§6. Courbes elliptiques et fonctions L

de façon effective les d pour lesquels $h(-d) = 2$; les bornes obtenues sont très grandes (Stark obtient par exemple $|d| < 10^{1100}$), mais Stark d'une part, Montgomery et Weinberger de l'autre, ont mis au point des méthodes qui permettent par un calcul sur ordinateur utilisant les zéros de la fonction zêta de Riemann (pour Stark) ou de séries $L(\chi, s)$ (pour Montgomery et Weinberger) de vérifier que, en dessous des bornes précédentes, tous les d pour lesquels $h(-d) = 2$ sont $\leqslant 427$.

Pour l'instant, aucune des méthodes précédentes n'a pu être appliquée au problème du nombre de classes h pour $h \geqslant 3$.

§ 6. Courbes elliptiques et fonctions L

Nous allons maintenant parler un peu des courbes elliptiques, car elles jouent un rôle fondamental dans la suite de l'histoire du problème de Gauss.

Considérons une équation de la forme

$$(W) \qquad y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6\,,$$

où les a_i sont dans $\mathbf{Q}$. La cubique projective E définie par l'équation homogène associée a un unique point à l'infini 0. Lorsque E est non singulière, on dit que E (ou plutôt que le couple $(E, 0)$) est une *courbe elliptique définie sur* $\mathbf{Q}$, et que (W) en est une *équation de Weierstrass*. Un changement de variables

$$(C) \qquad \begin{aligned} x &= u^2x' + r \\ y &= u^3y' + sx' + t \qquad (u, r, s, t \text{ dans } \mathbf{Q}, u \neq 0) \end{aligned}$$

conduit à une autre équation de Weierstrass (W') de E. On dit que l'équation (W) est *minimale* si les coefficients a_i sont entiers et si les équations (W') déduites de (W) par un changement de variables (C) avec u, r, s, t entiers et $u \neq \pm 1$, ne sont pas à coefficients entiers.

Une courbe elliptique E définie sur $\mathbf{Q}$ admet une équation minimale et toute autre équation minimale s'en déduit par un changement de variables (C) avec $u = \pm 1$ et r, s, t dans $\mathbf{Z}$.

Supposons désormais (W) minimale. Si l'on pose

$$\begin{aligned} X &= x + (a_1^2/12) + (a_2/3) \\ Y &= y + (a_1/2)x + (a_3/2)\,, \end{aligned}$$

l'équation (W) s'écrit $Y^2 = X^3 - (c_4/48)X - (c_6/864)$. Un calcul élémentaire montre que c_4, c_6 et $\Delta = (c_4^3 - c_6^2)/1728$ s'expriment comme polynômes

universels à coefficients entiers en a_1, a_2, a_3, a_4, a_6, donc sont *entiers*. Ces entiers *ne dépendent pas du choix de* (W), mais seulement de la courbe elliptique. On dit que Δ est le *discriminant minimal* de E.

Soit $E(\mathbf{Q})$ l'ensemble des points rationnels de E (i.e. les solutions $(x, y) \in \mathbf{Q}^2$ de l'équation (W), auxquelles on ajoute le point à l'infini 0). Il existe une unique structure de *groupe abélien* sur $E(\mathbf{Q})$, d'élément neutre 0, pour laquelle trois points de $E(\mathbf{Q})$ ont une somme nulle si et seulement si ce sont les points d'intersection (avec multiplicités) de E et d'une droite du plan projectif.

Pour obtenir des informations sur les solutions rationnelles de l'équation (W), on est amené à étudier le groupe $E(\mathbf{Q})$. Je pense qu'il n'est pas exagéré de prétendre que la majeure partie des travaux effectués et des notions introduites dans la théorie des courbes elliptiques ont pour but ultime de décrire $E(\mathbf{Q})$. Un théorème important dans cette direction est le théorème de Mordell-Weil: *le groupe* $E(\mathbf{Q})$ *est de type fini*, et est par suite isomorphe à $F \times \mathbf{Z}^r$ où F est un groupe fini et r un entier $\geqslant 0$ (que nous appellerons le rang de $E(\mathbf{Q})$). On a des informations précises sur F à la suite de travaux de Mazur (par exemple, on sait que F est d'ordre $\leqslant 16$); par contre, r reste pour l'instant mystérieux (on ne sait même pas s'il peut prendre des valeurs arbitrairement grandes, bien que l'on pense que tel est le cas).

Comme les coefficients de l'équation (W) sont entiers, on peut réduire cette équation modulo un nombre premier p, puis compter le nombre de ses solutions (x, y) dans $(\mathbf{Z}/p\mathbf{Z})^2$. Ce nombre ne dépend pas du choix de (W), mais seulement de E. D'après un théorème de Hasse, il est de la forme $p - a_p$ où a_p satisfait à l'inégalité

$$|a_p| < 2\sqrt{p}\,. \tag{31}$$

La *fonction* L_E *de Hasse-Weil* associée à la courbe elliptique est par définition la série de Dirichlet

$$L_E(s) = \prod_{p \mid \Delta} (1 - a_p p^{-s})^{-1} \prod_{p \nmid \Delta} (1 - a_p p^{-s} + p^{1-2s})^{-1}\,. \tag{32}$$

Ce produit converge pour $\mathrm{Re}\,(s) > 3/2$ d'après (31). Un cas particulier de conjectures générales sur les fonctions L associées à des variétés algébriques est:

CONJECTURE 1. *La fonction* $\Lambda_E(s) = (2\pi)^{-s}\Gamma(s)L_E(s)$ *admet un prolongement holomorphe à* $\mathbf{C}$, *borné dans toute bande verticale, et il existe* $\varepsilon_E \in \{-1, 1\}$ *et un entier* $N_E \geqslant 1$ *tels que* $\Lambda_E(2-s) = \varepsilon_E N_E{}^{s-1}\Lambda_E(s)$.

Posons $L_E(s) = \sum_{n=1}^{\infty} a_n n^{-s}$ et définissons sur le demi-plan de Poincaré $\{\tau \in \mathbf{C} \mid \mathrm{Im}(\tau) > 0\}$ une fonction f_E par

$$f_E(\tau) = \sum_{n=1}^{\infty} a_n e^{2\pi i n \tau}. \tag{33}$$

La théorie de Hecke, qui s'appuie sur la transformation de Mellin $\Lambda_E(s) = \int_0^{\infty} f_E(iy)\, y^{s-1} dy$, permet de montrer l'équivalence entre la conjecture 1 et la suivante:

CONJECTURE 1'. *Il existe* $\varepsilon_E \in \{-1, 1\}$ *et un entier* $N_E \geqslant 1$ *(les mêmes qu'avant) tels que* $f_E(-1/N_E\tau) = -\varepsilon_E N_E \tau^2 f_E(\tau)$.

On dispose de conjectures étendant la conjecture 1 aux séries $L_E(\chi, s) = \sum_{n=1}^{\infty} a_n \chi(n) n^{-s}$, avec χ caractère de Dirichlet. Généralisant le travail de Hecke, Weil [1]) a montré que ces conjectures pour tous les χ (ou même seulement pour une famille assez grande de χ) équivalent à la suivante sur f_E:

CONJECTURE 2 (Taniyama-Weil) [2]). *La fonction* f_E *satisfait à la conjecture* 1' *et est une forme modulaire parabolique de poids* 2 *pour* $\Gamma_0(N_E)$.

[La dernière assertion signifie que $f_E((a\tau+b)/(c\tau+d)) = (c\tau+d)^2 f(\tau)$ si $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ appartient au sous-groupe $\Gamma_0(N_E)$ de $SL_2(\mathbf{Z})$ formé par les matrices telles que N_E divise c, et que la fonction $\tau \mapsto f(\tau)\,\mathrm{Im}\,\tau$ est bornée sur le demi-plan de Poincaré.]

Une courbe elliptique E définie sur $\mathbf{Q}$ qui satisfait à la conjecture 2 est appelée *courbe elliptique modulaire* ou *courbe de Weil*. On sait que si la courbe E est à multiplications complexes, elle est de Weil. D'autre part, étant donnée une courbe elliptique E, il existe des algorithmes permettant de déterminer si elle est ou non une courbe de Weil. Cela a été appliqué à de nombreux exemples et toutes les courbes elliptiques étudiées se sont avérées être des courbes de Weil, conformément aux conjectures.

---

[1]) A. WEIL, *Über die Bestimmung Dirichletscher Reihen durch Funktionalgleichungen*, Math. Ann. 168 (1967), 149-156.

[2]) Lorsque cette conjecture est satisfaite, f_E est une newform au sens d'Atkin-Lehner, d'après un théorème de W. Li; l'entier N_E est le conducteur géométrique de la courbe elliptique E, d'après un théorème de Carayol; en particulier, les facteurs premiers de N_E sont les mêmes que ceux du discriminant minimal de E.

Birch et Swinnerton-Dyer ont émis une autre conjecture, stupéfiante car elle relie la fonction L_E, définie à partir des nombres de solutions de l'équation (W) sur les corps finis, au rang r de $E(\mathbf{Q})$ qui fournit une information sur les solutions rationnelles de l'équation (W). Cette conjecture suppose implicitement la conjecture 1 satisfaite:

CONJECTURE 3 (Birch et Swinnerton-Dyer). *Le rang r de $E(\mathbf{Q})$ est égal à l'ordre du zéro de la fonction L_E au point* 1.

(Birch et Swinnerton-Dyer donnent en outre une expression conjecturale de $\lim_{s\to 1}(s-1)^r L_E(s)$.)

§ 7. LE THÉORÈME DE GOLDFELD

Un pas décisif vers la solution effective du problème du nombre de classes a été franchi par Goldfeld en 1976. L'idée à la base de son travail est la suivante: Supposons que nous connaissions une série de Dirichlet $\sum_{n=1}^{\infty} a_n n^{-s}$ telle que pour tout caractère de Dirichlet $\chi: n \mapsto \left(\frac{-d}{n}\right)$ avec $-d$ discriminant fondamental, la série $\sum_{n=1}^{\infty} a_n \chi(n) n^{-s}$ ait un comportement analytique très différent de la série $\sum_{n=1}^{\infty} a_n \lambda(n) n^{-s}$ où λ est la fonction multiplicative introduite à la fin de II, § 2. On peut alors espérer d'après le principe de II, § 2, montrer de façon effective que lorsque d est grand, $h(-d)$ ne peut être petit.

De fait, Goldfeld montre [1]) qu'il suffit de *connaître une seule courbe elliptique E* définie sur $\mathbf{Q}$ telle que

— E soit une *courbe de Weil*;

— la fonction L_E ait un zéro *au moins triple* au point 1,

et d'appliquer l'idée précédente à la série de Dirichlet L_E pour obtenir des minorations effectives de nombres de classes. Celles-ci sont bien moins bonnes que celles que donne l'hypothèse de Riemann généralisée (cf. § 3):

---

[1]) D. M. GOLDFELD, *The conjecture of Birch and Swinnerton-Dyer and the class number of quadratic fields*, Journées Arithmétiques de Caen, Astérisque 41-42 (1977), 219-227.