Points rationnels et courbes elliptiques

Jérôme Gärtner

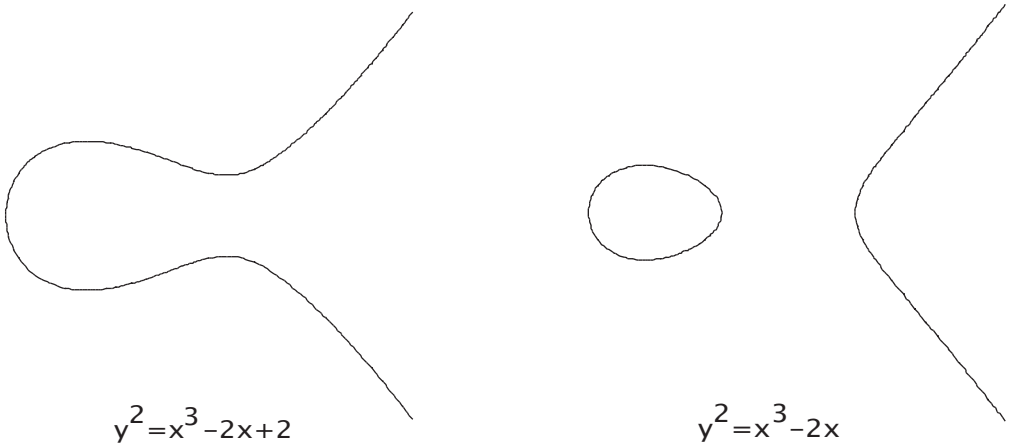


Table des matières

1 Introduction

Le but de cet article est d'introduire à une thématique qui intervient dans mon domaine de recherche, la *recherche de 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 de manière naïve, et enfin j'aborderai quelques questions ouvertes dans ces domaines.

Attention ! ce document n'est pas un exposé formel... ils comprend donc quelques imprécisions et incomplétudes (inévitables si on veut rester accessibles...)

2 Les points rationnels : qu'est-ce que c'est ?

2.1 Géométrie, arithmétique et géométrie

Tout le monde (ou presque !) connaît le théorème de Pythagore : *Dans un triangle rectangle la somme des carrés des côtés est égale au carré de l'hypoténuse (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 (il existe de tels triangles rectangles !). Par exemple : $3^2 + 4^2 = 5^2$, mais on a aussi $(5, 12, 13)$, $(8, 15, 17)$...

En fait une tablette babylonienne du début du deuxième millénaire avant notre ère, Plimpton 322, fournit déjà 15 tels triplets, dits *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 $x^2+y^2 = z^2$... Il ne peut y avoir de solutions à cette équation avec $z = 0$ autre que le triplet $(0, 0, 0)$ (car un carré est positif). Divisons donc par z^2 : on se ramène à chercher $(x, y, z) \in \mathbb{N}^3$ tels que $\left(\frac{x}{z}\right)^2 + \left(\frac{y}{z}\right)^2 = 1$... 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 $\mathbb{Q}$...

Qui 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 : c'est cela que l'on appelle *points rationnels du cercle*.

En général, étant donnée une courbe définie par un (système de) polynômes à coefficients rationnels (ou entiers, c'est la même chose) : $P \in \mathbb{Q}[X, Y]$, l'ensemble des *points rationnels de la courbe* définie par $\{(x, y) \in \mathbb{R}^2,\ P(x, y) = 0\}$ est l'ensemble des solutions dans $\mathbb{Q}^2$ à l'équation $P(x, y) = 0$.

L'avantage de cette reformulation est qu'elle permet décrire 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).

2.2 Description de tous les triplets Pythagoriciens

Deux idées générales :

La première idée est la suivante : si j'ai deux droites sécantes dont les équations dans un repère donné ont des coefficients rationnels (on appellera ces droites des droites "rationnelles"), leur point d'intersection est rationnel, et réciproquement, tout point rationnel du plan (ie : à coordonnées rationnelles) est intersection de deux droites "rationnelles".

On retiendra : **les points rationnels du plan sont exactement les intersections de droites rationnelles.**

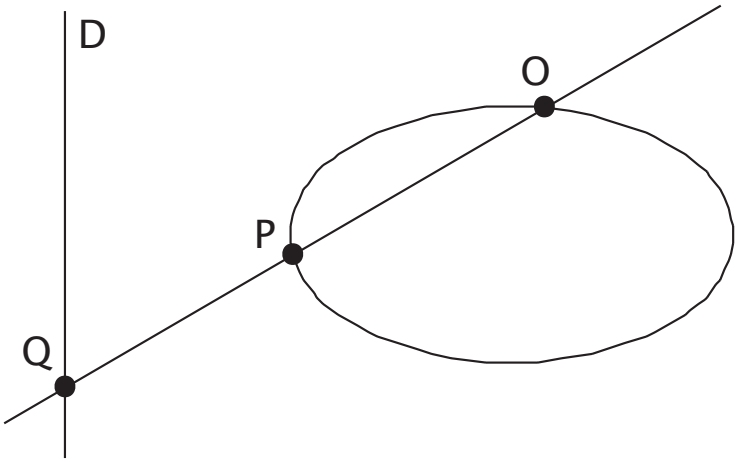
La deuxième est en fait un théorème que j'admettrai, le théorème de Bezout, qui d'une manière approximative dit la chose suivante :

si on connaît deux courbes, l'une définie par un polynôme de degré p, l'autre par un polynôme de degré q, elles ont en général pq points d'intersections.

On utilisera ce théorème dans le cas $p = 2$ et $q = 1$ (conique et droite), ainsi que dans le cas $p = 3$ et $q = 1$ (cubiques et droites). Dans ces deux cas, il est possible de démontrer ce théorème en résolvant un système d'équation polynomiales.

Points rationnels des coniques :

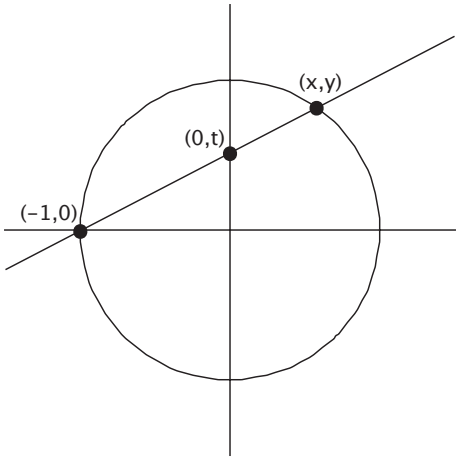
Une conique dont l'équation est donnée par un polynôme de degré 2, est dite rationnelle si le polynôme est à coefficients rationnel.



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, disons P (c'est l'énoncé faible du théorème de Bezout rappelé ci-dessus). Alors la description des points rationnels du plan rappelée ci-dessus, permet d'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).

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 $y = t(1 + x)$) :

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

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 bizarrement (? !) en prenant $t = \infty$).

D'une certaine manière, on peut dire que l'on a résolu notre problème... du moins dans sa nouvelle 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 2.1. *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 : Les identités remarquables fournissent $(n^2 - m^2)^2 + (2nm)^2 = (n^2 + m^2)^2$ donc les triplets $(n^2 - m^2, 2nm, n^2 + m^2)$ et $(2nm, n^2 - m^2, n^2 + m^2)$ avec $n \in \mathbb{Z}$ et $m \in \mathbb{Z}$ sont pythagoriciens. On va voir que tous les triplets pythagoriciens sont de ce type.

Supposons que (a, b, c) soit un triplet d'entiers avec $a^2 + b^2 = c^2$. On peut supposer a, b, c premiers entre eux deux à deux, quitte à simplifier par un diviseur commun. Posons

$x = \frac{a}{c}$ et $y = \frac{b}{c}$. Alors (x, y) est un point rationnel du cercle. Comme a et b sont premiers entre eux, ils ne sont pas tous les deux pairs. En fait ils ne peuvent pas non plus être tous les deux impairs : un nombre impair, élevé au carré est congru à 1 modulo 4. Donc si a et b sont impairs, $c^2 = a^2 + b^2$ est congru à 2 modulo 4, ce qui est impossible pour un carré (soit c est impair, et le carré est congru à 1 modulo 4, soit c est pair et le carré est congru à 0 modulo 4). On peut donc supposer par exemple que a est impair et b est pair.

Comme (x, y) est un point rationnel du cercle, on sait qu'il existe $t = \frac{m}{n} \in \mathbb{Q}$, que l'on choisit sous forme irréductible (*i.e.* m et n sont premiers entre eux), tel que

$$\frac{a}{c} = x = \frac{1 - \frac{m^2}{n^2}}{1 + \frac{m^2}{n^2}} = \frac{n^2 - m^2}{n^2 + m^2} \quad \text{et} \quad \frac{b}{c} = y = \frac{2\frac{m}{n}}{1 + \frac{m^2}{n^2}} = \frac{2mn}{n^2 + m^2}$$

Mais les fractions $\frac{a}{c}$ et $\frac{b}{c}$ sont supposées irréductibles : il existe donc λ tels que : $\lambda c = n^2 + m^2$, $\lambda b = 2mn$ et $\lambda a = n^2 - m^2$. Comme λ divise $n^2 + m^2$ et $n^2 - m^2$, il divise la somme et la différence, donc $2n^2$ et $2m^2$. Mais n et m sont premiers entre eux donc λ divise 2.

Supposons que $\lambda = 2$. Alors $2a = n^2 - m^2$ est pair, mais pas divisible par 4 (sinon 2 diviserait a, que l'on a supposé impair). Donc $n^2 - m^2$ est congru à 2 modulo 4, mais chaque carré est congru à 0 ou 1 modulo 4... donc $n^2 - m^2 \bmod 4 \in \{0, 1, 3\}$ et 2 n'est pas atteint. On a donc une contradiction qui fournit $\lambda = 1$.

Conclusion sur les triplets pythagoriciens :

On a réussi à décrire tous les triplets pythagoriciens. La démonstration que j'ai donnée ici illustre l'intérêt de l'étude des points rationnels sur les courbes. Il est possible de démontrer cette description uniquement avec des résultats enseignés en premier cycle. Une telle démonstration se trouve par exemple dans [14].

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

Une petite section pour conclure cette étude. 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 : l'existence des angles, de mesures d'angles etc... est quelque chose d'assez exceptionnel ! Il faut se rendre compte que l'on connaît énormément de propriétés sur les groupes abéliens. Une telle structure apporte beaucoup d'information sur l'ensemble des points rationnels du cercle.

Plus généralement, je vais expliquer ci-dessous que l'on peut munir une courbe elliptique d'une loi de groupe abélien. C'est ce phénomène qui, à mon avis, en fait des objets remarquables, et dont l'étude est relativement facile (comparé à d'autre objets géométriques). En général, on ne peut pas munir n'importe quoi d'une loi de groupe intéressante. Une généralisation des courbes elliptiques, les variétés abéliennes, est directement construites comme étant des groupes !

3 Et une courbe elliptique, c'est quoi ?

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 (pour ne pas dire que c'est la même chose !). Droites et coniques, bref ce qu'on a expliqué à la section précédente, sont les objets qui résolvent les équations diophantiennes de degré au plus 2 (*i.e.* : la recherche de solutions entières à une équation polynomiale à coefficients entiers de degré au plus 2). L'équation diophantienne la plus simple à considérer, hors celles dont on vient de parler, est la suivante : $y^2 = x^3 + c$: degré 2 en y et 3 en x. La courbe associée, qui est de la famille $y^2 = ax^3 + bx + c$ est une *courbe elliptique*. Ce sont probablement les courbes algébriques les plus simples, mis à part les coniques bien sûr. On sait beaucoup de choses sur les courbes elliptiques, mais malheureusement pas suffisamment. La suite de cette exposé va tenter d'effleurer le sujet.

3.1 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 $y^2 = x^3 + c$.

Cette équation a une propriété étonnante, due à Bachet (1621). Si on connaît une solution rationnelle $(x, y) \in \mathbb{Q}^2$, alors

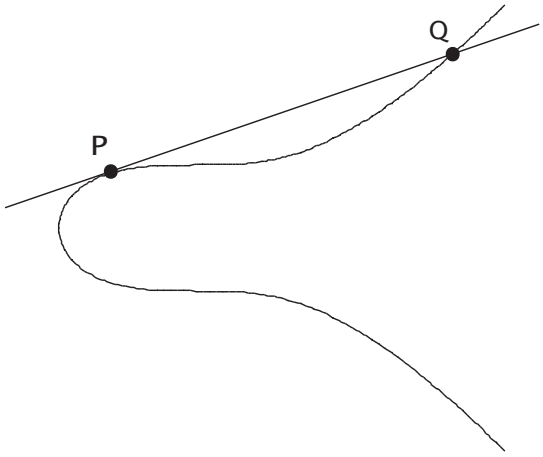
$$\left(\frac{x^4 - 8cx}{4y^2}, \frac{-x^6 - 20cx^3 + 8c^2}{8y^3}\right)$$

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 dupplication de Bachet, on obtient les solutions rationnelles suivantes :

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

D'où viennent ces formules compliquées ? Traçons la courbe d'équation $y^2 = x^3 + c$. Et plaçons le point $\mathrm{P}(x, y)$ 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, un fait général est qu'elle rencontre la courbe en un autre point, disons Q (c'est encore un cas du théorème de Bezout que j'ai mentionné en 2.2). 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, nous dirons que la courbe elliptique n'a pas (trop...) de torsion : le point $(3, 5)$ est un élément d'ordre infini du groupe de la courbe elliptique.

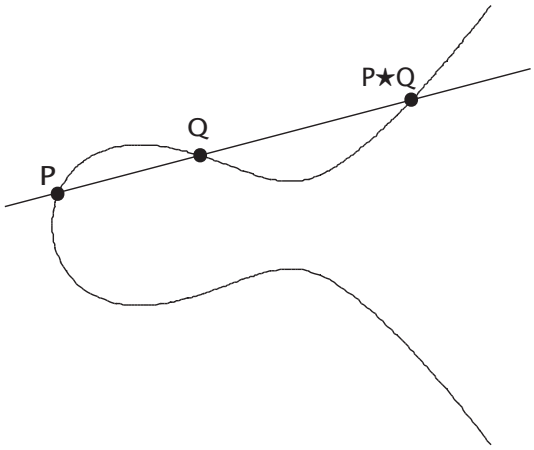
Un problème connexe On a vu dans le cas particulier de $y^2 - x^3 = c$ que l'on connaissait à peu près la forme que prenaient les solutions rationnelles, et on verra que cela ce généralise aux autres courbes. Une question naturelle à se poser est celle-ci : *parmi les solutions rationnelles, lesquelles 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.*

3.2 La loi de groupe : tangentes et cordes

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 s'annulent pas simultanément en un point de la courbe) on dit que la courbe est une *courbe elliptique*.

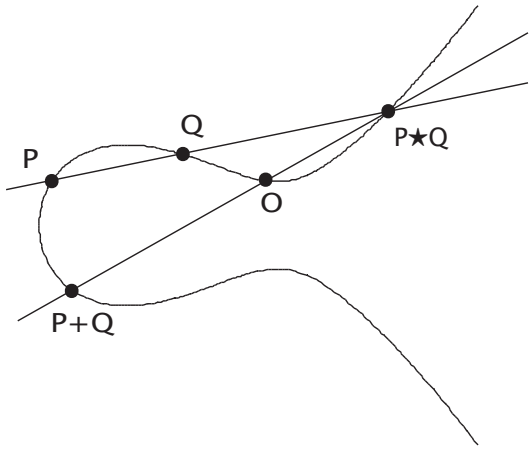
On dit d'une cubique qu'elle est rationnelle si tous ses coefficients le sont. Malheureusement, en général une droite rencontre une cubique en trois points (en comptant les multiplicités), et non deux comme avec les coniques. On ne peut donc pas étendre immédiatement le procédé que l'on a utilisé pour 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, Q d'une cubique rationnelle, un troisième point rationnel : P$\star$ 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. 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... (essayez de trouver l'élément neutre !) Ce qui en fait une loi peu intéressante.

On peut en fait modifier la loi $\star$ pour en faire une loi de groupe (pour simplifier on supposera dorenavant la courbe lisse : c'est-à-dire que les dérivées partielles en x et y de l'équation ne s'annulent pas simultanément). 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 $\star$ Q, puis tracer la droite (O, P $\star$ Q). Elle rencontre la cubique en un troisième point, le point P+Q. On a : P+Q=O$\star$(P $\star$ Q). C'est un point rationnel car O est rationnel.



La loi ainsi obtenue est commutative. O est l'élément neutre : O, P et P $\star$ O sont alignés, donc P+O = O $\star$ (P $\star$ O)=P. On peut vérifier que la construction de l'opposé $-$P d'un point est la suivante : tracer la tangente en O (la courbe est supposée lisse !), elle recoupe la cubique en S. La droite (PS) recoupe la cubique en un point, qui est $-$P. Il est plus difficile, mais néanmoins faisable, de montrer que la loi est associative (je ne vais pas m'y atteler ici, mais c'est fait par exemple dans [18]).

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.

Remarque : Une courbe elliptique, est une courbe cubique non-singulière, muni de sa loi de groupe. La théorie de Weierstrass permet de donner des équations explicites de ces courbes, avec des formules explicites pour l'addition, en coordonnées. Généralement on se place non pas dans le plan affine réel comme on l'a fait jusqu'à présent, mais dans le plan projectif complexe. Pour ceux qui connaissent, on peut montrer en particulier qu'il existe un unique point à l'infini pour une telle courbe elliptique. Ce point, considéré comme rationnel, est usuellement choisi comme origine pour la loi de groupe.

3.3 Les GROS théorèmes : Mordell/Weil et Siegel

Voici quelques résultats généraux sur les courbes elliptiques :

Théorème 3.1 (Mordell-Weil, première version)**.** *Si C est une cubique lisse i.e. une courbe elliptique, il existe un ensemble **fini** de points rationnels tels que tous les points rationnels de C se déduisent de cet ensemble fini par le procédé cordes et tangentes.*

*Le nombre minimal de points rationnels permettant de retrouver tous les points rationnels s'appelle le **rang** de la courbe.*

Le deuxième version de ce théorème défini plus précisément rang de la courbe.

Théorème 3.2 (Mordell-Weil, deuxième version)**.** *Le groupe associé à une courbe elliptique (le groupe des points rationnels, muni de la loi $+$), 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.*

Théorème 3.3 (Siegel)**.** *Une courbe elliptique n'a qu'un nombre fini de points entiers.*

Dans la prochaine section, je vais expliquer un problème ouvert relatif au rang des courbes elliptiques.

4 Un exemple de problème ouvert

Je vais essayer dans cette section d'expliquer un problème encore ouvert aujourd'hui, la conjecture de Birch et Swinnerton-Dyer (BSD). Ici plus que partout ailleurs, je ne parle évidemment pas en toute généralité. En particulier, je n'énonce qu'une version faible de la conjecture.

Prenons une courbe elliptique E "rationnelle". Elle est donnée par une équation de Weierstrass du type $\alpha y^2 = ax^3 + bx + c$ avec $\alpha, a, b, c \in \mathbb{Z}$. L'ensemble des diviseurs premiers des nombres α, a, b, c est fini. Si p est un nombre premier, posons $\widetilde{\alpha}, \widetilde{a}, \widetilde{b}, \widetilde{c} \in \mathbb{Z}/p\mathbb{Z}$ les réductions modulo p de α, a, b et c (c'est-à-dire les restes entre 0 et $p-1$ dans la division euclidienne par p). On peut alors considérer la courbe "réduite modulo p", c'est-à-dire dont l'équation est $\widetilde{\alpha}y^2 = \widetilde{a}x^3 + \widetilde{b}x + \widetilde{c}$, et dont on regarde les solutions dans $\mathbb{Z}/p\mathbb{Z}$. Dans la plupart des cas, la courbe réduite modulo p reste une cubique non singulière. $\mathbb{Z}/p\mathbb{Z}$ est un ensemble fini, il y a donc un nombre fini de solutions pour l'équation réduite (nécessairement !). On note l'ensemble des solutions $E(\mathbb{Z}/p\mathbb{Z})$. Posons $a_p = p + 1 - \mathrm{Card}(E(\mathbb{Z}/p\mathbb{Z}))$.

On a défini ces a_p si la courbe réduite est encore non singulière modulo p. Supposons que ce soit le cas pour tout p premier (en général, on sait ce qu'il se passe, et comment

bien définir les a_p dans tous les cas). On définit alors *la fonction L* attachée à E comme étant :

$$s \mapsto L(E,s) = \prod_p (1 - a_p p^{-s} + p^{1-2s})^{-1}$$

Cette fonction est d'une grande importance pour la théorie des courbes elliptiques, en particulier pour les questions de *modularité* (conjecture de Shimura/Tanyama/Weil, maintenant théorème de Wiles).

Rappelons que le théorème de Mordell-Weil définit un entier r, appelé le rang de la courbe E. Alors la conjecture BSD s'énonce ainsi :

L'ordre d'annulation de la fonction $L(E,s)$ en 1 est exactement r. Autrement dit, si $s \to 1$, la fonction $L(E,s)$ est équivalente à $k(s-1)^r$, où k est une certaine constante.

Remarquons que cette conjecture est de manière surprenante liée au problème des nombres congruents, qui est l'un des plus vieux problèmes non résolu (un nombre est dit congruent si il s'exprime comme l'aire d'un triangle à longueurs rationnelles). On pourra se référer à [3].

5 Introduction aux points de Heegner

Je vais présenter rapidement ici mon sujet de thèse. La théorie des nombres est la branche des mathématiques qui traite de manière plus ou moins élaborée les problèmes arithmétiques : répartition des nombres premiers, nombre de solutions à une équation diophantienne et ses aspects géométrique comme l'étude des points à coordonnées rationnels (ou entiers) sur des courbes/surfaces algébriques (définies par des polynômes).

Pour étudier une équation par exemple, il est assez utile d'étendre ses recherches à un ensemble plus grand que les nombres entiers. Un exemple serait celui du théorème des deux carrés, dû à Gauss, qui fournit une condition nécessaire et suffisante pour prédire si un nombre entier est somme de deux carrés ou non (résoudre l'équation $c = p^2+q^2$ d'inconnue $(p,q) \in \mathbb{Z}^2$). La démonstration la plus simple (à mon avis) passe par l'utilisation des entiers de Gauss (l'anneau $\mathbb{Z}[i] = \{a + ib,\ a,b \in \mathbb{Z}\}$). Pourquoi cet anneau au dessus de $\mathbb{Z}$ est-il plus intéressant que $\mathbb{Z}$ lui-même ? Parce que dans dans cet anneau, les nombres qui sont sommes de deux carrés se factorisent... On pourra consulter [13] pour une démonstration complète.

L'utilisation d'ensemble plus gros que celui des entiers s'est révélé être un succès dans la plupart des problèmes de théorie des nombres. Il est par exemple impressionnant que les premières démonstrations des deux théorèmes suivants :

Théorème 5.1 (des nombres premiers)**.** *Le nombre de nombres premiers inférieurs à n est équivalent à $\frac{n}{\ln n}$.*

Théorème 5.2 (de progression arithmétique de Dirichlet)**.** *Si a et b sont deux nombres premiers entre eux, il existe une infinité de nombres premiers congrus à a modulo b.*

passent par l'utilisation de fonctions sur $\mathbb{C}$. C'est pourquoi, en théorie algébrique des nombres on introduit des corps, que l'on appelle *corps de classes*. Ces corps contiennent $\mathbb{Q}$, et possèdent des propriétés très intéressantes du point de vu arithmétique. On a une très bonne compréhension théorique de ces corps mais malheureusement, pas très pratique. Un des principaux problèmes de nos jour est de rendre cette *théorie du corps de classe* effective, pour que l'on puisse vérifier les conjectures qui en dépendent à l'aide d'un ordinateur. C'est ce qu'on appelle le *12ème problème de Hilbert*. On connaît la réponse dans un cas

très particulier, celui de la *multiplication complexe*, qui utilise de manière fondamentale les propriétés de certaines courbes elliptiques.

Maintenant que l'on connaît deux objets intéressants, les courbes elliptiques et, plus vaguement, les corps de classes, que se passe-t-il si on cherche à mélanger les deux ? Autrement dit : *que sait-on des points d'une courbe elliptique qui ont des coordonnées dans un corps de classe donné ?* Réponse : théoriquement, on sait qu'ils sont utiles : ils sont par exemple le coeur de la démonstration de Gross/Zagier et Kolyvagin d'un cas particulier de la conjecture de Birch et Swinnerton-Dyer. En pratique, pas grand chose : on ne sait pas vraiment comment calculer ces points (c'est-à-dire expliquer à un ordinateur une manière de les représenter) car on est ramené au 12ème problème de Hilbert, qui n'est pas résolu. Dans le cas particulier dit "de multiplication complexe", leur existence a été prouvée et on sait comment ces *points de Heegner* sont liés entre eux...

La théorie de la multiplication complexe ne traite que d'un cas très particulier de corps de classe (les corps de classes de corps quadratiques imaginaires), et n'est pas vraiment généralisable dans l'état actuel des connaissances. C'est pourquoi Henri Darmon a proposé une construction conjecturale dans un autre cas particulier, à l'extrême opposé du cas traité par la théorie de la multiplication complexe. Mon travail consiste à généraliser la construction de Darmon, et actuellement je cherche à implémenter une de ces généralisations pour vérifier sa validité.

6 En vrac : échantillons de sujets accessibles autour des courbes elliptiques

Je vais essayer dans cette section de lister une partie des questions relatives aux courbes elliptiques accessibles aux étudiants de premier cycle. Certaines parties sont plus faciles que d'autres, ce qui ne tient que du nombre de pré-requis pour y comprendre le moindre mot...

6.1 Aspect historique : fonctions elliptiques

Pourquoi les courbes elliptiques s'appellent-elles elliptiques ? Parce qu'elles sont liées à l'étude des fonctions elliptiques : ce sont les fonctions que l'on cherche à intégrer pour trouver une rectification d'une ellipse. Par extension, on appelle souvent fonction elliptique une fonction de $\mathbb{C}$ dans $\mathbb{C}$ doublement périodique. Références : [12].

6.2 Aspect complexe

On peut regarder les solutions complexes d'une équation définissant une courbe elliptique. Il existe toute une théorie de ces points complexes, en particulier il apparaît un lien très important entre les courbes elliptiques et les réseaux : une courbe elliptique apparaît comme quotient de $\mathbb{C}$ par un réseau. Références : [2, 15, 4, 9, 16, 19].

6.3 Aspect cryptologie

Les courbes elliptiques, en particulier les réductions modulo p sont au coeur de la recherche actuelle en cryptologie, codes correcteurs et factorisations d'entiers. Ces aspects pratiques et algorithmiques (très à la mode) ne demandent pas de connaissance trop éloignées du programme de licence. Références : [10].

6.4 Aspect géométrique

Les courbes elliptiques peuvent apparaître de façon cachée dans certains grand théorèmes de géométrie. En particulier, le grand théorème de Poncelet n'est rien d'autre qu'une conséquence de la structure de groupe abélien d'une courbe elliptique... Attention, il faut connaître un minimum de géométrie projective ici. Référence : [1].

6.5 Aspect modulaire

Il existe un lien fondamental entre courbes elliptiques et formes modulaires, qui passe par les fonctions L. Pour aborder les formes modulaires, il est nécessaire au minimum de savoir ce qu'est un développement en série de Fourier... Références : [4, 9, 11, 15, 17]

7 Conclusion

Les courbes elliptiques sont des objets fondamentaux qui interviennent dans beaucoup de domaines mathématiques. Leur étude prend des aspects très différents suivant l'angle d'approche. La liste ci-dessus n'est pas exhaustive, mais on sort rapidement du bagage mathématique "normal" d'un étudiant de premier cycle. L'aspect le plus accessible pour qui souhaiterait travailler seul est l'aspect cryptologie (qui requiert moins de connaissances).

Commentaires sur la bibliographie : Pour apprendre des choses sur la théorie des nombres, les livres [14] et [15] sont accessibles. Ces livres traitent par exemple du théorème des deux carrés dont je parle plus haut. Le livre de Serre fournit une très bonne introduction aux formes modulaires et à la théorie analytique des nombres (pour sa deuxième partie), tandis que celui de Samuel est plus algébrique. Le livre [13] est un cours d'agèbre commutative. Il est bien écrit et on y trouvera des informations sur les théorème des deux carrés.

Le livre [6], issu en partie d'un cours de M1, est très bien construit et accessible. On y trouve tous les aspects de la théorie des nombres (algébrique et analytique), ainsi que de la cryptologie et une introduction aux codes correcteurs d'erreur. Les deux derniers chapitres introduisent aux courbes elliptiques et à certains problème ouvert. Sa lecture est à recommander à toute personne qui s'intéresse sérieusement à la théorie des nombres.

Le document [8] est élémentaire et contient déjà beaucoup d'informations sur la théorie des courbes elliptiques.

Les livres [5, 9, 10] sont accessibles et concernent les courbes elliptiques avec ou sans formes modulaires. [10] intéressera tous ceux qui veulent aborder la théorie algorithmique des nombres.

Le livre [18] est très clair. Ce livre est à la base de cet article. Il a l'avantage d'avoir été écrit pour des élèves du niveau licence 3/master 1, donc plus accessible que les ouvrages de références concernant les courbes elliptiques [7, 16, 17], ou les formes modulaires [4].

[11, 12] sont des notes de cours de Master 2. Parfois lisibles, parfois incompréhensibles pour un de premier cycle. Je déconseillerai en particulier de lire "Lectures on Etale cohomology" sur la page de Milne.

Les livres [2, 19] sont clairs, et ne sont cités que pour avoir des références d'analyse complexe nécessaire à la lecture des ouvrages les plus compliqués.

Les articles [1] et [3] sont des articles orienté vers la recherche, à mon avis plus durs à comprendre pour des élèves de premier cycle.

Références

[1] **H.J.M. Bos, C. Kers, F. Oort, D.W. Raven**, *Poncelet's closure theorem*, Expositiones Mathematicae, 1987, pages 289-364

[2] **H. Cartan**, *Théorie élémentaire des fonctions analytiques d'une ou plusieurs variables complexes*, Hermann

[3] **P. Colmez**, *Le probléme des nombres congruents, en lien avec la conjecture de Birch et Swinnerton-Dyer*, notes d'un exposé à l'école polytechnique : institut.math.jussieu.fr/ colmez

[4] **Diamond, Shurman**, *A first course in Modular Forms*, Springer GTM 228

[5] **Y. Hellegouarch**, *Invitation aux mathématiques de Fermat-Wiles*, Dunod 2000

[6] **M. Hindry**, *Arithmétique*, Calvage et Mounet, 2008.

[7] **D. Hüsemoller**, *Elliptic curves*, Springer, 1987

[8] **M. Joye**, *Introduction élémentaire à la théorie des courbes elliptiques*, http ://sciences.ows.ch/mathematiques/CourbesElliptiques.pdf

[9] **N. Koblitz**, *Elliptic curves and modular forms*, Springer

[10] **N. Koblitz**, *A course in n umber theory and cryptography*, Springer

[11] **J. Milne**, *Elliptic curves*, notes de cours sur jmilne.org

[12] **J. Nekovář**, *Elliptic curves*, notes de cours disponibles sur institut.math.jussieu.fr/ nekovar

[13] **D. Perrin**, *Cours d'algèbre*, Ellipses

[14] **P. Samuel**, *Théorie algébrique des nombres*, Hermann

[15] **J-P. Serre**, *Cours d'arithmétique*, P.U.F

[16] **J.H. Silverman**, *The Arithmetic of Elliptic Curves*, Springer 1986

[17] **J.H. Silverman**, *Advanced Topics in the Arithmetic of Elliptic Curves*, Springer 1994

[18] **J.H. Silverman, J. Tate**, *Rational Points on Elliptic Curves*, Springer Undergraduate Texts in Mathematics 1992

[19] **P. Vogel**, *Cours d'analyse complexe*, Dunod