LOI DE GROUPE SUR UNE COURBE ELLIPTIQUE

MATTHIEU LEGEAY

Introduction

Le but de cet exposé est d'étudier la structure de l'ensemble des points rationnels sur des courbes très importantes en théorie des nombres (et ailleurs) : les courbes elliptiques. Je vais dans un premier temps m'intéresser à la recherche de points rationnels dans les cas les plus simples (droites, coniques), puis j'introduirai les courbes elliptiques où l'on approfondira la loi de groupe de ces points rationnels, et enfin j'aborderai quelques applications et ouvertures dans ce domaine.

1. Les points rationnels

1.1. Géométrie, arithmétique et géométrie.

Tout le monde connaît le théorème de Pythagore : *Dans un triangle rectangle, la somme des carrés des côtés est égale au carré de l'hypothénuse (et réciproquement).*
Autrement dit, un triangle dont les longueurs des côtés sont a, b, c est rectangle si et seulement si $a^2 = b^2 + c^2$.

Question : Parmi les triangles rectangles, quels sont ceux qui ont leurs côtés de longueur entière ? On vient de voir que lesdites longueurs $a, b, c \in \mathbb{N}$ doivent vérifier $a^2 = b^2 + c^2$.

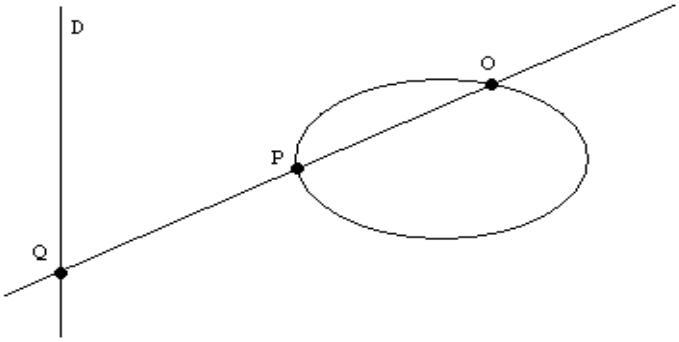
Ce problème a des solutions. Par exemple : $3^2 + 4^2 = 5^2$, mais on a aussi (5,12,13), (8,15,17)... Ces triplets sont appelés *triplets pythagoriciens.*
On est parti d'un problème géométrique (trouver les triangles rectangles à côtés de longueurs entières) pour aboutir à une *équation diophantienne* : trouver les solutions entières à l'équation $x^2 + y^2 = z^2$...Or il ne peut y avoir de solutions à cette équation avec $z = 0$ autre que le triplet (0,0,0). Divisons donc par z^2 : on se ramène à chercher $(x, y, z) \in \mathbb{N}^3$ tels que $\frac{x}{z}^2 + \frac{y}{z}^2 = 1$... mais si on oublie temporairement le lien avec les triangles rectangles, et si l'on pose $X = \frac{x}{z}$ et $Y = \frac{y}{z}$, on tombe sur l'équation $X^2 + Y^2 = 1$, dont on cherche les solutions dans $\mathbb{Q}$...
On connaît cette équation ? c'est celle du cercle de centre 0 et de rayon 1.
Géométriquement, on a donc ramené le problème des triplets pythagoriciens à la recherche de points à coordonnées rationnelles sur le cercle.

L'avantage de cette reformulation est qu'elle permet d'écrire simplement tous les triplets pythagoriciens. On est parti d'un problème géométrique (déterminer les triangles rectangles dont les longueurs des côtés sont entières) pour passer à l'arithmétique (équation diophantienne) et revenir à la géométrie (points rationnels du cercle).

1.2. Description de tous les triplets pythagoriciens.

Points rationnels des coniques : Une conique dont l'équation est donnée par un polynôme de degré 2, est dite rationnelle si le polynôme est à coefficients rationnels.

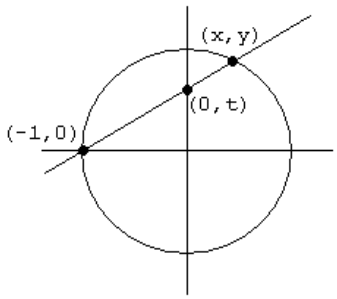
La connaissance d'un point rationnel de notre conique, disons O, et d'une droite D rationnelle, permet de décrire les autres points rationnels de la conique de la manière suivante : si Q est un point de la droite, traçons la droite (OQ). En général, elle rencontre la conique en un point autre que O (d'après le théorème de Bézout que nous verrons plus tard), disons P.



On peut alors affirmer que P est un point rationnel de la conique si et seulement si Q est un point rationnel de la droite (un moyen d'obtenir le point rationnel O' de la conique tel que (OO') soit parallèle à la droite D, est de changer de droite D...ou de travailler dans le plan projectif !). On a ainsi une correspondance entre les points rationnels de la conique et ceux de la droite (et ces derniers sont facilement descriptibles à l'aide d'un paramètre).

Que donne ce procédé dans le cas du cercle ?

Projetons le point (-1,0) sur l'axe des ordonnées, dans la direction d'un certain point (x, y) du cercle.



On obtient un point $(0, t)$. L'équation de la droite que l'on vient de tracer est $y = t(1 + x)$. Mais si le point (x, y) est sur le cercle et sur cette droite, on obtient l'équation :

$$1 - x^2 = y^2 = t^2(1 + x)^2$$

Si t est fixé, cette équation de degré 2 en x a pour solution évidente -1 (par construction), l'autre solution s'obtient en simplifiant par $1 + x \neq 0$ ce qui donne $1 - x = t^2(1 + x)$, que l'on résout pour obtenir (sachant que $y = t(1 + x)$) :

$$x = \frac{1 - t^2}{1 + t^2} \; et \; y = \frac{2t}{1 + t^2}$$

C'est une paramétrisation rationnelle du cercle car les coordonnées sont fractions rationnelles d'un paramètre. On voit sur ces formules que si t est rationnel, x et y sont des coordonnées d'un point rationnel du cercle. Réciproquement la formule $t = \frac{y}{1+x}$ montre qu'un point rationnel du cercle est obtenu à partir d'un paramètre rationnel.

Les points rationnels du cercles sont donc exactement les points obtenus par les formules $x = \frac{1-t^2}{1+t^2}$ et $y = \frac{2t}{1+t^2}$ avec $t \in \mathbb{Q}$ (il faut ajouter le point (-1,0), qui s'obtient en prenant $t = \infty$).

On a donc résolu notre problème dans sa formulation géométrique puisqu'un triplet pythagoricien (a, b, c) est en relation avec les points rationnels du cercle par la formule $x = \frac{a}{c}$ *et* $y = \frac{b}{c}$.

On peut en fait obtenir une description arithmétique des triplets pythagoriciens comme annoncé dans le théorème ci-dessous :

Théorème 1.1. *Les triplets pythagoriciens (a, b, c) sont exactement de la forme* $(n^2-m^2, 2nm, n^2+m^2)$ *ou* $(2nm, n^2-m^2, n^2+m^2)$ *avec* $n \in \mathbb{Z}$ *et* $m \in \mathbb{Z}$.

Démonstration. un peu de calcul... □

1.3. **A propos de l'ensemble des points rationnels du cercle...**

Une petite section pour terminer cette introduction. On a étudié le cercle et ses points rationnels... Que peut-on dire de la structure de l'ensemble des points rationnels ?

La formule de duplication des cosinus et sinus montre que c'est un groupe : si deux points P et Q sont repérés en coordonnées polaires par des angles α et β, on peut définir un point $P+Q$ dont l'angle admettra pour mesure la somme des mesures de α et β. Le point $P+Q$ aura alors pour abscisse $cos(\alpha)cos(\beta) - sin(\alpha)sin(\beta) \in \mathbb{Q}$ et pour ordonnée $sin(\alpha)cos(\beta) + sin(\beta)cos(\alpha) \in \mathbb{Q}$. Cette propriété de groupe abélien, intéressante en soi, semble particulière au cercle : existence des angles, de mesures d'angles etc...

Mais je vais expliquer ci-dessous que l'on peut, plus généralement, munir une courbe elliptique d'une loi de groupe abélien.

2. Loi de groupe sur les courbes elliptiques

Comme on l'a vu dans la section précédente, la recherche de points rationnels sur les courbes algébriques (définies par des polynômes) est profondément liée à la résolution d'équations diophantiennes. Droites et coniques, sont les objets qui résolvent les équations diophantiennes de degré au plus 2. Il va falloir fonctionner différemment pour pouvoir résoudre les problèmes de degré 3.

2.1. **Un peu d'histoire.**

Parmi les problèmes "historiques" en théorie des nombres, il y a la question suivante : Comment écrire un entier comme la différence d'un carré par un cube ? C'est exactement le problème de la résolution en nombres entiers de l'équation $y^2 = x^3 + c$ avec $c \in \mathbb{Z}$. Cette équation a une propriété étonnante, due à Bachet (1621). Si on connaît une solution rationnelle $(x, y) \in \mathbb{Q}^2$ alors

$$\left(\frac{x^4 - 8cx}{4y^2}, \frac{-x^6 - 20cx^3 + 8c^2}{8y^3}\right)$$

est aussi une solution rationnelle. Ce que Bachet ne savait pas, c'est que si la solution originale est telle que $xy \neq 0$ et si $c \neq 1, -432$, alors en répétant cette formule, on obtient une infinité de solutions rationnelles distinctes ! Autrement dit : *Si un entier (sauf 1 et -432) est la différence (non triviale) d'un carré et d'un cube, il l'est d'une infinité de manières différentes !*

Donnons un exemple : -2 peut s'écrire $5^2 - 3^3$, c'est-à-dire que (3,5) est solution rationnelle de l'équation $y^2 - x^3 = -2$. En appliquant la formule de duplication de Bachet, on obtient les solutions rationnelles suivantes :

$$(3, 5),\ \left(\frac{129}{100}, \frac{-383}{1000}\right),\ \left(\frac{2340922881}{7660^2}, \frac{113259286337292}{7660^3}\right)$$

D'où viennent ces formules compliquées ? Traçons la courbe d'équation $y^2 = x^3 + c$. Et plaçons le point $P(x, y)$ de la courbe, qui a pour coordonnées des nombres rationnels (c'est la solution que l'on connaît à l'avance).

Traçons la tangente en P à la courbe. Elle rencontre la courbe en un autre point, disons Q (c'est encore un cas du théorème de Bézout que je mentionnerai plus tard). Si on calcule les coordonnées de Q, on obtient la formule de Bachet. D'où le principe suivant : *l'arithmétique d'une courbe elliptique est déterminée par sa géométrie.*

Nous allons voir ci-dessous, que ce phénomène est général pour les courbes elliptiques, et tient du fait que l'on peut les munir d'une loi de groupe. Dans ce cadre, le point (3,5) est un élément d'ordre infini du groupe de la courbe elliptique.

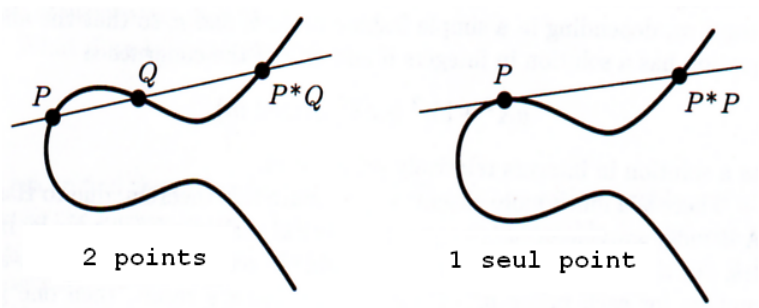
Un problème connexe On a vu dans le cas particulier de $y^2 - x^3 = c$ que l'on connaissait à peu près la forme que prenaient les solutions rationnelles, et on verra que cela ce généralise aux autres courbes. Une question naturelle à se poser est celle-ci : parmi les solutions rationnelles, lesquelles sont entières ? Ce problème, initié par Fermat dans les années 1650, avec la question de savoir si l'équation $y^2 - x^3 = -2$ n'avait que les deux solutions $(3, \pm 5)$, est autrement plus difficile, et n'était pas résolu à son époque. On doit à Axel Thue, le résultat suivant : *L'équation $y^2 - x^3 = c$ n'a qu'un nombre fini de solutions entières, pour tout entier c non nul.*

2.2. **Loi de groupe : tangentes et sécantes.**

On va chercher à étendre ce que l'on a fait pour les coniques aux cubiques : ce sont les courbes d'équations $ax^3 + bx^2y + cxy^2 + dy^3 + ex^2 + fxy + gy^2 + hx + iy + j = 0$. Si cette équation est non singulière (c'est-à-dire si les dérivées partielles ne sannulent pas simultanément en un point de la courbe) on dit que la courbe est une *courbe elliptique*.

On dit d'une cubique qu'elle est rationnelle si tous ses coefficients le sont. Malheureusement, en général une droite rencontre une cubique en trois points (en comptant les multiplicités), et non deux comme avec les coniques. On ne peut donc pas étendre immédiatement le procédé que l'on a utilisé pour les coniques.

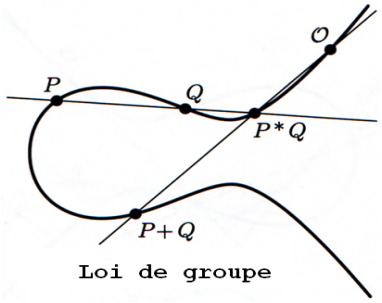
En contrepartie, on a le fait suivant : si on connaît 2 points rationnels sur une cubique rationnelle, on en connaît un troisième, le troisième point d'intersection de la droite passant par ces points avec la cubique (si un polynôme rationnel a deux racines rationnelles, alors la troisième l'est aussi). On peut donc construire géométriquement, partant de deux points rationnels P et Q d'une cubique rationnelle, un troisième point rationnel : $P * Q$, troisième point d'intersection de (PQ) avec la cubique.



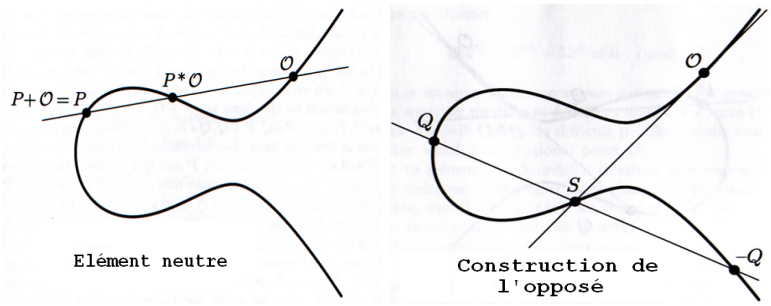
Imaginons que nous n'ayons qu'un seul point rationnel P, non singulier. Si on trace la tangente en P à la cubique (droite passant par P et... P !), on obtient (en général !) un autre point rationnel en prenant l'intersection avec la cubique. Ainsi, si on part de points rationnels, on peut, en traçant des droites, en obtenir d'autres... On a construit une loi de composition interne sur l'ensemble des points rationnels.

Malheureusement, cette loi n'est pas une loi de groupe... (pas d'élément neutre !). Ce qui en fait une loi peu intéressante.

On peut en fait modifier la loi $*$ pour en faire une loi de groupe (on supposera dorénavant la courbe elliptique). Fixons nous un point rationnel O, qui sera le neutre de notre groupe, et notons $+$ sa loi. On construit $P + Q$ de la manière suivante : d'abord, obtenir le troisième point d'intersection $P * Q$, puis tracer la droite passant par O et $P * Q$. Elle rencontre la cubique en un troisième point, le point $P + Q$.
On a : $P + Q = O * (P * Q)$. C'est un point rationnel car O est rationnel.



La loi ainsi obtenue est clairement commutative.
O est l'élément neutre : en effet O, P et $P * O$ sont alignés, donc $P + O = O * (P * O) = P$.
Comment obtenir les points opposés ? La construction est la suivante : tracer la tangente en O (la courbe est supposée elliptique), elle recoupe la cubique en S. La droite (PS) recoupe la cubique en un point, qui est $-P$.
Vérifions que cette construction nous donne bien les opposés. Additionnons Q et $-Q$. Pour ce faire, prenons le troisième point d'intersection de la courbe avec la droite passant par Q et $-Q$: c'est S. Maintenant joignons S et O et prenons à nouveau le troisième point d'intersection $S*O$: c'est O car la droite passant par O et S est la tangente à la courbe en O (elle passe donc "une fois" par S et "deux fois" par O). Ainsi $Q + (-Q) = O$.



La dernière marche,et pas la moindre, pour montrer que l'on a effectivement à faire à une loi de groupe est de prouver l'associativité de la loi

2.3. **Démonstration de l'associativité de la loi.**

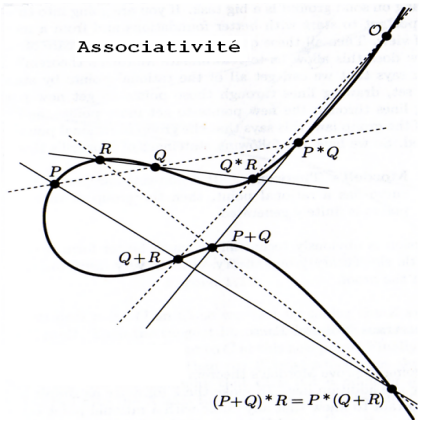
Soient P, Q, R trois points de la courbe. Il faut montrer : $(P + Q) + R = P + (Q + R)$.
Cependant, par construction de la loi $+$, il suffit en fait de montrer : $(P + Q) * R = P * (Q + R)$.

Pour trouver $P + Q$, on prend le troisième point d'intersection de la droite passant par O et $P * Q$ avec la courbe. La droite joignant $P + Q$ et R coupe la courbe en $(P + Q) * R$. On fait de même pour obtenir $P * (Q + R)$ en échangeant le rôle de P et R dans les deux précédentes lignes.

Ainsi sur le schéma ci-dessus, chacun des huit points de la courbe $O, P, Q, R, P * Q, Q * R, P + Q, Q + R$ appartient à une des droites en pointillé et à une des droites en trait continu. Considérons la droite en pointillé passant à travers $P+Q$ et R ainsi que la droite en trait continu passant à travers $Q + R$ et P. Leur intersection appartient-elle à la cubique ? Si oui, alors on a prouvé $(P + Q) * R = P * (Q + R)$ et c'est terminé.

Pour nous aider dans cette tâche, nous avons maintenant besoin de deux théorèmes forts en géométrie.

Théorème 2.1. *(de Bézout)*
Deux courbes planes de degrés m et n sans composantes communes ont exactement mn points d'intersection.



Je ne démontrerai pas ce théorème mais il faut prendre quelques précautions. Pour que le résultat soit correct, il faut :
- travailler dans le plan projectif, qui a un point de plus, le point à l'infini
- autoriser les coordonnées complexes
- compter les intersections avec multiplicité, par exemple les points de tangence ont une multiplicité plus grande que 1
On se sert immédiatement du théorème de Bézout pour affirmer que deux courbes cubiques ont 9 points d'intersection. Le second théorème est le suivant :

Théorème 2.2. *(des neufs points)*
Soient C, C_1 et C_2 trois courbes cubiques. Supposons que C passe par 8 des 9 points d'intersection de C_1 et C_2. Alors C passe par le neuvième point d'intersection.

Démonstration. C'est une démonstration non rigoureuse mais qui donne une bonne idée du problème général.
L'astuce est de considérer le problème de construction des courbes cubiques passant par un ensemble de points. Pour définir une courbe cubique, on doit donner 10 coefficients a,b,c,d,e,f,g,h,i,j. Si on multiplie tous ces coefficients par une même constante, on obtient la même courbe. Ainsi l'ensemble de toutes les cubiques est "de dimension 9".
Maintenant, si l'on veut que la cubique passe par un point de coordonnées données, cela impose une condition linéaire sur ces coefficients. Par conséquent, l'ensemble des cubiques passant par un point donné est "de dimension 8".
De même, à chaque fois que l'on impose que la cubique passe par un point donné, on impose à chaque fois une condition linéaire sur les coefficients. Ainsi, la famille des cubiques passant par huit points d'intersection de deux cubiques données est "de dimension 1".
Si $F_1(x,y) = 0$ et $F_2(x,y) = 0$ sont les équations de C_1 et C_2, la courbe C a alors une équation de la forme $\lambda_1 F_1 + \lambda_2 F_2 = 0$ pour un certain choix de λ_1 et λ_2.
Pour terminer, puisque le neuvième point est à la fois sur C_1 et sur C_2, alors $\lambda_1 F_1 + \lambda_2 F_2$ s'annule en ce point et C contient alors aussi ce point. □

Pour terminer notre démonstration de l'associativité, on pose C_1 l'union des trois droites en pointillé et C_2 l'union des trois droites en trait continu. Par construction, ces deux cubiques (dégénérées) s'intersectent aux neuf points précédemment nommés. Notre cubique originelle C passe par huit de ces points et ainsi, d'après le théorème, passe par le neuvième. Ceci prouve $(P+Q)*R = P*(Q+R)$ et la loi + construite sur les courbes elliptiques est bien une loi de groupe.

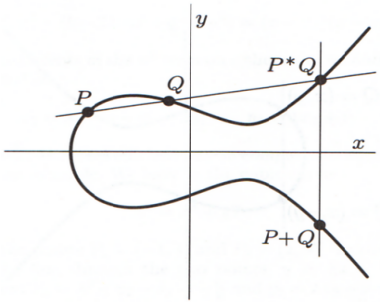
Remarque :
De quelle façon la loi que l'on a construite dépend du point O ? Soit O' un autre point rationnel, pris comme zéro d'une loi de groupe. L'application $P \mapsto P + (O' - O)$ est un isomorphisme entre les groupes C_O et $C_{O'}$ (son inverse est donné par $P \mapsto P - (O' - O)$).
Ainsi peut importe le choix du neutre, on obtiendra toujours le "même" groupe.

2.4. **Formules explicites pour la loi de groupe.**

On peut mettre l'équation de toute cubique possédant un point rationnel sous la forme appelée *forme normale de Weierstrass* :

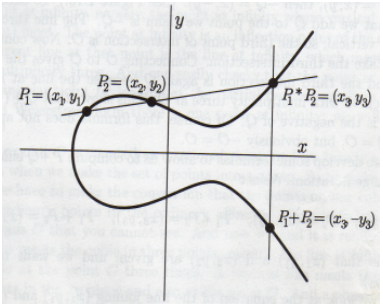
$$y^2 = x^3 + ax^2 + bx + c$$

Afin de donner des formules explicites et simples d'expression, on se place dans le plan projectif complexe et on choisit alors de prendre le point à l'infini comme élément neutre de la loi de groupe décrite précédemment (le point à l'infini est considéré rationnel). Comment construit-on $P + Q$ sur une cubique sous forme de Weierstrass ? Il suffit de prendre le prendre le symétrique par rapport à l'axe des x du troisième point d'intersection de la courbe avec (PQ).



Ainsi, dans ce cas, l'opposé d'un point est son symétrique par rapport à l'axe des x.

Changeons légèrement les notations pour commencer les calculs :
Soit $P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2)$, $P_1 * P_2 = (x_3, y_3)$, $P_1 + P_2 = (x_3, -y_3)$.
Supposons (x_1, y_1) et (x_2, y_2) donnés et cherchons (x_3, y_3).



On commence par regarder l'équation de la droite joignant P_1 et P_2 :
On a $y = \lambda x + \nu$, où $\lambda = \frac{y_2 - y_1}{x_2 - x_1}$ et $\nu = y_1 - \lambda x_1 = y_2 - \lambda x_2$.
Par construction, cette droite intersecte la courbe aux points (x_1, y_1) et (x_2, y_2). On obtient les coordonnées du troisième point d'intersection en substituant y par $\lambda x + \nu$, d'où :

$$y^2 = (\lambda x + \nu)^2 = x^3 + ax^2 + bx + c.$$

C'est à dire :

$$0 = x^3 + (a - \lambda^2)x^2 + (b - 2\lambda\nu)x + (c - \nu^2).$$

C'est une équation cubique dont les trois racines sont x_1, x_2 et x_3. Ainsi :

$$x^3 + (a - \lambda^2)x^2 + (b - 2\lambda\nu)x + (c - \nu^2) = (x - x_1)(x - x_2)(x - x_3).$$

Par identification, on trouve $\lambda^2 - a = x_1 + x_2 + x_3$ d'où :

$$x_3 = \lambda^2 - a - x_1 - x_2, \quad y_3 = \lambda x_3 + \nu.$$

Ces formules sont la manière la plus efficace de calculer la somme de deux points.

Regardons rapidement un exemple : soit la courbe cubique d'équation $y^2 = x^3 + 17$ avec les deux points $P_1 = (-1, 4)$ et $P_2 = (2, 5)$. Pour calculer $P_1 + P_2$, on calcule les coeeficients : $\lambda = \frac{1}{3}$ et $\nu = \frac{13}{3}$. Ainsi, $x_3 = -\frac{8}{9}$ et $y_3 = \frac{109}{27}$ d'où $P_1 + P_2 = (-\frac{8}{9}, -\frac{109}{27})$.

Mais que ce passe-t-il si $x_1 = x_2$? Trois possibilités :
- Soit $y_1 \neq y_2$ et dans ce cas nécessairement $y_1 = -y_2$. La droite qui joint les deux points est verticale, donc le troisième point $P + Q$ est le point à l'infini.
- Soit $y_1 = y_2 \neq 0$ et dans ce cas $P = Q$ n'est pas un point sur l'axe des abscisses. Donc on cherche $P + P = 2P$.
Par la relation $y^2 = f(x)$, on trouve :

$$\lambda = \frac{dy}{dx} = \frac{f'(x)}{2y}$$

Si l'on substitue cette relation dans les formules précédentes, que l'on remplace y^2 par $f(x)$ et que l'on met au même dénominateur, on obtient cette formule, appelée *formule de duplication* :

$$abscisse\ de\ 2(x, y) = \frac{x^4 - 2bx^2 - 8cx + b^2 - 4ac}{4x^3 + 4ax^2 + 4bx + 4c}$$

(on retrouve d'ailleurs la formule de Bachet en prenant $a = b = 0$)
- Soit $y_1 = y_2 = 0$ et dans ce cas la tangente à la courbe en ce point est verticale donc le troisième point $P + Q$ est le point à l'infini.

Si l'on reprend l'exemple précédent avec le point $P_1 = (-1, 4)$, on trouve $\lambda = \frac{3}{8}$.
Ainsi, $2P_1 = (\frac{137}{64}, -\frac{2651}{512})$.

3. Applications et ouvertures

3.1. **Points d'ordre fini.**

Un point P est dit d'ordre m si $mP = P + P + \cdots + P = O$ et $m'P \neq O$ pour tout entier $1 \leq m' \leq m$.
Si un tel m existe, P est d'ordre fini, sinon il est d'ordre infini.

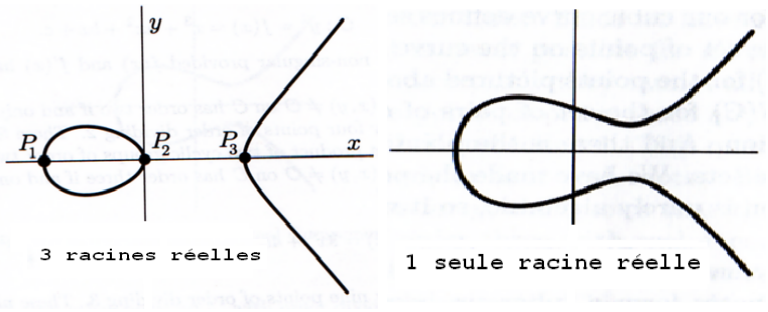
On va commencer l'étude par les points d'ordre 2 et 3. Pour ceci, on considère la courbe cubique sous forme de Weierstrass, avec le point à l'infini comme élément neutre du groupe.

Points d'ordre 2.

Ce sont les points satisfaisant $2P = 0$ et $P \neq O$. La condition $2P = O$ équivaut à $P = -P$. Puisque $-(x, y) = (x, -y)$, ces points vérifient alors $y = 0$. Ce sont donc les points :

$$P_1 = (\alpha_1, 0) \quad P_2 = (\alpha_2, 0) \quad P_3 = (\alpha_3, 0)$$

où $\alpha_1, \alpha_2, \alpha_3$ sont les racines du polynôme cubique $f(x) = x^3 + ax^2 + bx + c$.
Etudions alors la nature du sous-groupe $G = \{O, P_1, P_2, P_3\}$ des points d'ordre divisant 2 :
- Si l'on travaille avec des coordonnées complexes, alors il y a trois points distincts (car courbe non singulière) d'ordre 2 et ainsi G est le groupe de Klein $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.
- Si l'on travaille avec des coordonnées réelles, alors soit les trois racines précédentes sont réelles et G est aussi le groupe de Klein ; soit il n'y a qu'une seule racine réelle et alors G est $\mathbb{Z}/2\mathbb{Z}$.
- Si l'on travaille avec des coordonnées rationelles, alors G est le groupe de Klein, le groupe cyclique d'ordre 2 ou le groupe trivial suivant que f a 3, 1 ou 0 racines rationnelles.



Points d'ordre 3.

Ce sont les points vérifiant $3P = O$, ce qui équivaut à $2P = -P$. Un point d'ordre 3 satisfait donc $x(2P) = x(-P) = x(P)$ (et réciproquement). Pour trouver ces points, on utilise la formule de duplication démontrée dans le 2.4. On doit avoir :

$$x = \frac{x^4 - 2bx^2 - 8cx + b^2 - 4ac}{4x^3 + 4ax^2 + 4bx + 4c}$$

Ce qui, après calculs, donne :
x est racine du polynôme $g(x) = 3x^4 + 4ax^3 + 6bx^2 + 12cx + (4ac - b^2)$.
Mais puisque $x(2P) = \frac{f'(x)^2}{4f(x) - a - 2x}$, une autre expression de $g(x)$ est :

$$g(x) = 2f(x)f''(x) - f'(x)^2$$

g a alors 4 racines (complexes) distinctes (sinon f et f' auraient des racines communes).
Soient $\beta_1, \beta_2, \beta_3, \beta_4$ ses 4 racines et pour chaque β_i soit $\delta_i = \sqrt{f(\beta_i)}$.
Alors l'ensemble $(\beta_1, \pm\delta_1), (\beta_2, \pm\delta_2), (\beta_3, \pm\delta_3), (\beta_4, \pm\delta_4)$ est l'ensemble complet des points d'ordre 3 sur la courbe.
De plus, aucun δ_i ne peut être égal à 0 (sinon les points seraient d'ordre 2), donc cet ensemble contient 8 points distincts d'ordre 3.
Ainsi l'ensemble des points complexes d'ordre divisant 3 forme un groupe d'ordre 9 : c'est le groupe $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$.
Si l'on travaille avec des coordonnées réelles, le groupe des points d'ordre divisant 3 est le groupe $\mathbb{Z}/3\mathbb{Z}$.
Si l'on travaille avec des coordonnées rationnelles, c'est soit le groupe cyclique d'ordre 3, soit le groupe trivial.

Plus généralement.

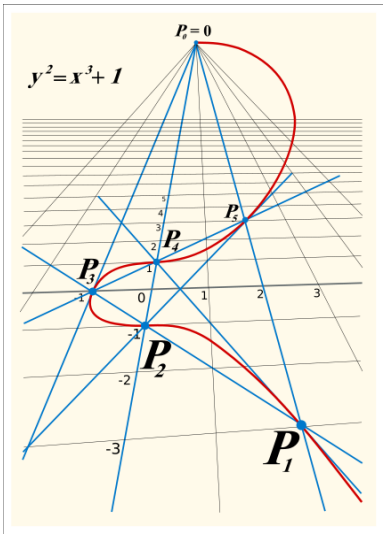
Le résultat le plus important est que tous les points à coordonnées rationnelles peuvent être construits par la méthode de la tangente et de la sécante à partir d'un nombre fini d'entre eux.

Théorème 3.1. *(Mordell-Weil)*
Le groupe des points rationnels, muni de la loi +, associé à une courbe elliptique est de type fini. Il est donc de la forme $\mathbb{Z}^r \times \mathbb{Z}/\alpha_1\mathbb{Z} \times \cdots \times \mathbb{Z}/\alpha_t\mathbb{Z}$. L'entier r est appelé le rang de la courbe.

Exemples.

- Soit la courbe d'équation $y^2 = x^3 + 1$.
Son rang est nul et cette courbe a 6 points à coordonnées rationnelles :
outre le point à l'infini, les points de coordonnées (2,3), (0,1), (-1,0), (0,-1), (2,-3). On peut prouver que ce groupe est cyclique d'ordre 6 et qu'il est engendré par le point (2, 3).
On a ainsi : (0,1)=2(2,3) (dans le sens de (2,3)+(2,3) pour la loi d'addition sur la courbe), (-1,0)=3(2,3), (0,-1)=-2(2,3)=4(2,3) et (2,-3)=-(2,3)=5(2,3) ; le point à l'infini est égal à 6(2, 3).
On voit ces relations sur le graphe réel de la courbe.

Par exemple, la tangente à la courbe au point de coordonnées (2,3) passe par le point (0,-1) dont le symétrique est (0,1), donc (0,1)=2(2,3). Les points de coordonnées (-1,0), (0,-1) et (2, -3) sont alignés, donc la somme des deux premiers est égale au point (2,3)...etc



- Soit la courbe d'équation $y^2 = x^3 + 109858299531561$.
Son rang est 5 et cette courbe a de plus trois points de torsion à coordonnées rationnelles, formant un groupe cyclique d'ordre 3. Son groupe de Mordell-Weil est donc isomorphe à $\mathbb{Z}^5 \times \mathbb{Z}/3\mathbb{Z}$.
Voici une liste de 5 points générateurs indépendants d'ordre infini (engendrant donc les 5 copies de $\mathbb{Z}$ dans le groupe de Mordell-Weil) :
(735532,630902573), (49704,15252915), (-4578,10476753), (-15260,10310419) et (197379,88314450).
Les trois points de torsion à coordonnées rationnelles sont le point à l'infini, le point (0,10481331), d'ordre 3, et son opposé. Tous les points à coordonnées rationnelles de cette courbe s'obtiennent alors à partir des 6 points explicités.

- Soit la courbe d'équation $y^2 = x^3 - 36x$.
Son groupe de Mordell-Weil est isomorphe à $\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Autrement dit, elle a quatre points à coordonnées rationnelles d'ordre divisant 2 : le point à l'infini et les trois points d'intersection avec l'axe des abscisses (0,0), (0,6), (0,-6).
Son rang est 1. Le sous-groupe cyclique infini est engendré par le point (12, 36).
À un changement de variable près, cette courbe est isomorphe à celle d'équation $6y^2 = x^3 - x$, liée à la recherche de triangles rectangles à côtés de longueur entière (autrement dit de triplets pythagoriciens) de même aire.
En effet, les côtés d'un tel triangle sont de la forme $d(p^2 - q^2), 2dpq, d(p^2 + q^2)$, pour un entier d quelconque et des entiers p et q, $p > q$, de parité différente. L'aire du triangle est alors $d^2pq(p^2 - q^2)$.
La recherche de triangles rectangles d'aire 6, par exemple, revient donc à la recherche de solutions rationnelles de l'équation $6y^2 = x^3 - x$.

3.2. **Les "gros" théorèmes.**

Théorème 3.2. *(Mazur)*
Soit C une courbe elliptique et supposons qu'il existe un point fini d'ordre m sur C.
Alors $1 \leq m \leq 10$ *ou m=12.*
Pus précisément, l'ensemble des points rationnels d'ordre fini forme un sous-groupe qui a l'une des deux formes suivantes :

(1) $\mathbb{Z}/N\mathbb{Z}$ *avec* $1 \leq N \leq 10$ *ou N=12*

(2) $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2N\mathbb{Z}$ *avec* $1 \leq N \leq 4$

Théorème 3.3. *(Nagell-Lutz)*
Soit la courbe elliptique d'équation $y^2 = f(x) = x^3 + ax^2 + bx + c$. *Soit* D *le discriminant du polynôme* $f(x)$,

$$D = -4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^2$$

Soit P=(x,y) un point rationnel d'ordre fini.
Alors x et y sont entiers et soit y=0 (et dans ce cas P est d'ordre 2), soit y divise D.

Théorème 3.4. *(Siegel)*
Une courbe elliptique n'a qu'un nombre fini de points à coordonnées entières.

3.3. **Application en cryptographie.**

L'étude de la loi de groupe sur les les courbes elliptiques a un intérêt pratique.
En effet, tout le monde connaît le théorème fondamental de l'arithmétique qui dit que tout entier ≥ 2 se factorise de manière unique en un produit de nombres premiers. Cependant si ce nombre entier est suffisamment grand (150 chiffres), on peut facilement savoir s'il n'est pas premier mais il est quasiment impossible de trouver en temps raisonnable la factorisation de celui-ci.
Le système R.S.A., et plus généralement les systèmes de chiffrement à clé publique, se basent sur cette difficulté que l'on a à factoriser un grand nombre pour envoyer des messages secrets (télécommunications, banque, institutions financières...) que l'on ne peut décoder sans la factorisation. Cela explique l'intérêt qu'on y porte.

Pour trouver la factorisation d'un grand nombre n, on peut essayer de le diviser par 2,3,... mais cela devient rapidement inefficace. (Pour un nombre à 100 chiffres, si on fait 1.000.000 de calculs à la seconde, il faudra environ $3,2 \times 10^{37}$ années ! ! !)

Ainsi, Lenstra a trouvé un algorithme probabiliste rapide qui emploie les courbes elliptiques. C'est une amélioration de la méthode de *factorisation p-1* de Pollard.
La factorisation de Lenstra tient compte du groupe d'une courbe elliptique aléatoire sur le corps fini $\mathbb{F}_p$. L'ordre du groupe d'une courbe elliptique sur $\mathbb{F}_p$ varie entre $p+1-2\sqrt{p}$ et $p+1+2\sqrt{p}$ (*Théorème de Helmut-Hasse*) aléatoirement.
L'algorithme de factorisation de Lenstra permettant de trouver un facteur d'un nombre donné n fonctionne de la manière suivante :
- Prendre une courbe elliptique aléatoire sur $\mathbb{Z}$ avec un point A sur elle. Alors, nous considérons la loi de groupe sur cette courbe modulo n (ceci est possible comme la plupart des résidus modulo n ont des inverses).
- Calculer kA dans ce groupe (à l'aide des formules déjà évoquées), où k est le produit de petits nombres premiers élevés aux petites puissances. Il peut donner un nombre premier en une fois, et est ainsi efficace.
- Avec un peu de chance, kA est l'élément zéro du groupe de la courbe elliptique dans $\mathbb{F}_p$, mais pas dans $\mathbb{F}_q$ pour un autre diviseur premier q de n. Alors nous pouvons trouver un facteur de n en prenant le PGCD de la première coordonnée de A et n, comme cette coordonnée sera zéro dans $\mathbb{F}_p$.
- Si cela ne marche pas, il suffit de recommencer avec une autre courbe et/ou un autre point de départ.

Références

- J.H. Silverman, J.Tate, Rational points on elliptic curves, Springer-Verlag, New York, 1992
- H. Cohen, G. Frey, R. Avanzi, C. Doche, T. Lange, K. Nguyen, F. Vercauteren, Handbook of Elliptic and hyperelliptic curve cryptography, Chapman and Hall/CRC, 2006
- Site de Wikipédia, Courbe elliptique
- Site de Wikipédia, Factorisation en courbe elliptique de Lenstra