Groupe de travail pour élèves de lycée

Discussions rationnelles d'une courbe et d'un triangle

par

Mehdi Tibouchi

(Texte produit et tapé par Xavier Caruso)

Le 9 novembre 2003

Contents

1 Problématique

1.1 Qu'est-ce qu'un nombre congruent ?

La question discutée dans cet exposé est très simple à poser. Un peu à l'instar du théorème de Fermat[1], cet énoncé fort simple d'arithmétique cache énormément de mathématiques compliquées que nous allons donc essayer de présenter.

Un entier n est dit *congruent* s'il est l'aire d'un triangle rectangle à côtés rationnels. Autrement dit n est congruent si et seulement s'il existe trois rationnels non nuls a, b et c tels que :

$$\begin{cases} a^2 + b^2 = c^2 \\ ab = 2n \end{cases}$$

Il s'agit d'une question très ancienne, qui aurait pu par exemple être posée par Diophante[2], bien que cela n'ait pas été le cas. Au sens strict, elle n'est pas encore résolue aujourd'hui ; toutefois, on a une idée conjecturale d'une solution très acceptable.

Mais examinons plutôt l'énoncé donné ci-dessus. On peut se demander pourquoi n est supposé être entier alors que les côtés a, b et c sont simplement supposés rationnels. En fait, cela n'a pas grande importance car il est équivalent de chercher les n entiers et les n rationnels. Plus précisément si le rationnel $\frac{u}{v}$ est congruent alors il en est de même de l'entier uv et réciproquement. En effet si l'on peut trouver a, b et c tels que :

$$\begin{cases} a^2 + b^2 = c^2 \\ ab = 2\frac{u}{v} \end{cases}$$

alors on peut écrire directement :

$$\begin{cases} (av)^2 + (bv)^2 = (cv)^2 \\ (av)(bv) = 2uv \end{cases}$$

La réciproque est tout aussi immédiate.

Plus généralement, si r et s sont deux rationnels, le rationnel r est congruent si et seulement si le rationnel rs^2 l'est. Autrement dit, pour la propriété de congruence, on peut regarder les rationnels à multiplication par un carré près. Or si on se donne un rationnel, en le multipliant par un carré on peut le faire devenir entier, mais on peut aussi, en choisissant bien le carré, faire en sorte que les exposants qui interviennent dans la décomposition en facteurs premiers de cet entier ne soient jamais supérieurs ou égaux à 2. Un tel entier est dit *sans facteur carré*, et en effet le seul carré qui le divise est 1.

Bref, on peut se contenter pour la question originale de regarder les entiers n qui sont sans facteur carré. Ce ne sera pas franchement intéressant par la suite, mais c'est quand même une remarque à avoir en tête.

En fait, trouver des nombres congruents est chose simple. On commence par déterminer ce que l'on appelle un *triplet pythagoricien*, c'est-à-dire trois entiers a, b et c tels que $a^2 + b^2 = c^2$ et on calcule bêtement le produit $\frac{ab}{2}$ qui donne donc un entier congruent.

[1] Le théorème dit qu'il n'existe pas d'entiers strictement positifs x, y et z vérifiant $x^n + y^n = z^n$ lorsque n est un entier supérieur ou égal à 3.

[2] Diophante a posé nombre de questions similaires ; il a d'ailleurs laissé son nom aux *équations diophantiennes* qui est un terme générique pour désigner les équations dont on ne cherche que les solutions entières (ou rationnelles).

Évidemment, il reste à déterminer des triplets pythagoriciens ce qui n'est pas forcément facile pour celui qui ne connaît pas. Mais pour commencer, on peut y aller au petit bonheur la chance, et tomber par exemple sur le triplet $(3,4,5)$ si on ne le connait pas déjà. Ainsi on trouve que $\frac{3\times 4}{2} = 6$ est un entier congruent. On peut ensuite trouver le triplet $(5,12,13)$ ce qui donne l'entier congruent 30.

Enfin, on peut donner la formule suivante :

$$\left(m^2-n^2\right)^2+(2mn)^2=\left(m^2+n^2\right)^2$$

formule qui permet d'obtenir toute une famille de triplets pythagoriciens et donc de nombres congruents.

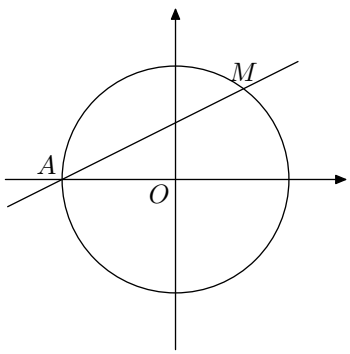
1.2 Un moyen de lister les nombres congruents

Précédemment, nous avons donné une formule pour obtenir toute une famille de nombres congruents. Nous allons voir ici qu'en fait, ce sont les seuls. Plus exactement, on a le théorème suivant :

Théorème 1. *Si a et b sont deux rationnels tels que $a^2+b^2=1$ et $a\neq -1$, alors il existe un rationnel t tel que*

$$a=\frac{1-t^2}{1+t^2} \quad et \quad b=\frac{2t}{1+t^2}$$

Ce théorème est en fait très facile à démontrer lorsque l'on a la bonne idée. L'ensemble des points du plan de coordonnées (x,y) vérifiant la relation $x^2+y^2=1$ est le cercle de centre l'origine est de rayon 1.



On place sur la figure le point A de coordonnées $(-1,0)$ et le point M de coordonnées (a,b). Ce sont tous deux des points du cercle à coordonnées rationnelles. Ainsi la pente de la droite (AM) est un nombre rationnel, disons t. Finalement l'équation de cette droite est $y=t\,(x+1)$.

Pour trouver a et b, il ne reste plus qu'à déterminer l'intersection de cette droite avec le cercle. On est donc amené à résoudre le système :

$$\begin{cases} x^2+y^2=1 \\ y=t\,(x+1) \end{cases}$$

On obtient ainsi $x^2+t^2\,(x+1)^2=1$. Bien sûr $x=-1$ est solution de cette équation de degré 2. Comme la somme des deux racines doit faire $\frac{2t^2}{1+t^2}$, on en déduit que :

$$a=\frac{-2t^2}{1+t^2}+1=\frac{1-t^2}{1+t^2}$$

On trouve ensuite facilement la valeur de b.

On constate plusieurs choses. Premièrement, si l'on ne cherchait que les a et b strictement positifs, il suffirait de se limiter aux rationnels t compris strictement entre 0 et 1, comme on le voit directement sur la figure.

Ensuite, ce théorème permet de déterminer complètement les triplets pythagoriciens : en effet, si (a, b, c) est un tel triplet, on a $\left(\frac{a}{c}\right)^2 + \left(\frac{b}{c}\right)^2 = 1$ et on est alors ramené au problème précédent. En écrivant ensuite $t = \frac{m}{n}$, on voit que les solutions données précédemment sont les seules, à permutation près de a et b, et à multiplication par un même entier près.

Enfin, cette classification permet de donner un algorithme pour lister tous les nombres congruents. Si l'on se restreint aux positifs disons[3], on voit qu'il suffit de commencer par lister tous les rationnels compris entre 0 et 1 et pour chacun d'eux de calculer l'expression $\frac{t\left(1-t^2\right)}{\left(1+t^2\right)^2}$ ou plus simplement l'expression $t\left(1-t^2\right)$, et éventuellement ensuite renormaliser le nombre en le multipliant par le bon carré pour qu'il devienne un entier sans facteur carré. Il n'est alors pas difficile, avec ce que l'on a fait précédemment, de se convaincre que l'on n'aura ainsi oublié aucun nombre.

Lister les nombres rationnels compris entre 0 et 1 n'est pas difficile. On commence par mettre ceux dont le dénominateur est 2, c'est-à-dire simplement $\frac{1}{2}$. Viennent ensuite ceux dont le dénominateur est 3, donc $\frac{1}{3}$, et $\frac{2}{3}$. Puis on passe à 4 (bien sûr, ce n'est pas la peine de mettre $\frac{2}{4}$ qui y est déjà). On obtient donc une liste qui commence ainsi :

$$\frac{1}{2}, \frac{1}{3}, \frac{2}{3}, \frac{1}{4}, \frac{3}{4}, \frac{1}{5}, \frac{2}{5}, \frac{3}{5}, \frac{4}{5}, \frac{1}{6}, \frac{5}{6}, \frac{1}{7}, \frac{2}{7}, \frac{3}{7}, \ldots$$

En faisant donc le calcul annoncé pour chaque rationnel listé précédemment, on obtient le début de la liste des nombres congruents :

$$6, 6, 30, 15, 21, 30, 210, 15, 5, 210, 330, 21, 70, 210, \ldots$$

On remarque que de nombreux entiers peuvent être listés plusieurs fois, mais en tout cas, une chose est sûre c'est qu'on les obtient ainsi tous.

Seulement la question que l'on aimerait résoudre, c'est savoir, étant donné un entier n, s'il est congruent ou non. S'il est congruent, bien sûr, on peut s'en sortir : on fait la liste et on attend qu'il tombe. Mais s'il ne l'est pas, on ne pourra jamais le savoir par ce moyen. En outre, ce n'est pas dit qu'un entier congruent arrive rapidement dans la liste précédente. Par exemple l'entier $n = 157$ qui est congruent arrive seulement pour :

$$t = \frac{(526\,771\,095\,761)^2}{(157\,841)^2 \times (4\,947\,203)^2}$$

ce qui correspond quand même à un rationnel relativement complexe, loin dans la liste.

1.3 Un entier qui n'est pas congruent

Si l'on a trouvé des entiers congruents, on ne sait toujours pas à ce stade s'il en existe qui ne le sont pas. Et pourtant il ne faut pas chercher loin : ni l'entier 1, ni l'entier 2 ne sont congruents par exemple.

[3] Ce qui n'est pas absurbe, vu qu'à l'origine un tel nombre représente l'aire d'un triangle rectangle.

Le premier exemple démontré est celui de l'entier 1 et la démonstration remonte à Fermat. Il s'agit donc de prouver qu'il n'existe pas d'entiers non nuls a, b, c et d vérifiant le système d'équations suivant :

$$\begin{cases} a^2 + b^2 = c^2 \\ ab = 2d^2 \end{cases}$$

Supposons qu'une telle solution existe et voyons ce que cela implique. Déjà, dans un premier temps, on peut supposer que a et b sont premiers entre eux. Si ce n'était pas le cas, leur PGCD diviserait à la fois c et d et on pourrait diviser les quatre entiers par ce PGCD, obtenant ainsi à une autre solution pour laquelle a et b sont premiers entre eux.

D'après ce que l'on a alors plus ou moins vu précédemment, on sait qu'il existe des entiers encore premiers entre eux m et n tels que par exemple :

$$a = m^2 - n^2 \quad ; \quad b = 2mn \quad ; \quad c = m^2 + n^2$$

Le produit ab vaut alors d'une part $2d^2$ et d'autre part $2mn\left(m^2 - n^2\right)$. Les entiers m et $m^2 - n^2$ sont premiers entre eux car si x était un diviseur commun de ces nombres, alors il diviserait à la fois m et n^2 et devrait donc forcément valoir 1. De même, n et $m^2 - n^2$ sont premiers entre eux. Ainsi, $mn\left(m^2 - n^2\right)$ est le produit de trois nombres premiers entre eux et c'est un carré. Chacun des facteurs est donc un carré. Autrement dit, il existe des entiers p, q et r tels que :

$$m = p^2 \quad ; \quad n = q^2 \quad ; \quad m^2 - n^2 = r^2$$

Mais alors $r^2 = p^4 - q^4 = \left(p^2 - q^2\right)\left(p^2 + q^2\right)$. Ces deux facteurs sont encore premiers entre eux, et donc sont tous les deux des carrés.

Ainsi on vient de prouver que si 1 est congruent, alors il existe deux entiers strictement positifs, disons s et t, tels que les quatre nombres s, t, $s+t$ et $s-t$ soient tous des carrés. Et nous allons montrer maintenant que ce dernier fait est impossible.

Pour ce faire, on utilise le principe de descente infinie : on suppose que de tels entiers existent, et à partir de ces entiers, on en construit d'autres, encore solutions du problème, et plus petits. Si l'on arrive à faire cela, on aura bien prouvé qu'il n'existe pas de solution. En effet, s'il en existait une, on pourrait construire éternellement une solution toujours plus petite, et ceci entre en contradiction avec le fait qu'il n'existe pas de suite infinie d'entiers strictement décroissante.

Supposons donc que $s = p^2$, $t = q^2$, $s + t = u^2$ et $s - t = v^2$. Alors $u^2 - v^2 = (u + v)(u - v) = 2q^2$. Comme u et v ont forcément même parité, les entiers $u+v$ et $u-v$ sont tous les deux pairs, et donc on a par exemple $u - v = 4a^2$ et $u + v = 2b^2$. Mais alors $p^2 = v^2 + q^2 = b^4 + 4a^4$ et on retrouve par le fait un triplet pythagoricien. On écrit donc :

$$b^2 = s'^2 - t'^2 \quad ; \quad 2a^2 = 2s't' \quad ; \quad p = s'^2 + t'^2$$

où s' et t' sont des entiers premiers entre eux. La seconde égalité prouve que s' et t' sont tous les deux des carrés. La première prouve que $s'+t'$ et $s'-t'$ en sont aussi. À l'évidence la troisième égalité prouve quant à elle que $s' < s$, la solution est donc plus petite en ce sens. Cela conclut.

Avec des méthodes qui ressemblent par certains points, on devrait réussir à démontrer que 2 non plus n'est pas congruent. Cela dit, maintenant, on aimerait une méthode un peu plus systématique pour savoir si un entier donné est ou n'est pas congruent. C'est ce que nous allons exposer par la suite.

2 Courbes elliptiques

2.1 Rapport avec les nombres congruents

On a vu que l'entier n était congruent si et seulement s'il est égal, à un carré près, à un nombre de la forme $t\left(1-t^2\right)$ pour un certain rationnel t. Une formulation équivalente est de dire que n est congruent si et seulement s'il existe deux rationnels s et t tels que :

$$s^2 n = t\left(1-t^2\right) = t - t^3$$

ou encore, en multipliant tout par n^3 :

$$(sn^2)^2 = n^2(tn) - (tn)^3 = (-tn)^3 - n^2 \cdot (-tn)$$

Ainsi en posant $x = -tn$ et $y = sn^2$, on obtient $y^2 = x^3 - n^2 x$.

Le calcul précédent prouve plus ou moins que l'entier n est congruent si et seulement s'il existe deux rationnels x et y, avec $y \neq 0$, tels que $y^2 = x^3 - n^2 x$.

C'est cette nouvelle équation que nous allons étudier par la suite.

Une *courbe elliptique* E est la donnée d'une équation de la forme précédente, enfin plutôt de la forme $y^2 = x^3 + ax + b$ où a et b sont disons des entiers[4]. Attention, E n'est pas du tout l'ensemble des solutions de l'équation, c'est simplement l'équation ; ainsi si l'on préfère, on peut dire qu'une courbe elliptique est simplement un couple d'entiers, en l'occurrence le couple (a, b), mais c'est moins parlant.

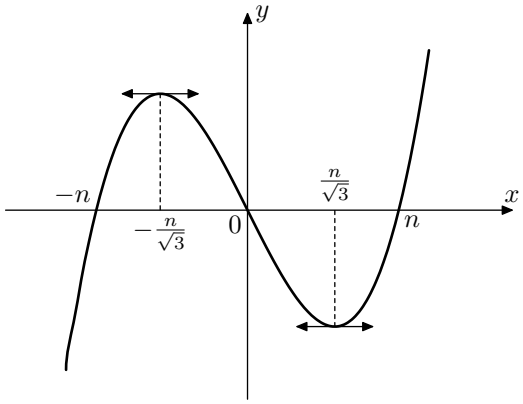
Maintenant, si on se donne E une courbe elliptique, on peut regarder ce que l'on appelle ses *points* à valeurs dans quelque chose. Par exemple, on définit ses points à valeurs dans $\mathbb{Q}$ (ou encore ses *points rationnels*) comme l'ensemble des couples $(x, y) \in \mathbb{Q}^2$ qui vérifient l'équation donnée par E. C'est cet ensemble de points que l'on note $E(\mathbb{Q})$. De même l'on définit $E(\mathbb{R})$ ou encore $E(\mathbb{C})$, respectivement comme les couples de réels ou de complexes qui vérifient l'équation[5].

Appelons E_n la courbe elliptique correspondant à l'équation $y^2 = x^3 - n^2 x$, c'est-à-dire si l'on préfère au couple $\left(-n^2, 0\right)$. Notre but consiste donc à étudier les points rationnels de E_n, c'est-à-dire l'ensemble $E_n(\mathbb{Q})$. Dans un premier temps, plutôt, nous allons dessiner $E_n(\mathbb{R})$ pour avoir une idée. C'est évidemment plus facile car l'on sait facilement reconnaître les carrés dans $\mathbb{R}$: ce sont exactement les nombres positifs ou nuls. On cherche donc juste à savoir pour x fixé si la quantité $x^3 - n^2 x$ est positive ; lorsque c'est le cas, il y a deux solutions en y, sinon il n'y en a pas.

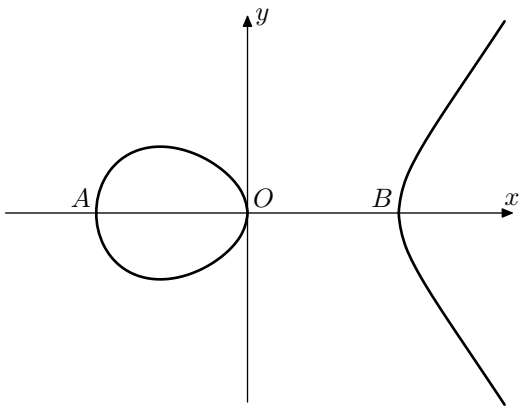
On pose $f(x) = x^3 - n^2 x = x(x-n)(x+n)$. Cette dernière écriture prouve que f s'annule en 0, n et $-n$ et seulement en ces points. D'autre part, on calcule $f'(x) = 3x^2 - n^2$. La dérivée s'annule donc en $\pm\frac{n}{\sqrt{3}}$. Elle est négative entre les deux racines et positive à l'extérieur des racines. Cela permet de construire le tableau de variation puis de donner l'allure de la fonction. Voici donc le graphe :

[4] Si a et b sont des éléments d'un anneau A, la courbe elliptique sera dite définie sur A. Si l'on ne précise pas, on sous-entend que la courbe elliptique est définie sur $\mathbb{Z}$. On impose en général en outre une condition dite de *lissité*, mais peu importe pour ce papier.

[5] Plus généralement, on peut définir $E(k)$ pour tout corps k de la même façon ; on peut même donner une définition de $E(B)$ pour tout anneau B. Si la courbe elliptique est définie sur un anneau A, on peut définir $E(B)$ pour toute B-algèbre A.



En prenant la racine carrée et son opposé lorsque f est positive, on arrive finalement au dessin de points réels de la courbe elliptique :



Notre but est répétons-le de savoir si la courbe dessinée ci-dessus admet des points à coordonnées rationnelles autres que les points O, A et B représentés précédemment.

2.2 Une opération sur les points d'une courbe elliptique

Nous allons réutiliser ici l'astuce dans la démonstration du théorème 1. On avait vu que lorsque l'on prenait une droite passant par un certain point du cercle, en l'occurrence A, elle recoupait forcément le cercle en un autre point rationnel.

Ici, c'est à peu près la même idée. Seulement, il faut prendre deux points sur la courbe elliptique : si on appelle P et Q des éléments de $E_n(\mathbb{R})$ disons, la droite (PQ) recoupe $E_n(\mathbb{R})$ en un troisième point R. En outre, il est important de remarquer que si les points P et Q sont *rationnels* (*i.e.* à coordonnées rationnelles), alors le troisième point d'intersection l'est aussi. En effet, si la droite (PQ) a pour équation $y = ax + b$, alors l'abscisse du point R vérifie :

$$(ax_R + b)^2 = x_R^3 - n^2 x_R$$

mais on sait que cette équation de degré 3 a déjà deux racines rationnelles qui sont donc x_P et x_Q. Comme la somme des trois racines doit être rationnelle puisqu'elle s'exprime en fonction des coefficients de l'équation, x_R est lui aussi rationnel. Plus précisément, on doit avoir :

$$x_P + x_Q + x_R = a^2 = \left(\frac{y_Q - y_P}{x_P - x_Q}\right)^2$$

et on accède ainsi à la valeur de x_R. (La dernière égalité provient du fait que a est la pente de la droite (PQ).) On aurait également pu utiliser l'expression du produit :

$$x_P \cdot x_Q \cdot x_R = b^2$$

et calculer x_R via cette formule.

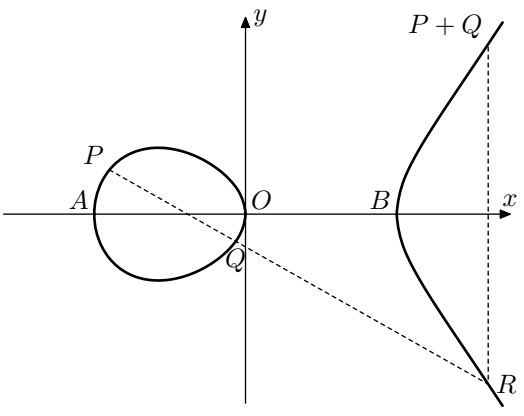
Il y a toutefois un léger écueil à ce que l'on vient de dire. Si la droite (PQ) est verticale (ce qui correspond donc moralement au cas $a = \infty$), elle ne recoupe pas la courbe. Pour ne pas avoir à toujours distinguer ce cas particulier, on convient de rajouter à la courbe ce que l'on appelle un *point à l'infini* dans la direction verticale. Par définition, ce point appartient à toutes les droites verticales et à aucune autre. En particulier, donc, lorsque l'on considère une droite qui passe par le point à l'infini, cela veut dire que l'on considère une droite verticale.

Par ce petit tour de passe-passe[6], ce que l'on a dit précédemment devient vrai de façon générale. Certes, les formules données n'ont pas toujours un sens, mais disons simplement que lorsqu'elles en ont un, elles sont justes. Également, on peut prendre $P = \infty$ dans la construction précédente, cela ne pose aucun problème. Le droite (PQ) est alors la verticale passant par le point Q : le point R est donc le symétrique de P par rapport à l'axe des abscisses.

Finalement, on peut aussi prendre $P = Q$: la droite (PQ) est alors la tangente à la courbe au point commun. Les formules données précédemment restent valables, comme on le voit simplement en passant à la limite.

Ainsi à partir de quelques points, on peut en obtenir de nombreux autres par cette construction. Et on a en fait déjà trois points sur la courbe, ce sont les points O, A et B. Seulement, à partir de ceux-là, on ne va en fait jamais obtenir de nouveaux points. Si P et Q sont confondus en l'un de ces trois points, le point R est toujours le point à l'infini. Sinon la droite (PQ) est l'axe des abscisses et recoupe la courbe au troisième point.

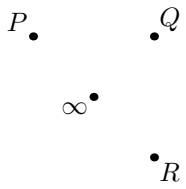
On n'est pas beaucoup plus avancé, donc. Cela dit, la construction qui précéde n'est pas inintéressante. Elle permet en fait de définir une addition sur les points de la courbe elliptique. Prenons P et Q deux points de la courbe elliptique. On vient de voir qu'ils définissent un troisième point R éventuellement rejeté à l'infini. Ce n'est pas lui la somme de P et Q, mais son symétrique par rapport à l'axe des abscisses, symétrique qui se situe encore sur la courbe. Par convention, le symétrique du point à l'infini est lui-même. Le schéma suivant illustre cette définition.



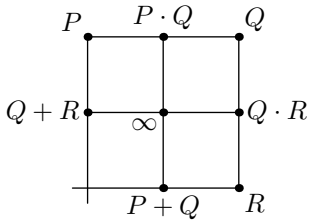
[6]C'est en realité bien plus qu'un tour de passe-passe, mais peu importe.

La propriété que l'on a cherchée à imposer *via* cette définition est que si trois points P, Q et R sont alignés sur la courbe elliptique, alors $P+Q+R=\infty$. Mais avant de pouvoir le dire, il faut prouver que cela a un sens, c'est-à-dire que le résultat de l'opération $P+Q+R$ ne dépend pas de l'ordre dans lequel on affectue les opérations. C'est ce que l'on appelle l'*associativité*.

Prenons donc trois points quelconques de la courbe elliptique, disons P, Q et R, et essayons de prouver que $(P+Q)+R=P+(Q+R)$. Pour simplifier le dessin, nous n'allons pas représenter la courbe elliptique, et nous allons en outre ramener le point à l'infini à distance fini[7]. On considère donc trois points P, Q et R dans le plan que l'on va pour l'instant supposer distincts du point à l'infini. On a la chose suivante :



La point associé aux points P et Q que l'on note $P\cdot Q$, est par définition le troisième point d'intersection de la droite (PQ) avec la courbe. Il est donc situé sur la droite (PQ). Plaçons-le un peu au hasard. La somme $P+Q$ est située quant à elle, sur la droite reliant le point $P\cdot Q$ au point à l'infini. De même on place les points $Q\cdot R$, $Q+R$:



Avec les notations précédentes, le point $(P+Q)\cdot R$ est sur la droite $((P+Q)\,R)$ et le point $P\cdot(Q+R)$ est sur la droite $(P\,(Q+R))$. Ce que l'on veut c'est que les symétriques de ces deux points soient confondus, c'est-à-dire en fait que ces deux points soient confondus. Pour prouver cela, il suffit de voir que la courbe passe forcément par le point d'intersection des deux droites précédemment citées, sachant déja évidemment que ladite courbe passe par les huit points représentés sur la figure.

On utilise alors le lemme suivant :

Lemme 1. *Considérons huit points en position générale. Alors il existe un neuvième point tel que toute cubique passant par les huit premiers passe également par le neuvième.*

Avant de démontrer cela, il convient de faire quelques remarques sur l'énoncé. Déjà que signifie en position générale ? Comme l'a dit Mehdi, le mieux que l'on puisse dire pour l'instant est de telle façon à ce que le lemme soit vrai . Enfin, ne vous tracassez pas, on soulignera dans la démonstration où cela intervient.

Ensuite qu'est-ce qu'une *cubique* ? C'est simplement une courbe définie par une équation de degré 3, c'est-à-dire de la forme :

$$a_1x^3+a_2x^2y+a_3xy^2+a_4y^3+a_5x^2+a_6xy+a_7y^2+a_8x+a_9y+a_{10}=0$$

[7]Cela ne devrait pas gêner les gens qui connaissent un peu de géométrie projective ; pour les autres, supposez s'il vous plaît que cela ne pose pas de problème, ou à la limite refaites le dessin en laissant le point à l'infini où il doit être, ça ne change strictement rien à la preuve.

où les a_i sont au choix des rationnels, des réels ou des complexes, selon l'endroit dans lequel on travaille.

Maintenant voyons comment se traduit notre hypothèse. Elle nous donne huit équations linéaires que doivent vérifier les a_i, une donc pour chaque point qui doit appartenir à la cubique. L'hypothèse en position générale signifie exactement ici que ces huit équations sont indépendantes, c'est-à-dire qu'il est impossible d'en déduire l'une d'elles en faisant des combinaisons linéaires des autres.

Ainsi pour trouver une cubique qui passe par ces huit points, on a à résoudre un système linéaire avec 10 inconnues et 8 équations. Pour cela, on choisit deux inconnues, par exemple a_1 et a_2, que l'on prend comme paramètres et on exprime les autres inconnues en fonction de celles-ci. Ainsi, on voit qu'il existe $F(x,y)$ et $G(x,y)$ deux équations de cubiques telles que toute cubique solution du système a pour équation :

$$\lambda F(x,y) + \mu G(x,y)$$

où λ et μ sont au choix des rationnels, des réels ou des complexes. Mais les cubiques définies par F et G ont déjà huit points d'intersection ; elles en ont donc un neuvième, comme on s'en aperçoit en résolvant l'équation de degré 9 qui résulte et en remarquant que l'on a déjà huit racines évidentes . Bref, on trouve ainsi un neuvième point, disons (x_0, y_0) tel que $F(x_0,y_0) = G(x_0,y_0) = 0$. Mais alors pour tous λ et μ, on a $\lambda F(x_0,y_0) + \mu G(x_0,y_0) = 0$ et le point (x_0,y_0) est bien sur toutes les cubiques passant par les huit premiers points.

Maintenant, il reste à conclure pour l'associativité. Pour cela, on remarque que la réunion des trois droites horizontales est définie par une équation de degré 3 ; c'est donc une cubique. En outre, elle passe par les huit points marqués sur la figure. De même la réunion des trois droites verticales est une cubique qui passe par ces mêmes huit points. D'après le lemme précédent, toute cubique passant par ces huit points, passe donc par un neuvième point, qui est forcément le dernier point d'intersection de nos deux triples droites .

On conclut en remarquant que les points de la courbe elliptique forment également une cubique. La courbe passe donc bien par le point par lequel on voulait qu'elle passe. Et cela conclut la démonstration.

Pas tout à fait en fait, car il reste à prouver que les huit points précédents sont toujours en position générale. Et ça va tellement pas de soi qu'il y a des cas où ça marche pas (sic !). Par contre, dans le cas des courbes elliptiques lisses[8], on peut montrer que c'est le cas pour au moins pour beaucoup de couples (P,Q) (mais pas forcément pour tous comme le montre l'exemple $P = Q$). On conclut alors typiquement par un argument de continuité.

Il reste à traiter le cas où l'un des points P ou Q était rejeté à l'infini, cas que nous avons laissé de côté tout à l'heure. Il est encore possible d'évoquer un argument de continuité ici, mais il y a bien plus simple et plus intéressant à remarquer. Pour tout point P de la courbe, on a $P + \infty = P$. C'est pour cette raison que l'on note souvent le point ∞ par le symbole 0, ce qui peut certes prêter à confusion de temps en temps. Ayant vu cela, il est trivial de vérifier la loi d'associativité lorsque le point à l'infini intervient.

[8] C'est-à-dire en gros sans point de rebroussement et sans point double, ce qui est bien le cas de E_n. Remarquez également que lorsqu'il y a un tel point, on est bien en mal de donner un sens au double de ce point : comment définit-on la tangente ? Pour des exemples, on pourra regarder les équations $y^2 = x^3$ et $y^2 = x^3 - 3x + 2$.

Recapitulons donc. On a déjà plus ou moins prouvé les choses suivantes à propos de notre nouvelle addition :

Propriété 1. *1. pour tous points P et Q éventuellement rejetés à l'infini, on a $P+Q = Q+P$;*

2. pour tous points P, Q et R éventuellement rejetés à l'infini, on a $(P+Q)+R = P+(Q+R)$;

3. pour tout point P éventuellement rejeté à l'infini, on a $P+\infty = P$;

4. pour tout point P éventuellement rejeté à l'infini, il existe un point P' tel que $P+P' = \infty$.

Le point 1 est totalement évident, les droites (PQ) et (QP) étant les mêmes. On a déjà vu les points 2 et 3. Pour le point 4, il suffit de remarquer que le point P' symétrique de P par rapport à l'axe des abscisses convient.

Le fait que ces quatre propriétés soient vérifiées nous dit que l'ensemble des points de la courbe elliptique E_n est muni d'une *structure de groupe abélien*. Mais peu importe la terminologie. On retiendra simplement que l'on a défini une addition vérifiant les propriétés naturelles de commutativité et d'associativité, admettant un 0 et que l'on peut faire aussi des soustractions (c'est le point 4).

2.3 La descente infinie revisitée

Nous allons ici donner une nouvelle preuve de la non-congruence de l'entier 1, une nouvelle preuve utilisant les courbes elliptiques.

Nous allons dans un premier temps nous intéresser aux points de la courbe elliptique qui peuvent être divisés par 2. Il existe en fait une caractérisation toute simple :

Propriété 2. *Un point P de la courbe elliptique E_n est un multiple de 2 (*i.e. *s'écrit $2Q$ pour un certain point Q) si et seulement si son abscisse x_P est telle que x_P, $x_P - n$ et $x_P + n$ sont tous les trois des carrés.*

On se rappelle que si S et T sont deux points de la courbe elliptique, on avait donné une méthode relativement simple pour calculer l'abscisse du point $S+T$ en fonction des abscisses de S et de T. Il suffit de dire que la droite passant par S et T a pour équation $y = ax+b$, et donc que les abscisses des trois points d'intersection de la droite avec la courbe sont les solutions de l'équation :

$$(ax+b)^2 = x^3 - n^2 x$$

En particulier, on a directement accès au produit des trois racines :

$$x_S \cdot x_T \cdot x_{S+T} = b^2$$

De même, on peut estimer le produit $(x_S+n)(x_T+n)(x_{S+T}+n)$. Ces nombres sont les trois racines du polynôme :

$$(a(x-n)+b)^2 = (x-n)^3 - n^2(x-n)$$

et donc on obtient :

$$(x_S+n)(x_T+n)(x_{S+T}+n) = (b-an)^2$$

Pareillement, on a aussi :

$$(x_S - n)(x_T - n)(x_{S+T} - n) = (b + an)^2$$

En particulier si $S = T = Q$, on obtient les relations suivantes :

$$\begin{aligned} x_{2Q} &= \left(\frac{b}{x_Q}\right)^2 \\ x_{2Q} + n &= \left(\frac{b - an}{x_Q + n}\right)^2 \\ x_{2Q} - n &= \left(\frac{b + an}{x_Q - n}\right)^2 \end{aligned}$$

Ces égalités prouvent un sens du théorème. La réciproque n'est alors pas franchement plus dure. Si on sait que les trois nombres x_P, $x_P + n$ et $x_P - n$ sont des carrés, disons respectivement de α, β et γ, on cherche une solution au système suivant :

$$\left\{ \begin{array}{rcl} b & = & \alpha x \\ b - an & = & \beta x + \beta n \\ b + an & = & \gamma x - \gamma n \end{array} \right.$$

système dont les inconnues sont les lettres a, b et x. Il n'est pas diffcile de le résoudre ; on trouve par exemple en faisant la somme des deux dernières lignes avant de soustraire la première :

$$x = \frac{n(\beta - \gamma)}{2\alpha - \beta - \gamma}$$

et le dénominateur est non nul par exemple grâce à la stricte concavité de la fonction racine carrée. Le réel x est alors l'abscisse d'un point Q tel que $P = 2Q$. Cela conclut la preuve de la proposition.

On remarque que dans l'énoncé de la proposition, on n'a pas précisé si le point P devait être rationnel, réel, complexe ou autre. En fait, cela fonctionne pour tous les cas. Mais bien sûr, si on suppose que le point P est rationnel, on va vouloir l'écrire comme le double d'un point Q encore rationnel, et la condition devra dire que les nombres x_P, $x_P + n$, $x_P - n$ sont tous les trois des carrés de rationnels. Pareil en remplaçant rationnel par réel ou complexe . Ainsi, ce lemme implique que tout point complexe de E_n est le double d'un autre point complexe, puisque tout nombre complexe est le carré d'un autre tel nombre. De même, un point réel de E_n est le double d'un autre si et seulement s'il est situé sur la branche de droite de la courbe.

Prouvons finalement que 1 n'est pas congruent. *Jusqu'à la fin de cette section, on a donc* $n = 1$. On prend un point P sur la courbe elliptique $E_n = E_1$. On veut simplement prouver qu'on peut le diviser par 2. Le résultat sera encore sur la courbe, et on pourra ainsi diviser par 2 à nouveau. C'est l'équivalent de la descente infinie de Fermat.

On prend donc un point P dans l'ensemble $E_1(\mathbb{Q})$. En réalité, on ne peut pas toujours le diviser par 2. Par contre, on peut toujours écrire $P = 2Q + R$ où R est soit le point O de coordonnées $(0, 0)$, soit le point A de coordonnées $(-n, 0)$, soit le point B de coordonnées $(n, 0)$ soit le point à l'infini (et dans ce cas, il est évidemment inutile d'ajouter R).

Montrons cela. Dans un premier temps, on peut supposer que P n'est aucun des quatre points cités ci-dessus. Notons x_P l'abscisse du point P. Si x_P est négatif, d'après ce que l'on a dit un peu avant, P n'a aucune chance d'être le double de quelqu'un. On commence donc, dans ce cas par ajouter O. On obtient ainsi un nouveau point qui a une abscisse positive. Ainsi, sans perte de généralité, on peut supposer $x_P > 0$ et donc en fait $x_P \geqslant n$.

On veut prouver que modulo un petit changement, à la fois x_P, $x_P + n$ et $x_P - n$ sont des carrés. Pour cela, on a besoin de la notion de *valuation p-adique*. La lettre p désigne un nombre premier. La valuation p-adique de l'entier x est le plus grand n qui soit tel que p^n divise x. Si l'on préfère, c'est l'exposant qui apparaît sur le nombre premier p dans la décomposition en facteurs premiers de x ; si le nombre premier n'apparaît pas, la valuation p-adique est simplement 0. La valuation p-adique de x se note souvent $v_p(x)$.

Il est ensuite possible de généraliser les valuations p-adiques aux nombres rationnels : si $x = \frac{a}{b}$, on pose $v_p(x) = v_p(a) - v_p(b)$. Cette valeur ne dépend pas de la fraction choisie. Les valuations p-adiques ont des propriétés intéressantes vis-à-vis de la somme et du produit :

Propriété 3. *Si x et y sont deux rationnels et si p est un nombre premier, alors :*

1. $v_p(xy) = v_p(x) + v_p(y)$
2. $v_p(x+y) \geqslant \min\{v_p(x), v_p(y)\}$ *avec égalité si* $v_p(x) \neq v_p(y)$

Ces propriétés sont enfantines à prouver mais elles sont souvent beaucoup plus utiles que ce que l'on pourrait bien croire à première vue.

Prouver qu'un nombre x est un carré revient avec le langage précédent exactement à prouver que $v_p(x)$ est pair pour tout nombre premier p. Estimons donc $v_p(x_P)$ pour un nombre premier p. Pour cela, il nous faut distinguer trois cas :

• si $v_p(x_P) = 0$, alors il est pair et il n'y a rien à faire.

• si $v_p(x_P) < 0$, alors étant donné que $v_p(n) = 0$ (car on rappelle que $n = 1$), on obtient $v_p(x_P + n) = v_p(x_P)$. Et de même $v_p(x_P - n) = v_p(x_P)$. De plus, si on désigne par y_P l'ordonnée du point P, on a :

$$y_P^2 = x_P^3 - n^2 x_P = x_P(x_P - n)(x_P + n)$$

et donc $2v_p(y_P) = v_p(x_P) + v_p(x_P - n) + v_p(x_P + n) = 3v_p(x)$ est un nombre pair. Cela conclut.

• si $v_p(x_P) > 0$, on a cette fois-ci $v_p(x_P + n) = v_p(x_P - n) = 0$ et on conclut pareillement.

Finalement x_P est toujours un carré. Exactement de la même façon, on montre que si p est différent de 2, $v_p(x_P + n)$ et $v_p(x_P - n)$ sont pairs (et même égaux). D'autre part, le produit de ces deux nombres vaut $\frac{y_P^2}{x_P}$ et est lui-même un carré. Ainsi on a l'alternative suivante. Soit $x_P + n$ et $x_P - n$ sont tous les deux des carrés, soit ils sont tous les deux des nombres de la forme $2r^2$, où r est un rationnel.

Dans le premier cas, on peut diviser P par 2 et on a gagné. Dans le deuxième, il faut introduire le point $P' = P + B$ où on rappelle que B est le point de coordonnées $(n, 0) = (1, 0)$. Le produit $(x_P + 1)(x_{P'} + 1)(x_B + 1) = 2(x_P + 1)(x_{P'} + 1)$ est alors encore un carré et donc il en est de même de $x_{P'} + 1$. De plus, la démonstration précédente s'applique encore au point P' et donc $x_{P'}$ est un carré, ainsi que $x_{P'} - 1$. On conclut ainsi.

Cependant, il n'y a encore rien jusqu'à maintenant qui nous assure que l'on aboutisse ainsi à une contradiction ; il n'y a aucun ordre sur la courbe elliptique qui nous dit que l'on décroît strictement en quelconque sens. Dans ce cas, il n'est pas bien difficile de faire les calculs à la main pour exprimer les coordonnées du point Q en fonction de celles de P, et d'exhiber alors une quantité strictement décroissante. Nous n'allons toutefois pas le faire, bien que cela soit très instructif pour voir que les calculs ci-dessus correspondent presque à la lettre aux calculs que Fermat avait menés.

Dans le cas plus général, ce sera encore cette méthode que l'on va appliquer. Là, on ne pourra plus faire les calculs à la main, et il va falloir trouver un nouvel argument pour remplacer la descente infinie. C'est une certaine notion de hauteur que l'on va introduire qui va se charger de cela, comme nous allons le voir dans la section suivante.

3 Étude générale des points rationnels

3.1 Essai de la descente infinie sur E_n

On reprend à partir de maintenant un entier n quelconque, et on veut étudier l'ensemble $E_n(\mathbb{Q})$ des points rationnels de la courbe elliptique E_n. L'idée pour cela est encore la même : on prend un point $P \in E_n(\mathbb{Q})$ et on essaie de le diviser par 2 une fois, deux fois et ainsi de suite, espérant ainsi diminuer la taille du point courant de la courbe. Si l'on peut faire cela indéfiniment, c'est qu'il n'y a pas de points sur la courbe autres que les points O, A et B.

Mais évidemment cela ne peut pas marcher génériquement, puisqu'il existe bien des entiers congruents, et donc des points sur certaines courbes elliptiques. Le problème en fait, c'est que, comme c'était déjà le cas précédemment, on ne va pas toujours pouvoir diviser exactement par 2 ; ce sera toujours possible mais seulement à quelque chose près. Quand ce quelque chose est réduit aux quatre points $\{O, A, B, \infty\}$, on pourra conclure. Sinon, on pourra conclure également en fait puisqu'il y aura du coup des points non triviaux sur la courbe.

Le premier résultat positif est le suivant :

Lemme 2. *Il existe un ensemble fini de points $\mathcal{R} \subset E_n(\mathbb{Q})$ tel que tout point $P \in E_n(\mathbb{Q})$ s'écrive $P = 2Q + R$ où $Q \in E_n(\mathbb{Q})$ et $R \in \mathcal{R}$.*

La démonstration ressemble fort à celle que l'on a faite dans le cas $n = 1$. Prenons P un point rationnel de E_n et un nombre premier p qui ne divise pas $2n$. Alors comme précédemment, on montre que $v_p(x_P)$, $v_p(x_P + n)$ et $v_p(x_P - n)$ sont tous les trois pairs.

Notons donc $p_1, \ldots, p_d$ l'ensemble (fini) des nombres premiers qui divisent $2n$. Choisissons $\varepsilon = \pm 1$ un signe, I, J et K trois sous-ensembles de $\{1, \ldots, d\}$ et regardons s'il existe un point $R \in E_n(\mathbb{Q})$ tel que l'on ait simultanément :

1. x_R est du même signe que ε ;
2. $v_{p_i}(x_R)$ impair si et seulement si $i \in I$;
3. $v_{p_j}(x_R + n)$ impair si et seulement si $j \in J$;
4. $v_{p_k}(x_R - n)$ impair si et seulement si $k \in K$

Si un tel point existe, on l'ajoute à l'ensemble $\mathcal{R}$, sinon, on ne fait rien.

Reprenons maintenant notre point P. On lui associe un signe, précisément le signe de x_P et trois sous-ensembles I, J et K de $\{1,\ldots,d\}$ définis par :

$$I = \{i \in \{1,\ldots,d\} \,/\, v_{p_i}(x) \text{ est impair}\}$$

et des formules analogues pour J et K. À cette donnée est associée un certain point R et le point $Q' = P - R$ est tel, comme nous l'avons déjà vu, que $x_P \cdot x_R \cdot x_{Q'}$, $(x_P + n)(x_R + n)\left(x_{Q'} + n\right)$ et $(x_P - n)(x_R - n)\left(x_{Q'} - n\right)$ sont tous les trois des carrés. On en déduit que $x_{Q'}$, $x_{Q'} + n$ et $x_{Q'} - n$ ont toutes leurs valuations p-adiques paires. En outre, la première des trois égalités précédentes nous assure que $x_{Q'}$ est positif, et donc puisque c'est l'abscisse d'un point de la courbe elliptique qu'il est plus grand que n.

Ainsi les trois nombres $x_{Q'}$, $x_{Q'}+n$ et $x_{Q'}-n$ sont des carrés et donc d'après la propriété 2, Q' s'écrit $2Q$ pour un certain $Q \in E_n(\mathbb{Q})$. Finalement on obtient bien $P = 2Q + R$ ce qui est le résultat annoncé ; les R possibles sont bien en nombre fini puisqu'il y a qu'un nombre fini de sous-ensembles de $\{1,\ldots,d\}$.

Le second point qui va permettre la descente infinie est l'introduction d'une notion de *hauteur* sur les points rationnels de E_n. Comme le dit Mehdi, il y a deux façons d'introduire une hauteur : soit de passer par des considérations assez élevées, soit de passer par des considérations assez basses . Nous n'allons toutefois présenter ni les unes ni les autres, mais simplement admettre le résultat suivant :

Théorème 2. *Il existe une fonction $\hat{h} : E_n(\mathbb{Q}) \to \mathbb{R}^+$ vérifiant les trois conditions suivantes :*

1. *$\hat{h}(P) = 0$ si et seulement s'il existe un entier d tel que $dP = \infty$*[9]
2. *pour tous P et Q, $\hat{h}(P+Q) + \hat{h}(P-Q) = 2\hat{h}(P) + 2\hat{h}(Q)$*
3. *pour tout réel A positif ou nul, l'ensemble des points $P \in E_n(\mathbb{Q})$ tel que $\hat{h}(P) \leqslant A$ est un ensemble fini.*

Un point P tel qu'il existe un entier d tel que $dP = \infty$ est un *point de torsion*. Il est remarquable de constater que le théorème précédent implique qu'il y a toujours un nombre fini de points de torsion ; il suffit pour cela de prendre $A = 0$ dans la troisième condition.

Armé de ce nouveau théorème, on peut enfin faire notre descente infinie correctement. On part d'un point $P \in E_n(\mathbb{Q})$ et on lui applique le lemme de division par 2. Il existe alors un point $Q_0 \in E_n(\mathbb{Q})$ et un point $R_0 \in \mathcal{R}$ tels que :

$$P = 2Q_0 + R_0$$

On peut réécrire cela sous la forme $2Q_0 = R_0 - P$ et en prenant les hauteurs de chaque côté, on obtient :

$$4\hat{h}(Q_0) = \hat{h}(R_0 - P) \leqslant 2\hat{h}(R_0) + 2\hat{h}(P)$$

et donc si $\hat{h}(R_0) < \hat{h}(P)$, il vient $\hat{h}(Q_0) < \hat{h}(P)$.

Et on peut continuer ainsi. On divise Q_0 par 2 en écrivant $Q_0 = 2Q_1 + R_1$ et comme précédemment si $\hat{h}(R_1) < \hat{h}(Q_0)$, on aura $\hat{h}(Q_1) < \hat{h}(Q_0)$. Et ainsi de suite. Cette manipulation ne permet hélas pas de conclure pour le problème initial, mais donne de précieuses informations sur la structure de l'ensemble $E_n(\mathbb{Q})$. Plus précisément, on a le théorème suivant :

[9] La notation dP correspond évidemment à la somme $P + P + \ldots + P$ (d fois).

Théorème 3 (Mordell-Weil). *Il existe un ensemble fini $\mathcal{S} \subset E_n(\mathbb{Q})$ tel que tout point $P \in E_n(\mathbb{Q})$ peut s'écrire comme une somme d'éléments de S en prenant éventuellement plusieurs fois les mêmes.*

C'est simplement la descente infinie entamée précédemment qui conclut : en divisant P par 2 suffisamment de fois, on en vient à écrire :

$$\begin{aligned} P &= 2Q_0 + R_0 \\ Q_0 &= 2Q_1 + R_1 \\ &\vdots \\ Q_{n-1} &= 2Q_n + R_n \end{aligned}$$

où tous les R_i sont dans R et où $\hat{h}(Q_n) < A$, A désignant la hauteur maximale d'un élément de R. Ainsi, on peut toujours écrire P comme une somme d'éléments de hauteur inférieure à A. Comme ces éléments forment un ensemble fini, le théorème est prouvé.

3.2 Le rang

La connaissance du seul résultat de Mordell-Weil permet de façon très formelle (*i.e.* sans vraiment utiliser le fait que l'on manipule des points d'une courbe elliptique) de déduire la structure précise de $E_n(\mathbb{Q})$.

Plus exactement rappelons qu'un point $P \in E_n(\mathbb{Q})$ est dit *de torsion* s'il existe un entier d tel que $dP = \infty$. Notons $E_n(\mathbb{Q})_{\text{tor}}$ l'ensemble des points de torsion. Cet ensemble est en fait stable par somme et par différence ; c'est ce que l'on appelle un *sous-groupe*. Il contient au moins quatre points qui sont A, O, B et ∞, le double de chacun des précédents points étant le point à l'infini.

Prenons maintenant des points $P_1, \ldots, P_r$ qui soient tels que tout point $P \in E_n(\mathbb{Q})$ puisse s'écrire sous la forme :

$$P = a_1P_1 + a_2P_2 + \ldots + a_rP_r + R$$

où les a_i sont des entiers relatifs et où R est un point de torsion. Bien sûr si un a_i est négatif, a_iP_i est l'élément qui ajouté à $-a_iP_i$ donne le point à l'infini.

Il est évidemment possible de choisir de tels points, justement d'après le théorème de Mordell-Weil. En outre, si on choisit ces points de sorte que r soit minimal, alors tout point P s'écrit *de façon unique* de la façon précédente.

Une fois ce résultat acquis, on aura une description très simple des points rationnels de la courbe elliptique. Un point pourra simplement être considéré comme la donnée de r entiers relatifs et d'un point de torsion... et on rappelle que l'on a déjà vu que les points de torsion sont en nombre fini. En outre, la description de l'addition sur les points de la courbe elliptique se transcrit directement à notre nouvelle description : si le point P correspond au $(r+1)$-uplet $(a_1, \ldots, a_r, R)$ et si le point P' correspond au $(r+1)$-uplet $(a'_1, \ldots, a'_r, R')$, alors le point $P+Q$ correspond évidemment au $(r+1)$-uplet $(a_1 + a'_1, \ldots, a_r + a'_r, R + R')$.

L'entier r déterminé précédemment s'appelle le *rang* de la courbe elliptique E_n. Il est évidemment uniquement déterminé puisqu'il a été choisi minimal parmi tous ceux vérifiant une certaine propriété. Cependant, il n'est pas clair que si l'on arrive à trouver d'autres points $P'_1, \ldots, P'_{r'}$ tels que tout point $P \in E_n(\mathbb{Q})$ s'écrive de façon unique sous la forme :

$$P = a'_1P'_1 + a'_2P'_2 + \ldots + a'_{r'}P'_{r'} + R'$$

où les a'_i sont des entiers relatifs et où R' est un point de torsion, il n'est pas clair, disions-nous, que si l'on arrive à faire cela alors $r = r'$. C'est pourtant vrai ! mais cela ne nous intéressera pas franchement.

Passons à la démonstration du résultat et supposons donc que, pour un certain P, l'on puisse écrire simultanément :

$$\begin{aligned} P &= a'_1P_1 + a'_2P_2 + \ldots + a'_rP_r + R' \\ &= a''_1P_1 + a''_2P_2 + \ldots + a''_rP_r + R'' \end{aligned}$$

On veut alors prouver que pour tout indice i, $a'_i = a''_i$ et que $R' = R''$. En faisant la différence de ces deux égalités, et en posant $a_1 = a'_i - a''_i$ et $R = R' - R''$, on obtient :

$$a_1P_1 + a_2P_2 + \ldots + a_rP_r + R = \infty$$

Notre but devient de prouver que $R = \infty$ et que tous les a_i sont nuls.

Pour cela, commençons par considérer $d = \textsc{Pgcd}\,(a_1, \ldots, a_r)$ et posons pour tout i, $x_i = \frac{a_i}{d}$. Le nombre x_i est encore un entier, et les x_i sont premiers entre eux dans leur ensemble. De plus on a :

$$d\,(x_1P_1 + x_2P_2 + \ldots + x_rP_r) + R = \infty$$

et si l'on se rappelle que R était défini comme la différence de deux points de torsion, on voit que R est encore un point de torsion et puis qu'il en est de même de la somme $Q^{(1)} = x_1P_1 + x_2P_2 + \ldots + x_rP_r$.

L'idée, maintenant, est de construire de nouveaux points $Q^{(2)}, \ldots, Q^{(r)}$ tels que tous les P_i puissent s'écrire comme une combinaison linéaire des $Q^{(j)}$, c'est-à-dire tels que pour tout indice i, il existe des entiers $a_{i1}, \ldots, a_{ir}$ vérifiant :

$$P_i = a_{i1}Q^{(1)} + \ldots + a_{ir}Q^{(r)}$$

Si l'on parvient à cela, on aura prouvé que tout point $P \in E_n\,(\mathbb{Q})$ s'écrit comme la somme d'un point de torsion et d'une combinaison linéaire de $Q^{(j)}$; il suffira pour cela de commencer par écrire $P = b_1P_1 + \ldots + b_rP_r + R$ pour certains entiers b_i et un certain point de torsion R, puis de remplacer chacun des P_i par l'expression donnée ci-dessus. Mais on a prouvé par ailleurs que $Q^{(1)}$ est déjà un point de torsion, donc il n'est pas nécessaire dans la somme obtenue au final. Ainsi, on sera parvenu à exhiber une famille de cardinal $r-1$ satisfaisant à la condition à laquelle ne peuvent satisfaire que les familles de cardinal au moins égal à r. C'est une contradiction !

Il ne reste donc plus qu'à construire les $Q^{(j)}$, et bien sûr cela se fait par récurrence. On a déjà le premier, ne le lâchons pas ! On cherche $Q^{(2)}$ sous la forme :

$$Q^{(2)} = y_1P_1 + \ldots + y_rP_r$$

pour certains entiers relatifs y_i. On aimerait déjà plus ou moins retrouver P_1 à partir seulement de $Q^{(1)}$ et de $Q^{(2)}$. Le plus ou moins est important : en fait, ce que l'on aimerait c'est qu'il existe des entiers p et q tels que :

$$pQ^{(1)} + qQ^{(2)} = P_1 + z_2P_2 + \ldots + z_rP_r$$

D'autre part, on aimerait pouvoir récurrer, et pour cela, on aimerait qu'il existe des entiers s et t tels que :

$$sQ^{(1)} + tQ^{(2)} = x'_2P_2 + x'_3P_3 + \ldots + x'_rP_r$$

les x'_i étant cette fois-ci des entiers relatifs premiers entre eux dans leur ensemble.

Faisons cela dans un premier temps, on expliquera ensuite comment cela permet de conclure. Il n'y a aucune condition sur les z_i, ils ne vont donc pas nous gêner. Ce qui est important dans la formule qui les fait intervenir, c'est que le coefficient devant P_1 est 1. Ainsi la seule condition qu'impose cette formule est l'existence d'entiers p et q tels que $px_1 + qy_1 = 1$, c'est-à-dire la relative primalité des entiers x_1 et y_1.

Voyons maintenant la seconde condition. Elle impose tout d'abord $sx_1 + ty_1 = 0$. Choisissons arbitrairement $s = y_1$ et $t = -x_1$. Comme les x'_i doivent être premiers entre eux, il faut s'assurer qu'il existe des entiers u_i tels que :

$$u_2x'_2 + u_3x'_3 + \ldots + u_rx'_r = 1$$

c'est-à-dire :

$$y_1\left(u_2x_2 + \ldots + u_rx_r\right) - x_1\left(u_2y_2 + \ldots + u_ry_r\right) = 1 \tag{1}$$

mais de tels u_i existent. En effet, notons $x = \textsc{Pgcd}\left(x_2, \ldots, x_r\right)$. On sait d'une part, d'après le théorème de Bézout[10], qu'il existe des entiers u_i premiers entre eux tels que :

$$u_2x_2 + \ldots + u_rx_r = x \tag{2}$$

D'autre part, comme tous les x_i sont supposés premiers entre eux, x et x_1 sont également premiers entre eux et donc il existe des entiers u et v tels que :

$$ux - x_1v = 1 \tag{3}$$

On pose $y_1 = u$ et on choisit des y_i tels que :

$$u_2y_2 + \ldots + u_ry_r = v \tag{4}$$

ce qui est possible puisque les u_i ont été choisis premiers entre eux.

En combinant (2), (3) et (4), on tombe bien sur (1) qui est précisément ce que l'on voulait. Récapitulons donc. On commence par choisir des entiers u_i premiers entre eux vérifiant l'équation (2). Une fois cela fait, on choisit u et v vérifiant l'équation (3), puis des entiers y_i vérifiant (4). Si l'on pose maintenant sans se préoccuper de quoi que ce soit, $z_i = y_1x_i - x_1x_i$, on vérifie que l'on a bien rempli toutes les conditions voulues.

Expliquons pour finir comment cela conclut la preuve. Si l'on applique plein de fois la construction précédente, on tombe sur des points $Q^{(j)}$ et plein d'entiers vérifiant les

[10] Ou une généralisation facile laissée au lecteur s'il ne la connaît pas.

conditions :

$$\begin{array}{rcccccl}
Q^{(1)} & = & x_1^{(1)}P_1 + x_2^{(1)}P_2 + x_3^{(1)}P_3 + \ldots + x_{r-1}^{(1)}P_{r-1} + x_r^{(1)}P_r & = & R^{(1)} \\
p^{(2)}R^{(1)} + q^{(2)}Q^{(2)} & = & P_1 + z_2^{(2)}P_2 + z_3^{(2)}P_3 + \ldots + z_{r-1}^{(2)}P_{r-1} + z_r^{(2)}P_r & = & S^{(2)} \\
s^{(2)}R^{(1)} + t^{(2)}Q^{(2)} & = & x_2^{(2)}P_2 + x_3^{(2)}P_3 + \ldots + x_{r-1}^{(2)}P_{r-1} + x_r^{(2)}P_r & = & R^{(2)} \\
p^{(3)}R^{(2)} + q^{(3)}Q^{(3)} & = & P_2 + z_3^{(3)}P_3 + \ldots + z_{r-1}^{(3)}P_{r-1} + z_r^{(3)}P_r & = & S^{(3)} \\
s^{(3)}R^{(2)} + t^{(3)}Q^{(3)} & = & x_3^{(3)}P_3 + \ldots + x_{r-1}^{(3)}P_{r-1} + x_r^{(3)}P_r & = & R^{(3)} \\
\vdots & & \vdots & & \\
p^{(r)}R^{(r-1)} + q^{(r)}Q^{(r)} & = & P_{r-1} + z_r^{(r)}P_r & = & S^{(r)} \\
s^{(r)}R^{(r-1)} + t^{(r)}Q^{(r)} & = & x_r^{(r)}P_r & = & R^{(r)}
\end{array}$$

Si l'on se rappelle que les $x_i^{(r)}$ sont premiers entre eux, on voit que la seule solution est $x_r^{(r)} = \pm 1$. Ainsi P_r s'exprime en fonction des $Q^{(j)}$ comme le montre la dernière ligne. La ligne précédente exprime à son tour P_{r-1}... et ensuite en sautant une ligne sur deux, on exprime tous les autres.

Rappelons, au cas où cette démonstration peut-être un peu laborieuse aurait pu déstabiliser le lecteur, que l'on vient de prouver le théorème suivant :

Théorème 4. *Il existe un unique*[11] *entier r et $P_1, \ldots, P_r$ des points rationnels de la courbe elliptique E_n tels que tout point $P \in E_n(\mathbb{Q})$ s'écrive de façon unique sous la forme :*

$$P = a_1P_1 + \ldots + a_rP_r + R$$

les a_i étant des entiers relatifs et $R \in E_n(\mathbb{Q})$ un point de torsion.

Nous l'avons déjà dit mais répétons-le : l'entier r précédemment déterminé s'appelle le *rang* de la courbe elliptique E_n.

Comme nous l'avons déjà dit également, le précédent théorème se déduit formellement du théorème de Mordell-Weil. Plus précisément, on a le résultat général suivant que nous donnons ici peut-être de façon anecdotique car il serait trop long d'en expliquer tous les termes. Seuls donc les initiés pourront comprendre.

Théorème 5 (Théorème de structure)**.** *Soit A un anneau principal et M un A-module de type fini. Alors il existe un entier r et des idéaux $I_1, \ldots, I_k$ tels que M soit isomorphe à la somme directe :*

$$A^r \oplus A/I_1 \oplus A/I_2 \oplus \ldots \oplus A/I_k$$

les entiers r et k pouvant éventuellement être nuls. L'entier r est uniquement déterminé et s'appelle le rang *de M. Si l'on impose en outre $I_1 \supset I_2 \supset \ldots \supset I_k$, alors l'entier k est aussi uniquement déterminé de même que les idéaux I_i.*

En particulier si $A = \mathbb{Z}$, tout groupe commutatif G de type fini est isomorphe à un produit direct :

$$\mathbb{Z}^r \times \mathbb{Z}/d_1\mathbb{Z} \times \mathbb{Z}/d_2\mathbb{Z} \times \ldots \times \mathbb{Z}/d_k\mathbb{Z}$$

[11] L'unicité n'a en fait pas été prouvée précédemment... elle est cependant vraie.

où r et k sont des entiers éventuellement nuls et où les d_i sont des entiers non nuls. L'entier r est uniquement déterminé et si l'on impose $d_1|d_2|\dots|d_k$, alors k aussi est uniquement déterminé au même titre que les d_i.

3.3 La torsion

Étudions l'ensemble $E_n(\mathbb{Q})_{\text{tor}}$. On a déjà vu qu'il était fini, mais en fait, on peut en dire bien plus. On peut prouver qu'il est toujours réduit aux quatre points évidents : O, A, B et ∞.

Toutefois, pour parvenir à ce résultat, il va falloir présenter $\mathbb{F}_p$, un copain de jeu pour ce paragraphe et les suivants. Soit p un nombre *premier*[12]. Alors $\mathbb{F}_p$ est simplement défini comme l'ensemble $\{0,\dots,p-1\}$.

Sur $\mathbb{F}_p$, on peut définir des opérations : une addition et une multiplication. Exactement, si i et j sont deux entiers strictement inférieurs à p, pour définir la somme $i+j$ (au sens de $\mathbb{F}_p$), on calcule la somme usuelle $i+j$ et on divise le résultat obtenu par p. La somme au sens de $\mathbb{F}_p$ est alors la reste de cette division. La doctrine à retenir est que lorsque l'on a que p nombres, il faut bien s'en accomoder !

La multiplication également ne pose pas de problème. Si i et j sont deux entiers strictement inférieurs à p, on commence par les multiplier puis comme précédemment le reste de la division du résultat précédemment obtenu par p fournit le produit ij qu sens de $\mathbb{F}_p$. Ainsi, par exemple dans $\mathbb{F}_7$, on a $3+4=0$ et $3\times 4=5$.

On a alors des propriétés sympathiques. Déjà quand n est un entier quelconque, on peut le voir dans $\mathbb{F}_p$: il suffit de faire la division euclidienne de n par p et de considérer le reste. Ainsi 17 vu dans $\mathbb{F}_7$ est 3. Maintenant, on a tout fait pour que cela soit compatible aux opérations d'addition et de multiplication. Autrement dit, si x vu dans $\mathbb{F}_p$ est $\bar{x}$ et si y est $\bar{y}$, alors $x+y$ est $\bar{x}+\bar{y}$ (cette dernière addition se faisant dans $\mathbb{F}_p$) et xy est $\bar{x}\bar{y}$.

Et cela ne s'arrête pas là ; on peut également soustraire et diviser. Soustraire, c'est simplement ajouter l'opposé. Et comme l'opposé d'un entier est encore un entier, on voit bien qu'il n'y aura pas de problème. Par contre la division est plus subtile : normalement lorsque l'on divise deux entiers, on tombe sur un rationnel. Il faut donc expliquer comment on peut voir les rationnels dans $\mathbb{F}_p$.

En fait, on ne peut pas tous les voir, mais seulement ceux dont le dénominateur n'est pas un multiple de p. Expliquons. Prenons $\frac{a}{b}$ un rationnel, avec b premier à p (c'est équivalent à ne pas être un multiple de p puisque l'on rappelle que p est choisi premier). Comme b est premier à p par le théorème de Bézout, il existe des entiers u et v tels que $ub+pv=1$. Donc si l'on note avec des barres, les mêmes entiers vus dans $\mathbb{F}_p$, on a $\bar{u}\bar{b}=1$, ce qui semble suggérer que si le rationnel $\frac{1}{b}$ doit être vu d'une certaine façon dans $\mathbb{F}_p$, c'est bien comme l'élément $\bar{u}$. Donc le rationnel $\frac{a}{b}$ devrait être, dans $\mathbb{F}_p$, l'élément $\bar{a}\bar{u}$... et c'est bien la définition que l'on prend.

On constate finalement que la définition ne dépend pas de la fraction choisie représentant un rationnel donné. Expliquons cette dernière phrase par un exemple. Supposons que l'on veuille voir $\frac{1}{3}$ dans $\mathbb{F}_7$. Les entiers 3 et 7 sont premiers entre eux et une relation de Bézout qui les lie est $3\times(-2)+7\times 1=1$. Ainsi d'après la définition précédente $\frac{1}{3}$ est dans $\mathbb{F}_p$ le nombre $\overline{-2}=5$. Mais on aurait pu faire la même chose avec la fraction $\frac{2}{6}$ et il serait agréable de trouver le même résultat. C'est en fait le cas : une relation liant 6 et

[12] La primalité est une hypothèse cruciale.

7 est $6 \times (-1) + 7 \times 1$ donc $\frac{1}{6}$ est représenté dans $\mathbb{F}_7$ par $\overline{-1} = 6$ et puis $\frac{2}{6}$ est représenté dans $\mathbb{F}_7$ par la produit $2 \times 6 = 5$ dans $\mathbb{F}_7$. C'est bien le même résultat !

Si on récapitule, dans $\mathbb{F}_p$, on arrive à voir tous les entiers et même tous les rationnels dont le dénominateur est premier à p. En particulier, si a et b sont deux éléments non nuls de $\mathbb{F}_p$, on sait donner un sens, dans $\mathbb{F}_p$, au quotient $\frac{a}{b}$. Ainsi, l'ensemble des $\mathbb{F}_p$-points de la courbe elliptique E_n a bien un sens. Il s'agit de l'ensemble des couples (x, y) tels que $y^2 = x^3 - n^2 x$, mais x et y étant des éléments de $\mathbb{F}_p$ et les opérations se faisant dans $\mathbb{F}_p$ une fois que l'on a converti l'entier n^2 en un élément de $\mathbb{F}_p$.

En outre, si on a $P = (x, y)$ un point rationnel de E_n, et si p ne divise ni le dénominateur de x, ni celui de y, on peut voir ces rationnels dans $\mathbb{F}_p$. Disons que l'on obtient $\bar{x}$ et $\bar{y}$. Le couple $(\bar{x}, \bar{y})$ est un élément de $E_n(\mathbb{F}_p)$ puisque les opérations sont compatibles. Bien évidemment, on peut avoir deux points rationnels P et Q qui induisent le même point de $E_n(\mathbb{F}_p)$ et il est aussi possible qu'un point de $E_n(\mathbb{F}_p)$ ne soit induit par aucun point rationnel.

Une dernière chose importante à remarquer, c'est que si P et Q sont des points rationnels de E_n qui se réduisent respectivement sur les points $\bar{P}$ et $\bar{Q}$ dans $E_n(\mathbb{F}_p)$, alors $P + Q$ se réduit sur le point $\bar{P} + \bar{Q}$. Il est facile de comprendre pourquoi : les coordonnées de la somme se calculent par des formules qui sont tout autant valables dans $\mathbb{Q}$ et dans $\mathbb{F}_p$. Faites le calcul si vous n'êtes pas convaincu !

Regardons maintenant l'ensemble $E_n(\mathbb{Q})_{\text{tor}}$, c'est un sous-ensemble fini de $E_n(\mathbb{Q})$. Appelons $x_1, \ldots, x_m$ les abscisses des points (qui ne sont pas à l'infini) de cet ensemble et écrivons pour tout i, $x_i = \frac{p_i}{q_i}$. Appelons q par exemple le produit des q_i. Considérons un nombre premier p supérieur à tous les qp_i. Tous les q_i sont alors premiers avec p et donc tous les éléments de $E_n(\mathbb{Q})_{\text{tor}}$ peuvent se réduire dans $E_n(\mathbb{F}_p)$. En outre, si $\frac{p_i}{q_i}$ et $\frac{p_j}{q_j}$ se réduisent sur le même élément, il en est de même des entiers $p_i q_j$ et $p_j q_i$. Mais ces deux entiers sont strictement inférieurs à p et donc on en déduit que l'on a une véritable égalité $p_i q_j = p_j q_i$ puis $\frac{p_i}{q_i} = \frac{p_j}{q_j}$.

Finalement pour p suffisamment grand, $E_n(\mathbb{Q})_{\text{tor}}$ peut être vu comme un sous-ensemble de $E_n(\mathbb{F}_p)$. Calculons le cardinal de ce dernier ensemble. Il s'agit donc de résoudre $y^2 = x^3 - n^2 x$ dans $\mathbb{F}_p$. Déjà, commençons par une chose plus simple. Prenons $a \in \mathbb{F}_p$ et résolvons $y^2 = a$ dans $\mathbb{F}_p$. Ici intervient crucialement l'hypothèse de primalité de p. Le résultat est la suivant : si $a = 0$, il y a une unique solution qui est $y = 0$, sinon, il y a soit deux solutions opposées, soit aucune solution[13].

Il va maintenant nous falloir admettre une chose[14] : si p est congru à 3 modulo 4, alors l'équation $y^2 + 1 = 0$ n'a pas de solution dans $\mathbb{F}_p$. Autrement dit -1 n'est pas un carré dans $\mathbb{F}_p$ lorsque p est congru à 3 modulo 4. En particulier si $x \in \mathbb{F}_p$ est non nul, un et un seul des deux nombres x et $-x$ admet une racine carrée (et en fait exactement deux).

Maintenant, on regarde. Prenons p premier congru à 3 modulo 4, plus grand disons que $2n + 1$ et aussi plus grand que tous les $p_i q$ précédents de sorte que l'on puisse voir $E_n(\mathbb{Q})_{\text{tor}}$ comme un sous-ensemble de $E_n(\mathbb{F}_p)$. La quantité $x^3 - n^2 x = x(x - n)(x + n)$ ne s'annule dans $\mathbb{F}_p$ que pour les trois valeurs 0, n et $-n$. Attention, cela n'est pas *a priori*

[13] Pourquoi ?

[14] Il s'agit d'une application directe du critère d'Euler : $a \in \mathbb{F}_p$ est carré si et seulement si $a^{\frac{p-1}{2}} = 1$ (dans $\mathbb{F}_p$). Ce critère se déduit simplement du petit théorème de Fermat qui dit que tout élément $a \in \mathbb{F}_p$ vérifie $a^{p-1} = 1$.

évident, et c'est bien vrai parce que p est choisi premier[15]. Pour ces trois valeurs de x, donc, on a un et un unique point de $E_n(\mathbb{F}_p)$.

Pour les autres valeurs de x, on en a soit 0 soit 2. Mais si on n'en a pas pour x, alors $x^3 - n^2x$ n'est pas un carré et donc son opposé en est un, et son opposé, c'est $-x^3 + n^2x = (-x)^3 - n^2(-x)$. Ainsi, on a deux solutions pour $-x$. Et réciproquement, si on a deux solutions pour x, on n'en a pas pour $-x$. On a donc en moyenne une solution par élément de $\mathbb{F}_p$. Ça en fait p. On n'oublie pas de rajouter le point à l'infini, on en a $p+1$.

On a donc vu l'ensemble qui nous intéresse, $E_n(\mathbb{Q})_{\text{tor}}$ comme un sous-ensemble d'un ensemble de cardinal $p+1$. Mais c'est mieux qu'un sous-ensemble, c'est un sous-groupe, c'est-à-dire que c'est un sous-ensemble stable par addition et soustraction. On utilise maintenant le théorème de Lagrange qui est le suivant :

Théorème 6 (Lagrange)**.** *Le cardinal d'un sous-groupe divise le cardinal du groupe.*

Cet énoncé paraît peut-être mystérieux, surtout que l'on n'a pas franchement défini précisément le sens de tous les mots. Peu importe. Pour ici, il suffit juste de remarquer qu'il implique que le cardinal de l'ensemble $E_n(\mathbb{Q})_{\text{tor}}$, cardinal que l'on va noter c, est un diviseur de $p+1$. Et ceci est valable pour tout nombre premier p congru à 3 modulo 4 et suffisamment grand.

On utilise maintenant encore un théorème, celui de Dirichlet. C'est le suivant :

Théorème 7 (Dirichlet)**.** *Si a et b sont deux entiers strictement positifs et premiers entre eux, alors il existe une infinité de nombres premiers congrus à a modulo b.*

Si le théorème de Lagrange n'est pas un résultat difficile, celui de Dirichlet est en revanche assez dur. Nous n'allons donc évidemment pas le prouver. Comment conclut-on maintenant ? Tout d'abord prenons un p suffisamment grand (qui existe d'après le théorème de Dirichlet) congru à 3 modulo 8. Alors p est bien congru à 3 modulo 4 et donc c doit diviser $p+1$. Mais $p+1$ est congru à 4 modulo 8, donc c ne peut être un multiple de 8. La plus grande puissance de 2 qu'il y a dans c est donc $2^2 = 4$.

De même prenons un nombre premier ℓ différent de 2. Alors il existe un nombre premier p congru à la fois à 3 modulo 4 et à 1 modulo ℓ. En effet, on voit que vérifier les congruences précédentes équivaut au seul fait d'être congru à $2\ell+1$ modulo 4ℓ ; ces deux derniers nombres étant premiers entre eux, on peut appliquer le théorème de Dirichlet. Le nombre $p+1$ est alors congru à 2 modulo ℓ et donc n'est pas un multiple de ℓ. Comme c doit diviser $p+1$, c ne peut diviser ℓ, et cela est vrai pour tout nombre premier impair ℓ.

En mettant tout bout à bout, on voit qu'il ne reste plus qu'une possibilité : c doit être égal à 4. On connaît déjà quatre éléments dans l'ensemble $E_n(\mathbb{Q})_{\text{tor}}$, on l'a donc déterminé complètement. C'est $E_n(\mathbb{Q})_{\text{tor}} = \{O, A, B, \infty\}$.

Le théorème 4 se réénonce de façon encore plus simple désormais :

Théorème 8. *Il existe un unique entier r et $P_1, \ldots, P_r$ des points rationnels de la courbe elliptique E_n tels que tout point $P \in E_n(\mathbb{Q})$ s'écrive de façon unique sous la forme :*

$$P = a_1P_1 + \ldots + a_rP_r + R$$

les a_i étant des entiers relatifs et R étant un des quatre points O, A, B ou ∞.

[15] Essayez d'écrire la démonstration, par exemple.

3.4 Reformulation du problème et résolution dans certains cas

À partir de maintenant, nous ne ferons plus aucune démonstration, ni même essaierons de donner les idées. Elles deviennent vraiment trop difficiles, et on va énoncer certains résultats qui restent conjecturaux au moment où ce texte est tapé.

Remarquons quand même que le théorème précédent implique directement que l'entier n est congruent si et seulement si le rang de la courbe elliptique E_n est strictement positif. En effet, on avait déjà dit que l'entier n était congruent si et seulement si E_n admettait un point rationnel autre que O, A, B et ∞. Avec la description précédente, le rapport avec le rang est immédiat.

Notre but est donc d'estimer le rang des courbes elliptiques E_n, ce qui est un problème délicat. Une façon d'y accéder est de retravailler quelque peu sur le lemme 2. Ce que l'on peut voir, c'est que le cardinal minimal d'un ensemble $\mathcal{R}$ convenable est directement relié au rang : c'est 2^{r+2}. Ainsi si l'on arrive à borner correctement cet ensemble $\mathcal{R}$, on pourra accéder à des majorations du rang.

Ainsi, on peut montrer le résultat suivant :

Théorème 9. *On suppose ici que n est un nombre premier impair. Alors :*

1. *si n est congru à 1 modulo 8, le rang de la courbe elliptique E_n est inférieur à 2 ;*
2. *si n est congru à 3 modulo 8, le rang de la courbe elliptique E_n est nul ;*
3. *dans tous les autres cas, le rang de la courbe elliptique E_n est inférieur à 1*

On attire l'attention sur le fait que ce résultat n'est valable que pour les nombres premiers. En particulier le dans tous les autres cas signifie bien dans tous les autres cas où n est premier . Avoir des majorations par 1 ou 2 n'est pas franchement intéressant pour nous, il faut l'avouer. Mais cela peut être intéressant dans l'absolu.

Toutefois, il y a quand même un cas important, c'est le deuxième. Si l'on admet que ce théorème est vrai (et même relativement facile), on a prouvé que tout nombre premier congru à 3 modulo 8 n'est pas congruent. En particulier, 3 n'est pas congruent ; 19 non plus n'est pas congruent.

3.5 Une conjecture pour accéder au rang

Il existe principalement une conjecture qui relie le rang d'une courbe elliptique à un autre objet de nature plus analytique. Bien qu'il s'agisse là de mathématiques fort intéressantes, nous ne sommes pas persuadé que le bref exposé qui va suivre puisse convaincre grand nombre de gens. Mais donnons-le quand même. On suppose vraiment à partir de maintenant que l'entier n est sans facteur carré.

On appelle N_p le cardinal de l'ensemble $E_n(\mathbb{F}_p)$. L'idée est que si le rang de E_n est grand, alors il y aura beaucoup de points dans $E_n(\mathbb{Q})$ et donc puisque beaucoup de ces points induisent des points dans $E_n(\mathbb{F}_p)$, il risque d'y avoir beaucoup de points dans $E_n(\mathbb{F}_p)$. Bien sûr, cette constatation est tout sauf rigoureuse, mais c'est l'idée de départ.

On dispose en contrepartie du théorème suivant :

Théorème 10 (Hasse)**.** *Avec les notations précédentes, on a toujours la majoration :*

$$|N_p - (p+1)| \leqslant 2\sqrt{p}$$

Ainsi l'idée précédente ne se concrétise pas forcément de la meilleure façon puisque N_p ne peut pas franchement varier, mais faisons quand même avec.

Maintenant le problème revient à calculer N_p. Pour cela, étonnamment, on introduit une fonction annexe qui est la suivante :

$$L(E_n, s) = \prod_{p \not| 2n} \frac{1}{1 - a_p p^{-s} + p^{1-2s}}$$

où s est un nombre complexe et où a_p vaut par définition $a_p = N_p - (p+1)$. Ce produit infini est convergeant lorsque la partie réelle de s est strictement supérieure à $\frac{3}{2}$. Toutefois, on peut prolonger cette fonction, de façon naturelle dirions-nous, à $\mathbb{C}$ privé de quelques points. En particulier, on sait définir sa valeur en 1. Moralement, ça devrait être :

$$L(E_n, s) = \prod_{p \not| 2n} \frac{1}{1 - \frac{a_p}{p} + \frac{1}{p}} = \prod_{p \not| 2n} \frac{p}{N_p}$$

et donc effectivement ce nombre devrait être grand lorsque N_p est petit, et petit lorsque N_p est grand.

En fait la conjecture précise est la suivante :

Conjecture 1. *Le rang de la courbe elliptique E_n est supérieur ou égal à 1 si et seulement si $L(E_n, 1) = 0$.*

Plus précisément, en fait, on a :

Conjecture 2 (Birch et Swinnerton-Dyer)**.** *Le rang de la courbe elliptique E_n est égal à l'ordre d'annulation*[16] *de la fonction $s \mapsto L(E_n, s)$ en 1.*

Le sens direct de la première conjecture est démontré, *i.e.* on sait que si le rang de E_n est supérieur ou égal à 1 alors la fonction $L(E_n, s)$ s'annule en $s = 1$. En particulier, si elle ne s'annule pas en cette valeur, le rang de E_n est nul, et donc l'entier n est congruent.

On sait aussi, d'après un résultat relativement récent de Nekovář, que les deux nombres que l'on souhaite comparer dans la seconde conjecture, s'ils ne sont pas égaux, ont en tout cas la même parité.

Reste donc à donner une méthode pour calculer un peu plus explicitement la fonction $L(E_n, s)$. Cela résulte d'une équation fonctionnelle vérifiée par la fonction en question. Exactement, définissons la fonction Λ *via* la formule :

$$\Lambda(s) = \left(\frac{\sqrt{N}}{2\pi}\right)^s \Gamma(s) L(E_n, s)$$

où N est défini comme étant égal à $32n^2$ si n est impair, et à $16n^2$ sinon et où Γ désigne la fonction d'Euler définie par la formule :

$$\Gamma(s) = \int_0^{+\infty} t^{s-1} \exp(-t)\, \mathrm{d}t$$

[16] Le rang d'annulation de la fonction f en 1 est le nombre de zéros que l'on trouve au début de la suite des dérivées successives de f en 1.

Sa valeur en un entier k strictement positif est $(k-1)!$ (lire $k-1$ factorielle), c'est-à-dire le produit $1 \times 2 \times \ldots \times (k-1)$.

L'équation fonctionnelle vérifiée par $L(E_n, s)$ se traduit sur la fonction Λ *via* la formule :

$$\Lambda(2-s) = \varepsilon_n \Lambda(s)$$

avec $\varepsilon_n = 1$ si n est congru à 1, 2 ou 3 modulo 8 et $\varepsilon_n = -1$ sinon.

Dans le cas où $\varepsilon_n = -1$, cette dernière équation implique $\Lambda(1) = 0$ et puis $L(E_n, 1) = 0$. Ainsi d'après la première conjecture énoncée précédemment, l'entier n serait congruent. On peut même obtenir ce résultat en ne se basant sur aucune conjecture. En effet, l'équation fonctionnelle prouve non seulement que la fonction L s'annule en 1, mais plus généralement que l'ordre d'annulation en ce point est impair. D'après donc la résultat de Nekovář, le rang de la courbe elliptique E_n est également impair, et donc non nul.

On a donc le théorème suivant :

Théorème 11. *Si l'entier n est sans facteur carré et congru à 5, 6 ou 7 modulo 8, alors n est congruent.*

Et finalement un dernier résultat :

Théorème 12 (Tunnel)**.** *Soit n un entier sans facteur carré. Alors :*

1. *si n est impair, $L(E_n, 1) = 0$ si et seulement si le nombre de représentations de n sous la forme $2x^2 + y^2 + 8z^2$ (x, y, z entiers relatifs) est double du nombre de représentations sous la forme $2x^2 + y^2 + 32z^2$;*
2. *si n est pair, $L(E_n, 1) = 0$ si et seulement s'il y a deux fois plus de représentations de $\frac{n}{2}$ sous la forme $4x^2 + y^2 + 8z^2$ que sous la forme $4x^2 + y^2 + 32z^2$.*

On obtient comme cela un critère simple, en tout cas facilement vérifiable sur machine, pour la congruence. En outre, si la conjecture de Birch et Swinnerton-Dyer est vraie, on en obtient un également pour la non-congruence. Par exemple, on peut rapidement faire la vérification pour $n = 157$.

Bibliographie commentée

La référence principale est une traduction par Lemmermeyer d'un article de Guy Henniart. Lemmermeyer l'appelle *Congruent Numbers, Elliptic Curves and Modular Forms* et ne sait apparemment plus où a été publié l'original. La traduction est disponible en ligne ([1]).

Une autre référence en ligne précieuse est le cours de J. Milne sur les courbes elliptiques, qui est relativement élémentaire et fort riche. À télécharger sur son site ([2]).

Les livres en français au sujet des courbes elliptiques sont à notre connaissance, et c'est regrettable, fort rares. Comme exception notable, on peut citer [3]. Il contient peu de démonstrations, mais essaie de faire sentir la saveur de quelques grandes idées arithmétiques.

Pour le lecteur qui veut par ailleurs préciser ses connaissances en matière d'algèbre générale , on peut recommander [4].

Plus en rapport avec le sujet de l'exposé, il faut sans doute citer [5], qui prend le thème des nombres congruents comme fil conducteur, et développe en particulier le lien avec les formes modulaires, ce qui lui permet d'expliquer d'où provient l'énoncé sans cela très mystérieux du résultat de Tunnel.

Plus élémentaires, on peut mentionner deux beaux livres d'introduction à l'arithmétique des courbes elliptiques : [6] qu'on peut vraiment mettre entre toutes les mains, et [7] qui demande un peu plus de prérequis et est écrit dans un style plus concis, mais met l'accent sur des aspects différents et peut-être plus profonds.

Dans un genre très différent, [8] enthousiasmera particulièrement les amateurs de géométrie et de topologie.

Une bibliographie sur les courbes elliptiques ne serait pas vraiment complète sans la mention de [9] qui fait figure de référence canonique sur cette question. Ce n'est pas un livre tout à fait élémentaire, mais il est abordable sans connaissance préalable en géométrie algébrique : toutes les notions nécessaires sont introduites de façon assez lumineuse dans les deux premiers chapitres.

Enfin, sur les aspects historiques, [10] est une référence incontournable. On peut citer aussi le magnifique ouvrage [11] qui, s'il n'est pas aussi encyclopédique que le précédent, est toujours d'une lecture passionnante.

References

[1] `http://public.csusm.edu/public/FranzL/publ/guy.pdf`

[2] `http://www.jmilne.org/math/CourseNotes/math679.html`

[3] Y. Hellegouarch, *Introduction aux mathématiques de Fermat-Wiles*, Dunod, 2001

[4] M. Demazure, *Cours d'algèbre*, Cassini, 1997

[5] N. Koblitz, *Introduction to elliptic curves and modular forms*, Graduate texts in Mathematics, **94**, Springer, 1984

[6] J.H. Silverman, J. Tate, *Rational points on elliptic curves*, Undergraduate texts in Mathematics, Springer, 1992

[7] J.W.S. Cassels, *Lectures on Elliptic Curves*, LMS Student Texts, **24**, Cambridge University Press, 1991

[8] H. McKean, V. Moll, *Elliptic Curves : function theory, geometry, arithmetic*, Cambridge University Press, 1999

[9] J.H. Silverman, *The Arithmetic of Elliptic Curves*, Graduate texts in Mathematics, **106**, Springer, 1986

[10] L.E. Dickson, *History of the theory of numbers*, Stechert, 1934

[11] A. Weil, *Number theory, an approach through history from Hammurapi to Legendre*, Birkhäuser, 1984