MT10

Mathématiques pour la cryptographie

Partie 3

Courbes Elliptiques

Walter SCHÖN

Cryptosystèmes basés sur les courbes elliptiques

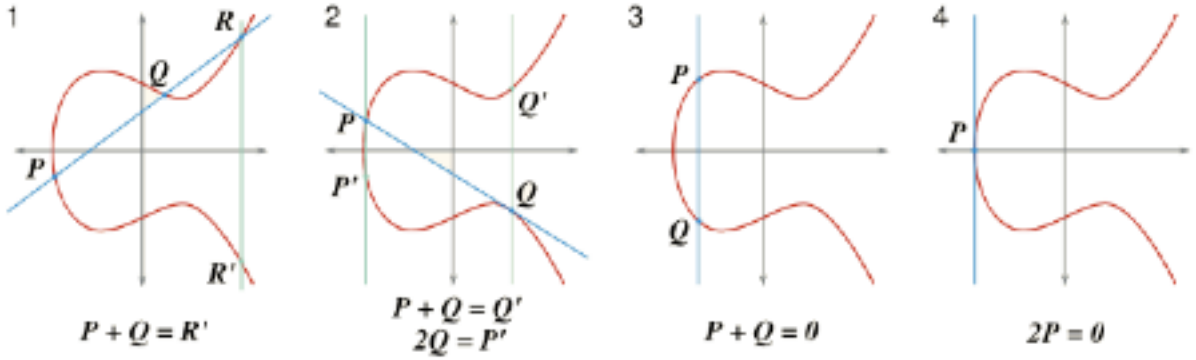
- Sont probablement l'avenir des cryptosystèmes à clé publique
- Sont basés sur les courbes elliptiques (cubiques non singulières) sur les corps dans lesquels est définie une loi de groupe (« addition » de points)
- Les éléments du groupe sont les points de K*K (où K est un corps) vérifiant une équation du troisième degré dite Equation de Weierstrass (peut être réduite pour K de caractéristique différente de 2 et 3) :

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

- Auxquels est ajouté un point à l'infini qui est l'élément neutre de la loi de groupe
- Les courbes elliptiques ont été utilisés par Andrew Wiles dans la démonstration du théorème de Fermat en 1994

Cryptosystèmes basés sur les courbes elliptiques

- La définition de la loi de groupe « addition » des points peut être vue graphiquement de la manière suivante :



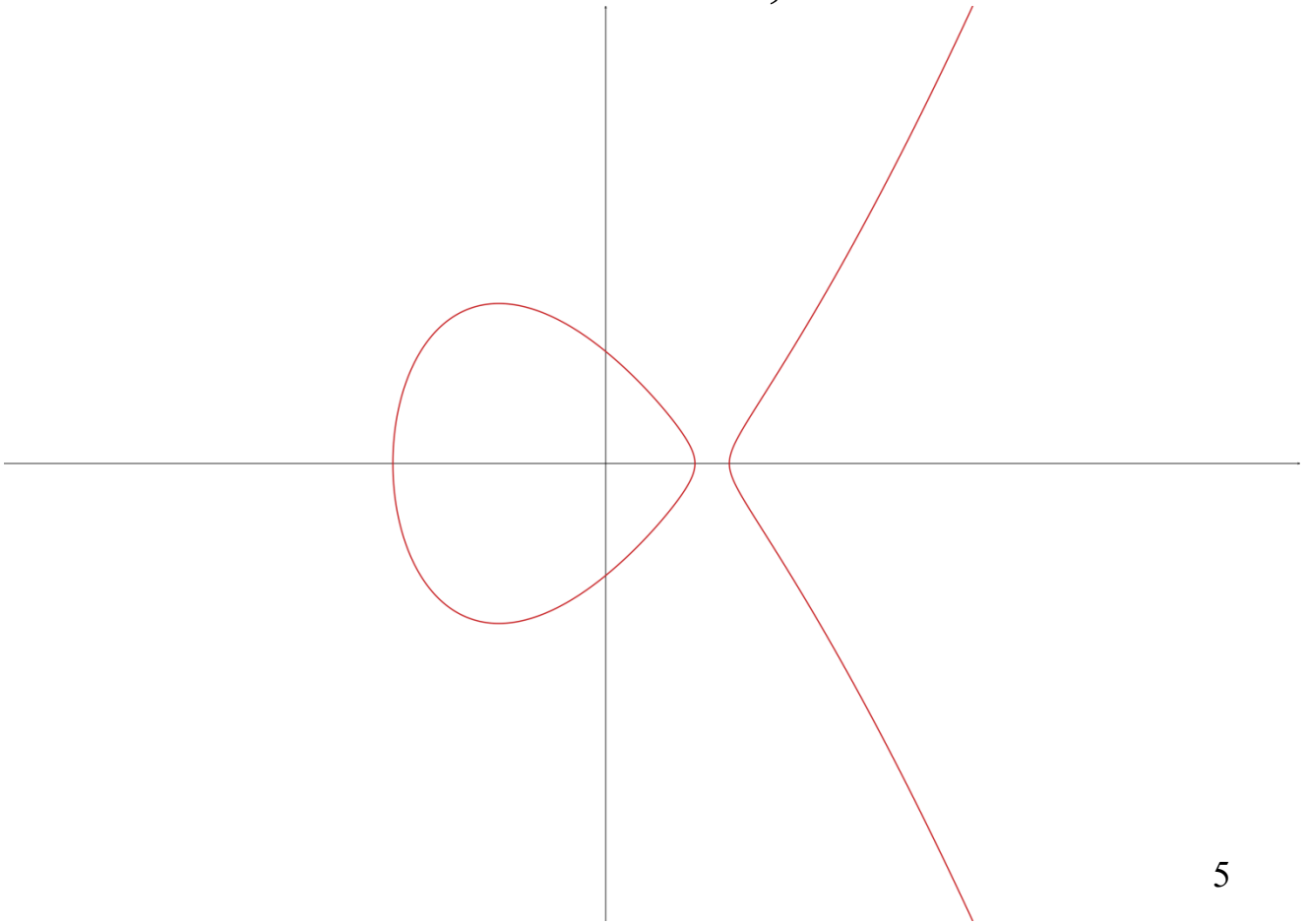
- Il est alors facile de « multiplier » un point par un entier n (l'additionner n fois avec lui même)
- Il est très difficile d'effectuer l'opération inverse (problème analogue au logarithme discret) : utilisé donc pour des cryptosystèmes à clé publique très robustes avec des clés plus petites

Courbes elliptiques

- On appelle courbe elliptique les points c'est à dire les doublets (x,y) de K*K (où K est un corps) vérifiant l'équation de Weierstrass $y^2 = x^3+px+q$ (en général p et q appartiennent à K, mais on peut envisager qu'ils appartiennent à un sous-corps)
- Le polynôme x^3+px+q doit de plus ne pas avoir de racine multiple (cubique non singulière) ce qui se traduit par $4p^3+27q^2 /= 0$
- Le corps K peut être Q, R, C ou n'importe lequel des corps finis étudiés ci-avant $F(p^m)$ avec p premier et m entier strictement positif (p différent de 2 ou 3)
- Le cas des corps de caractéristique p égale 2 ou 3 est particulier et contraint à l'usage de l'équation de Weierstrass généralisée $y^2+a_1xy+a_3y=x^3+a_2x^2+a_4x+a_6$

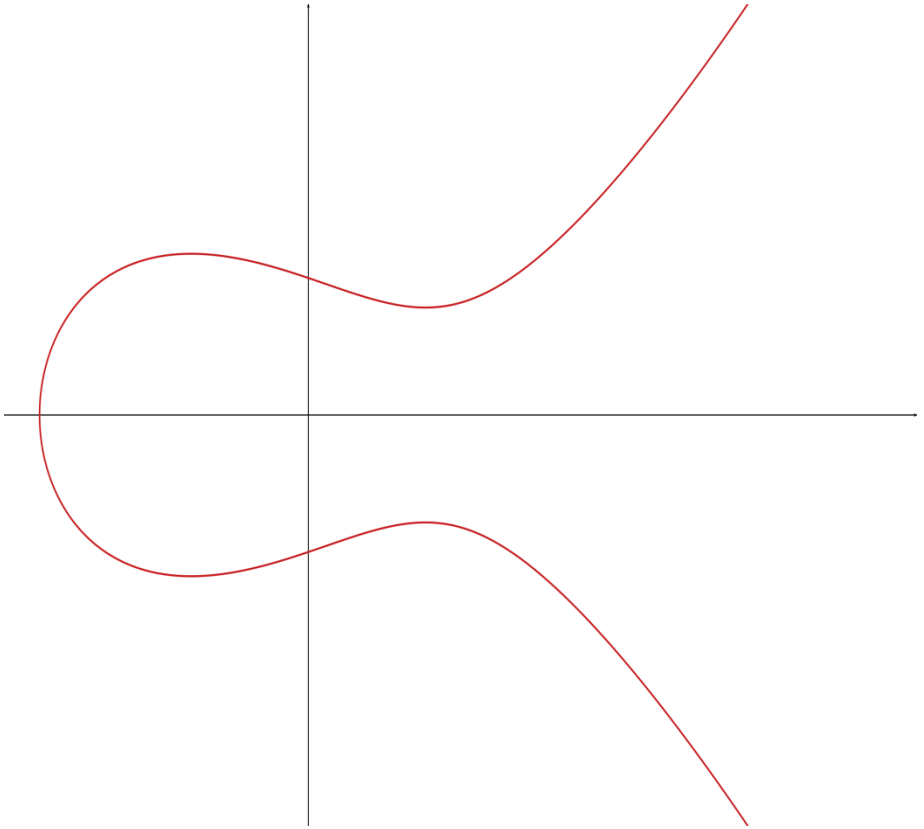
Courbes elliptiques

- Il est pratique d'illustrer les calculs sur les courbes elliptiques car le cas des courbes définies sur R où les opérations ont une interprétation géométrique simple
- Lorsque x^3+px+q a trois racines réelles distinctes, la courbe a l'allure suivante :



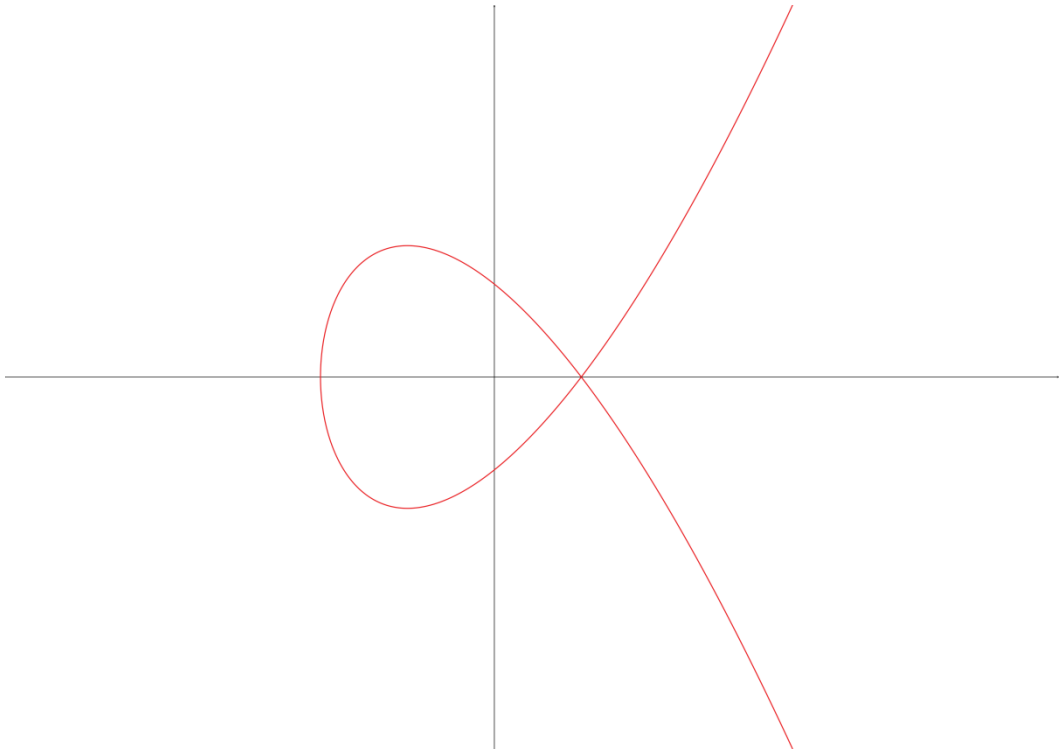
Courbes elliptiques

- Lorsque x^3+px+q n'a qu'une racine réelle, la courbe a l'allure suivante :

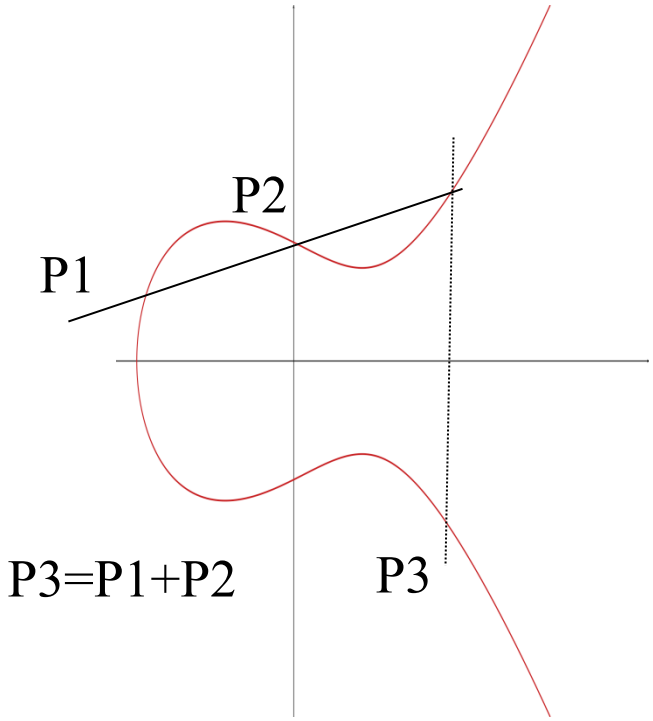


Courbes elliptiques

- Lorsque x^3+px+q a une racine double la courbe a l'allure suivante : il existe un point où la courbe n'admet pas de tangente. Dans le cas d'une racine triple la courbe a un point anguleux et n'admet non plus pas de tangente en ce point. Ces deux cas sont dits singuliers



Courbes elliptiques : loi de groupe



- ✓ Sur une courbe elliptique non singulière est définie une loi de groupe notée « addition des points » avec la règle suivante :
- ✓ Une droite non parallèle à l'axe des y passant par deux points de la courbe passe nécessairement par un troisième (qui peut dans certains cas coïncider avec P1 ou P2 si la droite P1P2 est tangente à la courbe en P1 ou P2)

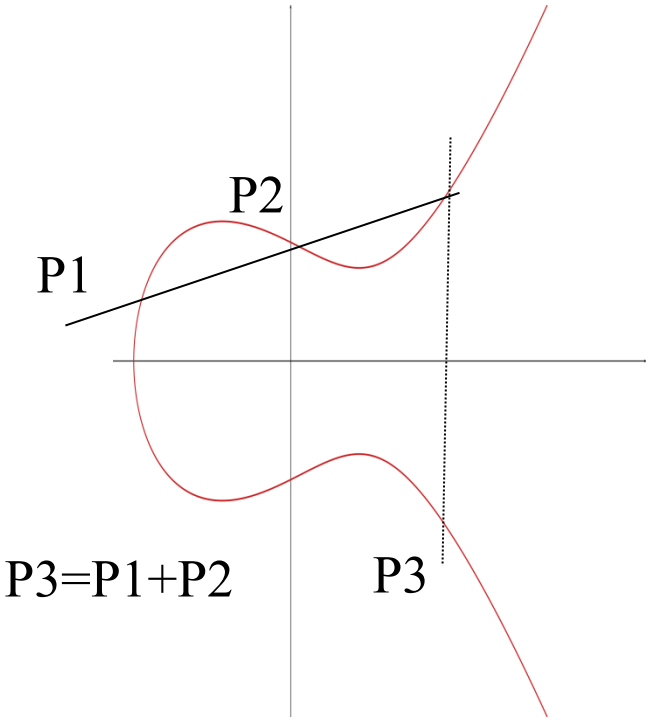
Le point P3 « somme » est par définition le symétrique de ce troisième point d'intersection par rapport à l'axe des abscisses

Courbes elliptiques : loi de groupe

Calcul des coordonnées du point « somme » :

Pente de la droite P1P2

$$m = \frac{(y_2 - y_1)}{(x_2 - x_1)}$$



Equation de la droite $y=y_1+m(x-x_1)$

Equation donnant les points d'intersection de la droite et de la courbe $\left[y_1 + m(x - x_1)\right]^2 = x^3 + px + q$

Soit : $x^3 + px + q - \left[y_1 + m(x - x_1)\right]^2 = 0$

Cette équation a par définition 3 racines x_1, x_2 et x_3, donc cette équation s'écrit également $(x-x_1)(x-x_2)(x-x_3) = 0$ dont le coefficient de x^3 vaut bien 1 et le coefficient de x^2 vaut $-(x_1+x_2+x_3)$

Par conséquent $m^2=(x_1+x_2+x_3)$

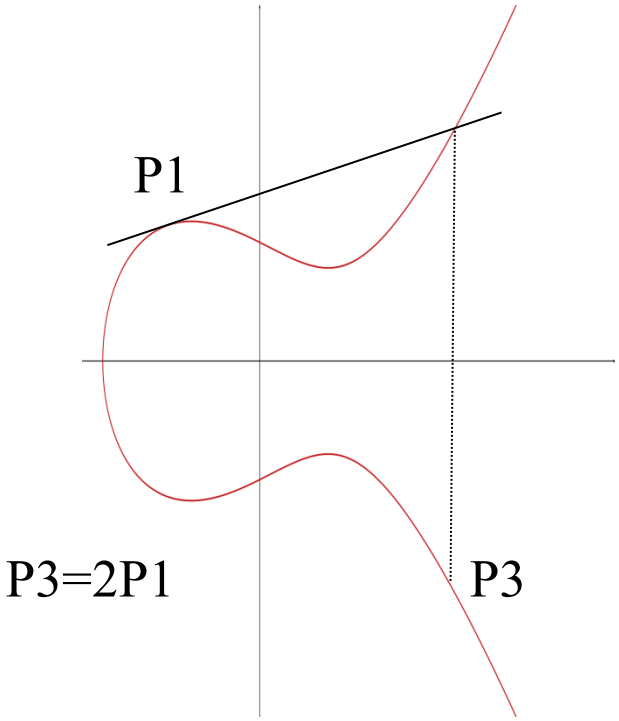
$x_3=m^2-x_1-x_2$ et $y_3=m(x_1-x_3)-y_1$ (opposé de l'ordonnée du point d'intersection).

Ce calcul est valable dès que P1 et P2 sont distincts même lorsque la droite P1P2 est tangente à la courbe en l'un des points P1 ou P2

Courbes elliptiques : loi de groupe

Le cas du « doublement » d'un point est par contre particulier :

Additionner un point avec lui-même consiste à prendre la tangente à la courbe en ce point. La pente de la tangente est donnée par $m = \frac{dy}{dx} = \frac{3x_1^2 + p}{2y_1}$



Equation de la droite $y=y_1+m(x-x_1)$

Equation donnant les points d'intersection de la droite et de la courbe $\left[y_1 + m(x - x_1)\right]^2 = x^3 + px + q$

Soit : $x^3 + px + q - \left[y_1 + m(x - x_1)\right]^2 = 0$

Cette équation a par définition 1 racine double x_1 et une racine simple x_3, donc cette équation s'écrit également

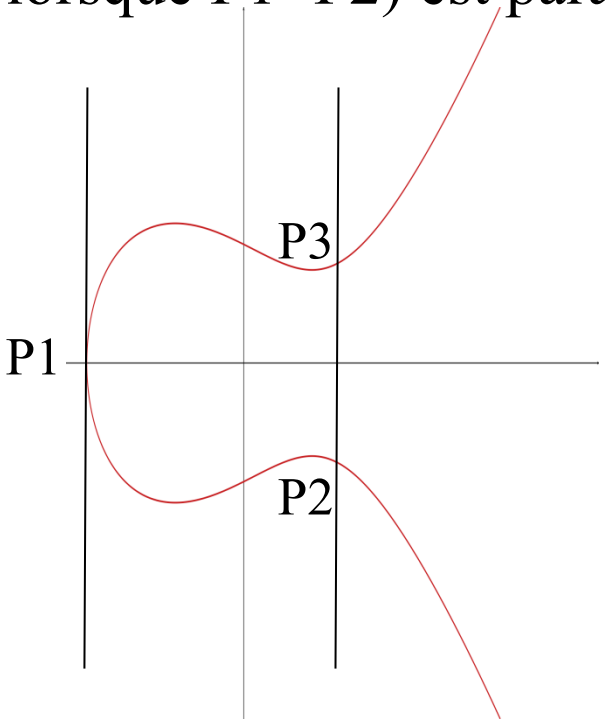
$(x-x_1)(x-x_1)(x-x_3) = 0$ dont le coefficient de x^3 vaut bien 1 et le coefficient de x^2 vaut $-(2x_1+x_3)$

Par conséquent $m^2=(2x_1+x_3)$

$x_3=m^2-2x_1$ et $y_3=m(x_1-x_3)-y_1$ (opposé de l'ordonnée du point d'intersection).

Courbes elliptiques : loi de groupe

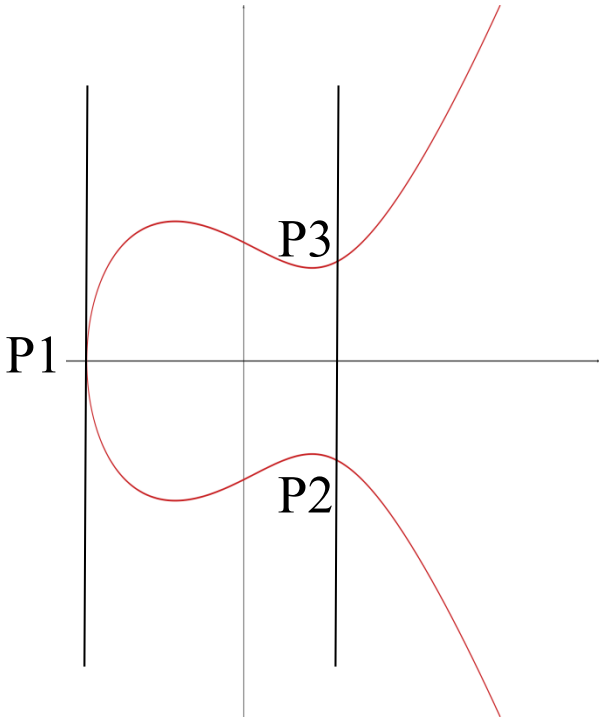
La définition du double d'un point nécessite que la tangente à la courbe soit définie en tout point donc que la courbe ne soit pas singulière (pas de croisement ni de point de rebroussement).
Reste un cas à traiter : celui où la droite P1P2 (ou la tangente en P1 lorsque P1=P2) est parallèle à l'axe des y



On définit alors le « point à l'infini » dans la direction y noté ∞ où toutes les droites parallèles à y (ainsi que la courbe lorsque x et y tendent vers l'infini) se rencontrent.
Considérez (formalisation rigoureuse ci-après) que toutes les droites parallèles à y se rencontrent en ce point, qui n'est ni en haut ni en bas (ou à la fois en haut et en bas), ou peut être derrière ce tableau ?
Cette considération vaut pour toute direction du plan, il y a un point à l'infini pour chaque direction possible des droites du plan.

Courbes elliptiques : loi de groupe

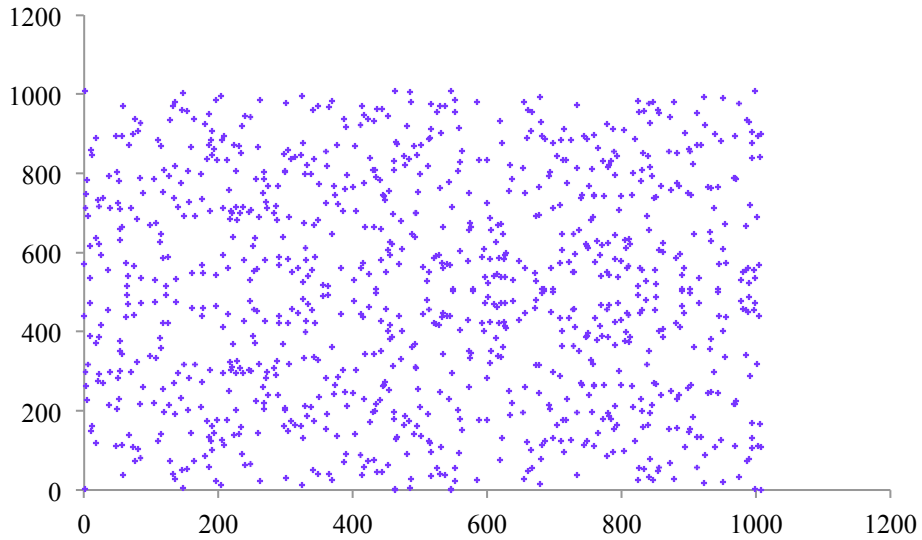
On rajoute alors ce « point à l'infini » comme élément du groupe, dont il constitue l'élément neutre pour la loi de groupe « addition ».



Par définition dans cet exemple :
$2P1=P2+P3=\infty$
Par ailleurs quel que soit le point P élément du groupe (donc y compris pour ∞ lui même) :
$P+\infty=\infty+P=P$
La loi de groupe est commutative (ce que l'on voit facilement par son interprétation géométrique)
La loi de groupe est bien associative (ce qui est moins évident par des considérations géométriques mais peut être vérifié par l'utilisation des formules explicites données plus haut)

Courbes elliptiques : loi de groupe

Les calculs qui précèdent demeurent valables quel que soit le corps K sous-jacent. Evidemment l'interprétation géométrique qui précède n'est plus très évidente lorsque K est un corps fini…



La courbe elliptique $y^2=x^3+x+2$ définie sur Z/1009Z…

Bien que cela puisse vous paraître encore plus bizarre, il est absolument nécessaire de conserver la notion de point à l'infini.

On a construit une magnifique structure algébrique, entièrement cohérente avec les lois de groupe… bien que pas très intuitive !

Notion de point à l'infini

On vous a sans doute déjà dit que deux droites parallèles se coupent à l'infini…

Oui mais (pensez vous en votre for intérieur…) est-ce l'infini « de devant » ou bien celui « de derrière » ?

Avant de formaliser cela rigoureusement, notez bien qu'il serait fort gênant que deux droites non parallèles se croisent en un point et deux droites parallèles se croisent en deux…

Par conséquent commencez à vous faire à l'idée qu'il n'y a qu'un seul infini qui est à la fois « devant » et « derrière » (en haut et en bas de l'axe y dans le cas de nos courbes elliptiques).
De plus trouvez-vous que la notion « d'en bas » et « d'en haut » ait encore beaucoup de sens quand on travaille dans un corps fini ?

Coordonnées homogènes

✓La formalisation de cette notion passe par l'introduction des coordonnées projectives ou coordonnées homogènes

✓On étend la notion de plan affine sur un corps K qui est l'ensemble des doublets (x,y) où $x,y \in K$

✓Plan projectif sur K : ensemble des classes d'équivalence des triplets (x,y,z), $x,y,z \in K$ et non tous nuls avec la relation d'équivalence notée $\approx$:

✓$(x_1,y_1,z_1) \approx (x_2,y_2,z_2)$ s'il existe $\lambda \in K^*$ / $(x_2,y_2,z_2) = (\lambda x_1, \lambda y_1, \lambda z_1)$

✓La classe d'équivalence est notée (x:y:z) où (x,y,z) est l'un des représentants

✓Si $z \neq 0$, on peut diviser par z et par conséquent les classes correspondantes sont les (x:y:1) $x,y \in K$ qui sont les points « finis » (points du plan affine)

✓Si $z=0$ alors le point est « à l'infini » (au moins l'une des deux autres coordonnées x,y est non nulle). Noter que (x,y,0) et (-x,-y,0) sont deux représentants du même point à l'infini (il n'y a qu'un point à l'infini par direction)

Coordonnées homogènes

✓Un polynôme en x,y,z est dit homogène de degré n si tous ses monômes $ax^iy^jz^k$ où $a \in K$ ont le même degré total n : i+j+k=n pour tout monôme

✓Si F(x,y,z) est un polynôme homogène de degré n, alors pour $\lambda \in K$ $F(\lambda x,\lambda y,\lambda z)=\lambda^n F(x,y,z)$, en particulier si F s'annule pour un représentant d'un point du plan projectif, F s'annule pour tous les représentants de ce point

✓Il faut donc ne manipuler que des polynômes homogènes si l'on veut pouvoir parler de points du plan projectif où le polynôme s'annule

✓Par exemple $x^2+2y-3z$ qui n'est pas homogène s'annule en (1,1,1) mais vaut 2 en (2,2,2)

✓On convient donc de rendre toute expression polynômiale homogène en insérant les puissances de z nécessaires pour la rendre homogène : ainsi l'équation d'une droite non verticale $y=a_1x+b_1$ devient sous forme homogène $y=a_1x+b_1z$

Intersection de deux droites non parallèles

✓ La recherche de points communs à deux droites non verticales revient à rechercher les doublets (x,z) où $(a_2-a_1)x+(b_2-b_1)z=0$, ce qui pour des droites non parallèles ($a_2 \neq a_1$) donne donc :
$x/z = (b_1-b_2)/(a_2-a_1)$ et $y/z=(a_2b_1-a_1b_2)/(a_2-a_1)$ qui donne en coordonnées homogènes le point d'intersection « non à l'infini » que l'on obtient avec des calculs dans le plan affine :
$((b_1-b_2)/(a_2-a_1), (a_2b_1-a_1b_2)/(a_2-a_1), 1)$.

✓ De manière tout à fait semblable la recherche de points communs à une droite non verticale $y=a_1x+b_1$ et une droite verticale $x=c_2$ revient à rechercher les doublets (y,z) où $y=a_1c_2z+b_1z$ soit :
$y/z=a_1c_2+b_1$ et $x/z=c_2$ qui donne en coordonnées homogènes le point d'intersection « non à l'infini » que l'on obtient avec des calculs dans le plan affine : $(c_2, a_1c_2+b_1, 1)$.

Coordonnées homogènes

Cas de droites parallèles non verticales ($a_2=a_1=a$ et $b_2\neq b_1$) :

✓La recherche de points donne cette fois $z=0$ et comme x,y et z sont non tous nuls, $x\neq 0$ et $y=ax$ ce qui donne en coordonnées homogènes le point (1,a, 0) qui représente le point à l'infini dans la direction $y=ax$

Cas de droites parallèles verticales :

✓De même si l'on recherche l'intersection entre deux droites parallèles verticales $x=c_1$ et $x=c_2$ ($c_2\neq c_1$) on obtient en passant en coordonnées homogènes $x=c_1z=c_2z$, soit $z=x=0$ donc nécessairement $y\neq 0$ et les coordonnées homogènes du point d'intersection sont (0,1,0), point à l'infini dans la direction de l'axe y

✓L'équation d'une courbe elliptique $y^2=x^3+px+q$ devient en coordonnées homogènes $y^2z=x^3+pxz^2+qz^3$ dont on retrouve les points du plan affine en faisant $z=1$. Pour trouver les points à l'infini, on fait $z=0$, soit $x=0$ donc $y\neq 0$, le point à l'infini dans la direction de l'axe y, de coordonnées homogènes (0,1,0) est donc le seul point à l'infini sur la courbe.

Courbes elliptiques : loi de groupe

Un exemple simple : $y^2=x^3+x+2$ définie dans Z/5Z

y	y^2	x	x^3	x^3+x+2
0	0	0	0	2
1	1	1	1	4
2	4	2	3	2
3	4	3	2	2
4	1	4	4	0

La courbe n'a que les trois points (4,0), (1,2) et (1,3), le groupe a 4 éléments avec ∞

Rappel des formules :

$m=\frac{(y_2-y_1)}{(x_2-x_1)}$ (points distincts) $m=\frac{3x_1^2+p}{2y_1}$ (Calcul de 2P1)

$x_3=m^2-x_1-x_2$ et $y_3=m(x_1-x_3)-y_1$

Calcul de (4,0)+(1,2) : $m=2*(-3)^{-1}=2*2^{-1}=2*3=1$,
$x_3=1-4-1=1$, $y_3=1*(4-1)-0=3$, (4,0)+(1,2)=(1,3)
Calcul de (4,0)+(1,3) : $m=3*(-3)^{-1}=3*2^{-1}=3*3=4$,
$x_3=16-4-1=1$, $y_3=4*(4-1)-0=2$, (4,0)+(1,3)=(1,2)
Calcul de 2*(1,2) : $m=(3*1+1)*(2*2)^{-1}=4*4^{-1}=1$
$x_3=1-2=4$, $y_3=1*(1-4)-2=0$, 2*(1,2)=(4,0)

Calcul de 2*(1,3) :
$m=(3*1+1)*(2*3)^{-1}=4*1^{-1}=4$
$x_3=16-2=4$, $y_3=4*(1-4)-3=0$,
2*(1,3)=(4,0)
Par ailleurs on voit que :
2*(4,0)=(1,2)+(1,3)=∞

Courbes elliptiques : loi de groupe

Un exemple simple : $y^2=x^3+x+2$ définie dans Z/5Z

	(4,0)	(1,2)	(1,3)	∞
(4,0)	∞	(1,3)	(1,2)	(4,0)
(1,2)	(1,3)	(4,0)	∞	(1,2)
(1,3)	(1,2)	∞	(4,0)	(1,3)
∞	(4,0)	(1,2)	(1,3)	∞

Les calculs précédents donnent donc la table d'addition :
Noter que ce groupe est cyclique avec pour générateurs (1,2) et (1,3)
Il est donc isomorphe au groupe additif Z/4Z (dont les générateurs sont 1 et 2 et dont le troisième élément non nul (2) est d'ordre 2)

Calcul de (4,0)+(1,2) : $m=2*(-3)^{-1}=2*2^{-1}=2*3=1$,
$x_3=1-4-1=1$, $y_3=1*(4-1)-0=3$, (4,0)+(1,2)=(1,3)
Calcul de (4,0)+(1,3) : $m=3*(-3)^{-1}=3*2^{-1}=3*3=4$,
$x_3=16-4-1=1$, $y_3=4*(4-1)-0=2$, (4,0)+(1,3)=(1,2)
Calcul de 2*(1,2) : $m=(3*1+1)*(2*2)^{-1}=4*4^{-1}=1$
$x_3=1-2=4$, $y_3=1*(1-4)-2=0$, 2*(1,2)=(4,0)

Calcul de 2*(1,3) :
$m=(3*1+1)*(2*3)^{-1}=4*1^{-1}=4$
$x_3=16-2=4$, $y_3=4*(1-4)-3=0$,
2*(1,3)=(4,0)
Par ailleurs on voit que :
2*(4,0)=(1,2)+(1,3)=∞