LE THÉORÈME DE FERMAT
INVITATION À L'ARITHMÉTIQUE DES COURBES ELLIPTIQUES

KARIM BELABAS

Table des matières

1. Géométrie projective

1.1. **Plan projectif.** Soit K un corps ; pour le moment vous pouvez penser à $K = \mathbb{Q}$ ou $\mathbb{R}$, on veut essentiellement un ensemble muni des quatre opérations élémentaires $+$, $-$, $\times$, $/$ (avec diviseur $\neq 0$). On appelle *plan affine* l'ensemble $\mathbb{A}^2(K) := K^2$ des couples d'éléments de K, et *plan projectif* l'ensemble $\mathbb{P}^2(K)$ des triplets non nuls dans K^3, à homothétie près[1]. On peut se représenter un point projectif $(x : y : z)$ comme le point ordinaire $(x/z, y/z)$, *sauf* quand $z = 0$, auquel cas on a affaire à des "points à l'infini". On peut donc se représenter $\mathbb{P}^2(K)$ comme $\mathbb{A}^2(K) \cup D_\infty$, où D_∞ est une

Date: 2001.

[1] $(x : y : z) \simeq (\lambda x : \lambda y : \lambda z)$ pour tout $\lambda \in K^*$, $x, y, z \in K$ non tous nuls.

droite (projective, on peut aussi la voir comme une droite ordinaire munie d'un point à l'infini).

C'est un objet intéressant parce que, du point de vue arithmétique, il permet de passer naturellement de problèmes entiers à des problèmes rationnels et vice-versa et que, du point de vue géométrique, il évite des distinctions inutiles. Par exemple, dans $\mathbb{A}^2(\mathbb{R})$, on a trois sortes de coniques : hyperboles, ellipses, paraboles. Dans $\mathbb{P}^2(\mathbb{R})$, ces trois types n'en font plus qu'un, à un changement de repère immédiat près.

1.2. **Courbes.** Soit $k \subseteq K$ un corps. On appelle courbe (projective, plane, définie sur k) de degré n une équation $\mathcal{C} : P_n(X, Y, Z) = 0$ où P_n est homogène de degré n à coefficients dans k. On a plutôt coutume d'imaginer une courbe comme un ensemble de points, mais il est souvent avantageux de considérer les solutions de cette équation dans K, en faisant varier K : $\mathbb{C}$, $\mathbb{R}$, $\mathbb{Q}$, $\mathbb{Z}/p\mathbb{Z}$, $\mathbb{Q}_p$, ... La donnée fondamentale est bien l'équation. Les points de la courbe dans $\mathbb{P}^2(K)$ sont notés $\mathcal{C}(K)$; remarquer que la valeur $P(x, y, z)$ n'est pas bien définie si $(x : y : z) \in \mathbb{P}^2(K)$, mais que la condition $P(x, y, z) = 0$ l'est ! On a le joli résultat suivant :

Théorème 1.1 (Bézout). *Dans $\mathbb{P}^2(\mathbb{C})$, deux courbes de degré m et n distinctes se coupent exactement en mn points*[2]*, à condition de compter avec la bonne multiplicité les points où les courbes sont tangentes.*

Par exemple, ce théorème dit que deux droites (courbe de degré 1) distinctes se coupent en un point unique ; si elles sont parallèles, elles se coupent en un point de D_∞ bien sûr !

1.3. **Points rationnels, Points p-adiques.** En particulier $\mathcal{C}(\mathbb{Q})$ est l'ensemble des *points rationnels* de $\mathcal{C}$. Si p est premier, la situation sur chaque $\mathbb{Z}/p\mathbb{Z}$ est souvent plus simple que sur $\mathbb{Q}$, et permet parfois de conclure. Par exemple s'il existe p tel que $\mathcal{C}(\mathbb{Z}/p\mathbb{Z}) = \emptyset$, alors on a aussi $\mathcal{C}(\mathbb{Q}) = \emptyset$: ainsi $Y^2 - 5X^2 = 3$ n'a pas de points sur $\mathbb{Z}/5\mathbb{Z}$, donc l'équation n'a pas de solutions rationnelles. On peut généraliser cette idée et considérer les solutions modulo p^2, p^3, ... ce qui conduit à introduire $\mathbb{Z}_p$ l'ensemble des suites d'approximations modulo p^i, $i \geqslant 1$, et $\mathbb{Q}_p$ son corps des fractions. Sur $\mathbb{R}$ aussi, on peut identifier des obstructions : $X^2 + Y^2 = -1$ n'a pas de points sur $\mathbb{R}$, donc sur $\mathbb{Q}$ non plus. Pour une conique (degré 2) la réciproque est vraie : si les $\mathcal{C}(\mathbb{Q}_p)$ et $\mathcal{C}(\mathbb{R})$ sont non vides, il y a un point dans $\mathcal{C}(\mathbb{Q})$. D'une certaine façon, la situation sur $\mathbb{R}$ et sur l'ensemble des $\mathbb{Q}_p$ approche convenablement la situation sur $\mathbb{Q}$.

Il n'est pas évident de produire un exemple, mais c'est faux en général : on peut avoir $\mathcal{C}(\mathbb{R}) \neq \emptyset$, et $\mathcal{C}(\mathbb{Q}_p) \neq \emptyset$ (il y a des solutions modulo p^k pour tout k) pour tout p, et pourtant ne pas avoir de points dans $\mathcal{C}(\mathbb{Q})$. Ce phénomène peut se produire dès que $\deg(\mathcal{C}) > 2$. La courbe $3X^3 + 4Y^3 + 5Z^3 = 0$ est un exemple célèbre, dû à Selmer ; la démonstration est un peu longue mais élémentaire, voir [3].

2. Coniques – Théorie algébrique des nombres

Le théorème de Bézout dit qu'une droite coupe une conique (degré 2) en exactement 2 points ; considérons par exemple le cercle : $X^2+Y^2 = 1$, d'équation projective $X^2+Y^2 = Z^2$. Supposons que nous nous intéressons à ses points rationnels. Il n'y a pas de tel point à l'infini puisque -1 n'est pas un carré, donc autant travailler dans le plan affine. Une

[2] il faudrait écrire $\#(\mathcal{C}_1(\mathbb{C}) \cap \mathcal{C}_2(\mathbb{C})) = mn$. Sur $\mathbb{R}$ ou dans le plan *affine* on a seulement $\leqslant mn$.

droite passant par le point $(-1,0)$, d'équation paramétrique $X+1=tY$ (pour simplifier, excluons la droite horizontale) recoupe le cercle en un unique autre point :

$$X=\frac{t^2-1}{t^2+1},\quad Y=\frac{2t}{t^2+1}$$

On voit qu'il s'est produit un petit miracle : on obtient une paramétrisation par des *fractions rationnelles* définies sur $\mathbb{Q}$, et non pas sur $\mathbb{C}$ par exemple. En particulier, pour des valeurs $t\in\mathbb{Q}$, on trouve $(X,Y)\in\mathbb{Q}^2$. On voit tout de suite que la correspondance est bijective, au point $(1,0)$ près. Le point $(-1,0)$ n'a rien de magique d'ailleurs, le même phénomène se produira en partant d'un point rationnel quelconque, par exemple $(3/5,4/5)$, en excluant un autre point.

Le phénomène se généralise facilement : si une conique $\mathcal{C}$ a un point rationnel, on obtient une telle paramétrisation qui établit une bijection entre $\mathcal{C}(\mathbb{Q})$ et $\mathbb{Q}$, à un nombre fini de points près. Donc la situation sur $\mathbb{Q}$ n'est pas très intéressante : soit il n'y a pas de point et il n'y a rien à dire, soit il y en a un et on paramètre par une droite. Ceci dit, cette paramétrisation rationnelle ne nous aide pas à trouver les points entiers. Mais sur $\mathbb{Z}$ apparaissent plusieurs phénomènes remarquables : examinons la conique $X^2-DY^2=e$.

2.1. **Nombres algébriques.** On est conduit à introduire le corps $\mathbb{Q}(\sqrt{D})=\{a+b\sqrt{D}:\ a,b\in\mathbb{Q}\}$ et une nouvelle arithmétique (sur $\mathbb{Z}[\sqrt{D}]=\{a+b\sqrt{D}:\ a,b\in\mathbb{Z}\}$). Si $z=x+\sqrt{D}y$, on note $\overline{z}:=x-\sqrt{D}y$ et $N(z):=z\overline{z}=x^2-dy^2$ (c'est bien sûr une généralisation du module complexe). En particulier, l'existence ou non d'un z vérifiant $z\overline{z}=e$ va dépendre de propriétés de factorisation de e en produit de "nombres premiers" dans $\mathbb{Z}[\sqrt{D}]$: si on a unicité de factorisation on peut en déduire z. C'est hélas rarement le cas, on ne sait même pas si cela se produit pour une infinité de D ! On a le même problème avec l'équation de Fermat qui s'écrit

$$X^n=Z^n-Y^n=\prod_{j=1}^{n}(Z-\zeta^jY)$$

pour $\zeta:=\exp(2i\pi/n)$. Le théorème fondamental de l'arithmétique sur $\mathbb{Z}$ dit que tout entier se factorise de façon unique en produit d'éléments irréductibles (les nombres premiers), aux éléments inversibles près (±1). Quand le théorème analogue est valide dans $\mathbb{Z}[\zeta]$, on montre assez facilement que l'équation n'a pas de solutions (voir [8]). Hélas, il est faux pour presque tout n.

2.2. **Addition.** N est une fonction multiplicative et s'il existe une solution z, alors tous les zu, avec $u\in\mathbb{Z}[\sqrt{D}]$, $Nu=1$, sont aussi solutions. On considère donc dorénavant le cas $e=1$ (équation de Pell-Fermat). L'égalité

$$N((x+\sqrt{D}y)(a+\sqrt{D}b))=N(x+\sqrt{D}y)N(a+\sqrt{D}b)$$

donne l'identité

$$(xa+dyb)^2-D(ya+xb)^2=(x^2-Dy^2)(a^2-Db^2)$$

Donc si on pose $(a,b)[+](x,y):=(xa+Dyb,ya+xb)$, la loi $[+]$ induit une structure de groupe abélien, de neutre $\mathbf{O}:=(1,0)$, sur les points (rationnels par exemple) de

l'hyperbole $\mathcal{H} : X^2 - DY^2 = 1$. Si P est un point de $\mathcal{H}(K)$, on note

$$[n]P := \underbrace{P[+]\dots[+]P}_{n}$$

Dans le cas $D = -1$, avec $e(\alpha) := \exp(2i\pi\alpha)$, on trouve $e(\alpha)[+]e(\beta) = e(\alpha+\beta)$. Donc l'"addition" sur le cercle est simplement l'addition habituelle transportée par l'exponentielle complexe. En particulier, elle correspond à la ... multiplication des affixes $e(\alpha)$, et $[n]z$ correspond à l'exponentiation z^n.

2.3. **Finitude.** S'il existe $n > 0$ tel que $[n]P = \mathbf{O}$, on dit que le point P est *de torsion* (la suite $\mathbf{O}$, P, $[2]P$, $[3]P$, ... se mord la queue) et le plus petit tel n est appelé *ordre* de P ; sinon P est d'*ordre infini*. Les seuls points de torsion dans $\mathcal{H}(\mathbb{Q})$ sont d'affixe ± 1, $\pm e(1/2)$ (si $D = -1$), $\pm e(1/3)$ et $\pm e(2/3)$ (si $D = -3$). Ils forment donc un sous-groupe fini, en fait cyclique d'ordre 2, 4, ou 6.

Dernier miracle, on peut décrire $\mathcal{H}(\mathbb{Z})$ de façon *finie* et explicite : si $D = d^2$ ou $D < 0$ il n'y a que des points de torsion. Sinon, il y a des points d'ordres infini (... une infinité !), mais tout point entier s'écrit $P_t + [n]P_0$, où P_t est de torsion (on a vu que la liste des possibilités est courte) et $P_0 = (x_0, y_0)$ est un point d'ordre infini *fixé* qui ne dépend que de D, le plus "petit" d'entre eux (tel que $\varepsilon_0 := x_0 + y_0\sqrt{D} > 1$ soit minimal). $\mathcal{H}(\mathbb{Q})$ n'admet pas de telle description au moyen d'un nombre fini de générateurs, mais elle est avantageusement suppléée par la paramétrisation rationnelle.

Il existe des algorithmes efficaces pour calculer P_0 (voir [4]), même si ses coordonnées deviennent vite gigantesques, possiblement de l'ordre de $\exp(\sqrt{D})$. Par exemple le célèbre problème des bœufs du Soleil [2, T.2, pp.545–547], attribué à Archimède probablement apocryphe, mais revient à résoudre sur $\mathbb{Z}$ l'équation

$$X^2 - 4729494Y^2 = 1, \quad \text{où } 9314 \text{ divise } Y$$

La solution fondamentale P_0 correspond à

$$\varepsilon_0 = 109931986732829734979866232821433543901088049 + 50549485234315033074477819735540408986340\sqrt{4729494}$$

et la plus petite solution satisfaisant la condition de divisibilité est $[2329]P_0$, soit un troupeau de $7.76\ 10^{206545}$ têtes (solution de Amthor, 1880).

2.4. **Fonction L.** Pour simplifier la discussion, on suppose dorénavant que $D \equiv 2, 3 \pmod 4$ est sans facteur carré. Les solutions dans $\mathbb{Z}[\sqrt{D}]$ de l'équation $|Nz| = 1$ sont appelées *unités* de $\mathbb{Z}[\sqrt{D}]$ (ce sont les éléments inversibles, tels qu'il existe $u \in \mathbb{Z}[\sqrt{D}]$ avec $uz = 1$).

Quel que soit p premier, le nombre d'éléments de $\mathcal{H}(\mathbb{Z}/p\mathbb{Z})$ est $p+1$; parmi eux $p - a_p$ points sont dans $\mathbb{A}(\mathbb{Z}/p\mathbb{Z})$, où

$$a_p := \begin{cases} 1 & \text{si } D \text{ est un carré non nul de } \mathbb{Z}/p\mathbb{Z}, \\ -1 & \text{si } D \text{ n'est pas un carré de } \mathbb{Z}/p\mathbb{Z}, \\ 0 & \text{si } D \equiv 0 \pmod p. \end{cases}$$

On rassemble tous ces renseignements obtenus localement (sur $\mathbb{Z}/p\mathbb{Z}$) en un objet global (lié à $\mathcal{H}(\mathbb{Q})$) :

$$L(\mathcal{H}, s) := \prod_{p \text{ premier}} \frac{1}{1 - a_p p^{-s}}$$

A priori, c'est une fonction définie pour $\mathrm{Re}(s) > 1$.

Théorème 2.1 (Dirichlet). *L se prolonge analytiquement en une fonction entière. Au voisinage de 0, on a l'équivalent*

$$L(\mathcal{H}, s) \sim 2\frac{hR}{w}s^r \tag{1}$$

où

$$\begin{cases} r = 1,\ R = \log(x_0 + \sqrt{D}y_0) & \text{si } D > 0 \text{ (cf. § précédent),} \\ r = 0,\ R = 1 & \text{sinon,} \end{cases}$$

et w est le nombre d'unités de torsion (2, 4 ou 6). L'entier h est le cardinal d'un groupe fini (le groupe des classes) qui mesure l'obstruction à ce que le théorème fondamental de l'arithmétique soit vrai dans $\mathbb{Z}[\sqrt{D}]$: il vaut 1 si et seulement si tout élément se décompose de façon unique en produit d'irréductibles, à une unité près.

3. Courbes elliptiques – Préliminaires

Au niveau des points rationnels, une conique ayant un point rationnel (degré 2) et une droite (degré 1) ont le même comportement, donc le degré n'est pas un très bon indicateur. On regroupe les courbes en grandes classes ou *genres*, définis à partir de leur degré, mais aussi de leurs points singuliers, et dans cette classification les droites et les coniques forment le genre numéro 0. Les courbes de genre 1 ayant un point rationnel sont appelées *courbes elliptiques*. Après un changement de repère envoyant le point rationnel à l'infini, elles se ramènent toutes à une équation cubique simple[3] :

3.1. **Définition.** On appelle *courbe elliptique* sur k une équation de la forme

$$\mathcal{E} : Y^2 = X^3 + aX + b$$

où $a, b \in k$ et le membre de droite n'a pas de racines multiples ($4a^3+27b^2 \neq 0$). S'il avait des racines multiples, la courbe aurait un point double P sur k et on obtiendrait une paramétrisation de $\mathcal{E}$ comme dans le cas des coniques en considérant les droites passant par P (qui n'auraient qu'un seul autre point d'intersection avec $\mathcal{E}$) ; on obtiendrait en fait une courbe de genre 0.

On associe à $\mathcal{E}$, la courbe projective $Y^2Z = X^3+aXZ^2+bZ^3$. Cela revient à adjoindre le point à l'infini $\mathbf{O} := (0 : 1 : 0)$ à $\mathcal{E}$. Si vous n'aimez pas la géométrie projective, ce n'est pas grave, imaginez le comme un point d'ordonnée infinie, qui rencontre toutes les droites verticales. On note $\mathcal{E}(K)$ l'ensembles des points de $\mathcal{E}$ (des solutions de l'équation $\mathcal{E}$) à coordonnées dans K, y compris le point à l'infini.

3.2. **Loi de groupe.** La propriété fondamentale des courbes elliptiques est qu'elles possèdent une structure naturelle de groupe algébrique, comme l'hyperbole de Pell-Fermat : c'est-à-dire qu'il existe une loi d'addition sur leur points, donnée par des fonctions algébriques des coordonnées.

Géométriquement, la loi d'addition $[+]$ est donnée par la construction suivante, par corde et tangente : si $P, Q \in \mathcal{E}(K)$, la corde PQ coupe $\mathcal{E}(K)$ en un unique troisième point R'. Soit R le point d'intersection de la droite verticale $\mathbf{O}R'$ avec $\mathcal{E}(K)$: on pose $P[+]Q := R$.

[3] si k est de caractéristique 2 ou 3, il faut autoriser une équation un peu plus générale, de la forme $Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6$, toujours sans points singuliers.

Les cas dégénérés se traitent de façon naturelle : si $A = B$, la droite AB désigne la tangente en A à $\mathcal{E}(K)$; si $P = Q = \mathbf{O}$, on pose $R = \mathbf{O}$. On obtient les formules suivantes, pour $P = (x_P, y_P)$, $Q = (x_Q, y_Q)$, $R = P[+]Q = (x_R, y_R)$:

$$x_R := -x_P - x_Q + m^2 \quad \text{et} \quad y_R := -y_P + m(x_P - x_R)$$

où

$$m := \begin{cases} (y_Q - y_P)/(x_Q - x_P) & \text{si } P \neq Q \\ (dy/dx)_P := (3x_P^2 + a)/(2y_P) & \text{si } P = Q \end{cases}$$

Le cas $P \neq Q$ et $x_P = x_Q$ ne peut arriver que si $Q = P'$ (P et Q sont symétriques par rapport à l'axe horizontal) et dans ce cas $P[+]Q$ est le point à l'infini $\mathbf{O}$. Il n'est pas évident de voir que $[+]$ est une loi associative (c'est-à-dire que $(P[+]Q)[+]R = P[+](Q[+]R)$ pour tout P, Q, $R \in \mathcal{E}(K)$), mais c'est vrai. Il y a une jolie démonstration géométrique (soient 8 points en position générale, alors chaque cubique passant par ces points passe par un 9-ème point indépendant de la courbe). Votre logiciel de calcul formel favori y arrivera très bien aussi, mais c'est assez lourd : il y a beaucoup de cas particuliers à vérifier, si des points sont confondus.

On voit alors facilement que $[+]$ définit une loi de groupe commutatif sur $\mathcal{E}(K)$, de neutre $\mathbf{O}$ ($\mathbf{O}[+]P = P$) et l'opposé de P est le point P' qui est son symétrique par rapport à l'axe horizontal. Ces formules sont algébriques, donc valables sur $\mathcal{E}(K)$, pour un corps K quelconque, par exemple $K = \mathbb{Q}$ mais aussi sur $K = \mathbb{Z}/p\mathbb{Z}$; il suffit de savoir inverser un élément non nul.

3.3. **Finitude.** Il n'y a pas de paramétrisation rationnelle comme pour les coniques, mais $\mathcal{E}(\mathbb{Q})$ est cette fois de type fini, et $\mathcal{E}(\mathbb{Z})$ est fini. Le sous-groupe de torsion est fini (il y a ici aussi très peu de possibilités, son cardinal est plus petit que 16), et un nombre fini de points rationnels engendrent tous les autres : tout point est somme d'un point de torsion P_t et d'une combinaison linéaire de P_i, $i = 1, \ldots, r$ où les P_i sont d'ordre infini. Le r minimal est appelé *rang* de $\mathcal{E}(\mathbb{Q})$, mais il n'y a plus de règle simple pour le calculer, et il n'y a pas non plus d'algorithme complet, même déraisonnable ! Il y a une méthode, initiée par la descente de Fermat qui marche dans la plupart des cas concrets, mais a priori on ne sait obtenir qu'un encadrement pour r. C'est en particulier lié au fait qu'une courbe plus compliquée qu'une conique peut avoir des points dans tous les $\mathbb{Q}_p$ et dans $\mathbb{R}$ sans qu'il y en ait dans $\mathbb{Q}$. On pense que le rang r peut devenir arbitrairement grand si $\mathcal{E}$ varie. Voici le record actuel, obtenu par spécialisation d'un paramètre dans une famille de Mestre :

Théorème 3.1 (Martin-McMillen). *La courbe elliptique*

$$y^2 + xy + y = x^3 - 19252966408674012828065964616418441723x + 32685500727716376257923347071452044295907443056345614006$$

est de rang au moins 23 *sur* $\mathbb{Q}$ *(on ne sait pas prouver qu'elle est de rang* 23 *; l'équation est donnée sous une forme non-standard pour que ses coefficients soient plus petits, mais c'est bien une courbe elliptique).*

Preuve. Les points $P_1, \dots, P_{23}$ sont indépendants dans $\mathcal{E}(\mathbb{Q})$:

$P_1 =$(169021360446217242755846613925 95/119224493521,
$-$ 6945551978497199367980755230860973943085824881 2/41166906143372569)
$P_2 =$(664788227246610382163477204657 1/30891226081,
$-$ 171370238447109871400493873099459538929462135 44/5429411004770479)
$P_3 =$(127722933203564970666484672759 2/2961427561, 144338084333927239745872103074239201669630404 6/161157926442059)
$P_4 =$(175483477191647698213209065 1/369369961, 4941213072098788690444330115275871038879 6/7098921280459)
$P_5 =$(902743031953703698667092998/307406089, 65384341040093032650247499528307090293535389750958437)
$P_6 =$(103579510135061476534950819/45091225, 230697883363551870088729854504374414548/302787575875)
$P_7 =$(317620445694077660039737525 5/14054813809, 14113810892913497531647688085589210029472047 1666240341498377)
$P_8 =$(294369842136676487233 95/17956, 56573350120462407053573194528022 33/2406104)
$P_9 =$(1127027270330215920, 3523978127407100674110377602)
$P_{10} =$(686462445028218997115 15/139129, $-$39456365194588240358046887343510581 6/51895117)
$P_{11} =$(119626759538163665617 95/1369, $-$11679627683163195928765715173170 44/50653)
$P_{12} =$(305206808054026951757573 55/3345241, $-$15191511458906140310075969810653233311 2/6118445789)
$P_{13} =$(114497755380507560193576353 16/967521025, $-$11507750319084169189551153656516344945016 51/30094741482625)
$P_{14} =$(496941824398262166179559177 0/1285294201, 184569435055535326366697454229180527073 27/46079082400051)
$P_{15} =$(480465113537612829840777315/160801, $-$10531550647702714814852169224678207441368/64481201)
$P_{16} =$(979071542846797779179825421660 35/57601436172721,
964874722537391293613786748114488474882993683572/4371696135204725654 81)
$P_{17} =$(249989354826313432718977195/4397409, 394115627677600726379274563037933493799 6/9221366673)
$P_{18} =$(548400741230865078083881 35/3996001, 387496978790653709721061294119215460988/7988005999)
$P_{19} =$(969014131906380158018946942 0/87590881, $-$95314407807994290636090367003653666959354 2/819763055279)
$P_{20} =$(882142442406602738753880/76729, $-$77539455668083765129216637769887473 4/21253933)
$P_{21} =$(281217595039522693658198 4/24025, 47126242719731099651600390857893913 67/3723875)
$P_{22} =$(712626973710101740607975233707137 1/2947180538019481,
830154545759986840069002057269682226865053507996 84/159996363164349841378621)
$P_{23} =$(2143448685801212487450/841, 1009984922118966827735475374820 8/24389)

□

3.4. **Fonction L.** La conjecture de Birch et Swinnerton-Dyer (BSD, ≈ 1960) interprète le rang r comme l'ordre du zéro de la fonction $L(\mathcal{E}, s)$ de Hasse-Weil, définie en terme du nombre de points de $\mathcal{E}$ sur tous les corps finis. En gros, elle s'écrit

$$L(\mathcal{E}, s) \approx \prod_{p \text{ premier}} \frac{1}{1 - a_p p^{-s} + p^{1-2s}}$$

où $\#\mathcal{E}(\mathbb{Z}/p\mathbb{Z}) = p+1-a_p$ ($\approx$ car il faut exclure les p divisant le discriminant $4a^3+27b^2$, sinon sur $\mathbb{Z}/p\mathbb{Z}$, $\mathcal{E}$ n'est plus une courbe elliptique ; il faut rajouter un facteur correctif pour ces premiers).

Théorème 3.2 (Hasse). *Les coefficients $a_p := p + 1 - \mathcal{E}(\mathbb{Z}/p\mathbb{Z})$ vérifient l'inégalité $|a_p| < 2\sqrt{p}$.*

Ceci permet de définir $L(\mathcal{E}, s)$ pour $\mathrm{Re}(s) > 3/2$. On conjecturait depuis longtemps que cette fonction se prolongeait analytiquement en une fonction entière ; c'est maintenant une conséquence des travaux de Wiles, et de leur descendance.

BSD prédit alors un équivalent de la forme $L(\mathcal{E}, s) \sim \lambda(s-1)^r$ au voisinage de 1, où λ est donnée par une formule explicite, analogue à (1). Jusqu'aux travaux de Wiles on ne savait même pas, en général, si $L(\mathcal{E}, s)$ était définie au voisinage de $s = 1$! On ne sait pas si le "groupe fini" analogue du groupe des classes dans la conjecture BSD (groupe de Tate-Shafarevich) est toujours fini ou pas.

Cette fonction et ses dérivées successives sont estimables sur ordinateur ; malheureusement, sans résultat théorique, il est impossible de prouver que la valeur approchée obtenue, même calculée à des milliers de décimales, est bien un zéro exact. On obtient ainsi une valeur (doublement) conjecturale pour le rang.

On pourrait s'intéresser ensuite aux courbes de genre g supérieur à 2 (il existe des courbes de tout genre $g \in \mathbb{N}$), mais il n'y a plus de loi de groupe comme pour les

deux premiers genres. En particulier il est beaucoup plus difficile de construire des points rationnels. Faltings (1983) a montré que $\mathcal{C}(\mathbb{Q})$ est fini, dès que le genre de $\mathcal{C}$ est supérieur à 2. On peut en déduire qu'à exposant $n > 3$ fixé, l'équation de Fermat $X^n + Y^n = Z^n$ n'a qu'un nombre fini de solutions $(x : y : z) \in \mathbb{P}^2(\mathbb{Q})$, mais on ne sait rien sur la taille de ces solutions éventuelles. La démonstration de Wiles n'utilise pas le théorème de Faltings.

4. Courbes Elliptiques – Applications

4.1. **Factorisation dans $\mathbb{Z}$.** (voir [4] ou [6]). Soit N un entier impair. A cause du petit théorème de Fermat, il est facile de se convaincre que N est probablement premier si $a^{N-1} \equiv 1 \pmod N$ pour plusieurs a choisis au hasard (cette exponentiation est facile à faire, même si N a des milliers de chiffres). Cette méthode est due à Fermat lui-même. En fait, il existe une infinité de N non premiers qui passent ce test pour tout a premier à N, les nombres de Carmichael. Mais on peut le modifier de façon à ce qu'au moins $3/4$ des entiers $a < N$ trahissent un entier N non premier. La modification repose sur le fait que si $x^{2^k} = 1$ dans $\mathbb{Z}/N\mathbb{Z}$, alors soit $x = 1$, soit il y a un -1 dans la chaîne des x^{2^i}, $i < k$. En d'autres termes, on a $X^{2^k} - 1 = (X-1)\prod_{0 \leqslant i < k}(X^{2^i}+1)$.

On désire maintenant factoriser N. Lenstra (≈ 1980) a inventé une très jolie (et très efficace) méthode utilisant les courbes elliptiques, sur $\mathbb{Z}/N\mathbb{Z}$. Ce n'est pas un corps, mais on peut utiliser les mêmes formules pour définir une addition sur $\mathcal{E}(\mathbb{Z}/N\mathbb{Z})$. Un élément de $\mathbb{Z}/N\mathbb{Z}$ est inversible si et seulement si il est premier à N. Donc la loi d'addition ne marche pas quand un dénominateur n'est pas premier à N. Mais justement ! Son pgcd avec N est plus grand que 1, et s'il est non nul modulo N, ce pgcd fournit un facteur non trivial de N !

Soit p le plus petit diviseur premier (inconnu) de N. Si un entier de la taille de p n'a que des petits facteurs premiers (où "petit" est défini en fonction de p), on dit qu'il est *friable*. Si on se donne $P \in \mathbb{P}^2(\mathbb{Z}/N\mathbb{Z})$, il est immédiat de trouver $\mathcal{E}_{a,b} : Y^2 = 4X^3 + aX + b$ tels que $P \in \mathcal{E}_{a,b}(\mathbb{Z}/N\mathbb{Z})$. Alors la réduction de P modulo p appartient à $\mathcal{E}_{a,b}(\mathbb{Z}/p\mathbb{Z})$; si l'ordre de ce dernier groupe est friable, l'ordre de P aussi. En calculant $Q := [n]P$ sur $\mathcal{E}(\mathbb{Z}/N\mathbb{Z})$ pour n un multiple adéquat de tous les petits premiers, la réduction de Q modulo p sera le point $\mathbf{O}$ de $\mathcal{E}(\mathbb{Z}/p\mathbb{Z})$. Donc une inversion requise pour l'addition dans $\mathcal{E}(\mathbb{Z}/N\mathbb{Z})$ sera impossible, ce qui dévoile p. Si rien d'intéressant ne se produit, on jette $\mathcal{E}$ et P et on choisit une autre courbe.

Cette méthode généralise une idée de Pollard qui utilisait le groupe $\{(\mathbb{Z}/p\mathbb{Z})^*, \times\}$, d'ordre $p-1$ au lieu de $\{\mathcal{E}(\mathbb{Z}/p\mathbb{Z}), [+]\}$, d'ordre $p + 1 - a_p$. La méthode de Pollard est nettement plus restrictive puisqu'elle ne marche que si $p-1$ est friable, alors qu'en faisant varier $\mathcal{E}$, on obtient des groupes d'ordre là aussi proche de p, mais variant dans un intervalle de longueur $4\sqrt{p}$, à cause de l'inégalité $|a_p| < 2\sqrt{p}$. Un grand nombre d'entre eux devrait donc être d'ordre friable. Cette méthode est d'autant plus efficace que N a de petits diviseurs : elle extrait facilement des facteurs de 20 chiffres d'entiers gigantesques. Par contre, elle n'est pas capable d'attaquer les entiers utilisés en cryptologie (par exemple pour RSA, voire plus bas), qui sont produits de deux grand nombres premiers de même taille.

4.2. **Preuve de Primalité.** On utilise aussi ce type de méthodes pour *prouver* qu'un entier N est premier. Il y a un analogue très simple de la méthode de Pollard :

Théorème 4.1. *S'il existe un entier g tel que*

$$g^{N-1} \equiv 1 \pmod{N}$$

mais

$$g^{(N-1)/\ell} \not\equiv 1 \pmod{N}$$

pour tout diviseur premier ℓ de $N-1$, alors N est premier.

Un tel g est en pratique facile à trouver. Bien sûr, il faut être capable de factoriser $N-1$! Soit $N_0 = N$; la situation favorable est la suivante : $N_0 - 1$ est friable, à un gros facteur N_1 près, qui à l'air premier ; il suffit alors de montrer que N_1 est premier, et on recommence. On construit ainsi une suite strictement décroissante d'entiers N_i tels que la primalité de N_{i+1} prouve celle de N_i. La suite $(g_0, N_0), (g_1, N_1), \ldots$ est un *certificat de primalité* de N puisque le théorème permet immédiatement de vérifier la primalité de chacun des N_i, donc de $N = N_0$. Le problème c'est qu'il n'y a aucune raison que cette situation favorable se produise, *i.e.* que tous les N_i soient essentiellement friables. La généralisation aux courbes elliptiques est bien plus agréable :

Théorème 4.2. *Soit N un entier premier à 6, $\mathcal{E}$ une courbe elliptique sur $\mathbb{Z}/N\mathbb{Z}$, et soit $P \in \mathcal{E}(\mathbb{Z}/N\mathbb{Z})$. On note m le cardinal* [4] *de $\#\mathcal{E}(\mathbb{Z}/N\mathbb{Z})$ et on choisit un diviseur s de m. Si pour chaque diviseur premier ℓ de s, $(m/\ell)P := (x_\ell : y_\ell : z_\ell)$ satisfait $(z_\ell, N) = 1$, alors pour tout diviseur premier p de N, on a $s \mid \#\mathcal{E}(\mathbb{Z}/p\mathbb{Z})$.*

Dans les conditions du théorème, l'inégalité de Hasse, qui s'écrit aussi

$$\#\mathcal{E}(\mathbb{Z}/p\mathbb{Z}) < (\sqrt{p}+1)^2$$

implique facilement que si $s > (\sqrt[4]{N}+1)^2$, alors $N = p$, *i.e.* N est premier.

L'algorithme de Goldwasser et Kilian choisit des $\mathcal{E}$ au hasard tant que $m(\mathcal{E})$ n'est pas friable, possiblement à un gros facteur s près, qui a l'air premier. Un point P satisfaisant les conditions du théorème est alors facile à trouver : la plupart des points de la courbe conviennent. La primalité de s, qui entraîne celle de N, est montrée de même. Comme pour la factorisation, on a beaucoup de liberté pour choisir $\mathcal{E}$, donc beaucoup de choix pour m, contrairement à la méthode utilisant $(\mathbb{Z}/p\mathbb{Z})^*$. Le problème vient de ce qu'il reste quand même difficile de calculer $\#\mathcal{E}(\mathbb{Z}/p\mathbb{Z})$ quand p est vraiment grand. Une variante nettement moins naïve de ce test (due à Atkin) permet de certifier la primalité d'entiers de l'ordre de 6000 chiffres décimaux. C'est un résultat pratique : on ne dispose pas d'un *théorème* garantissant l'arrêt en un temps explicite raisonnable (polynomial).

4.3. **Cryptologie clé publique.** (voir [6]). Si G est un ensemble muni d'une addition $[+]$ (associative) et si a et b sont deux entiers, alors $[a]([b]x) = [b]([a]x) = [ab]x$ pour tout $x \in G$. Supposons que deux personnages A et B ne se connaissent pas et veulent échanger une clé de chiffrement à usage unique (pour un unique message, par exemple dans le cadre d'un achat via Internet). Etant donné $\{G, [+]\}$ et x publics, A et B choisissent un entier (respectivement a et b) chacun dans leur coin et transmettent à leur correspondant respectivement $[a]x$ et $[b]x$. Chacun des deux peut alors facilement reconstituer $[ab]x$, et l'utiliser comme clé de chiffrement / déchiffrement. Cette idée, fondatrice des méthodes de clé publique (où l'information nécessaire au chiffrage n'a

[4] Schoof a inventé un algorithme ingénieux (amélioré par Elkies et Atkin) pour calculer m très efficacement en supposant que N est bien premier. Il fonctionne en devinant $a_N := N + 1 - \mathcal{E}(\mathbb{Z}/N\mathbb{Z})$ modulo de petits premiers, et en reconstruisant a_N grâce au lemme Chinois et à l'inégalité de Hasse.

pas besoin d'être protégée, ce qui facilite grandement sa transmission), est due à Diffie et Hellman (1976), originellement pour $G = (\mathbb{Z}/p\mathbb{Z})^*$.

On appelle *logarithme discret* sur G l'opération qui à partir de $[a]x$ et x fournit un a solution (en notation multiplicative $[a]x \to x^a$, l'appellation est plus naturelle), et on note $\log_x [a]x := a$. Un espion éventuel des échanges entre A et B ne dispose au mieux que de x, $[a]x$, et $[b]x$ et il semble difficile d'en déduire $[ab]x$ si le problème du logarithme discret est ardu sur G.

En particulier, on peut prendre $G = \{(\mathbb{Z}/p\mathbb{Z})^*, \times\}$, mais il existe une attaque efficace. L'idée est très simple, fondée sur les mêmes propriétés de friabilité que pour la factorisation : on cherche beaucoup d'entiers c tels que $x^c \mod p$, vu comme entier, soit friable ; avec suffisamment de c on peut calculer $\log_x p_i$ pour tous les "petits" premiers en inversant la matrice donnant la factorisation des x^c en fonction des p_i. Pour un b arbitraire, il suffit ensuite de trouver un c tel que bx^c soit friable pour obtenir $\log_x(b)$ en fonction de c et des $\log_x p_i$ qui sont maintenant connus. Les records actuels pour le calcul de logarithmes discrets par ce type de méthode sont de l'ordre de 120 chiffres pour p.

Par contre si $G = \{\mathcal{E}(\mathbb{Z}/p\mathbb{Z}), [+]\}$ est une courbe elliptique, cette attaque ne marche pas : il n'y a pas de bonne notion de friabilité. A l'heure actuelle, même un premier de 50 chiffres constitue une excellente protection[5]. Evidemment, plus les nombres à traiter sont petits, plus il est facile de programmer les algorithmes d'échanges (notamment le calcul de $[a]P$ dans $\mathcal{E}(\mathbb{Z}/p\mathbb{Z})$) sur des processeurs peu sophistiqués, par exemple des cartes à puces.

Le codage RSA (Rivest, Shamir, Adleman 1977) est proche de cette procédure d'échange de clés, mais fondé sur la difficulté à factoriser un grand entier $N = pq$, où p et q sont premiers, de tailles comparables. Cette fois-ci il n'y a plus symétrie, mais un chef qui connaît p et q et calcule une paire d'entiers (c, d) tels que $cd = 1 \pmod{\phi(N)}$, où $\phi(N) := (p-1)(q-1)$. Il garde d à l'abri (d comme déchiffrer, c'est une clé secrète), et publie c (chiffrer, clé publique).

Une généralisation immédiate du petit théorème de Fermat, due à Euler, indique que $x^{\phi(N)} = 1 \pmod N$ pour tout entier x premier à N. Donc les transformations de $\mathbb{Z}/N\mathbb{Z}$ données par $x \to x^c$ et $y \to y^d$ sont inverses l'une de l'autre. Si un message $0 < x < N$ est chiffré par la transformation $x \to y := x^c \pmod N$, le calcul $y^d \pmod N$ redonne le x initial. Ici, la difficulté vient de ce qu'on ne sait pas calculer d à partir de c sans connaître $\phi(N)$, ni $\phi(N)$ à partir de N sans p ou q. Le chef peut donc publier sans crainte c et N et n'importe qui pourra lui envoyer des messages qu'il sera seul à pouvoir déchiffrer.

RSA offre l'avantage de permettre une authentification des message, *i.e.* un procédé de signature : si on vous soumet un message x, vous pouvez le signer avec votre clé secrète d : $x \to y := x^d$. Toute personne connaissant votre clé publique c, que vous n'avez aucune raison de cacher puisque sa découverte ne compromet en rien le système, peut alors vérifier votre signature par la transformation $y \to y^c$. Si elle obtient le message intelligible x, elle a la « preuve » que vous connaissez la clé secrète.

[5]Le record actuel (04/2000) est de 32 chiffres, en 200000 MIPS-années (l'équivalent de 500 ans de calcul sur PC 450Mhz), répartis sur 9500 ordinateurs.

A cause des progrès dans les techniques de factorisations, N doit être grand[6]. Donc RSA est relativement coûteux à mettre en pratique pour de gros volumes de données, ou pour de petites calculettes. Elle est surtout utilisée comme procédé de signature (cartes bleues).

4.4. **Nombres congruents.** (voir [5]). On appelle *triplet pythagoricien* un point rationnel $(x : y : z) \in \mathcal{C}(\mathbb{Q})$ du cercle $\mathcal{C} : X^2 + Y^2 = Z^2$. Ce sont les dimensions d'un triangle rectangle à cotés de longueurs rationnelles. On dit qu'un entier n est *congruent* s'il est l'aire d'un tel triangle ($= XY/2$). Par exemple 6 est congruent (associé à $(3 : 4 : 5)$), 5 aussi $(3/2 : 20/3 : 41/6)$, 157 aussi pour

$$X = \frac{411340519227716149383203}{21666555693714761309610}, \quad Y = \frac{6803298487826435051217540}{411340519227716149383203}$$

$$Z = \frac{224403517704336969924557513090674863160948472041}{8912332268928859588025535178967163570016480830}$$

(c'est la plus "petite" solution).

Fermat a montré par descente infinie que 1 n'est pas congruent, c'est équivalent au "théorème de Fermat" pour l'exposant 4. On montre que n est congruent si et seulement si la courbe elliptique $\mathcal{E}_n : Y^2 = X^3 - n^2X$ a un point rationnel d'ordre infini, et ce point donne un triplet pythagoricien convenable, en fait une infinité.

BSD implique alors que n est congruent si et seulement si $L(\mathcal{E}_n, 1) = 0$. En fait l'implication est un théorème de Coates-Wiles (1977), à cause de la forme spéciale de $\mathcal{E}_n$ (courbe à multiplication complexe) ; seule la réciproque (si $L(\mathcal{E}_n, 1) = 0$, alors n est congruent) est conjecturale.

Théorème 4.3 (Tunnell, 1983). *Si n, entier impair sans facteur carrés, est congruent alors*

$$2\#\{x, y, z \in \mathbb{Z} : n = 2x^2 + y^2 + 32z^2\} = \#\{x, y, z \in \mathbb{Z} : n = 2x^2 + y^2 + 8z^2\}$$

(pour n pair, on a un critère analogue : il faut remplacer n par $n/2$ et $2x^2$ par $4x^2$.) Si BSD est vraie pour la courbe $\mathcal{E}_n$, alors la réciproque est aussi vraie.

Ce théorème permet de prouver très facilement qu'un entier donné, par exemple 1, n'est pas congruent. C'est très certainement la démonstration la plus compliquée du théorème de Fermat pour l'exposant 4 !

4.5. **Formes modulaires, Grand Théorème de Fermat !** Une forme modulaire de poids $k \in \mathbb{N}$ est une fonction analytique sur le demi-plan de Poincaré $\{z \in \mathbb{C}, \mathrm{Im}(z) > 0\}$

$$f(z) = \sum_{n \geqslant 0} a_n e(nz), \quad \text{où } e(z) := e^{2i\pi z}$$

présentant de nombreuses symétries, du type $f((az+b)/(cz+d)) = (cz+d)^k f(z)$ pour un k fixé et pour toute matrice inversible $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ à coefficients entiers[7]. Comme la plupart des objets que nous avons considéré dans ce texte, ces fonctions (pour un k et un groupe de transformations donnés) bénéficient d'une propriété de finitude : elles constituent un espace vectoriel de dimension finie, dont certaines bases sont explicites et ont des

[6]Le record actuel (1999) pour la factorisation d'un N type RSA est de 155 chiffres, en 8000 MIPS-années.

[7]vérifiant possiblement des conditions supplémentaires, des congruences par exemples, auquel cas on est amené à généraliser la définition en remplaçant le facteur $e(nz)$ par $e(nz/\ell)$ pour un entier ℓ fixé.

propriétés remarquables. Etant donné une forme modulaire, dont on connaît quelques coefficients, on peut alors l'exprimer comme combinaison linéaire explicite des fonctions de la base, et en déduire des identités hautement non triviales entre leurs coefficients. C'est ainsi que Tunnell montre son théorème, en reliant des formes modulaires dont certains coefficients sont les $L(\mathcal{E}_n, 1)$ (on veut qu'ils s'annulent) et d'autres dont les coefficients comptent les représentations de n par des formes quadratiques ternaires.

La conjecture de Shimura-Taniyama-Weil (STW) énonce que $L(\mathcal{E}, s)$ est une forme modulaire de poids 2, à un changement de notation près ($n^{-s} \to e(nz)$). C'est elle que Wiles a montré, pour une très large classe de courbes $\mathcal{E}$. La démonstration a été complétée depuis : STW est vraie pour toute courbe elliptique définie sur $\mathbb{Q}$ (Breuil, Conrad, Diamond, Taylor, 2000). Cela prouve en particulier que $L(\mathcal{E}, s)$ est entière.

Or STW entraîne le théorème de Fermat : soit p un premier et

$$a^p + b^p = c^p$$

une solution non triviale ($abc \neq 0$) de l'équation de Fermat pour l'exposant p. On considère la courbe elliptique $Y^2 = X(X - a^p)(X - b^p)$ et la fonction L associée, qui est une forme modulaire de poids 2 par l'argument de Wiles. A partir de celle-ci, on construit, par un argument difficile de Ribet (1986), une forme modulaire non triviale dans un espace que l'on sait être nul, d'où une contradiction.

Références

[1] Archimède, *Oeuvres*, Blanchard, Paris, 1960.
[2] J. W. S. Cassels, *Lectures on elliptic curves*, Cambridge University Press, Cambridge, 1991.
[3] H. Cohen, *A course in computational algebraic number theory*, third ed., Springer-Verlag, 1996.
[4] N. Koblitz, *Introduction to elliptic curves and modular forms*, second ed., Springer-Verlag, New York, 1993.
[5] N. Koblitz, *A course in number theory and cryptography*, second ed., Springer-Verlag, New York, 1994.
[6] J. H. Silverman, *The arithmetic of elliptic curves*, Springer-Verlag, New York, 1986.
[7] L. C. Washington, *Introduction to cyclotomic fields*, second ed., Springer-Verlag, 1997.