IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 20, Issue 3, Ver. II (May. - June. 2018), PP 63-72
www.iosrjournals.org

La Preuve De La Conjecture De Birch Et Swinnerton-Dyer

M. Sghiar
9 allée capitaine Jean Bernard Bossu, 21240, Talant, France.
Corresponding Author : M. Sghiar

Abstract *: The purpose of this article is to demonstrate the Birch and Swinnerton-Dyer Conjecture : If L is the function associated to an elliptic curve, then the order of the zero of L at s = 1 is exactly the order of the curve. In particular, the curve admits an infinity of rational points if and only if* $L(1)=0$.
Résumé *: Le but de cet article est de démontrer la Conjecture de Birch et Swinnerton-Dyer : Si L est la fonction associée à une courbe elliptique, alors l'ordre d'annulation de la fonction L en s=1 est exactement l'ordre de la courbe. En particulier, la courbe admet une infinité de points rationnels si et seulement si* $L(1)=0$.
Keywords *: Birch, Swinnerton-Dyer, L-function, courbe elliptique, zêta de Riemann,*

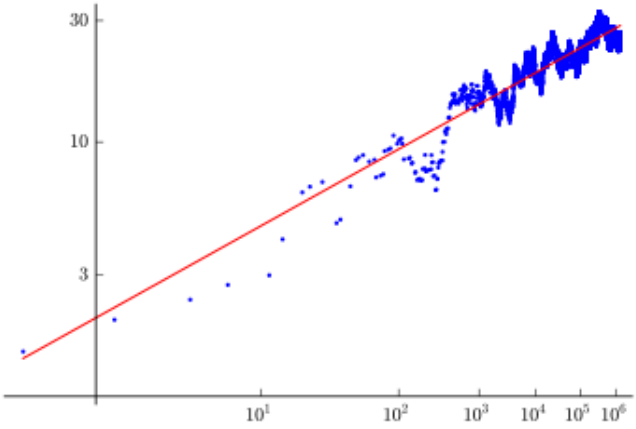
Date of Submission: 26-05-2018 Date of acceptance: 11-06-2018

1- Introduction :

En mathématiques, la **conjecture de Birch et Swinnerton-Dyer** [16] prédit que pour toute courbe elliptique sur le corps des rationnels, l'ordre d'annulation en 1 de la fonction L associée est égal au rang de la courbe. Elle prédit même la valeur du premier terme non nul dans le développement limité en 1 de cette fonction L.

Ouverte depuis plus de quarante ans, la conjecture n'a été démontrée que dans des cas particuliers. Et largement reconnue comme un des problèmes mathématiques les plus difficiles et les plus profonds encore ouverts au début du XXIe siècle.

Au début des années 1960, Bryan Birch et Peter Swinnerton-Dyer ont utilisé l'ordinateur EDSAC au laboratoire informatique de l'université de Cambridge pour calculer le nombre de points modulo *p* (désigné par *Np*) pour un grand nombre de nombres premiers *p* sur des courbes elliptiques dont le rang était connu. À partir de ces résultats numériques, ils émirent la conjecture que *Np* pour une courbe *E* de rang *r* suit la loi asymptotique : $\prod_{p\leq x} \frac{N_p}{p} \approx C \log(x)^r$ pour une certaine constante *C*. Un résultat dont le directeur de thèse de Birch, J. W. S. Cassels était sceptique au début.



A plot of $\prod_{p\leq x} \frac{N_p}{p}$ *for the curve* $y^2 = x^3 - 5x$ *as X varies over the first 100000 primes. The X-axis is log(log(X)) and Y-axis is in a logarithmic scale so the conjecture predicts that the data should form a line of*

slope equal to the rank of the curve, which is 1 in this case. For comparison, a line of slope 1 is drawn in red on the graph.

Cela les conduisit à faire une conjecture sur le comportement de la fonction L d'une courbe elliptique *L(E,s)* en *s* = 1, à savoir qu'il y aurait un zéro d'ordre *r* en ce point.
Une version plus précise de la conjecture fut ensuite proposée, décrivant le coefficient de Taylor principal de la fonction L en *s* = 1 en fonction d'invariants arithmétiques de la courbe étudiée par Tate, Shafarevich et d'autres. (voir [10] et [12]).

La conjecture de Birch et Swinnerton-Dyer a été démontrée seulement dans les cas particuliers suivants :
1. En 1976, John Coates et Andrew Wiles ont démontré que si *E* est une courbe sur un corps de nombres *F* avec multiplication complexe par un corps quadratique imaginaire *K* de nombre de classes 1, *F=K* ou **Q**, et si *L(E,1)* n'est pas 0 alors *E* possède seulement un nombre fini de points rationnels. Ceci fut étendu par Nicole Artaud au cas où *F* est une extension abélienne finie de *K*.
2. En 1983, Benedict Gross et Don Zagier ont montré que si une courbe elliptique modulaire possède un zéro d'ordre 1 en *s* = 1 alors elle possède un point rationnel d'ordre infini.
3. En 1990, Victor Kolyvagin a montré qu'une courbe elliptique modulaire *E* pour laquelle *L(E,1)* n'est pas zéro est de rang 0, et une courbe elliptique modulaire *E* pour laquelle *L(E,1)* possède un zéro d'ordre 1 en *s* = 1 est de rang 1.
4. En 2001, Christophe Breuil, Brian Conrad, Fred Diamond et Richard Taylor, étendant les travaux d'Andrew Wiles, ont démontré (théorème de modularité) que toutes les courbes elliptiques sur **Q** sont modulaires, ce qui étend les deux résultats précédents à toutes les courbes elliptiques sur **Q**.
5. En 2010, Manjul Bhargava et Arul Shankar ont annoncé une preuve que le rang moyen du groupe de Mordell-Weil d'une courbe elliptique sur **Q** est majoré par 7/6. En combinant ceci avec la preuve annoncée de la conjecture principale de la théorie d'Iwasawa pour GL(2) par Chris Skinner et Éric Urban, ils concluent qu'une proportion non nulle de courbes elliptiques sur **Q** sont de rang analytique nul (d'après le résultat de Kolyvagin, ces courbes vérifient la conjecture de Birch et Swinnerton-Dyer).

Depuis, rien n'a été démontré pour les courbes de rang supérieur à 1 bien que les calculs laissent penser que la conjecture est vraie.
Le but de cet article est de donner une preuve de la conjecture de Birch et Swinnerton-Dyer qui est un des sept problèmes du prix du millénaire recensés et mis à prix en 2000 par l'Institut de mathématiques Clay.

2- Rappel et définitions :

La **fonction zêta** d'une courbe elliptique E sur un corps fini F_p est en quelque sorte une fonction génératrice rassemblant les informations sur le nombre de points de la courbe dans toutes les extensions (finies) du corps de base. Plus précisément :

$$Z(E/F_p,T)=\exp\left(\sum_{n=1}^{\infty} card\left(E(F_{p^n})\frac{T^n}{n}\right)\right) \quad (1)$$

Où F_p est le corps fini à p éléments.

La somme à l'intérieur de l'exponentielle ressemble au développement d'un logarithme et, de fait, il est connu que la fonction zêta Z ainsi définie est une fonction rationnelle :

$$Z(E/F_p,T)=\frac{1-a_pT+pT^2}{(1-T)(1-pT)} \quad (2)$$

La fonction de **Hasse-Weil** de la courbe elliptique E sur $\mathbb{Q}$ est alors définie en rassemblant toutes ces informations locales (c'est-à-dire pour chaque nombre premier *p*). Elle est définie par :

$$L(E/\mathbb{Q},s)=\prod_p (1-a_p p^{-s}+\epsilon(p)\,p^{1-2s})^{-1} \tag{3}$$

où $\epsilon(p)=1$ si la courbe a bonne réduction en p et 0 sinon (dans ce dernier cas p est dit mauvais premier).

Ce produit converge seulement pour $\Re(s)>\frac{3}{2}$ Mais la conjecture de Helmut Hasse [13] prédisait que la fonction *L* admet un prolongement analytique à tout le plan complexe et vérifie une équation fonctionnelle liant, pour tout s , sa valeur en s à sa valeur en 2-s .
La conjecture de Hasse est maintenant, depuis 1999, démontrée ([2] [12] et [13]) comme conséquence de la preuve de la conjecture de Shimura-Taniyama-Weil : cette dernière affirme en effet que toute courbe elliptique définie sur $\mathbb{Q}$ est modulaire . Donc sa fonction zêta de Hasse-Weil est égale à la fonction *L* associée à une forme modulaire, pour laquelle le prolongement analytique était déjà connu.
La fonction *L* de Hasse-Weil est donc définie en tout point du plan complexe.

Posons :

$$Z^*(E/F_p,T)=\exp\left(\sum_{n=1}^{\infty} card(E(F_{p^n})\frac{T^n}{n}\right) \tag{4}$$

$$L^*(E/\mathbb{Q},s)=\prod_p Z^*\left(\frac{E}{F_p},\frac{1}{p^s}\right) \tag{5}$$

Notons $E(\mathbb{Q})$ le groupe *E*(ℚ) des points de la courbe à coordonnées rationnelles. Et rappelons ces trois théorèmes :

Théorème : $E(\mathbb{Q})$ est la somme directe d'un nombre fini de copies de $\mathbb{Z}$ et de groupes cycliques finis : $E(\mathbb{Q})=\mathbb{Z}^r\oplus E(\mathbb{Q})^{tors}$

Théorème de Mazur : le sous groupe de torsion $E(\mathbb{Q})^{tors}$ de $E(\mathbb{Q})$ est l'un des 15 groupes suivants : $\mathbb{Z}/N\mathbb{Z}$ pour $N=1,2,\ldots,10$ ou $N=12$, ou $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2N\mathbb{Z}$ avec $N=1,2,3,4$.

Théorème (Mordell-Weil [4]) : le groupe $E(\mathbb{Q})$ est un groupe abélien de type fini : $E(\mathbb{Q})\sim\mathbb{Z}^r\oplus\mathbb{Z}/b_1\mathbb{Z}\oplus..\oplus\mathbb{Z}/b_k\mathbb{Z}$

Remarque 1 : Ce sont ces trois théorèmes ci-dessus qui m'ont inspiré la preuve de la conjecture de BSD. En effet il y a une analogie entre les ensembles $E(\mathbb{Q})$ et $\mathbb{Z}$: dans $E(\mathbb{Q})$ il existe un nombre fini de points qui engendrent tout les autres points de $E(\mathbb{Q})$. De même, dans $\mathbb{Z}$, pour tout entier k on peut trouver k points convenables de $\mathbb{Z}$ qui vont engendrer ce dernier ensemble.

3- Etude du lien entre le rang de la courbe elliptique et le rang de $L^*(E/\mathbb{Q},s)$ au point 1 :

Le but dans ce paragraphe est de démontrer la proposition suivante :

Proposition 3.1: $rang\, L^*(E/\mathbb{Q},s)=rang(E(\mathbb{Q}))+1$

D'abord des équations 2 et 3 on a cette équation à un facteur près (ce facteur résulte des mauvais p) :

$$L(E/\mathbb{Q},s)=\prod_p \left(Z(E/F_p,p^{-s})(1-p^{-s})(1-p^{1-s})\right)^{-1} \tag{6}$$

Donc :

$$L(E/\mathbb{Q},s)=\left(\prod_p Z^*(E/F_p,p^{-s})\right)\zeta(s)\zeta(1-s) \tag{7}$$

Soit :

$$L(E/\mathbb{Q},s)=L^*(E/\mathbb{Q},s)\zeta(s)\zeta(1-s) \tag{8}$$

Où ζ est la fonction de Riemann (voir [5] [6] [7] [8]).

Lemme 3.1 :

i- Si $PGCD(a_1,\ldots,a_r)=1$ alors on a : $\mathbb{Z}=\mathbb{Z}a_1+\ldots+\mathbb{Z}a_r$. Et comme $1=\sum_{i=1}^r \beta_i a_i$, alors $z=\sum_{i=1}^r z\beta_i a_i,\ \forall\ z\in\mathbb{Z}$, et on pose $\pi_i(z)=z\beta_i$. (les β_i sont fixes)

ii- Si N est un entier non nul fixé, alors $z=\sum_{i=1}^r zN\beta_i\frac{a_i}{N},\ \forall\ z\in\mathbb{Z}$, et $\mathbb{Z}=N\beta_1\mathbb{Z}\frac{a_1}{N}\oplus\ldots\oplus N\beta_r\mathbb{Z}\frac{a_r}{N}$

Preuve : Résulte du fait que $\mathbb{Z}$ est un anneau principal.

Lemme 3.2 :

Si G est un groupe additif de cardinal n fini , alors il existe $g_1,\ldots,g_r$ des éléments de G tels que : $\forall\ g\in G, g=\sum_{i=1}^r \alpha_i g_i$ avec $\alpha_i\in\mathbb{Z}, r\le n$.

De plus $0=\sum_{i=1}^r \alpha_i g_i\Leftrightarrow\alpha_i=0,\ \forall\ i\in\{1,\ldots,r\}$. Autrement dit : $G=\mathbb{Z}/k_1\mathbb{Z}\,g_1\oplus\ldots\oplus\mathbb{Z}/k_r\mathbb{Z}\,g_r$

Preuve : $\{g_1,\ldots,g_n\}$ est une famille génératrice . Si $\{g_1,\ldots,g_r\}$ est une famille génératrice minimale alors $G=\mathbb{Z}/k_1\mathbb{Z}\,g_1\oplus\ldots\oplus\mathbb{Z}/k_r\mathbb{Z}\,g_r$.

Définition : r est dite la dimension ou le rang du groupe G si $\{g_1,\ldots,g_r\}$ est de cardinal minimal .

Posons :

$$L_{a_i}^*(s)=\exp\left(-\sum_{p\ premier,k\in\mathbb{N}^*}\pi_i(card(E(F_{p^k})))a_i\frac{p^{-ks}}{k}\right) \tag{9}$$

Soit Π_i la projection définie de $E(\mathbb{Q})$ sur $\mathbb{Z}$ par : $\pi_i(\sum_{i=1}^{r} \alpha_i a_i) = \alpha_i$

Π_i est bien définie grâce au **lemme 3.1.**

Pour k et p fixes, posons :

$$L^*_{a,k,p}(s)\pi_i(\mu) = \exp\left(-\pi_i(\mu)\, a\, \frac{p^{-ks}}{k}\right) \qquad (10)$$

Corollaire 3.1 :

Si G est un groupe de cardinal fini $n \geq 1$, alors il existe $b_1, \ldots, b_k$ des éléments de $\mathbb{Q}$ et $N \in \mathbb{N}$ tels que $\mathbb{Z} = N\mathbb{Z}\, b_1 \oplus \ldots \oplus N\mathbb{Z}\, b_k$.
De plus les éléments $b_1, \ldots, b_k$ peuvent être choisis dans tout intervalle $]0, \epsilon[$ avec $\epsilon \neq 0$
et $k = 1 + rang(G)$.
Dans ce cas si $z = \sum_{i=1}^{k} \beta_i b_i$, on pose $\pi_i(z) = \beta_i$.

Corollaire 3.2 :

Si G est un groupe de cardinal fini $n \geq 1$, alors il existe des éléments $b_1, \ldots, b_k$ de $\mathbb{Z}$ et N un élément de $\mathbb{N}^*$ tels que $\mathbb{Z} = \frac{1}{N}\mathbb{Z}\, b_1 \oplus \ldots \oplus \frac{1}{N}\mathbb{Z}\, b_k$ avec $b_i \geq 1 \; \forall\, i$ et $k = 1 + rang(G)$. Dans ce cas si $z = \sum_{i=1}^{k} \beta_i b_i$, on pose $\pi_i(z) = \beta_i$.

Remarque 2 : le choix de k tel que $k = 1 + rang(G)$ se justifie par le fait que pour les courbes elliptiques, pour pouvoir y introduire une loi de groupe on a rajouté un point neutre à l'infini. Ce qui y correspond le rajout d'une dimension.

Corollaire 3.3 : Le groupe $E(\mathbb{Q})$ est un groupe abélien de type fini et il existe $b_1, \ldots, b_{k+1}$ des éléments de $\mathbb{Q}$ et $l_1, \ldots, l_{k+1}$ des éléments de $\mathbb{N}$ tels que :
i- $E(\mathbb{Q}) = \mathbb{Z}^r \oplus E(\mathbb{Q})^{tors} \subset a_1\mathbb{Z} \oplus \ldots \oplus a_{r+1}\mathbb{Z} \oplus (\mathbb{Z}/l_1\mathbb{Z})b_1 \oplus \ldots \oplus (\mathbb{Z}/l_{k+1}\mathbb{Z})b_{k+1}$ (à un isomorphisme près) avec $k = card(E(\mathbb{Q})^{tors})$.

ii- On peut choisir les bases $\{b_1, \ldots, b_{k+1}\}$ et $\{a_1, \ldots, a_{r+1}\}$ telles que : $a_i \leq \frac{1}{2(r+k+1)} \; \forall\, i$ et $b_i \leq \frac{1}{2(r+k+1)} \; \forall\, i$ de même on peut choisir des a_i tels que $a_i > 1 \; \forall\, i$.

iii- De plus, il existe $N \in \mathbb{N}$ tels que $\mathbb{Z} = N\mathbb{Z}\, b_1 \oplus \ldots \oplus N\mathbb{Z}\, b_{k+1}$, et il existe des entiers relatifs β_i et M un entier non nul fixé, tels que : $\mathbb{Z} = M\beta_1\mathbb{Z}\, a_1 \oplus \ldots \oplus M\beta_{r+1}\mathbb{Z}\, a_{r+1}$.

iv- Enfin pour des b_i assez petits ($b_i \leq \frac{1}{(1+card\ E(\mathbb{Q})^{tors})^3}$), si $\{b'_1,\ldots,b'_{k+1}\}$ est une autre base avec $b'_i \in (\mathbb{Z}/l_1\mathbb{Z})b_1 \oplus \ldots \oplus (\mathbb{Z}/l_{k+1}\mathbb{Z})b_{k+1}\ \forall\ i$ alors $b'_i < \frac{1}{card\ E(\mathbb{Q})^{tors}} < 1\ \forall\ i$ si $card\ E(\mathbb{Q})^{tors} \neq 0$.

Preuve : se déduit de ce qui précède et du fait que $\mathbb{Z}^r$ est infini contrairement à $E(\mathbb{Q})^{tors}$ qui est fini.

3-1- Si le rang de la courbe elliptique est non nul et le rang sous groupe de torsion est nul :

Proposition 3.1.1 :

$$\prod_{i=1}^{r+1} L^*_{a_i}(s) = \prod_p Z^*\left(\frac{E}{F_p}, \frac{1}{p^s}\right) = L^*(E/\mathbb{Q}, s)$$

Preuve :

En fixant k et p et en utilisant l'équation 10 on aura :

$$\prod_{i=1}^{r+1} L^*_{a_i,k,p}(s)^{\pi_i(\sum_{i=1}^{r+1}\alpha_i a_i)} = \exp\left(-\left(\sum_{i=1}^{r+1}\alpha_i a_i\right)\frac{p^{-ks}}{k}\right) \quad (11)$$

En posant :

$$card(E(F_{p^k})) = \sum_{i=1}^{r+1}\alpha_i a_i \quad (12)$$

On déduit de l'équation 11 :

$$\prod_{i=1}^{r+1}\prod_{p\ premier,\ k\in\mathbb{N}^*} L^*_{a_i,k,p}(s)^{\pi_i(card(E(F_{p^k})))} = \exp\left(-\sum_{p\ premier,\ k\in\mathbb{N}^*} card(E(F_{p^k}))\frac{p^{-ks}}{k}\right) \quad (13)$$

Et par suite, des équations 9 , 10 et 13:

On déduit que :

$$\prod_{i=1}^{r+1} L_{a_i}^*(s) = \exp\left(-\sum_{p\ premier,\ k\in\mathbb{N}^*} card(E(F_{p^k}))\frac{p^{-ks}}{k}\right) \quad (14)$$

Ainsi des équations 4, 5, et 14 on a :

$$\prod_{i=1}^{r+1} L_{a_i}^*(s) = \prod_p Z^*\left(\frac{E}{F_p}, \frac{1}{p^s}\right) = L^*(E/\mathbb{Q}, s) \quad (15)$$

D'où le résultat.

Corollaire 3.1.1 :

$$\prod_{i=1}^{r+1} L^{*a_i}(s) = L^*(E/\mathbb{Q}, s) \quad (16)$$

Preuve :

Se déduit de 15 et du fait que $L_{a_i}^*(s) = L^{*a_i}(s)$

Théorème 3.1.1

Si $L^*(E/\mathbb{Q}, s) = \sum_{i=0}^{\infty} c_i (s-1)^{r_i}$, alors $r_0 = r(E(\mathbb{Q}))+1$.

Preuve : De l'équation 16 on déduit que :

$$r_0 = \sum_{i=1}^{r+1} r_0 a_i \quad (17)$$

En utilisant le corollaire 3.3 on peut choisir la base $\{a_1, \ldots, a_{r+1}\}$ de deux façons :

- Si la base $\{a_1, \ldots, a_{r+1}\}$ est telle que $a_i \geq 1\ \forall\ i$, alors $r_0 \geq r+1$.

- Si la base $\{a_1, \ldots, a_{r+1}\}$ est telle que $a_i \leq \frac{1}{r_0}\ \forall\ i$, alors $r_0 \leq r+1$, et par suite $r_0 = r+1$.

D'où le théorème.

3-2- Si le rang $r(E(\mathbb{Q}))$ de la courbe elliptique est nul et le rang du sous groupe de torsion est non nul .

Soit k la dimension du sous groupe de torsion de $E(\mathbb{Q})$ ($k \geq 1$).

Comme ci-dessus, on voit que :

$$\prod_{i=1}^{k+1} L^{*b_i}(s) = L^*(E/\mathbb{Q}, s) \tag{18}$$

Théorème 3.2.1

Si $L^*(E/\mathbb{Q}, s) = \sum_{i=0}^{\infty} c_i (s-1)^{t_i}$, alors $t_0 = r(E(\mathbb{Q})) = 0$.

Preuve :

De l'équation 18, on déduit que :

$$t_0 = t_0 \sum_{i=1}^{k+1} b_i \tag{19}$$

En utilisant le corollaire **3.1** , on peut choisir la base $\{b_1, \ldots, b_{k+1}\}$ telle que $b_i \in]0, \epsilon[$ avec ϵ assez petit. Il s'en suit que $t_0 = 0$.

3- 3- Si le rang $r(E(\mathbb{Q}))$ de la courbe elliptique est non nul et le rang du sous groupe de torsion est non nul .

Théorème 3.3.1

Si $L^*(E/\mathbb{Q}, s) = \sum_{i=0}^{\infty} c_i (s-1)^{u_i}$, alors $u_0 = r(E(\mathbb{Q})) + 1$.

Cette fois, on tient compte des deux bases : $\{a_1, \ldots, a_{r+1}\}$ et $\{b_1, \ldots, b_k\}$.

Comme ci-dessus on aura :

$$\prod_{i=1}^{r+1} L^{*a_i}(s) \prod_{i=1}^{k} L^{*b_i}(s) = L^*(E/\mathbb{Q}, s) \tag{20}$$

Et par suite :

$$u_0 = \sum_{i=1}^{r+1} u_0 a_i + \sum_{i=1}^{k} u_0 b_i \tag{21}$$

De même, en choisissant convenablement la base $\{a_1, \ldots, a_{r+1}\} \cup \{b_1, \ldots, b_k\}$ on déduit que $u_0 = r + 1$.

D'où la proposition.

4- La preuve de la conjecture de Birch et Swinnerton-Dyer :

Théorème 4.1 (Conjecture de Birch et Swinnerton-Dyer) : L'ordre du zéro de la fonction *L* de la courbe elliptique *E* au voisinage de *s* = 1 est égal au rang de *E*.

Preuve :

En multipliant par $(s-1)s$ les deux membres de l'équation 8 ci-dessus, on aura :

$$s(s-1)L(E/\mathbb{Q},s)=(s-1)\zeta(s)L^{*}(E/\mathbb{Q},s)s\zeta(1-s) \tag{22}$$

Or en utilisant le développement de Laurent au voisinage de 1 de la fonction ζ :

On aura :

$$\zeta(s)=\frac{1}{s-1}+\lambda+\sum_{1}^{\infty}(-1)^{n}\frac{\lambda_{n}}{n!}(s-1)^{n} \tag{23}$$

Où λ est la constante d'Euler Mascheroni et où les λ_{n} sont les *nombres de Stieltjes* .

Comme $(s-1)\zeta(s)$ et $s\zeta(1-s)$ sont entières , alors des équations 22 et 23 ci-dessus, on déduit qu' on a :

$$rang\,L(E/\mathbb{Q},s) \leq rang\,L^{*}(E/\mathbb{Q},s) \tag{24}$$

En utilisant les équations 8 et 23 on peut écrire :

$$L(E/\mathbb{Q},s)=L^{*}(E/\mathbb{Q},s)\frac{f(s)}{s(s-1)} \tag{25}$$

Où $f(s)$ est une fonction entière en s.

On en déduit en utilisant la **proposition 3.1** que :

$$rang\,L(E/\mathbb{Q},s) = rang\,L^{*}(E/\mathbb{Q},s)-1=rang(E(\mathbb{Q})) \tag{26}$$

Corollaire 4.1 : Si L est la fonction associée à une courbe elliptique, alors l'ordre d'annulation de la fonction L en $s=1$ est exactement l'ordre de la courbe. En particulier, la courbe admet une infinité de points rationnels si et seulement si $L(1)=0$.

Remarque : On constate un point commun entre les fonctions L , ζ , et f (Voir [5 à 9]) :

l'annulation de la fonction L au point 1 nous renseigne sur l'existence et le nombre des points rationnels, les zéros de la fonction ζ de Riemann nous renseignent sur la distribution des nombres premiers, et l'annulation de la fonction f [9] en un point d'un graphe de cardinal n permet de savoir l'existence ou non des cycles hamiltoniens (f permet même de les trouver en un temps polynomial $O(n^3)$).

5- Conclusion

L' analogie entre les ensembles $E(\mathbb{Q})$ et $\mathbb{Z}$: dans $E(\mathbb{Q})$ il existe un nombre fini de points qui engendrent tout les autres points, et dans $\mathbb{Z}$, pour tout entier k non nul on peut trouver k points de $\mathbb{Z}$ qui engendrent ce dernier ensemble m'a permis avec les k points convenablement choisis - $k = 1+rang(G)$ - de prouver la conjecture de Birch et Swinnerton-Dyer.

Le choix de $k = 1+rang(G)$ se justifie par le fait que pour les courbes elliptiques, pour pouvoir y introduire une loi de groupe, on a rajouté un point neutre à l'infini. Ce qui y correspond le rajout d'une dimension supplémentaire.

Bien que c'est la **fonction zêta** d'une courbe elliptique qui a permis l'introduction de la **fonction de Hasse-Weil**, il me semble que les mathématiciens ont compté le plus sur la fonction de **Hasse-Weil** seule pour donner une preuve de la conjecture **de Birch et Swinnerton-Dyer.** Le lecteur constatera l'importance de l'utilisation de la **fonction zêta** d'une courbe elliptique Z et de sa duale Z^* - vu leur forme exponentielle et les propriétés de cette dernière – dans la preuve de la dite conjecture.

Références :

[1] B. Birch and H. Swinnerton-Dyer, Notes on elliptic curves II, Journ. reine u. angewandte Math. 218 (1965), 79–108.

[2] C. Breuil, B. Conrad, F. Diamond, and R. Taylor, On the modularity of elliptic curves over Q: wild 3-adic exercises, J. Amer. Math. S oc. 14 (2001), 843–939.

[3] J. Coates and A. Wiles, On the conjecture of Birch and Swinnerton-Dyer, Invent. Math. 39 (1977), 223–251.

[4] L. Mordell, On the rational solutions of the indeterminate equations of the third and fourth degrees, Proc. Cambridge Phil. Soc. 21 (1922-23), 179–192.

[5] M. Sghiar (Décembre 2015) , Des applications génératrices des nombres premiers et cinq preuves de l'hypothèse de riemann, Pioneer Journal of Algebra, Number Theory and its Applications , Volume 10, Numbers 1-2, 2015, Pages 1-31.

[6] M. Sghiar (Livre) Cinq preuves de l'Hypothèse de Riemann, Éditions Universitaires Européennes, ISBN-13 :978-3-639-54549-4

[7] M. sghiar. , The mertens function and the proof of the riemann's hypothesis international journal of engineering and advanced technology (ijeat) isnn:2249-8958, volume- 7 Issue-2, December 2017. (see also : https://hal.archives-ouvertes.fr/hal-01667383/document)

[8] M. Sghiar, vulgarisation des six preuves de l'hypothèse de riemann : https://hal.archives-ouvertes.fr/hal-01586017/document

[9] M. Sghiar "Les Nombres Graphiques Et Le Problème P=NP . IOSR Journal of Mathematics (IOSR-JM) 14.3 (2018): 26-29 .

[10] J. Tate, On the conjectures of Birch and Swinnerton-Dyer and a geometric analog, Seminaire Bourbaki 1965/66, no. 306.

[11] J. Tate, The arithmetic of elliptic curves, Invent. Math. 23 (1974), 179–206.

[12] R. Taylor, A. Wiles, Ring-theoretic properties of certain Hecke algebras, Ann. Math. 141 (1995), 553–572.

[13] A. Weil, Collected Papers, Vol. II, Springer-Verlag, New York, 1979.

[14] wikipedia , https://fr.wikipedia.org/wiki/Conjecture de Birch et Swinnerton-Dyer

[15] wikipedia , https://fr.wikipedia.org/wiki/Courbe elliptique

[16] Andrew Wiles, « The Birch and Swinnerton-Dyer conjecture », dans James Carlson, Arthur Jaffe et Andrew Wiles, *The Millennium prize problems*, AMS, (ISBN 978-0-821-83679-8)

IOSR Journal of Computer Engineering (IOSR-JCE) is UGC approved Journal with Sl. No. 5019, Journal no. 49102.

M. Sghiar. " La Preuve De La Conjecture De Birch Et Swinnerton-Dyer." IOSR Journal of Computer Engineering (IOSR-JCE) 20.3 (2018): 63-72.