Introduction au domaine de recherche : la conjecture de Birch et Swinnerton-Dyer

Matteo Tamiozzo

17 Juin 2016

Table des matières

1 Introduction

Un problème très général et ancien en théorie des nombres consiste à déterminer l'ensemble des solutions rationnelles d'une équation à plusieurs inconnues à coefficients rationnels. Un exemple célèbre est l'équation $x^n + y^n = z^n$, n étant un entier positif. Pour $n = 2$ elle admet bien sûr un nombre infini de solutions rationnelles, et pour $n > 2$ le dernier théorème de Fermat, démontré par Andrew Wiles et Richard Taylor ([Wil95, TW95]), affirme que cette équation n'a pas de solution avec x, y, z non nuls.

Considérons plus en général un polynôme homogène $f(x, y, z) \in \mathbb{Q}[x, y, z]$. Supposons que la courbe projective complexe C définie par l'équation $f = 0$ soit lisse ; il s'agit donc d'une surface de Riemann. On veut décrire l'ensemble $C(\mathbb{Q})$ des solutions (à multiplication par un scalaire non nul près) de l'équation $f = 0$. On dispose des résultats suivants :

1. Si la courbe C a genre 0 alors soit $C(\mathbb{Q}) = \emptyset$, soit $C(\mathbb{Q})$ est infini. De plus, on peut toujours déterminer si $C(\mathbb{Q})$ est vide ou pas (grâce du principe local-global de Hasse Minkowski, voir [Ser96, Ch. 1]).
2. Si le genre de C est plus grand que 1, alors $C(\mathbb{Q})$ est toujours fini. C'est un résultat très important (et difficile) du a Faltings ([Fal83]).

Le cas qui reste, c'est à dire celui des courbes de genre 1, est le cas que va nous intéresser dans la suite. Dans ce cas l'ensemble $C(\mathbb{Q})$ peut être vide, fini ou infini. L'un des buts de beaucoup

de recherche contemporaine en théorie des nombres est de donner une méthode pour décrire la structure de $C(\mathbb{Q})$. Par example, une question très simple qui est encore ouverte est trouver une procédure qui détermine, pour n'importe quelle courbe C de genre 1, si $C(\mathbb{Q})$ est fini ou infini.

La conjecture de Birch et Swinnerton-Dyer donne un réponse très élégante à ces problèmes, reliant la structure de l'ensemble $C(\mathbb{Q})$ aux propriétés d'une fonction analytique, la fonction L, associée à la courbe C. Le but de cette introduction au domaine de recherche est d'expliquer en détail l'énoncé de cette conjecture, ainsi que de donner un aperçu des résultats connus à ce propos.

2 Généralités sur les courbes elliptiques

Définition 2.1. Soit K un corps. Une courbe elliptique E sur K est une courbe projective lisse de genre 1 définie sur K, munie d'un point $O \in E(K)$.

Concrètement, une telle courbe peut toujours s'écrire comme lieu des zéros d'une équation de la forme :

$$y^2z + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz^2 + a_6z^3$$

Si E/K est une courbe elliptique, on peut montrer que l'ensemble $E(K)$ des points de E à coordonnées dans K est muni naturellement d'une structure de groupe abélien. L'étude de $E(K)$ revient donc à déterminer la structure de ce groupe.

Dans la suite on va s'intéresser surtout au cas $K = \mathbb{Q}$. Dans ce cas (et plus en général, si K est un corps de nombres) on a le résultat classique suivant :

Théorème 2.2. *(Mordell-Weil, 1922) Le groupe $E(\mathbb{Q})$ est un groupe abélien de type fini.*

On donne les grands lignes de la preuve de ce théorème, que nous amène à introduire des invariants cruciales dans l'étude de l'arithmétique des courbes elliptiques. On montre d'abord que, pour tout entier $n \geq 2$, le groupe $E(\mathbb{Q})/nE(\mathbb{Q})$ est fini. Pour cela on considère l'application $[n] : E \longrightarrow E$, qui envoi un point P sur nP. Notons $E[n]$ l'ensemble des points de n-torsion dans $E(\bar{\mathbb{Q}})$. On a une suite exacte de $Gal(\bar{\mathbb{Q}}/\mathbb{Q})$-modules :

$$0 \longrightarrow E[n] \longrightarrow E(\bar{\mathbb{Q}}) \xrightarrow{n} E(\bar{\mathbb{Q}}) \longrightarrow 0$$

La suite exacte longue en cohomologie correspondante donne une suite exacte :

$$0 \longrightarrow E(\mathbb{Q})/nE(\mathbb{Q}) \xrightarrow{\delta} H^1(\mathbb{Q}, E[n]) \longrightarrow H^1(\mathbb{Q}, E)[n] \longrightarrow 0 \tag{1}$$

Pour chaque nombre premier p on a une suite exacte analogue à (1), avec $\mathbb{Q}_p$ en lieu de $\mathbb{Q}$. On obtient ainsi un diagramme commutatif :

$$\begin{array}{ccccccccc}
0 & \longrightarrow & E(\mathbb{Q})/nE(\mathbb{Q}) & \xrightarrow{\delta} & H^1(\mathbb{Q}, E[n])) & \longrightarrow & H^1(\mathbb{Q}, E)[n] & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow{\scriptstyle \prod_p res_p} & \overset{\alpha}{\searrow} & \downarrow{\scriptstyle \prod_p res_p} & & \\
0 & \longrightarrow & \prod_p E(\mathbb{Q}_p)/nE(\mathbb{Q}_p) & \xrightarrow{\prod_p \delta_p} & \prod_p H^1(\mathbb{Q}_p, E[n]) & \longrightarrow & \prod_p H^1(\mathbb{Q}_p, E)[n] & \longrightarrow & 0
\end{array}$$

On définit le n-groupe de Selmer de $E/\mathbb{Q}$ par :

$$Sel_n(E/\mathbb{Q}) = ker\left(H^1(\mathbb{Q}, E[n]) \xrightarrow{\alpha} \prod_p H^1(\mathbb{Q}_p, E)[n]\right)$$

et le groupe de Tate-Shafarevich de $E/\mathbb{Q}$ par :

$$Ш(E/\mathbb{Q}) = ker\left(H^1(\mathbb{Q}, E) \xrightarrow{\prod_p res_p} \prod_p H^1(\mathbb{Q}_p, E)\right)$$

On trouve ainsi une suite exacte :

$$0 \longrightarrow E(\mathbb{Q})/nE(\mathbb{Q}) \longrightarrow Sel_n(E/\mathbb{Q}) \longrightarrow Ш(E/\mathbb{Q})[n] \longrightarrow 0$$

On peut montrer que $Sel_n(E/\mathbb{Q})$ est un groupe fini ; la finitude de $E(\mathbb{Q})/nE(\mathbb{Q})$ en découle.

La deuxième partie de la preuve consiste à introduire une "mesure" de la taille des points de $E(\mathbb{Q})$. Il s'agit d'une application $h_{NT} : E(\mathbb{Q}) \longrightarrow \mathbb{R}_{\geq 0}$, appelée *hauteur de Neron-Tate*, satisfaisant les propriétés suivantes :

1. $h_{NT}(mP) = m^2 h_{NT}(P) \quad \forall P \in E(\mathbb{Q}),\ \forall m \in \mathbb{Z}$
2. L'accouplement

$$\langle \cdot, \cdot \rangle_{NT} : E(\mathbb{Q}) \times E(\mathbb{Q}) \longrightarrow \mathbb{R}$$
$$(P, Q) \mapsto \frac{1}{2}\left(h_{NT}(P+Q) - h_{NT}(P) - h_{NT}(Q)\right)$$

   est bilinéaire.
3. Pour tout $C > 0$ l'ensemble $H_C = \{P \in E(\mathbb{Q}) \mid h_{NT}(P) \leq C\}$ est fini.

On montre enfin facilement que $E(\mathbb{Q})$ est engendrée par H_C, où $C = max\{h_{NT}(P_i)\}$, les P_i étant un système de représentants de $E(\mathbb{Q})/nE(\mathbb{Q})$.

D'après le théorème de Mordell-Weil on peut écrire $E(\mathbb{Q})$ sous la forme $\mathbb{Z}^r \oplus T$ pour un certain entier r, T étant un groupe abélien fini. On appelle r le rang de la courbe elliptique E ; on le notera parfois $rk(E(\mathbb{Q}))$.
La partie de torsion T est très bien comprise pour les courbes elliptiques sur $\mathbb{Q}$, grâce à un théorème de Mazur ([Maz78]) qui affirme que T est isomorphe à un des groupes $\mathbb{Z}/n\mathbb{Z}$, pour $1 \leq n \leq 10$ et $n = 12$, ou $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z}$ pour $n \leq 4$. Le point crucial est donc, étant donnée une courbe elliptique $E/\mathbb{Q}$, de déterminer son rang. On sait encore très peu à ce propos. Par example, il est conjecturé qu'il existent des courbes elliptiques sur $\mathbb{Q}$ de rang arbitrairement grand, mais on ne connait pas encore de courbe elliptique de rang plus grand que 28. Par ailleurs, les courbes elliptiques de grand rang devraient être assez rares : on conjecture que, "en moyen", 50% des courbes elliptiques sur $\mathbb{Q}$ a rang 0, 50% a rang 1 et le 0% a rang ≥ 2. Des progrès à ce propos ont été obtenus récemment par Bhargava [1] (voir [BSZ14]).

3 La fonction L d'une courbe elliptique

3.1 fonctions zêta

Définition 3.1. Soit X un $\mathbb{Z}$-schéma de type fini. La fonction zêta de X est le produit formel :

$$\zeta(X, s) = \prod_x \frac{1}{1 - N(x)^{-s}}$$

le produit étant sur tous les points fermés de X ; on dénote par $N(x)$ le cardinal du corps résiduel du point fermé x (appelé *norme* de x).

1. Médaille Fields en 2014.

Exemple 3.2. On a

$$\zeta(Spec\,\mathbb{Z}, s) = \prod_p \frac{1}{1 - \frac{1}{p^s}}$$

On retrouve ainsi la fonction zêta de Riemann. Plus généralement, soit $\mathcal{O}_K$ l'anneau des entiers d'un corps de nombres K. On a $\zeta(Spec\,\mathcal{O}_K, s) = \prod_{\mathfrak{p}} \frac{1}{1-N(\mathfrak{p})^{-s}}$; c'est la fonction zêta de K, notée $\zeta_K(s)$. On rappelle les propriétés analytiques fondamentales de cette fonction :

1. le produit formel définissant $\zeta_K(s)$ converge dans le demi plan $Re\, s > 1$, où il définit une fonction holomorphe jamais nulle.
2. $\zeta_K(s)$ admet un prolongement analytique à une fonction méromorphe sur $\mathbb{C}$, avec un seul pôle simple en $s = 1$.
3. Notons $\Gamma_{\mathbb{R}}(s) = \pi^{-s/2}\Gamma(s/2)$, $\Gamma_{\mathbb{C}}(s) = 2(2\pi)^{-s}\Gamma(s)$ et Δ_K le discriminant de K. Soit r_1 (resp. $2r_2$) le nombre de plongements réels (resp. complexes) de K dans $\mathbb{C}$. La fonction :

   $$\Lambda_K(s) = |\Delta_K|^{s/2}\Gamma_{\mathbb{R}}(s)^{r_1}\Gamma_{\mathbb{C}}(s)^{r_2}\zeta_K(s)$$

   satisfait l'équation fonctionnelle

   $$\Lambda_K(s) = \Lambda_K(1 - s) \tag{2}$$

4. Le résidu de $\zeta_K(s)$ en $s = 1$ vaut :

   $$res_{s=1}\zeta_K(s) = \frac{2^{r_1}(2\pi)^{r_2}h_K R_K}{w_K\sqrt{|\Delta_K|}} \tag{3}$$

   où h_K est le nombre de classe de K (i.e. le cardinal du groupe des classes d'idéaux $Pic(\mathcal{O}_K)$), w_K est le nombre de racines de l'unité dans $\mathcal{O}_K$ et R_K est le régulateur de K, défini comme le covolume du réseau dans $H = \{\mathbf{x} \in \mathbb{R}^{r_1+r_2} : \sum_{i=1}^{r_1+r_2} x_i = 0\}$ donné par l'image de l'application :

   $$\begin{aligned}\mathcal{O}_K^{\times} &\longrightarrow \mathbb{R}^{r_1+r_2}\\ x &\mapsto (log|\sigma_1(x)|, \ldots, log|\sigma_{r_1}(x)|, 2log|\tau_1(x)|, \ldots 2log|\tau_{r_2}(x)|)\end{aligned}$$

   où les σ_i (resp. τ_j) sont les plongements réels (resp. complexes, à conjugaison près) de K dans $\mathbb{C}$.

Enfin, on conjecture que $\zeta_K(s)$ satisfait l'analogue de l'hypothèse de Riemann, c'est à dire que tout zéro non trivial de $\zeta_K(s)$ appartient à la droite $Re\, s = \frac{1}{2}$.

Remarque 3.3. En général, on peut montrer que, si X est un $\mathbb{Z}$-schéma de type fini de dimension d, alors $\zeta(X, s)$ définit une fonction holomorphe sur le demi plan $Re\, s > d$. On s'attend aussi que toute fonction zêta puisse se prolonger en une fonction méromorphe sur $\mathbb{C}$, satisfaisant une equation fonctionnelle de la forme (2) et une analogue de l'hypothèse de Riemann. Ceci n'est connu que dans certains cas particuliers.

Remarque 3.4. La formule (3), connue sous le nom de *formule du nombre des classes*, exprime le résidu en $s = 1$ de la fonction $\zeta_K(s)$ en termes d'invariants arithmétiques globaux de l'anneau $\mathcal{O}_K$. En général, appelons *valeur spéciale* d'une fonction méromorphe $L(s)$ en un nombre complexe k, noté $L^*(k)$, le premier terme du développement de Taylor de $L(s)$ en $s = k$. Par exemple, Euler a découvert les jolies formules suivantes :

$$\zeta^*(2n) = (-1)^{n+1}\frac{B_{2_n}(2\pi)^{2n}}{2(2n)!} \quad \forall n \geq 1$$

où $B_n \in \mathbb{Q}$ est le n-ième nombre de Bernoulli (i.e. le n-ième terme du dévéloppement en série de $\frac{t}{e^t-1}$). Par ailleurs, l'équation (3) s'écrit :

$$\zeta_K^*(1) = \frac{2^{r_1}(2\pi)^{r_2} h_K R_K}{w_K \sqrt{|\Delta_K|}} \tag{4}$$

On observe dans les exemples concrets (et on conjecture en général) que les valeurs spéciales de la fonction zêta d'un schéma X aux entiers (ou demi-entiers) s'écrivent comme produit d'un "régulateur", une "période" et un nombre rationnel, qui encodent beaucoup d'information arithmétique où géométrique sur X.

Exemple 3.5. Soit X une variété projective lisse sur $\mathbb{F}_p$ de dimension d. Tout point fermé de X a norme p^k pour un certain entier k. On en déduit qu'il existe une série formelle $Z(X,T)$ qui vérifie

$$\zeta(X,s) = Z(X,p^{-s})$$

Les conjectures de Weil, démontrées par Weil lui-même dans le cas des courbes, et par Grothendieck et Deligne en général, affirment que la fonction $Z(X,T)$ est une fonction rationnelle, qui s'écrit sous la forme

$$Z(X,T) = \prod_{j=0}^{2d} P_j(X,T)^{(-1)^{j+1}}$$

où chaque P_j est un polynôme. Précisément, on a

$$P_j(T) = det(1 - TFr | H^j_{et}(X \times \bar{\mathbb{F}}_p, \mathbb{Q}_l))$$

où Fr dénote le morphisme de Frobenius et l est un premier différent de p (on peut montrer que $P_j(T)$ ne dépend pas du choix de l). De plus, $Z(X,T)$ satisfait une equation fonctionnelle et l'analogue de l'hypothèse de Riemann.

Soit maintenant X une variété projective lisse de dimension d sur $\mathbb{Q}$. Soit p un nombre premier, et supposons que X ait bonne réduction en p ; notons X_p la réduction de X modulo p. On a alors, d'après le théorème de changement de base lisse :

$$Z(X_p,T) = \prod_{j=0}^{2d} det(1-TFr_p | H^j_{et}(X_p \times \bar{\mathbb{F}}_p, \mathbb{Q}_l))^{(-1)^{j+1}} = \prod_{j=0}^{2d} det(1-TFr_p | H^j_{et}(X \times \bar{\mathbb{Q}}, \mathbb{Q}_l))^{(-1)^{j+1}}$$

On voudrait définir la fonction zêta de $X/\mathbb{Q}$ comme étant le produit des facteurs locaux $\zeta_p(X,s) := Z(X_p, p^{-s})$. Il reste à étendre la définition de $\zeta_p(X,s)$ aux premiers p de mauvaise réduction. On pose, pour p quelconque :

$$\zeta_p(X,s) = \prod_{j=0}^{2d} det(1 - p^{-s} Fr_p | H^j_{et}(X \times \bar{\mathbb{Q}}, \mathbb{Q}_l)^{I_p})^{(-1)^{j+1}}$$

Comme Fr_p agit sur le sous espace de $H^j_{et}(X \times \bar{\mathbb{Q}}, \mathbb{Q}_l)$ invariant par l'action du groupe d'inertie I_p cette définition ne dépend pas du choix de Frobenius en p ; de plus, elle étend bien celle donnée pour les premiers de bonne réduction.

Définition 3.6. Soit $X/\mathbb{Q}$ une variété projective lisse de dimension d et p un premier. On définit, pour $0 \leq j \leq 2d$:

$$L_p(H^j(X), s) = det(1 - p^{-s} Fr_p | H^j_{et}(X \times \bar{\mathbb{Q}}, \mathbb{Q}_l)^{I_p})^{-1}$$

et

$$L(H^j(X), s) = \prod_p L_p(H^j(X), s)$$

On appelle $L(H^j(X), s)$ une *fonction L de Hasse-Weil* de X. Enfin, la *fonction zêta de Hasse-Weil* de X est :

$$\zeta(X, s) = \prod_{j=0}^{2d} L(H^j(X), s)^{(-1)^j}$$

On a donc associé à chaque variété projective lisse X sur $\mathbb{Q}$ une fonction zêta, fabriquée en collectant des informations locales (i.e. modulo p, pour chaque premier p). De plus, cette fonction se décompose en produit de plusieurs morceaux, les fonctions L de X. Bien sûr, il est conjecturé que les fonctions L, comme les fonctions zêta, ont un prolongement méromorphe à $\mathbb{C}$, ainsi qu'une equation fonctionnelle. On va parler en détail de ces conjectures dans le cas des courbes elliptiques dans la prochaine section.

Exemple 3.7. Soit X une courbe projective lisse sur $\mathbb{Q}$. Dans ce cas $d = 1$, et on trouve $L(H^0(X), s) = \zeta(s)$, $L(H^2(X), s) = \zeta(s-1)$; si on note $L(X, s) = L(H^1(X), s)$ on a :

$$\zeta(X, s) = \frac{\zeta(s)\zeta(s-1)}{L(X, s)}$$

3.2 Fonction L d'une courbe elliptique

Soit maintenant $E/\mathbb{Q}$ une courbe elliptique. On définit la fonction L de E par :

$$L(E, s) = L(H^1(E), s)$$

Remarque 3.8. On n'a pas besoin de connaitre la cohomologie étale pour comprendre qu'est-ce que c'est $L(E, s)$. En effet, on a un isomorphisme canonique $H^1_{et}(E \times \bar{\mathbb{Q}}, \mathbb{Q}_l) \simeq T_l(E) \otimes_{\mathbb{Z}_l} \mathbb{Q}_l$, où $T_l(E) = \varprojlim E[p^n]$ est le module de Tate l-adique de E.

Si p est un premier de bonne réduction pour E, notons $a_p = p + 1 - \#E(\mathbb{F}_p)$. On a

$$\zeta(E_p, s) = \frac{1 - a_p p^{-s} + p^{1-2s}}{(1 - p^{-s})(1 - p^{1-s})}$$

et $L_p(E, s) = (1 - a_p p^{-s} + p^{1-2s})^{-1}$. L'hypothèse de Riemann pour $\zeta(E_p, s)$ implique que $|a_p| \leq 2\sqrt{p}$. On en déduit facilement que $L(E, s)$ définit une fonction holomorphe sur le demi-plan $Re\ s > 3/2$.
Si p est un premier de mauvaise réduction, on dit que E a réduction additive (resp. multiplicative déployée, resp. multiplicative non déployée) si la réduction de E modulo p a un point double (resp. un node avec tangentes définies sur $\mathbb{F}_p$, resp. un node avec tangentes pas définies sur $\mathbb{F}_p$). Avec cette terminologie, on a :

$$L_p(E, s) = \begin{cases} 1 & \text{si } E \text{ a reduction additive en } p \\ (1 - p^{-s})^{-1} & \text{si } E \text{ a réduction multiplicative déployée en } p \\ (1 + p^{-s})^{-1} & \text{si } E \text{ a réduction multiplicative non déployée en } p \end{cases}$$

La fonction L d'une courbe elliptique $E/\mathbb{Q}$ possède les bonnes propriétés qu'on souhaite. Précisément :

1. $L(E, s)$ se prolonge en une fonction holomorphe sur $\mathbb{C}$.

2. Soit $\Lambda(E,s) = N^{s/2}\Gamma_{\mathbb{C}}(s)L(E,s)$, où N est le *conducteur* de E (il s'agit d'un entier positif dont les facteurs sont les premiers de mauvaise réduction pour E). La fonction $\Lambda(E,s)$ vérifie l'équation fonctionnelle :

$$\Lambda(E,s) = w\Lambda(E,2-s)$$

pour un certain $w \in \{\pm 1\}$.

Ces deux propriétés découlent du travail de Breuil, Conrad, Diamond et Taylor, qui ont généralisé les résultats dans [Wil95, TW95]. Précisément, elles sont une conséquence du théorème de modularité (aussi connu, avant le 2001, avec le nom de conjecture de Taniyama-Shimura-Weil), qu'on va maintenant énoncer.

Pour tout entier positif N, notons $\Gamma_0(N)$ le sous groupe de $\mathbb{SL}_2(\mathbb{Z})$ formé des matrices de la forme $\begin{pmatrix} a & b \\ Nc & d \end{pmatrix}$.

Le groupe $\mathbb{SL}_2(\mathbb{Z})$ agit naturellement sur le demi-plan de Poincaré $\mathbb{H}$. Notons $Y_0(N)$ le quotient $\Gamma_0(N)\backslash\mathbb{H}$. Ses points paramètrent les classes d'isomorphisme des couples (E,H), où E est une courbe elliptique sur $\mathbb{C}$ et H un sous groupe cyclique de E d'ordre N. On peut munir $Y_0(N)$ d'une structure de surface de Riemann, qu'on peut compactifiér en rajoutant un nombre fini de points ; on obtient ainsi une surface de Riemann compacte notée $X_0(N)$. On sait que $X_0(N)$ est une courbe algébrique complexe. Mieux, $X_0(N)$ a un modèle défini sur $\mathbb{Q}$ (toujours noté $X_0(N)$). Le théorème de modularité peut s'énoncer sous la forme suivante :

Théorème 3.9. *(Théorème de modularité, 2001, [BCDT01]) Soit E une courbe elliptique sur $\mathbb{Q}$ de conducteur N. Il existe un morphisme non constant (défini sur $\mathbb{Q}$)*

$$\pi : X_0(N) \longrightarrow E$$

On peut déduire du théorème de modularité que la fonction $L(E,s)$ est égal à la fonction L d'une forme modulaire pour $\Gamma_0(N)$ de poids 2 (voir [DS07] pour une introduction aux formes modulaires). Le prolongement analytique et l'équation fonctionnelle de $L(E,s)$ découlent des propriétés analogues des fonctions L des formes modulaires, qui sont bien connues et faciles à obtenir.

Remarque 3.10. Les fonctions $L(H^j(X),s)$ sont aussi appelées *fonctions L motiviques* (ces sont, en gros, les fonctions L qui viennent du monde géométrique), tandis que les fonctions L des formes modulaires sont un cas particulier de *fonctions L automorphes* (des objets plutôt analytiques). Le théorème de modularité s'inscrit donc dans le cadre général du programme de Langlands, dont l'un des buts consiste essentiellement à montrer que toute fonction L motivique est automorphe. Le lecteur intéressé pourra consulter l'excellent article [Gel84] pour une introduction au programme de Langlands, qui est un domaine de recherche en plein développement actuellement.

4 La conjecture de Birch et Swinnerton-Dyer

4.1 Énoncé

Soit $E/\mathbb{Q}$ une courbe elliptique. On rappelle qu'on a $E(\mathbb{Q}) = \mathbb{Z}^r \oplus E(\mathbb{Q})_{tor}$, où $E(\mathbb{Q})_{tor}$ est un groupe abélien fini. L'accouplement de Neron-Tate s'étend à une forme quadratique non dégénérée sur $E(\mathbb{Q}) \otimes \mathbb{R}$. Introduisons les invariants suivants associés à E :

1. Soit $P_1, \ldots, P_r$ une base de la partie libre de $E(\mathbb{Q})$. Le *régulateur* de $E/\mathbb{Q}$, noté $R(E)$, est le déterminant de la matrice $(\langle P_i, P_j\rangle_{NT})$. C'est le carrée du covolume du réseau $E(\mathbb{Q})/E(\mathbb{Q})_{tor}$ dans $E(\mathbb{Q}) \otimes \mathbb{R}$ (on remarque l'analogie avec la définition de régulateur d'un corps de nombres donnée avant).

2. Soit p un nombre premier. Soit $E^0(\mathbb{Q}_p)$ le sous-groupe de $E(\mathbb{Q}_p)$ formé des points dont la réduction modulo p est un point non singulier. Le nombre de Tamagawa de E en p, noté c_p, est :
$$c_p = [E(\mathbb{Q}_p) : E_0(\mathbb{Q}_p)]$$
En particulier, $c_p = 1$ si p est un premier de bonne réduction pour E.
Les nombres de Tamagawa peuvent aussi se définir plus géométriquement de la façon suivante : soit $\mathcal{E}/\mathbb{Z}$ le modèle de Néron de $E/\mathbb{Q}$. Soit $\mathcal{E}_{\mathbb{F}_p}$ la fibre de $\mathcal{E}$ en p, $\mathcal{E}^0_{\mathbb{F}_p}$ la composante connexe de l'identité de $\mathcal{E}_{\mathbb{F}_p}$ et $\Phi_{E,p} = \mathcal{E}_{\mathbb{F}_p}/\mathcal{E}^0_{\mathbb{F}_p}$ le groupe des composantes connexes de $\mathcal{E}_{\mathbb{F}_p}$. On a alors $c_p = \#\Phi_{E,p}(\mathbb{F}_p)$ (en particulier, ceci montre que c_p est fini).
3. Soit ω la différentielle de Néron de E (i.e. un générateur de l'espace des différentielles invariantes de $\mathcal{E}/\mathbb{Z}$). On pose $\Omega_E = \int_{E(\mathbb{R})} \omega$.

On peut finalement énoncer la conjecture de Birch et Swinnerton-Dyer.

Conjecture 4.1. *(Birch et Swinnerton-Dyer, 1960s) Soit $E/\mathbb{Q}$ une courbe elliptique.*

1. *Le rang de E est égal à l'ordre de $L(E,s)$ en $s = 1$:*
$$rk(E(\mathbb{Q})) = ord_{s=1} L(E,s) \tag{5}$$
2. *Le groupe de Tate-Shafarevich $Ш(E/\mathbb{Q})$ est fini.*
3. *La valeur spéciale de $L(E,s)$ en $s = 1$ vaut :*
$$L^*(E,1) = \frac{\Omega_E(\prod_p c_p) R(E) \# Ш(E/\mathbb{Q})}{\#E(\mathbb{Q})^2_{tor}} \tag{6}$$

Plusieurs remarques sont en ordre.

(a) D'abord, cette conjecture est une autre manifestation du principe général selon lequel les fonctions L des variétés algébriques, dont la construction n'utilise que des informations *locales*, encodent des propriétés arithmétiques et géométriques *globales* des variétés. On peut voir ça comme étant une version sophistiquée du principe local-global.

(b) Le point 1. est déjà très intéressant ; c'est dans cette forme que la conjecture est énoncée dans la liste des problèmes du prix du millénaire (voir la description officielle par Wiles dans [Wil06]). Par example, l'équivalence $L(E,1) \neq 0 \Leftrightarrow E(\mathbb{Q})$ est fini permettrait de résoudre l'ancien problème des nombres congruents (étant donnée un entier positif n, déterminer s'il existe un triangle rectangle à cotés de longueur rationnelle et d'aire n).

(c) Le point 2., très important en soi, est souvent appelée "conjecture de Tate-Shafarevich".

(d) La formule (6), dont on remarque l'analogie très stricte avec la formule (4), exprime la valeur spéciale de $L(E,s)$ en $s = 1$ en termes d'invariants globaux de la courbe elliptique E.

(e) Le terme $P(E) = \Omega_E(\prod_p c_p)$ peut s'interpréter comme une "période". On trouve ainsi que la valeur spéciale $L^*(E,1)$ vérifie (conjecturalement) $L^*(E,1) \equiv P(E)R(E) \pmod{\mathbb{Q}^*}$, comme on s'attend en général (voir la remarque 3.4).

(f) Un énoncé similaire est conjecturé pour les courbes elliptiques sur un corps de nombres quelconque, et aussi sur les corps de fonctions (i.e. corps de degré de transcendance 1 sur un corps fini).

4.2 Panorama des résultats connus

Le cas qu'on connait mieux est celui des courbes elliptiques sur un corps de fonctions. Soit k le corps des fonctions d'une courbe projective lisse C sur un corps fini. Soit E/k une courbe elliptique. On peut montrer qu'il existe une surface elliptique projective régulière $\mathcal{E} \to C$ dont la fibre spéciale est E.

Le théorème suivant est du à Tate ([Tat95]) et Milne ([Mil75]).

Théorème 4.2. *On a toujours l'inégalité $ord_{s=1}L(E/k,s) \geq rk(E(k))$. De plus, les assertions suivantes sont équivalentes :*

1. *On a l'égalité $ord_{s=1}L(E/k,s) = rk(E(k))$.*
2. *Le groupe $Ш(E/k)$ est fini.*
3. *Il existe un premier l tel que le sous groupe de l-torsion $Ш(E/k)[l^\infty]$ de $Ш(E/k)$ est fini.*
4. *Une formule analogue à (6) est vérifiée.*
5. *La conjecture de Tate pour $\mathcal{E}$ est vraie.*

Pour certaines courbes elliptiques E/k on sait montrer que une des conditions du théorème est satisfaite ; par exemple, on sait que la conjecture de Tate est vraie si $\mathcal{E}$ est une surface $K3$, donc dans ce cas la conjecture de Birch et Swinnerton-Dyer pour E/k est vérifiée.

Dans la suite on va plutôt s'intéresser au cas des courbes elliptiques sur $\mathbb{Q}$, qui est beaucoup plus dur. On commence par discuter un énoncé plus faible, la *conjecture de parité* :

Conjecture 4.3. *(Conjecture de parité) Soit $E/\mathbb{Q}$ une courbe elliptique. On a :*

$$rk(E(\mathbb{Q})) \equiv ord_{s=1}L(E,s) \pmod 2$$

Fixons un nombre premier p. En prenant la limite directe des suites exactes dans (1) pour $n = p^k$ on trouve une suite exacte :

$$0 \to E(\mathbb{Q}) \otimes \mathbb{Q}_p/\mathbb{Z}_p \to Sel_{p^\infty}(E/\mathbb{Q}) \to Ш(E/\mathbb{Q})[p^\infty] \to 0$$

On sait que $Ш(E/\mathbb{Q})[p^\infty]$, s'il est fini, est muni d'un accouplement alterné et non dégénéré (l'accouplement de Cassels-Tate), donc il a forcement cardinal pair. La conjecture de parité découle donc de la finitude (conjecturée) de $Ш(E/\mathbb{Q})[p^\infty]$ et de l'énoncé suivant :

Théorème 4.4.

$$ord_{s=1}L(E,s) \equiv r_p(E/\mathbb{Q})$$

où $r_p(E/\mathbb{Q})$ dénote le $\mathbb{Z}_p$-rang du dual de Pontryagin de $Sel_{p^\infty}(E/\mathbb{Q})$ (c'est à dire le $\mathbb{Z}_p$-module $Hom_{cont}(Sel_{p^\infty}(E/\mathbb{Q}), \mathbb{Q}_p/\mathbb{Z}_p)$).

Ce résultat à été démontré en 2001 par Nekovář ([Nek01]) pour les premiers p tels que la réduction E_p de E modulo p soit une courbe elliptique ordinaire (i.e. $(p+1) \nmid \#E_p(\mathbb{F}_p)$). Beaucoup plus généralement, les frères Dokchitser ont démontré dans [DD11] que, pour tout corps de nombres K et toute courbe elliptique E/K, la finitude de $Ш(E/K)$ implique la conjecture de parité.

Pour ce qui concerne la conjecture de Birch et Swinnerton-Dyer, un premier résultat a été obtenu par Coates et Wiles en 1977 (voir [CW77]). Le progrès plus significatif est du à Kolyvagin, qui, en utilisant les travaux de Gross-Zagier et sa méthode des *systèmes d'Euler*, a démontré le théorème suivant :

Théorème 4.5. *(Gross-Zagier-Kolyvagin, [Kol90, Kol91]) Soit $E/\mathbb{Q}$ une courbe elliptique. Si $ord_{s=1}L(E,s) \leq 1$ alors :*

1. *$rk(E(\mathbb{Q})) = ord_{s=1}L(E,s)$*
2. *$Ш(E/\mathbb{Q})$ est fini.*

Pour donner une idée des techniques utilisées dans la preuve de ce résultat, qui sont à peu près les seules qu'on connait pour attaquer la conjecture 4.1, on va esquisser la démonstration du résultat plus faible suivant (voir [Gro91] pour une preuve complète) :

Théorème 4.6. *Soit $E/\mathbb{Q}$ une courbe elliptique de conducteur N, K un corps quadratique imaginaire tel que tout facteur premier de N est totalement décomposé dans K (on appelle cette condition "hypothèse de Heegner"). Si E n'est pas une courbe elliptique à multiplication complexe (voir la définition 4.8 ci dessous) alors :*

1. *$ord_{s=1}L(E/K,s) = 1 \Longrightarrow E(K)$ a rang un.*
2. *Pour presque tout premier p le groupe $Ш(E/K)[p]$ est trivial.*

Remarque 4.7. En utilisant ce résultat on peut déduire les cas particuliers suivants de la conjecture 4.1 : si $E/\mathbb{Q}$ est une courbe elliptique sans multiplication complexe et $ord_{s=1}L(E,s) \leq 1$, alors $ord_{s=1}L(E,s) = rk(E(\mathbb{Q}))$.

On expliquera maintenant comment on peut montrer ce théorème.
On rappelle d'abord que, d'après le théorème de modularité, il existe un morphisme non constant $\pi : X_0(N) \longrightarrow E$.

Définition 4.8. Une courbe elliptique $E/\mathbb{C}$ est dite *à multiplication complexe* si $\mathbb{Z} \subsetneq End(E)$. Dans ce cas $End(E)$ est un ordre dans un corps quadratique imaginaire K.

La théorie de la multiplication complexe montre que une courbe elliptique E avec multiplication complexe par un ordre dans un corps quadratique imaginaire K est définie sur une extension abélienne finie de K. Par example, soit $\mathcal{O}_K$ l'anneau des entiers de K. L'image de $\mathcal{O}_K$ par un plongement $K \hookrightarrow \mathbb{C}$ est un réseau, et la courbe elliptique $\mathbb{C}/\mathcal{O}_K$ a anneau des endomorphismes isomorphe à $\mathcal{O}_K$, et est définie sur le corps de classe de Hilbert de K, noté $K[1]$.

Soit K comme dans l'énoncé du Théorème 4.6. L'hypothèse de Heegner implique qu'il existe un idéal $\mathcal{N}$ de $\mathcal{O}_K$ tel que $\mathcal{O}_K/\mathcal{N} \simeq \mathbb{Z}/N\mathbb{Z}$. La couple $(\mathbb{C}/\mathcal{O}_K, \mathcal{N}^{-1}/\mathcal{O}_K)$ correspond à un point $x(1) \in X_0(N)(K[1])$. Plus généralement, si n est un entier premier à N et $\mathcal{O}_{n,K}$ est l'ordre dans K de conducteur n, la couple $(\mathbb{C}/\mathcal{O}_{n,K}, (\mathcal{N} \cap \mathcal{O}_{n,K})^{-1}/\mathcal{O}_{n,K})$ donne un point $x(n) \in X_0(K[n])$ (où $K[n]$ est une extension abélienne de K de groupe de Galois canoniquement isomorphe à $Pic(\mathcal{O}_{n,K})$). Notons $y(n) = \pi(x(n)) \in E(K[n])$, et posons

$$P(1) = \sum_{\sigma \in Gal(K[1]/K)} \sigma y(1) \in E(K)$$

Le premier outil clé dans la preuve du Théorème 4.6 est la formule suivante, due à Gross-Zagier ([GZ86]) :

$$L'(E/K,1) = Ch_{NT}(P(1)) \tag{7}$$

où C est une constante non nulle (explicite, mais n'ayant pas d'intérêt pour nous). Comme $L'(E/K,1) \neq 0$, la formule (7) implique que $P(1)$ a ordre infini. En particulier $rk(E(K)) \geq 1$. Il reste à démontrer l'inégalité opposée.

Choisissons un premier p tel que :

1. $Gal(\mathbb{Q}(E[p])/\mathbb{Q}) \simeq GL_2(\mathbb{Z}/p\mathbb{Z})$ (comme E n'est pas à multiplication complexe cette condition est vérifiée pour presque tout p, d'après le théorème de l'image ouverte de Serre) ;

2. $P(1) \notin pE(K)$ (cette condition est vérifiée pour presque tout p car $P(1)$ n'est pas un point de torsion).

L'idée cruciale, due à Kolyvagin, est d'utiliser les points $y(n)$ pour construire un système de classes de cohomologie, indexées par un certain ensemble Λ :

$$\kappa = \{c(n) \mid n \in \Lambda\} \subset H^1(K, E[p])$$

La classe $c(1)$ n'est rien d'autre que l'image de $P(1)$ par l'application de Kummer

$$\delta : E(K)/pE(K) \hookrightarrow H^1(K, E[p])$$

Comme $P(1) \notin pE(K)$ on a donc $c(1) \neq 0$.

Les classes de cohomologie $c(n)$ vérifient des relations de compatibilité très fortes et, une fois qu'on sait que au moins une de ces classes est non nulle, ces relations impliquent l'existence d'une infinité de classes non nulles, qu'on peut utiliser pour borner la dimension de $Sel_p(E/K)$. En particulier, on peut montrer l'implication :

$$c(1) \neq 0 \Longrightarrow dim_{\mathbb{F}_p} Sel_p(E/K) = 1$$

Le Théorème 4.6 en découle immédiatement, en vue de la suite exacte (1) (avec K à la place de $\mathbb{Q}$).

Pour conclure, on va mentionner les développements plus récents liés à la conjecture de Birch et Swinnerton-Dyer.
Les travaux de Kato ([Kat04]) et les résultats récents de Skinner-Urban ([SU14]) sur la conjecture principale d'Iwasawa pour GL_2 permettent de démontrer que, si $E/\mathbb{Q}$ est une courbe elliptique et p un nombre premier (satisfaisant certains hypothèses techniques), on a l'implication :

$$r_p(E/\mathbb{Q}) = 0 \Longrightarrow L(E, 1) \neq 0$$

Ce résultat, joint avec le théorème de Gross-Zagier-Kolyvagin, implique que les trois assertions suivantes sont équivalentes :

1. $r_p(E/\mathbb{Q}) = 0$
2. $rk(E(\mathbb{Q})) = 0$ et $Ш(E/\mathbb{Q})$ est fini
3. $ord_{s=1} L(E, s) = 0$

De plus, la p-partie de la formule (6) est vérifiée, c'est à dire qu'on a, en notant v_p la valuation p-adique :

$$v_p\left(\frac{L^*(E,1)}{\Omega_E}\right) = v_p\left(\frac{(\prod_p c_p)\#Ш(E/\mathbb{Q})}{\#E(\mathbb{Q})^2_{tor}}\right)$$

Grâce au travail de Zhang ([Zha14]), qui a démontré la non trivialité du système de Kolyvagin κ (sous certaines conditions techniques), on a aussi l'implication (pour p premier vérifiant des hypothèses convenables) :

$$r_p(E/\mathbb{Q}) = 1 \Longrightarrow L'(E, 1) \neq 0$$

On en déduit l'équivalence des assertions suivantes :

1. $r_p(E/\mathbb{Q}) = 1$
2. $rk(E(\mathbb{Q})) = 1$ et $Ш(E/\mathbb{Q})$ est fini
3. $ord_{s=1} L(E, s) = 1$

De plus, la p-partie de la formule (6) est vérifiée dans ce cas :

$$v_p\left(\frac{L^*(E,1)}{\Omega_E R(E)}\right) = v_p\left(\frac{(\prod_p c_p)\#Ш(E/\mathbb{Q})}{\#E(\mathbb{Q})^2_{tor}}\right)$$

Remarque 4.9. Ces résultat résument essentiellement tout ce qui est actuellement connu sur la conjecture de Birch et Swinnerton-Dyer. Ils démontrent presque complètement, modulo des hypothèses techniques, la conjecture pour les courbes elliptiques $E/\mathbb{Q}$ de rang au plus un. Les méthodes connues ne s'appliquent pourtant pas aux courbes elliptiques de rang supérieur. Notamment, les approches connues aujourd'hui utilisent de façon cruciale des formules explicites (par example la formule de Gross-Zagier) qui permettent de donner une interprétation "cohomologique" des valeurs des dérivées de $L(E,s)$ (par example, on a vu que la formule de Gross-Zagier relie $L'(E/K,1)$ à la classe $c(1) \in H^1(K,E[p])$). Aucune formule de ce type n'est connue pour les dérivées d'ordre supérieur à 1, ce qui empêche de généraliser les idées introduites jusqu'ici.

Références

[BCDT01] C. Breuil, B. Conrad, F. Diamond, and R. Taylor, *On the modularity of elliptic curves over $\mathbb{Q}$: wild 3-adic exercises*, J. Amer. Math. Soc. **14** (2001), no. 4, 843–939.

[BSZ14] M. Bhargava, C. Skinner, and W. Zhang, *A majority of elliptic curves over $\mathbb{Q}$ satisfy the Birch and Swinnerton-Dyer conjecture*, preprint (2014).

[CW77] J. Coates and A. Wiles, *On the conjecture of Birch and Swinnerton-Dyer*, Invent. Math **39** (1977), no. 3, 223–251.

[DD11] T. Dokchitser and V. Dokchitser, *Root numbers and parity of ranks of elliptic curves*, J. Reine Angew. Math.. **658** (2011), 39–64.

[DS07] F. Diamond and J. Shurman, *A first course in modular forms*, Springer, 2007.

[Fal83] G. Faltings, *Endlichkeitssätze für abelsche varietäten über zahlkörpern*, Invent. Math **73** (1983), no. 3, 349–366.

[Gel84] S. Gelbart, *An elementary introduction to the langlands program*, Bull. Amer. Math. Soc. **10** (1984), no. 2, 177–219.

[Gro91] B. H. Gross, *Kolyvagin's work on modular elliptic curves*, L-functions and arithmetic, London Math. Soc. Lecture Note Ser., no. 153, Cambridge University Press, 1991, pp. 235–256.

[GZ86] B. H. Gross and Don B. Zagier, *Heegner points and derivatives of L-series*, Invent. Math. **84** (1986), no. 2, 225–320.

[Kat04] K. Kato, *p-adic Hodge theory and values of zeta functions of modular forms*, Cohomologies p-adiques et applications arithmétiques **295** (2004), 117–290.

[Kol90] V. A. Kolyvagin, *Euler systems*, The Grothendieck Festschrift, Vol. II, Progr. Math., no. 87, Birkhäuser Boston, 1990, pp. 435–483.

[Kol91] ———, *On the structure of Shafarevich-Tate groups*, Algebraic geometry, Lecture Notes in Math., no. 1479, Springer, 1991, pp. 94–121.

[Maz78] B. Mazur, *Modular curves and the Eisenstein ideal*, Inst. Hautes Études Sci. Publ. Math. **47** (1978), 33–186.

[Mil75] J. Milne, *On a conjecture of Artin and Tate*, Ann. of Math. (2) **102** (1975), no. 3, 517–533.

[Nek01] J. Nekovář, *On the parity of ranks of Selmer groups II*, C. R. Acad. Sci. Paris Sér. I Math. **332** (2001), no. 12, 99–104.

[Ser96] J.P. Serre, *A course in arithmetic*, Springer, 1996.

[SU14] C. Skinner and E. Urban, *The Iwasawa main conjectures for GL_2*, Invent. Math. **195** (2014), no. 1, 1–277.

[Tat95] J. Tate, *On the conjectures of Birch and Swinnerton-Dyer and a geometric analog*, Séminaire Bourbaki 1965/66, vol. 9, Soc. Math. France, 1995, p. 415–440.

[TW95] R. Taylor and A. Wiles, *Ring-theoretic properties of certain Hecke algebras*, Ann. of Math.(2) **141** (1995), no. 3, 553–572.

[Wil95] A. Wiles, *Modular elliptic curves and Fermat's last theorem*, Ann. of Math.(2) **141** (1995), no. 3, 443–551.

[Wil06] ———, *The Birch and Swinnerton-Dyer conjecture*, The millenium prize problems, Clay Math. Inst., 2006, `http://www.claymath.org/sites/default/files/birchswin.pdf`, pp. 31–41.

[Zha14] W. Zhang, *Selmer groups and the indivisibility of Heegner points*, Camb. J. Math. **2** (2014), no. 2, 191–253.