SÉMINAIRE N. BOURBAKI

BARRY MAZUR

# Courbes elliptiques et symboles modulaires

*Séminaire N. Bourbaki*, 1973, exp. n° 414, p. 277-294

<http://www.numdam.org/item?id=SB_1971-1972__14__277_0>

© Association des collaborateurs de Nicolas Bourbaki, 1973, tous droits réservés.

L'accès aux archives du séminaire Bourbaki (http://www.bourbaki.ens.fr/) implique l'accord avec les conditions générales d'utilisation (http://www.numdam.org/conditions). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

*Article numérisé dans le cadre du programme*
*Numérisation de documents anciens mathématiques*
http://www.numdam.org/

Séminaire BOURBAKI 414-01
24e année, 1971/72, n° 414 Juin 1972

# COURBES ELLIPTIQUES ET SYMBOLES MODULAIRES

par Barry MAZUR

## § 1. Introduction

Eichler et Shimura se sont aperçus de l'importance des courbes algébriques sur $\mathbb{Q}$ uniformisables par des fonctions modulaires de $\Gamma_0(N)$, et ont obtenu de remarquables résultats sur l'arithmétique de ces courbes. Le mémoire de Weil [11] permet d'espérer que l'on obtient ainsi toutes les courbes elliptiques sur $\mathbb{Q}$. La structure "géométrique" qu'une telle uniformisation fournit sur une courbe elliptique est un outil puissant pour l'étude de ses séries $L$, et de ses points rationnels sur les corps de nombres abéliens et les corps finis.

Cette structure géométrique (en particulier le symbole modulaire du § 3 ci-dessous) mérite d'être examinée systématiquement. Son étude a été commencée par Birch [2] et continuée par Manin [5].

## § 2. Les courbes modulaires

Puisque nous voulons conserver la lettre $H$ pour l'homologie, posons :

$U$ = demi-plan supérieur ;

$\bar{U} = U \cup \mathbb{Q} \cup \{i\infty\}$ ( $P = \mathbb{Q} \cup \{i\infty\}$ est l'ensemble des pointes).

On donne à $\bar{U}$ la topologie traditionnelle dans la théorie des formes modulaires : une base de voisinages d'une pointe finie $s$ est donnée par les ensembles $\{s\} \cup D$ où $D$ est un disque ouvert dans $U$ tangent à la droite réelle au point $s$.

$\Gamma = PSL(2, \mathbb{Z})$ agit sur $\bar{U}$ par les transformations homographiques :

$$\gamma(z) = \begin{pmatrix} a & b \\ c & d \end{pmatrix}(z) = \frac{az + b}{cz + d}.$$

Par définition, $\Gamma_0(N)$ est le sous-groupe de $\Gamma$ représenté par les éléments $\gamma$ tels que $c \equiv 0 \bmod N$. Le groupe $\Gamma_0(N)$ agit sur $U$ de façon proprement

discontinue et le quotient $Y = \Gamma_0(N)\backslash\bar{U}$ est muni d'une structure d'une courbe analytique compacte (et alors algébrique). (Voir [9] pour les détails.) D'après Igusa [4], il existe un modèle $X = X_0(N)$ qui est une courbe projective et lisse sur $\mathbb{Q}$ dont le relèvement sur $\mathbb{C}$ s'identifie à $Y$.

[A vrai dire, Igusa a fait nettement plus que cela. Il décrit un schéma $X_0(N)/\mathbb{Z}$ qui est normal, et propre sur $\mathbb{Z}$, lisse sur $\mathbb{Z}[1/N]$.]

Table :

| genre de $X_0(N)$ | Valeurs de $N$ |
|---|---|
| 0 | $1 \leq N \leq 10$ ; 12, 13, 16, 18, 25 |
| 1 | 11, 14, 15, 17, 19, 20, 21, 24, 27, 32, 36, 49 |
| 2 | 22, 23, 26, 28, 29, 31, 37, 50 |

## § 3. Le Symbole Modulaire

Soient $P = \mathbb{Q} \cup \{i\infty\}$ l'ensemble des pointes, et $P_0 \subset P$ le sous-ensemble des pointes congrues à 0 par rapport à $\Gamma_0(N)$. Il est facile de voir que $P_0$ est donné par les nombres rationnels à dénominateur premier à $N$.

Notons $\langle s,r\rangle$ un chemin dans $\bar{U}$ qui commence au point $s \in \bar{U}$ et aboutit à $r$. Alors $\langle s,r\rangle$ est déterminé à homotopie près, puisque $\bar{U}$ est contractile, et, si $r$ est congrue à $s$ sous l'action de $\Gamma_0(N)$, l'image de $\langle s,r\rangle$ dans $Y$ détermine une classe de lacets dans $Y$, à homotopie pointée près. Ecrivons

$$\langle r\rangle \in \pi_1(Y, 0)$$

la classe induite par l'image de $\langle 0,r\rangle$ pour $r \in P_0$. Notons par $\{r\}$ l'image de $\langle r\rangle$ dans $H_1(Y, \mathbb{Z})$ et par $\{s,r\}$ l'image de $\langle s,r\rangle$. On a donc l'application $\{\ \} : P_0 \to H_1(Y, \mathbb{Z})$. Cette application s'étend à l'ensemble de toutes les pointes pourvu qu'on prenne l'homologie à coefficients réels :

$$\begin{array}{ccc} \{\ \} : P & \to & H_1(Y, \mathbf{R}) \\ \downarrow & & \downarrow \\ \{\ \} : P_o & \to & H_1(Y, \mathbf{Z}) \ . \end{array}$$

Pour donner la définition de cette extension de $\{\ \}$, appelée : le symbole modulaire, on se sert de l'identification

$$H_1(Y, \mathbf{R}) \xrightarrow{\sim} \mathrm{Hom}_{\mathbf{C}}(H^o(Y, \Omega^1_{Y/\mathbf{C}}) ; \mathbf{C})$$

$$z \mapsto \int_z \quad \text{(en tant que fonctionnelle linéaire sur les formes différentielles)}$$

et on pose

$$\{s,r\} = \int_{\langle s,r\rangle} : H^o(Y, \Omega^1_{Y/\mathbf{C}}) \to \mathbf{C} \ ,$$

et $\{r\} = \{0,r\}$ .

Formules

a) $\langle 0\rangle = 1 \in \pi_1(Y,0)$

b) $\langle r_1\rangle^{-1}\langle r_2\rangle = \langle \gamma(r_1)\rangle^{-1}\langle \gamma(r_2)\rangle$ pour tout $\gamma \in \Gamma_o(N)$ et $r_1, r_2 \in P_o$ .

c) $\langle \gamma(r)\rangle = \langle r\rangle$ si $r \in P_o$ , et $\gamma \in \Gamma_o(N)$ est parabolique. (Par définition, $\gamma$ est parabolique s'il laisse fixe une pointe de $P$ .)

Remarques.- On a, par réduction, des versions abéliennes des formules ci-dessus, valables pour le symbole modulaire. Les formules se démontrent facilement par de petits dessins. Prenons (b) par exemple : La classe dans $\pi_1(Y)$ qui apparaît dans le membre de gauche de (b) est représentée par la classe d'homotopie pointée du chemin $\langle r_1, r_2\rangle$ . Mais dans le membre de droite, la classe est donnée par $\gamma\langle r_1, r_2\rangle$ ce qui est visiblement la même chose dans $\pi_1(Y)$ .

Puisque $\gamma = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ laisse la pointe $i\infty$ fixe, c'est un élément parabolique dans $\Gamma_o(N)$ . D'après la formule (c) ,

$$\langle r + 1 \rangle = \langle r \rangle \ .$$

Autrement dit, la fonction $\langle\ \rangle$ (ainsi que le symbole modulaire) est bien défini sur $P_o$ modulo 1 .

En ce qui concerne la non-trivialité de la fonction $\langle\ \rangle$ , on a le résultat suivant :

Lemme 1.- Les applications

$$\langle\ \rangle : P_o \bmod 1 \ \to \ \pi_1(Y,0)$$

$$\{\ \} : P_o \bmod 1 \ \to \ H_1(Y,\mathbb{Z})$$

sont surjectives.

Démonstration.

Soit $\tilde{U} \subset U$ le sous-espace des points $u$ dont le stabilisateur dans $\Gamma_o(N)$ est trivial. $\Gamma_o(N)$ agit librement sur $\tilde{U}$ , et le quotient $\tilde{Y}$ est le complément d'un nombre fini de points dans $Y$ (à savoir : les points elliptiques et paraboliques dans $Y$ ). On se donne un point $u \in \tilde{U}$ , et on désigne par la même lettre son image dans $\tilde{Y}$ et $Y$ . On a un triangle commutatif,

$$\begin{array}{ccc} \pi_1(\tilde{Y},u) & \to & \pi_1(Y,u) \\ & \searrow \quad \nearrow & \\ & \Gamma_o(N) & \end{array}$$

où la flèche ascendante est donnée par la règle $\gamma \mapsto \langle u\,,\,\gamma(u)\rangle$ , et les deux autres flèches sont les morphismes naturels. Par des raisonnements topologiques classiques, ces deux autres flèches sont surjectives. Il s'ensuit que la flèche ascendante l'est aussi. Le lemme est alors démontré, après un changement de point de base (de $u$ jusqu'à $0$ ).

Considérons maintenant les opérateurs de Hecke $T_p$ $(p \nmid N)$ qui agissent sur $H^o(Y\,,\,\Omega^1)$ par la formule :

$$(\omega | T_p)(z) \ = \ \omega(pz) + \sum_{k=0}^{p-1} \omega\left(\frac{z+k}{p}\right) \ .$$

On en tire facilement les formules donnant l'action de $T_p$ sur $H_1(Y\,,\,\mathbb{R})$ ,

d'où

$$(1) \qquad T_p\{s,r\} = \{ps,pr\} + \sum_{k=0}^{p-1} \{\frac{s+k}{p}, \frac{r+k}{p}\}$$

et pour $\{r\} = \{0,r\}$ ,

$$T_p\{r\} = \{pr\} + \sum_{k=0}^{p-1} \{\frac{r+k}{p}\} - \sum_{k=0}^{p-1} \{\frac{k}{p}\} .$$

Remarque.- Le symbole modulaire a été introduit par Birch [2] dans ses études sur la conjecture de Birch et Swinnerton-Dyer. Il l'a utilisé afin de calculer la valeur en $s = 1$ de la série $L$ associée à certaines courbes elliptiques. Manin [5] a entrepris une étude systématique des symboles $\{\ \}$ , et en a déduit sa formule de réciprocité (7.b ci-dessous) alors que Swinnerton-Dyer et moi-même avons trouvé le symbole modulaire essentiel dans notre théorie des séries $L$ p-adique associées aux courbes de Weil [10].

## § 4. Les courbes de Weil

Soient $E/\mathbb{Q}$ une courbe elliptique (une variété abélienne de dimension 1 ) sur $\mathbb{Q}$ et $\omega$ une différentielle de Néron de $E$ , c'est-à-dire un des deux générateurs de $H^0(E/\mathbb{Z}, \Omega^1_{E/\mathbb{Z}}) \approx \mathbb{Z}$ , où $E/\mathbb{Z}$ est le modèle de Néron de $E$ , sur $\mathbb{Z}$ . On considère $\omega$ comme différentielle de première espèce de $E/\mathbb{Q}$ .

Considérons un morphisme non constant défini sur $\mathbb{Q}$ ,

$$(*) \qquad \begin{array}{ccc} X_o(N) & \xrightarrow{\varphi} & E \\ i\infty & \longmapsto & 0 . \end{array}$$

L'image réciproque $\varphi^*\omega$ de $\omega$ par $\varphi$ est une forme différentielle de première espèce sur $X_o(N)$ , que l'on peut interpréter comme une forme modulaire parabolique sur $U$ , de poids 2 . Il résulte des "relations de congruence pour les correspondances modulaires" de Eichler-Shimura [9] et Igusa [4] que $\varphi^*\omega$ est vecteur propre des opérateurs de Hecke $T_p$ , où $p$ ne divise pas $N$ ; les valeurs propres $\lambda_p$ correspondantes sont des entiers, et l'on a

$$N_p = 1 + p - \lambda_p ,$$

où $N_p$ est le nombre de points rationnels de $E/\mathbb{Z}$ définis sur $\mathbb{F}_p$. Remarquons que, d'après la propriété universelle du modèle de Néron, et le fait que $X_o(N)/\mathbb{Z}[\frac{1}{N}]$ est lisse, $E/\mathbb{Z}[\frac{1}{N}]$ est un schéma abélien.

Lorsqu'en outre la forme modulaire $\varphi^*\omega$ est primitive pour $\Gamma_o(N)$ ("new form" d'Atkin-Lehner [1]), nous dirons que $\varphi$ est une paramétrisation (faible) de Weil de la courbe elliptique $E$.

Lemme 2.- Soit $q = e^{2\pi i z}$ l'uniformisante standard de $X_o(N)$ au point $i\infty$. Soit $\varphi$ une paramétrisation faible de Weil. Alors, le développement de Fourier de $\varphi^*\omega$ s'écrit

$$(2) \qquad \varphi^*\omega = c. \sum_{n \geq 1}^{\infty} \lambda(n) q^n = c.\Omega , \quad \text{avec } c \in \mathbb{Q}^* , \ \lambda(1) = 1 , \ \lambda(p) = \lambda_p$$

pour tout nombre premier $p \nmid N$.

Remarque.- Le fait que $\lambda(1) \neq 0$ implique que $\varphi$ est étale à $i\infty$.

Si $E$ possède une paramétrisation faible de Weil, on dira que $E$ est une courbe de Weil faible ([1]).

Lemme 3.- Soit $\varphi : X \to E$ une paramétrisation faible de Weil. Les trois conditions suivantes sont équivalentes :

a) Le noyau du morphisme induit sur les jacobiennes

$$\varphi : J_o(N)/\mathbb{Q} \to E/\mathbb{Q}$$

est une variété abélienne (i.e. c'est un groupe algébrique connexe $\mathbb{Q}$).

b) Le morphisme induit sur l'homologie,

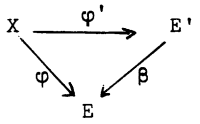
---

([1]) Cette notion est un peu différente de celle de Manin [5]. Pour $N = 11$, il y a 3 courbes de Weil faibles au sens ci-dessus ; 2 d'entre elles sont des courbes de Weil au sens de Manin, et une seule est une courbe de Weil (tout court) au sens donné plus loin.

$$\varphi : H_1(X, \mathbb{Z}) \rightarrow H_1(E, \mathbb{Z})$$

est surjectif.

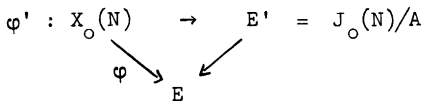
c) $\varphi$ est **maximal** au sens suivant : s'il existe un triangle commutatif




avec $\varphi'$ une paramétrisation faible de Weil, alors $\beta$ est un isomorphisme.

DÉFINITION.- Une **paramétrisation** de Weil est une paramétrisation faible de Weil qui jouit des conditions de maximalité du lemme 2. Une courbe de Weil E est une courbe elliptique qui possède une paramétrisation de Weil.

La démonstration du lemme 3 est strictement élémentaire. On voit facilement que n'importe quelle paramétrisation faible de Weil peut être dominée par une paramétrisation de Weil. Soit $A/\mathbb{Q}$ la composante connexe de l'élément neutre dans le noyau de $Jac(\varphi)$, le morphisme induit par $\varphi$ sur les jacobiennes. Définissons




et $\varphi'$ est visiblement une paramétrisation de Weil. Par conséquent n'importe quelle courbe de Weil faible est isogène à une courbe de Weil.

L'essentiel de ce qu'on connait au sujet des courbes de Weil est rassemblé dans la liste suivante :

A. La théorie d'Atkin-Lehner [1] montre :

Soit E une courbe elliptique sur $\mathbb{Q}$. Une paramétrisation de Weil pour E est unique, au signe près (si elle existe).

B. Un théorème de Serre ([8], p. IV-14) entraîne :

Soit $E$ une courbe elliptique sur $\mathbb{Q}$ d'invariant modulaire non entier. S'il existe une forme parabolique de poids 2 pour $\Gamma_o(N)$ telle que

$$f|T_p = \lambda_p f \qquad (\text{où } \lambda_p = 1 + p - N_p)$$

pour presque tout $p$, alors $E$ est une courbe de Weil faible.

**C.** Soit $\Omega$ une "new form" de poids 2 sous $\Gamma_o(N)$. Supposons que $\Omega = \Sigma \lambda(n) q^n$ telle que $\lambda(1) = 1$, et que les $\lambda(n)$ sont des entiers. Il existe alors une courbe de Weil $\varphi : X \to E_\Omega$ telle que $\varphi^*\omega = c.\Omega$ avec $c \in \mathbb{Q}^*$. (cf. [9]).

D. Théorème de Weil [11]. Grosso modo, ce théorème affirme qu'une courbe elliptique $E/\mathbb{Q}$ est une courbe de Weil faible si et seulement si les séries $L(E, \chi, s)$ satisfont à une équation fonctionnelle d'un type prescrit, pour suffisamment de caractères de Dirichlet $\chi$. C'est ce théorème de Weil qui donne l'espoir que la conjecture suivante est vraie :

CONJECTURE (de Weil).- Toute courbe elliptique $E/\mathbb{Q}$ est une courbe de Weil faible.

Il revient au même de dire : Dans n'importe quelle classe d'isogénie de courbes elliptiques sur $\mathbb{Q}$, il existe une et une seule courbe de Weil et sa paramétrisation de Weil est unique au signe près.

Etant donné une paramétrisation faible $\varphi : X_o(N) \to E$, l'entier $N$ ne dépend que de $E$, d'après le théorème 1 (b). Appelons-le le conducteur analytique de $E$. Par contre, le nombre rationnel $c = c(\varphi) \in \mathbb{Q}^*$ défini par $\varphi^*\omega = c.\Omega$ dépend effectivement de la paramétrisation faible.

CONJECTURE.- Soit $E$ une courbe de Weil faible. Alors, son conducteur analytique est donné par la recette suivante :

$$N = \prod_p p^{(\mathrm{ord}_p \Delta - m_p(E) + 1)}$$

où $p$ parcourt les nombres premiers de mauvaise réduction pour $E/\mathbb{Z}$.

Ici, $|\Delta|$ est le minimum des valeurs absolues des discriminants des équations cubiques sur $\mathbb{Z}$ qui donne $E/\mathbb{Q}$, et $m_p(E)$ est le nombre de composantes irréductibles de la fibre du modèle de Néron de $E$ sur $\mathbb{F}_p$. Le membre de droite est appelé le conducteur (tout court) de $E$. On sait que le nombre premier $p$ apparaît avec l'exposant 1 si et seulement si la fibre du modèle de Néron en $p$ est de type multiplicatif. Si $p \geq 5$, et si la fibre de Néron est de type additif, l'exposant de $p$ est 2. Dans le cas restant ($p = 2, 3$, réduction additive) l'exposant est au moins 2. (Voir la formule de Ogg [6].)

En se servant de la lissité de $X_o(N)/\mathbb{Z}[\frac{1}{N}]$, on voit que, si un nombre premier divise le conducteur de $E$, il divise aussi son conducteur analytique.

Au sujet du nombre $c(\varphi)$, on ne sait pas grand chose. On ignore s'il y a des paramétrisations de Weil avec $c(\varphi) \neq \pm 1$, mais on a très peu d'exemples. Puisque $c(-\varphi) = -c(\varphi)$, il est convenable de choisir le signe de la paramétrisation de Weil tel que $c(\varphi)$ soit positif. Grâce à des résultats récents de Deligne et Rapoport, on peut montrer que $c$ est presqu'un entier (à savoir : $c \in \mathbb{Z}[1/n]$ où $n$ est le produit de tous les nombres premiers $p$ tels que $p^2$ divise $N$).

Exemples.- Maintenant, référons à la Table du § 1.

Pour les valeurs de $N$ telles que le genre de $X_o(N)$ est nul, il n'existe pas de courbes de Weil de conducteur analytique $N$. Pour les douze valeurs telles que le genre de $X_o(N)$ est égal à 1, $X_o(N)$ est elle-même une courbe de Weil, et la paramétrisation est simplement l'identité. Parmi les valeurs de $N$ telles que le genre de $X_o(N)$ est égal à 2, il n'y a que trois valeurs ($N = 26, 37, 50$) telles que des paramétrisations de Weil $\varphi : X_o(N) \to E$ existent, et pour chacune de celles-ci, il y a précisément deux paramétrisations de Weil. Elles sont données par division par des involutions de $X_o(N)$ [10].

## § 5. Le symbole modulaire pour une paramétrisation de Weil faible

Soit $\varphi : X_0(N) \to E$ une paramétrisation de Weil faible, et désignons par la même lettre le morphisme induit sur l'homologie

$$\varphi : H_1(X_0(N), \mathbb{Z}) \to H_1(E, \mathbb{Z}) .$$

Par composition, on définit le symbole modulaire à valeurs dans l'homologie de $E$ :

$$\begin{aligned} \varphi : P_0 \bmod 1 &\to H_1(E, \mathbb{Z}) \\ \{r\} &\to \varphi(r) = \varphi(\{r\}) . \end{aligned}$$

Puisque $\varphi$ est défini sur $\mathbb{R}$, $\varphi$ commute à la conjugaison complexe, donnée par l'involution $z \mapsto -\bar{z}$ sur $\bar{U}$. Il s'ensuit que la symétrisée et l'anti-symétrisée de $\varphi$

$$\varphi^{\pm}(r) = \varphi(r) \pm \varphi(-r) ,$$

prennent leurs valeurs dans $H_1(E, \mathbb{Z})^{\pm} \subset H_1(E, \mathbb{Z})$, les sous-espaces propres pour la conjugaison complexe dont les valeurs propres sont $\pm 1$ respectivement. Or, on a une identification <u>canonique</u> $H_1(E, \mathbb{Z})^{\pm} \cong \mathbb{Z}$. Cela se voit parce qu'une paramétrisation de Weil donne une orientation du lieu réel de $E$, par le procédé suivant : soit $\tau$ un vecteur tangent réel descendant de $X_0(N)$ au point $i\infty$ ; puisque $\varphi$ est étale au point $i\infty$, on a $d\varphi(\tau) \neq 0$, et on utilise $d\varphi(\tau)$ pour orienter $E(\mathbb{R})$.

## § 6. Formules provenant des opérateurs de Hecke

Posons $I = \{0, i\infty\} \subset H_1(X_0(N), \mathbb{R})$. Alors,

(3) $$(1 + p - T_p)I = \sum_{k=0}^{p-1} \{\frac{k}{p}\}$$ pour tout nombre premier $p \nmid N$.

(4) $$-(1 + p - T_p)\{\alpha, i\infty\} = \{p\alpha, \alpha\} + \sum_{k=0}^{p-1} \{\frac{\alpha + k}{p}, \alpha\}$$ pour tout nombre premier $p$, et tout $\alpha \in \mathbb{Q}$.

Démonstration. Les deux affirmations proviennent directement de la formule (1).

Etant donnée une paramétrisation de Weil $\varphi$ , les formules ci-dessus se traduisent ainsi :

$$(5) \qquad N_p\varphi(I) = \sum_{k=0}^{p-1} \varphi\left(\frac{k}{p}\right) \qquad \text{dans } H_1(E, \mathbb{R})$$

$$(6) \qquad -N_p\varphi(\alpha, i\infty) = \varphi(p\alpha, \alpha) + \sum_{k=0}^{p-1} \varphi\left(\frac{\alpha+k}{p}, \alpha\right)$$

où $N_p = 1 + p - \lambda_p$ .

THÉORÈME 1 (Manin [5]).- Soient $\varphi : X_0(N) \to E$ une paramétrisation (faible) de Weil, et $\alpha \in X_0(N)$ une pointe. Alors $\varphi(\alpha)$ est d'ordre fini dans $E$ . Le symbole modulaire prend ses valeurs dans $H_1(E, \mathbb{Q})$ .

Démonstration.

L'argument de Manin est très beau. Il suffit de montrer que $\varphi(\alpha, i\infty) \in H_1(E, \mathbb{Q}) \subset H_1(E, \mathbb{R})$ pour n'importe quelle pointe $\alpha \in \mathbb{Q}$ . Pour cela, on regarde la formule (6). Si l'on peut trouver un nombre premier $p \nmid N$ tel que chaque terme qui apparaît dans le membre de droite de (6) se trouve dans $H_1(E, \mathbb{Z})$ , on a gagné, parce que $N_p$ ( = nombre de points rationnels de $E$ sur $\mathbb{F}_p$ ) est un entier positif.

On cherche alors, des nombres premiers $p$ tels que

$$(7) \qquad \alpha \underset{\Gamma_0(N)}{\sim} p\alpha \,, \qquad \alpha \underset{\Gamma_0(N)}{\sim} \frac{\alpha+k}{p} \quad (k \text{ entier}).$$

Mais les conditions nécessaires et suffisantes pour que $\alpha$ et $\alpha' \in \mathbb{Q}$ soient équivalents sous $\Gamma_0(N)$ sont faciles à décrire ([5] 2.2) :

(i) il y a une factorisation $N = n.m$ telle que $\alpha, \alpha'$ s'expriment en fractions réduites $\alpha = \frac{u}{vn}$ $\alpha' = \frac{u'}{v'n}$ $(vv', N) = 1$ ,

(ii) $uv \equiv u'v' \mod (n,m)$ .

La démonstration se termine en constatant que, lorsque $p \equiv 1 \bmod N$, les conditions (7) sont satisfaites pour $\alpha$ et $\alpha' = p\alpha$, $\frac{\alpha + k}{p}$.

Remarques.- Dans certains cas particuliers, on a des renseignements plus précis sur l'ordre de $\varphi(\alpha)$. Par exemple, un calcul récent de Ogg [7] montre que, lorsque $N$ est un nombre premier, le diviseur $(0) - (i\infty)$ est d'ordre :

$$\text{numérateur } [(N-1)/12]$$

dans la jacobienne $J_0(N)$.

## § 7. L'arithmétique Modulo p d'une courbe de Weil

Considérons la courbe complexe $X(N) = \Gamma(N)\backslash\bar{U}$ qui est un revêtement fini de $X_0(N)$. Le groupe $PSL(2, \mathbb{Z}/N)$ agit de façon naturelle sur $X(N)$. Posons

$$I = \{0, i\infty\} \in H_1(X(N), \mathbb{R})$$

et
$$I^\tau = \tau(\{0, i\infty\}) = \{\tau(0), \tau(i\infty)\} = \{\frac{b}{d}, \frac{a}{c}\} \in H_1(X(N), \mathbb{R}),$$

pour
$$\tau = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in PSL(2, \mathbb{Z}/N).$$

En projetant dans l'homologie de $X_0(N)$, on obtient une application

$$\Gamma_0(N)\backslash PSL(2, \mathbb{Z}/N) = \mathbb{P}^1(\mathbb{Z}/N) \to H_1(X_0(N), \mathbb{Q})$$

$$\tau \mapsto I^\tau = \{\tau(0), \tau(i\infty)\} = \{\frac{b}{d}, \frac{a}{c}\}.$$

Les relations satisfaites par cette application peuvent être décrites agréablement au moyen des matrices

$$s = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad t = \begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix}$$

d'ordre 2 et 3 respectivement. On a

$$I^\tau + I^{\tau s} = 0$$

$$I^\tau + I^{\tau t} + I^{\tau t^2} = 0$$

### (a) Matrices de Heilbronn de niveau $\ell$

Par une "matrice de Heilbronn de niveau $\ell$ " on entend une expression en

entiers

$$\sigma : \ell = xx' + yy' \quad ; \quad (x,y) = (x',y') = 1 \quad ; \quad x > y > 0 \quad ; \quad x' > y' \geq 0 .$$

Si $y' = 0$, on exige que $x = \ell$, $x' = 1$, et que $1 \leq y \leq \ell/2$.

A une telle expression $\sigma$ on associe la matrice dans $SL(2, \mathbb{Z}[\frac{1}{\ell}])$ désignée par la même lettre

$$\sigma = \begin{pmatrix} y'/\ell & -x'/\ell \\ x & y \end{pmatrix} .$$

Lorsque $\ell$ est premier à $N$, on définit

$$I^{\sigma} = I^{\bar{\sigma}} \in H_1(X_o(N), \mathbb{Q})$$

où $\bar{\sigma}$ est l'image de la matrice $\sigma$ dans $PSL(2, \mathbb{Z}/N)$.

(b) Formule de Réciprocité de Manin

Si $p$ est un nombre premier qui ne divise pas $2N$, alors

$$(\sum_{\sigma} I^{\sigma})^{+} = (1 + p - T_p)I \in H_1(X_o(N), \mathbb{Q})^{+}$$

où $\sigma$ parcourt les matrices de Heilbronn de niveau $p$, et $+$ signifie la symétrisation par la conjugaison complexe.

Remarque.- Soit $\varphi : X_o(N) \to E$ une paramétrisation faible de Weil. Considérons la fonction

$$y : \Gamma_o(N) \backslash PSL(2, Z/N) = \mathbb{P}^1(Z/N) \to \mathbb{Z}$$

qui est définie par la règle $y(\tau) = \varphi^{+}(I^{\tau})$.

En appliquant la fonction $\varphi^{+}$ à la formule ci-dessus on en tire

COROLLAIRE.-

$$\sum_{\sigma} y(\sigma) = N_p \cdot \varphi(I) \qquad \text{pour n'importe quel nombre premier } p \nmid N .$$

(La sommation porte sur toutes les matrices de Heilbronn de niveau $p$.)

Notons que le corollaire nous donne un moyen de calculer les $N_p$ dans le cas où $\varphi(I) \neq 0$. La formule est assez efficace en pratique parce que la fonc-

tion $y$ associée à la courbe de Weil faible $E$ est très facile à trouver pour les petites valeurs de $N$ .

D'après les conjectures de Birch et Swinnerton-Dyer, $\varphi(I)$ n'est pas nul si et seulement si $E$ ne possède qu'un nombre fini de points rationnels sur $\mathbb{Q}$ .

(c) Démonstration de la Formule de Réciprocité

Définissons les polynômes $[C_1,C_2,\ldots,C_n] \in \mathbb{Z}[C_1,C_2,\ldots,C_n]$ par :

$$[\ ] = 1 \quad , \quad [C_1] = C_1 \quad , \quad [C_1,C_2] = C_2C_1 + 1$$

$$[C_1,\ldots,C_n] = C_n[C_1,\ldots,C_{n-1}] + [C_1,\ldots,C_{n-2}] \qquad \text{pour } n \geq 3 .$$

Heilbronn [3] démontre par récurrence la formule

$$(8) \qquad [C_1,\ldots,C_n] = [C_1,\ldots,C_m][C_{m+1},\ldots,C_n] + [C_1,\ldots,C_{m-1}][C_{m+2},\ldots,C_n]$$

pour $1 \leq m < n$ .

La relation entre ces polynômes et les fractions continues est la suivante :

Ecrivons

$$a/\ell = \cfrac{1}{c_1 + \cfrac{1}{c_2 + \cfrac{1}{\ddots + \cfrac{1}{c_n}}}} \qquad c_n \geq 2$$

où $(a\,,\,\ell) = 1$ , $0 < a < \ell/2$ . On a $c_1 \geq 2$ . Afin d'indiquer sa dépendance de $a/\ell$ , écrivons $n = n(a/\ell)$ .

On trouve facilement

$$a = [c_2,\ldots,c_n] \quad ; \quad \ell = [c_1,\ldots,c_n] .$$

Si $0 < a < \ell/2$ , $(a\,,\,\ell) = 1$ , et si $0 \leq j < n(a/\ell)$ , on peut associer au couple $(a/\ell\,,\,j)$ une matrice de Heilbronn $\sigma_{(a/\ell\,,\,j)}$ de niveau $\ell$ par la règle

$$x = [c_1,\ldots,c_{n-j}] \qquad y = [c_1,\ldots,c_{n-j-1}]$$

$$x' = [c_n,\ldots,c_{n-j+1}] \qquad y' = [c_n,\ldots,c_{n-j+2}]$$

(où, par convention, $y' = 0$ si $j = 0$ ).

Il est facile de voir que cette règle établit une correspondance biunivoque entre de tels couples et les matrices de Heilbronn de niveau $\ell$ :

$$(a/\ell\ ,\ j) \longmapsto \sigma_{(a/\ell\ ,\ j)} .$$

On a alors, pour $\ell$ premier et impair :

$$\sum_{0<a<\ell} \{a/\ell\} = \sum_{0<a<\ell/2} \{a/\ell\}^+ = \Big( \sum_{0<a<\ell/2} \sum_{j=0}^{n(a/\ell)-1} I^{\sigma_{(a/\ell\ ,\ j)}} \Big)^+$$

$$= \Big( \sum_{\sigma} I^{\sigma} \Big)^+$$

où, dans la dernière sommation, $\sigma$ parcourt les matrices de Heilbronn de niveau $\ell$. La formule de réciprocité provient de là et de la formule (5).

## § 8. Le Symbole modulaire et l'arithmétique globale d'une courbe de Weil

Soit $\varphi : X_o(N) \to E$ une paramétrisation de Weil. La première motivation pour la construction du symbole modulaire était de trouver une façon finie d'exprimer les valeurs $L(E\ ,\chi\ ,1)$ pour les caractères de Dirichlet $\chi$ .

On choisit la définition suivante de la série $L$ de $E$ , tordue par $\chi$ :

$$L(E\ ,\chi\ ,s) = \sum_{n=1}^{\infty} \chi(n)\lambda(n)\cdot n^{-s}$$

où les $\lambda(n)$ sont les coefficients de la "new form" $\Omega$ (§ 5, Lemme 2) telle que $\varphi^*\omega = c\cdot\Omega$ .

Voici l'énoncé :

Pour un caractère de Dirichlet non trivial $\chi$ de conducteur $m$ premier à $N$ , posons $G(\chi) = \sum_{a \bmod m} \bar{\chi}(a)\varphi(a/m) \in H_1(E\ ,\mathbb{Z})$ . On peut plonger $H_1(E\ ,\mathbb{Z})$ dans $\mathbb{C}$ par intégration de la différentielle de Néron, et :

THÉORÈME 2 ([2], [5]).- *Si $\chi$ est non trivial,*

$$c\cdot L(E\ ,\chi\ ,1) = \chi(-1)g(\chi)\cdot\frac{G(\chi)}{m}$$

*où $g(\chi)$ est la somme de Gauss,* $g(\chi) = \sum_{b \bmod m} \chi(b)e^{2\pi i\frac{b}{m}}$ .

Pour le caractère trivial, on a :

THÉORÈME 3.- $c \cdot L(E, 1) = \varphi(I)$ .

Il est instructif de réécrire la conjecture de Birch et Swinnerton-Dyer pour les courbes de Weil en termes de la fonction $\varphi$ . Pour cela, nous prenons un point de vue géométrique qui sera développé dans un article (en préparation) de Swinnerton-Dyer et moi-même [10].

Considérons $I = \{iy \mid 0 \leq y \leq \infty\}$ comme intervalle orienté de $i\infty$ à $0$ , qui est contenu dans le lieu réel de la courbe $X_0(N)$ . L'arc $I \subset X_0(N)$ est appelé le chemin fondamental.

Puisque la paramétrisation de Weil $\varphi : X_0(N) \to E$ est définie sur $\mathbb{R}$ , $\varphi$ envoie le chemin fondamental dans la composante neutre du lieu réel de $E$ qui est un cercle orienté. Par définition, $\varphi(i\infty) = 0 \in E$ , et d'après le théorème 1, $\varphi(0)$ est d'ordre fini dans $E$ . Si l'on écrit $\varphi(I) = M \cdot \int_{E(\mathbb{R})} \omega$ , alors $M$ est un nombre rationnel qui s'interprète comme le "nombre d'enroulements" du chemin fondamental autour de $E(\mathbb{R})$ par l'application $\varphi$ .

On appelle $M$ le nombre d'enroulements de la courbe de Weil $E$ .

Conjecture (faible) de Birch et Swinnerton-Dyer

1) $M = 0$ si et seulement si $E(\mathbb{Q})$ est infini.

2) Si $M \neq 0$ , on a la formule

$$M = \pm c \prod_p n_p \cdot [Ш] / \eta^2$$

où $[Ш]$ est l'ordre du groupe de Shafarévitch-Tate de $E$ , $\eta = [E(\mathbb{Q})]$ , et $n_p$ est le nombre de composantes rationnelles de la fibre de Néron de $E$ sur $\mathbb{F}_p$ .

Observons que, si le nombre d'enroulements de $\varphi : I \to E(\mathbb{R})$ est nul, il est nécessaire que $\varphi$ possède au moins un point critique sur $I$ . Appelons ces points

les points critiques fondamentaux de $E$ . Le résultat suivant n'est pas difficile à démontrer :

THÉORÈME 4.- L'ordre de zéro de $L(E, s)$ au point $s = 1$ est inférieur ou égal au nombre de points critiques fondamentaux de $E$ .

(A paraître dans [10].)

En supposant la vérité de la conjecture de Birch et Swinnerton-Dyer, on obtient que le rang de $E(\mathbb{Q})$ est inférieur ou égal au nombre de points critiques fondamentaux de $E$ .

Pour chaque point critique $P \in I'$, considérons $\varphi(P) \in E$ qui est évidemment rationnel sur un corps algébrique. Posons $Tr(P)$ = somme des $\mathbb{Q}$-conjugués de $\varphi(P)$ dans $E$ ; c'est un point de $E(\mathbb{Q})$ . Soit $E^*(\mathbb{Q}) \subset E(\mathbb{Q})$ le sous-groupe engendré par les $Tr(P)$ où $P$ parcourt les points critiques fondamentaux. Il serait intéressant de déterminer la structure du sous-groupe $E^*(\mathbb{Q})$ .

Exemple.- Parmi les 18 courbes de Weil provenant de la table du § 1, il n'y en a qu'une qui possède un nombre infini de points rationnels. Elle est de conducteur analytique 37 , et d'équation

$$E : \quad y^2 + y = x^3 - x , \qquad \text{cf. [10].}$$

Elle ne possède qu'un point critique fondamental qui est rationnel sur $\mathbb{Q}(\sqrt{37})$ .

D'après le théorème 4, la vérité de la conjecture de Birch et Swinnerton-Dyer entraîne que $E(\mathbb{Q})$ est de rang 1 . On peut vérifier que $E(\mathbb{Q})$ ne possède pas de torsion. On montre [10] que $E^*(\mathbb{Q})$ est engendré par le point $(6, -15)$ qui est divisible par 6 dans $E(\mathbb{Q})$ .

Pour la jolie histoire des douze courbes de Weil de la forme $X_o(N)$ (où genre $\{X_o(N)\} = 1$ ) , le lecteur doit se reporter à l'article de G. Ligozat (Courbes Modulaires de genre 1 ) à paraître.

BIBLIOGRAPHIE

[1] A. ATKIN, J. LEHNER - Hecke Operators on $\Gamma_0(N)$ , Math. Annalen, Bd. 185, n° 2 (1970), 134-160.

[2] B. BIRCH - Elliptic Curves : A Progress report, Summer conference on number theory sponsored by the Amer. Math. Soc. at Stony Brook (1971).

[3] H. HEILBRONN - Average Length of a class of Continued Fractions, Abh. aus Zahlentheorie und Anal., London, Plenum.

[4] J. IGUSA - Kroneckerian Models of fields of elliptic modular functions, Amer. J. of Math., 81 (1959), p. 561-577.

[5] Y. MANIN - Points paraboliques et fonctions zêta des courbes modulaires [en russe], Izv. Akad. Nauk, 36 (1972), p. 19-66.

[6] A. OGG - Elliptic Curves and Wild Ramification, Amer. J. of Math, 89 (1967), p. 1-21.

[7] A. OGG - Rational Points on certain elliptic modular curves, (à paraître).

[8] J.-P. SERRE - Abelian $\ell$-adic representations and elliptic curves, New York, Benjamin, 1968.

[9] G. SHIMURA - Introduction to the Arithmetic Theory of Automorphic Functions, Math. Soc. Japan, 11 (1971), Princeton Univ. Press.

[10] B. MAZUR and H. P. F. SWINNERTON-DYER - The p-adic L-series of elliptic curves, (en préparation).

[11] A. WEIL - Über die Bestimmung Dirichletscher Reihe durch Funktionalgleichungen, Math. Ann., 168 (1967), p. 149-156.