Astérisque

L. SZPIRO

Discriminant et conducteur des courbes elliptiques

Astérisque, tome 183 (1990), p. 7-18

<http://www.numdam.org/item?id=AST_1990__183__7_0>

Société Mathématique de France
Astérisque 183 (1990)

DISCRIMINANT ET CONDUCTEUR DES COURBES ELLIPTIQUES

L. Szpiro

Cet exposé présente une conjecture sur le discriminant des courbes elliptiques (conjecture 1 dans le texte). Ce sujet a été traité par de nombreux auteurs depuis que je m'en suis préoccupé. (Citons : [V], [O] [H]). Je n'ai donc pas voulu trop alourdir le contenu de ce court exposé et me suis contenté,en tentant de garder l'intelligibilité du texte, de n'y inclure que des faits non écrits ailleurs.

Le premier paragraphe expose la conjecture et en donne la preuve pour le corps de fonctions via la classe de Kodaira-Spencer.

Le deuxième paragraphe explique les exemples de Frey, qui donnent de mirifiques conséquences de la conjecture 1. D'autres conséquences seront expliquées dans le reste du séminaire. Au paragraphe 3 nous étudions le discriminant des courbes de Weil et nous donnons des exemples, dus à A. Douady, qui montrent la difficulté des problèmes qui se posent.

Les notations et conventions adoptées dans cet article sont celles de [Sz 1] et de [D]. En particulier une courbe elliptique sera toujours munie d'une section unité ([D]) , si elle a un modèle semi-stable celui-ci sera régulier ([Sz 1]) (compactification relative du modèle de Néron). Je remercie le référée de la revue Astérisque pour le travail minutieux effectué sur ce court article.

L'exposé oral du séminaire sur ce sujet a été fait par M. Hindry. Je me suis inspiré de ses notes [H] dans le § 2 .

1. UNE CONJECTURE SUR LE DISCRIMINANT DES COURBES ELLIPTIQUES.

En 1978 j'ai démontré le théorème qui suit, reliant le "discriminant" et le "conducteur" d'une courbe elliptique sur un corps de fonctions. La démonstration de cet énoncé est essentiellement contenue dans [Sz 1]. Mais, bien des mathématiciens s'en sont plaints, car les énoncés de loc. cit. semblent ne concerner que les courbes de genre au moins deux.

THÉORÈME 1. Soit $f : E \to C$ un morphisme propre et plat d'une surface E, lisse sur un corps k, dans une courbe C, projective, lisse de genre q et géométriquement connexe sur e. Supposons que la fibre générique de f soit une courbe elliptique lisse et géométriquement connexe sur le corps de fonctions de C. Supposons de plus que f ne soit pas isotrivial et que ses fibres dégénérées soient semi-stables. Alors, si Δ_E est le diviseur discriminant de f et si s est le nombre de points géométriques de C dont la fibre n'est pas lisse on a :

$$\deg \Delta_E \leq p^e \, 6(2q - 2 + s)$$

où p est la caractéristique de k, et p^e le degré d'inséparabilité du morphisme de C dans la droite des "j", déduit de f. (Si la caractéristique de k est nulle on convient que $p^e = 1$).

Démonstration. On a deux suites exactes fondamentales :

$$(1) \quad 0 \to f^* \Omega^1_{C/k} \to \Omega^1_{E/k} \to \Omega^1_{E/C} \to 0$$

$$(II) \quad 0 \to \Omega^1_{E/C} \to \omega_{X/C} \to \bigoplus_{\substack{P \text{ singulier} \\ \text{dans sa fibre}}} k(P) \to 0$$

où $\Omega^1_{Y/Z}$ est le faisceau des différentielles de Y sur Z, et $\omega_{Y/Z}$ est le faisceau dualisant relatif si $Y \to Z$ est localement d'intersection complète.

Notons S le diviseur réduit de C tel que $E \to C$ soit lisse sur $C - S$. En appliquant le fonteur f_* aux deux suites on obtient :

a) un morphisme

$$f_* \Omega^1_{E/C} \to R^1 f_* f^* \Omega^1_{C/k} = \Omega^1_{C/k} \otimes \omega_E^{-1}$$

où $\omega_E = f_* \omega_{E/C}$ (notons que $\omega_{E/C} = f^* \omega_E$). Ce morphisme coïncide avec l'application de Kodaira-Spencer sur $C - S$ (qui ici n'est autre que la dérivée de l'application j).

b) $$0 \to f_* \Omega^1_{E/C} \to \omega_E \to \bigoplus_{P \text{ singulier}} k(P)$$

On déduit de cette suite exacte que

$$f_* \Omega^1_{E/C} \simeq \omega_E(-S) \qquad (S \text{ est réduit !!})$$

On a donc, par a) et b) un morphisme

$$\omega_E^{\otimes 2} \to \Omega^1_{C/k}(S)$$

qui est non nul quand la dérivée de l'application j ne s'annulle pas. En caractéristique zéro c'est le cas si j n'est pas constant, en caractéristique $p > 0$ c'est le cas si f n'est pas un "pull-back" par le morphisme de Frobénius de C.

En prenant les degrés de ces deux faisceaux inversibles, et en notant qu'on a $\deg \Delta_E = 12 \deg \omega_E$ on obtient le théorème 1. □

Notons qu'il est apparu, plus tard, de nombreuses démonstrations différentes (Frey [F1], Hindry-Silverman [H,S] par la formule d'Hurwitz quand $k = \mathbb{C}$ et encore plus tard par "a,b,c" [O] en toute caractéristique).

L'analogie entre les corps de nombres et les corps de fonctions d'une variable pousse à conjecturer un énoncé analogue pour les courbes elliptiques sur un corps de nombres. Cette analogie est renforcée par la théorie d'Arakelov, qui en mettant des métriques, dites permises, aux places à l'infini donne un degré "naturel" $\deg_{Ar}(\omega_E)$ au faisceau ω_E défini plus haut.

Ces idées se trouvent confortées par le théorème suivant dont j'ai publié une démonstration dans [Sz 2] :

THÉORÈME. Soit E une courbe elliptique semi-stable sur un corps de nombres K alors on a :

$$12 \deg_{Ar}(\omega_E) = \log \text{Norme}_{K/\mathbb{Q}} (\Delta_{min}(E)) .$$

J'ai donc soumis, notamment à l'occasion de l'école d'été de Hanovre en septembre 82, la conjecture suivante :

CONJECTURE 1. Soit K un corps de nombres, il existe une constante $\sigma(K)$ ne dépendant que de K telle que, pour toute courbe elliptique E sur K, de conducteur N_E et de discriminant minimal Δ_E on ait :

$$\text{Norme}_{K/\mathbb{Q}} (\Delta_E) \leq (\text{Norme}_{K/\mathbb{Q}}(N_E))^{\sigma(K)} .$$

On peut énoncer une conjecture plus optimiste :

CONJECTURE 1 forme forte. Soit K un corps de nombres. Alors pour tout nombre réel positif ε, il existe une constante $C(K,\varepsilon)$ telle que :

pour toute courbe elliptique E sur K de discriminant minimal Δ_E et de conducteur N_E on ait

$$\text{Norme}_{K/\mathbb{Q}}(\Delta_E) \leq C(K,\varepsilon)\ (\text{Norme}_{K/\mathbb{Q}}(N_E))^{6+\varepsilon}$$

Notons que Masser ([M]) a montré qu'on ne peut espérer un exposant plus petit que $6+\varepsilon$.

2. LES COURBES DE FREY.

G. Frey [Fr 1] a donné de très brillants exemples de courbes elliptiques semi-stables. Rappelons brièvement sa construction.

Soient a,b,c des entiers sans facteurs communs tels que $a+b = c$. Considérons la courbe elliptique $E_{a,b,c}$ d'équation (non minimale)

$$y^2 = x(x+a)\ (x-b)$$

Frey montre les faits suivants :

a) Si $2^4/a$ et $b \equiv -1\ (4)$ alors $E_{a,b,c}$ est semi-stable.

b) Dans ce cas son équation minimale est donnée par

$$y^2 + xy = x^3 + \frac{a-b-1}{4}\,x^2 - \frac{abx}{16}$$

c) Toujours sous les hypothèses de a) le discriminant minimal de $E_{a,b,c}$ est égal à $2^{-8}\,a^2\,b^2\,c^2$.

Si on applique la conjecture 1 a une courbe de Frey on obtient :

$$\text{Si } a+b = c \qquad (a,b) = 1 \qquad \text{alors}$$

$$|abc| \leq 2^8 \left(\prod_{p|abc} p\right)^{\sigma/2} \qquad \text{où } \sigma = \sigma(\mathbb{Q})$$

Je ne résiste pas à appliquer cette conjecture à une solution hypothétique

de l'équation de Fermat : $x^p + y^p = z^p \qquad (xyz) \neq 0$

la conjecture 1 impliquerait que :

$$p \leq \frac{8 \log 2}{\log xyz} + \frac{\sigma}{2}$$

ce qui prouverait, au moins, "Fermat asymptotique".

Notons aussi que si l'on regarde les solutions entières d'une équation de la forme

$$a_1 X^{n_1} + a_2 X^{n_2} = a_3 X^{n_3}$$

où les a_i sont premiers entre eux, la conjecture 1 implique qu'il existe une constante $C(a_1,a_2,a_3)$ telle que : l'équation ci-dessus n'ait pas de solutions toutes non nulles et premières entre elles pour $\inf(n_i) \geq C(a_1,a_2,a_3)$.

J. Oesterlé dans [O] a donné les exemples suivants qui montrent que dans la conjecture 1 forte on ne peut prendre $\varepsilon = 0$:

Partant de trois nombres premiers entre eux a_0,b_0,c_0 tels que $a_0 + b_0 = c_0$ définissons la suite (a_n,b_n,c_n) par :

$$c_{n+1} = c_n^2 \qquad b_{n+1} = (a_n - b_n)^2 \qquad a_{n+1} = 4\, a_n\, b_n$$

on voit facilement que $a_n + b_n = c_n$ et que ces trois nombres n'ont pas de facteur commun.

Pour tout nombre entier n notons $R(n)$ (pour radical de n) le produit sans facteurs carrés des nombres premiers divisant n . Le lecteur vérifiera facilement qu'on a :

$$\frac{a_{n+1}\, b_{n+1}\, c_{n+1}}{R(a_{n+1}\, b_{n+1}\, c_{n+1})^3} \cdot \frac{R(a_n\, b_n\, c_n)^3}{a_n\, b_n\, c_n} \geq 4$$

et donc que $\Delta(E_{a_n,b_n,c_n}) \Big/ N\left(E_{a_n,b_n,c_n}\right)^6$ n'est pas borné.

Remarque : Le processus de récurrence définissant la suite a_n, b_n, c_n peut s'interpréter de la façon suivante : c'est la multiplication par 2 dans le groupe multiplicatif $\mathbb{C}_m$ réalisé comme le cercle de rayon 1 dans $\mathbb{C}$. En effet, un triplet tel que $a+b = c$ conne sur une extension quadratique de $\mathbb{Q}$ un point $\left(\sqrt{\frac{a}{b}}, \sqrt{\frac{b}{c}}\right)$ du cercle $x^2 + y^2 = 1$, il est alors facile de voir que les formules pour $\sin 2\theta$ et $\cos 2\theta$ expliquent la récurrence. Il serait intéressant de voir ce que donne la multiplication par deux sur une courbe elliptique ayant des points d'ordre infini et une équation en trois monomes (e.g. $Y^3 = X^3 + 6$) .

On a vu plus haut, en utilisant les courbes de Frey que la conjecture 1 prend la forme "lycéenne" suivante : Il existe une constante k telle que si a,b,c sont des entiers sans facteurs communs satisfaisant à $a+b = c$ alors $|abc| \leq \left(\prod_{p|abc} p\right)^k$

(sous la forme forte : pour tout $\varepsilon > 0$ il existe une constante $C(\varepsilon)$ telle que

$$|abc| \leq C(\varepsilon) \left(\prod_{p|abc}\right)^{3+\varepsilon}$$

Masser et Oesterlé ont proposé, alors, la conjecture suivante : $a+b = c$, mêmes hypothèses alors

$$\sup(|a|,|b|,|c|) \leq \left(\prod_{p|abc} p\right)^{\ell}$$

(ℓ une constante). Il est clair que la conjecture 1 implique celle-ci si on ne dit rien sur ℓ . La forme forte de la conjecture de Masser Oesterlé est : Pour tout $\varepsilon > 0$ il existe une constante $C(\varepsilon)$ telle que si $a+b = c$ (a,b,c sans facteur communs) alors

$$\sup(|a|,|b|,|c|) \leq C(\varepsilon) \left(\prod_{p|abc} p\right)^{1+\varepsilon}$$

Cette forme forte ne semble pas être conséquence de la conjecture 1 forte. Par contre elle implique clairement la conjecture forte sur $|abc|$ et même la forme forte de la conjecture 1 (cf. par exemple Vojta) en raisonnant sur l'équation :

$$c_4^3 - c_6^2 = 1728\ \Delta .$$

Notons qu'en étudiant le discriminant d'une courbe de Frey quotientée par un point d'ordre 2 comme dans [Sz 2] on voit que

$|\Delta_{min}(E)| \leq C(\varepsilon)\ N(E)^{6+\varepsilon}$

implique $\sup(|a|,|b|,|c|) \leq C'(\varepsilon) \left(\prod_{p|abc} p\right)^{6/5+\varepsilon}$.

En effet la valeur absolue du discriminant d'un tel quotient bien choisi d'une courbe de Frey est égal à

$$2^{-4}\ abc^4 \qquad (2^4|a \text{ , et } a,b,c \text{ sont positifs }) .$$

Remarquons enfin une autre conséquence - conjecturale donc - de la conjecture 1 : Il existe une constante σ telle que pour tout nombre entier a

$$a \leq \left(\prod_{p|a(a+1)} p\right)^{\sigma}$$

3. LES COURBES DE WEIL.

Une courbe elliptique E sur $\mathbb{Q}$ est dite de Weil si elle est dominée par une courbe modulaire $X_0(N)$, le morphisme $\varphi : X_0(N) \to E$ étant défini sur $\mathbb{Q}$. On dit de plus que E est une courbe de Weil forte si $H_1(\varphi,\mathbb{Z})$ (ou $\pi_1(\varphi)$) est surjectif. Shimura [Sh] a montré qu'il y a correspondance bianivoque entre les courbes de Weil fortes images de $X_0(N)$ et les nouvelles formes modulaires de poids deux, et de niveau N .Carayol, [C], a montré que pour une courbe de Weil

forte E , image de $X_0(N)$, N est égal au conducteur de E . Taniyama a conjecturé que toute courbe elliptique sur $\mathbb{Q}$ est de Weil. A. Weil [W] a montré que si une courbe elliptique E sur $\mathbb{Q}$, ainsi que ses différentes "tordues", ont une fonction L satisfaisant une equation fonctionnelle attendue quand on change s en $2-s$, alors la transformée de Mellin de la fonction L de E est une forme modulaire de poids 2 . Par le résultat de Shimura cité plus haut et le théorème de Faltings (conjecture de Tate) on en déduit qu'une telle courbe elliptique est de Weil.

On voit ainsi, bien qu'à l'heure actuelle la conjecture de Taniyama ne soit pas démontrée, qu'il est crucial de tester une conjecture sur les courbes elliptiques, sur les courbes de Weil. Un effort dans ce sens a été entrepris par Golfeld ([G] et Mestre-Oesterlé [M-O]. Il est raisonnable de dire que c'est G. Frey qui a eu le premier l'intuition que la conjecture de Taniyama entrainait "Fermat" via la conjecture 1. On ne sait pas, au moment où j'écris ces lignes que la conjecture 1 est vraie pour les courbes de Weil.

Notons cependant que Ribet [R] a montré que "Taniyama" implique "Fermat" mais sans passer par la conjecture 1 .

PROPOSITION 1. Soit E une courbe de Weil forte f la nouvelle forme modulaire de poids 2 et de niveau N , normalisée, correspondant à E . Si α est une différentielle de Néron sur E on à $\varphi^*\alpha = c\, f\, dz$ où c (constante de Manin) est un entier.

On conjecture que $|c| = 1$ et on sait, par Raynaud, que si N est sans facteur carré, $|c|$ est borné absolument. Si $\| f \|$ est la norme de Peterson de f et $h_F(E)$ la hauteur modulaire de E (introduite par Faltings-Arakelov) on a :

$$\frac{1}{2} \log \deg \varphi = h_F(E) + \log \| f_E \| + \log |c| + \log 2\pi$$

(cf. par exemple [Si]).

D'autre part Faltings a démontré [Fa 1] au moins quand E est semi-stable sur $\mathbb{Q}$ (ici N sans facteurs carrés), qu'on a :

$$12\, h_F(E) = \log |\Delta_{min}(E)| - \log |\Delta(\tau)\ \mathrm{Im}(\tau)^6|$$

On voit ainsi qu'une borne polynomiale

$$\deg \varphi \leq N^{\rho} \qquad (\rho \text{ indépendant de } N \text{ et } E)$$

implique la conjecture 1 car on sait minorer polynomialement le carré scalaire de Peterson (cf. [G]).

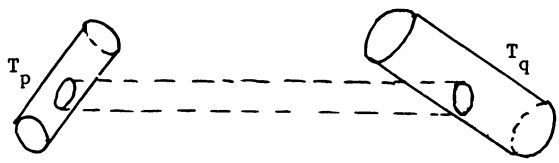
On peut naturellement se demander si on peut borner le degré d'un morphisme φ, non constant, d'une courbe X de genre $g \geq 2$ dans une courbe elliptique E sur $\mathbb{C}$, en fonction de g. (Notons que le genre de $X_0(N)$ est polynomial en N). On voit, comme le genre de E vaut un, que la formule de Hurwitz ne donne rien ! D'autre part, il faut imposer $H_1(\varphi)$ surjectif sinon les isogénies de E retirent tout espoir. Même dans ce cas là, A. Douady nous a fourni les exemples simples suivants qui, pour nous, signifient que le problème de borner le degré de φ est de nature arithmétique.

Exemples de A. Douady. Soient p et q deux entiers premiers entre eux nous allons construire un morphisme algébrique sur $\mathbb{C}$, d'une courbe de genre 2, X, dans une courbe elliptique E, surjectif sur les H_1 et de degré $p+q$.

Soient trois tores T_1, T_p, T_q que nous considérons comme des cylindres dont les extrémités sont identifiées. De plus T_i sera de

longueur i ($i = 1, p, q$) et de même base. On envoie les tores T_p et T_q sur T_1 par les morphismes φ_p et φ_q correspondants aux identifications : T_p est l'empilement de p tores identiques à T_1 et T_q est l'empilement de q tores identiques à T_1 .

Soit α_1 , un "segment de droite" assez petit dans T_1 et soient α_p et α_q deux "segments de droites" s'envoyant bijectivement sur α_1 . Remplaçant les α_i , $i = p,q$ par des "cercles" C_i on peut recoller T_p et T_q selon C_p et C_q



on obtient ainsi une surface topologique compacte X de genre 2, avec un morphisme continu de degré $p+q$, $\varphi : X \to T_1 = E$, ramifié seulement en deux points (les extrémités de α_1) .

On a les deux faits suivants :

a) $H_1(X) \to H_1(T_1)$ est surjectif : si σ et τ sont les générateurs de $H_1(T_1)$ (cf. le dessin) σ , $p\tau$ et $q\tau$ sont dans l'image de φ . p et q étant premiers entre eux, σ et τ sont dans l'image de φ $H_1(\varphi)$.

b) Fixant une structure algébrique (analytique) sur T_1 , c'est un théorème de Riemann qu'il existe une structure algébrique sur X qui rende φ un morphisme algébrique.

U.R.A. 0213 du C.N.R.S.
"Analyse complexe et Géométrie"
Université de Paris VI
I.H.P.
11, rue Pierre et Marie Curie
75005 - PARIS CEDEX 05

BIBLIOGRAPHIE

[C] CARAYOL H. "Sur les représentations ℓ-adiques associées aux formes modulaires de Hilbert". Ann. Sc. ENS 19 (1986), 409-468.

[F 1] FALTINGS G. "Calculus on arithmétic surfaces". Annals of Maths. vol. 119 (1984) 387-424.

[F 2] FALTINGS G. "Endlichkeitssätze fur abelshe varietäten über Zalhenkörpern". Inventiones Math. vol. 73, Fasc. 3 (1983), 349-366.

[Fr] FREY G. "Links between elliptic curves and certain dioplantine equations". Annales universitatis Saraviensis, series mathematicae I., 1986.

[G] GOLFELD D. "Modular elliptic curves and dioplantine problems" à paraître.

[H.S.] HINDRY M. et SILVERMAN J.H. "The cannonical height and integral points on elliptic curves". Inv. Math. 93, 419-450 (1988).

[H] HINDRY M. "a,b,c , conducteur, discriminant". Preprint PARIS VI, 1988.

[M] MASSER. "On a conjecture of Szpiro". Ce volume.

[M.S] MAZUR B. et SWINNERTON-DYER H.P.F. "Arithmetic of Weil curves". Inv. Math. 25 (1974) 1-61.

[O] OESTERLE J. "Nouvelles approches du << théorème >> de Fermat". Séminaire Bourbaki n° 694, 1988.

[Sh] SHIMURA G. "Arithmetic theory of arithmetic functions". Publications of the mathematical society of Japan, Iwanami Shoten Publishers and Princeton University press 1971.

[Si] SILVERMAN J.H. "Heights and elliptic curves" in Arithmetic Geometry, Springer-Verlag New York 1986.

[Sz 1] SZPIRO L. "Propriétés numériques du faisceau dualisant relatif" dans "Séminaire sur les pinceaux de courbes de genre au moins deux" Astérisque n° 89.

[Sz 2] SZPIRO L. "Sur les propriétés numériques du dualisant relatif d'une surface arithmétique" à paraître volume Grothendieck.

[V] VOJTA P. "Diophantine approximations and value distribution theory". Lecture notes in math., 1239, Springer-Verlag 1987.

[W] WEIL A. "Zeta function and Mellin transform". Algebraic geometry Bombay 1968, TIFR 1969, 400-402.