28	17	36	33	21	2	14	30	∞
y	15	19	30	19	1	6	8	15	11	6	9	12	23	13	24	∞

Visualiser sur une même figure matlab plusieurs groupes elliptiques du plan $F_{37} \times F_{37}$

Le corps F_{49} est obtenu en adjoignant au corps F_7 .un élément *i* de carré valant -1. Ainsi, les éléments de F_{49} sont décrits par $z = a + i\,b$, (a,b) parcourant $F_7 \times F_7$.

Définir un élément z de F_{49} comme une structure à trois champs z.a et z.b, z.num, le dernier champ étant le numéro du complexe (de 0 à 48)

Visualiser sur une même figure matlab plusieurs groupes elliptiques du plan $F_{49} \times F_{49}$

Les complexes sur F_5 ne fonctionnent pas directement: Pourquoi?

Comment faire des groupes elliptiques dans le plan $F_{25} \times F_{25}$

c) Structure de groupe sur une courbe elliptique:

Pour ne pas alourdir la programmation, on se limite au cas des corps $\mathbb{F}_p$ avec p premier.

rq pratique:

Pour réaliser les calculs, on a besoin de faire des divisions, i.e de connaître l'inverse dans $\mathbb{Z}/p\mathbb{Z}$:

(Attention à la fonction modulo sur les entiers négatifs)

Calcul de l'inverse de b modulo p (algorihme d'Euclide étendu)

- u_0 <--- 0, u_1 <--- 1 , r_0 <--- p , r_1 <--- mod (b , p).
- Boucle:
    - r_2 <--- r_0 mod r_1, q_1 <--- r_0 div r_1
    - Sortir si $r_2 = 0$, et l'inverse de b modulo p est u_1.
    - r_0 <---r_1 , r_1 <---r_2 , aux <--- u_1 , u_1 <--- Mod(u_0 - q_1 u_1 , b) , u_0 <--- aux
- FinBoucle

Tester votre fonction, et présenter ces tests.

Faire une fonction C calculant P+Q dans $\mathbb{Z}/p\mathbb{Z}$, sachant que P et Q sont dans $E_{a,b}$

exemple d'opération: (9 , 6) et (1 , 15) sont sur $E_{1,1}$ car $6^2 = 9^3 + 9 + 1$ et $15^2 = 1^3 + 1 + 1$

$\lambda = (15 - 6).(1 - 9)^{-1} = 22$, $x = \lambda^2 - 1 - 0 = 30$ $y = \lambda\,(9 - 30) - 6 = 13$

On a donc (9 , 6) $\oplus$ (1 , 15) = (30 ,13)

Recherche du groupe engendré par un point p:

Ce groupe comporte ν éléments: < p > = { ∞ , p , 2p , 3p , ... , (ν - 1) p }, ν étant caractérisé comme étant le premier entier réalisant ν p = ∞.

Le dernier élément de la liste (et donc le test d'arrêt) correspond à l'opposé de p.

Groupe < p > engendré par un point p appartenant au groupe $E_{a,b}$

- Si l'ordonnée de p est 0, < p > = { p , ∞ } , et FIN
- Calculer q = p $\oplus$ p et l'ajouter à < p >

    © La pente est $\lambda = (3\, x_p^2 + a) . (2\, y_p)^{-1}$

- Boucle:
    - Si l'opposé de q est p, compléter < p > avec ∞. FIN
    - Calculer q <--- q $\oplus$ p et l'ajouter à < p >

        © La pente est $\lambda = (y_q - y_p) . (x_q - x_p)^{-1}$

- FinBoucle.

Exemple: Le groupe engendré par (0 ,1) du groupe elliptique E = $E_{1,1}$ dans le plan $\mathbb{F}_{37} \times \mathbb{F}_{37}$:

x	0	28	35	9	21	25	21	9	35	28	0	∞
y	1	22	19	6	12	0	25	31	18	15	36	∞

.

Factorisation d’un entier par la méthode des courbes elliptiques de Lenstra.

Le principe:

***** Si on connaît un élément x de $\mathbb{Z}/n\mathbb{Z}$, non inversible, alors GCD (x , N) est différent de 1 et fournit un diviseur non trivial de n *****

En effet, si on envisage les deux possibilités:

- Si GCD (x, N) = 1, alors il existe (Bezout) un couple (u , v) d’entiers relatifs tel que x u + N v = 1.On en déduit que x(-u) = 1 Mod N, et x admet -u comme inverse modulo N.
- Si g = GCD (x, N) > 1, alors y = N/g est un entier, et x y = N (x / g) = 0 Mod N.Dans l’égalité x y = 0, on ne peut pas simplifier par x, ce qui veut dire que x n’est pas inversible.

La méthode de Lenstra:

***** Réaliser un parcours dans $\mathbb{Z}/n\mathbb{Z}$, qui nous fasse rencontrer un élément non inversible *****

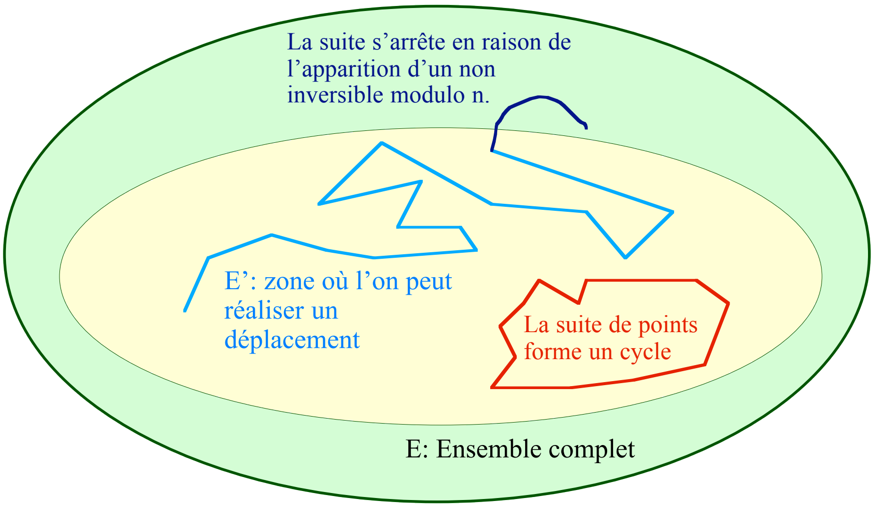
n est un entier premier avec 6. Une courbe elliptique $E_{a,b}(n)$ est la partie de $(\mathbb{Z}/n\mathbb{Z})\times(\mathbb{Z}/n\mathbb{Z})$ définie par l’équation cartésienne: $y^2 = x^3 + a\,x + b$, $4\,a^3 + 27\,b^2$ doit être inversible.

En complétant $E_{a,b}(n)$ par un objet que l’on note ∞, point à l’infini, on peut définir une opération $\oplus$ non partout définie:

Principe de l’algorithme de Lenstra:

Ce qui est recherché, c’est l’apparition d’une impossibilité de poursuivre la liste des multiples de P_0. En effet si (x , y) est le dernier point cherché, et (x_0 , y_0) les coordonnées de P_0, on a alors $GCD(x - x_0, N)$ qui est un facteur >1 de N.

Quand on tombe sur un cycle, on peut retenter un trajet sur une autre courbe (changer a).



Factorisation d’un entier p (Elliptic Curve Method)

- Choisir un point P de [1..p-1]x[1..p-1]
- Boucle (a)
  - Choisir a dans [1 .. p-1]
  - Boucle (n)
    - Calculer n P
    - sortir si des deux boucles si un non inversible μ est trouvé
  - fin (boucle)
- fin(Boucle)
- Le pgcd de p et μ est un diviseur de p.

Annexe1: **Algorithme d'Euclide étendu**

Cet algorithme fournit l'inverse u d'un entier r_0 modulo r_1: Il résout donc l'équation

$$u\, r_0 = 1 \quad \text{mod } r_1$$

On pose l'algorithme d'Euclide usuel: liste de divisions euclidiennes successives jusqu'à un reste nul.

$r_0 = q_1\, r_1 + r_2 \qquad 0 < r_2 < r_1$

$r_1 = q_2\, r_2 + r_3 \qquad 0 < r_3 < r_2$

...

$r_{m-2} = q_{m-1}\, r_{m-1} + r_m \qquad 0 < r_m < r_{m-1}$

$r_{m-1} = q_m\, r_m \qquad 0 < r_m < r_{m-1}$

On a pgcd(r_0 , r_1) = pgcd(r_1 , r_2) = ... = pgcd(r_{k-1} , r_k) = ... = pgcd(r_{m-1} , r_m) = r_m

Une première application est donc le calcul du PGCD.

La suite initialisée par $u_0 = 0$, $u_1 = 1$ et vérifiant la récurrence $u_k = \text{Mod}(u_{k-2} - q_{k-1}\, u_{k-1} , r_0)$ vérifie pour tout entier k $\leq m$, $r_1\, u_k \equiv r_k$ modulo r_0.

Preuve:

La proposition est vraie pour k = 0 et k = 1. Supposons $r_1\, t_{k-2} \equiv r_{k-2}$ et $r_1\, t_{k-1} \equiv r_{k-1}$ modulo r_0 ,

$r_1\, u_k \equiv r_1\, u_{k-2} - q_{k-1}\, r_1\, u_{k-1}$

et $r_1\, u_k \equiv r_{k-2} - r_{k-1}\, q_{k-1} = r_k$

En parcourant l'algorithme d'Euclide et en tenant à jour la suite t_k, on obtient simultanément

- r_m = pgcd (r_0 , r_1)
- Une écriture $r_m = r_1\, u_m + r_0\, v$ { v à calculer par $v = (r_m - r_1\, u_m) / r_0$ }

Lorsque r_0 et r_1 sont premiers entre eux, u_m est l'inverse de r_1 dans $Z / r_0 Z$.

Annexe 2: Cryptage à l'aide des courbes elliptiques