Séminaire Delange-Pisot-Poitou.
Théorie des nombres

JACQUES VÉLU

Lois de réciprocité liées aux courbes elliptiques

Séminaire Delange-Pisot-Poitou. Théorie des nombres, tome 14, n° 1 (1972-1973), exp. n° 9, p. 1-5

<http://www.numdam.org/item?id=SDPP_1972-1973__14_1_A7_0>

Séminaire DELANGE-PISOT-POITOU
(Théorie des nombres)
14e année, 1972/73, n° 9, 5 p.

11 décembre 1972

LOIS DE RÉCIPROCITÉ LIÉES AUX COURBES ELLIPTIQUES

par Jacques VÉLU

1. Introduction.

Pour tout nombre premier p, appelons N_p le nombre de solutions sur le corps $\underset{\sim}{F}_p$ de l'équation :

$$y^2 + xy + y = x^3 + x^2 - 8x + 6 .$$

Un calcul donne les valeurs suivantes :

p	11	13	17	19	23	29	31	37	41	43	47	53	59	61
N_p	11	11	15	25	20	22	33	29	46	50	47	59	69	68

Nous pouvons constater sur ces valeurs la propriété suivante :

$$(1) \qquad \begin{cases} \text{Si } p \equiv \pm 2^a \pmod{35} , \\ \text{alors } N_p \equiv p(1 - 14^a) - 8^a \pmod{37} . \end{cases}$$

Par exemple pour $p = 11 \equiv 2^8 \pmod{35}$, on a

$$\begin{aligned} N_p = 11 &\equiv 11(1 - 14^8) - 8^8 \pmod{37} \\ &\equiv 11(1 - 26) - 10 \\ &\equiv 11 + 11^2 - 10 \equiv 11 \end{aligned}$$

Nous allons expliquer pourquoi les congruences (1) sont vraies pour tout p.

2. Rappel sur les courbes elliptiques [1].

(A) Une courbe elliptique $\mathcal{E}$, définie sur un corps k, admet un modèle affine non singulier du type

$$(2) \qquad y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6 \quad \text{avec les } a_i \in k .$$

Pour tout corps $K \supset k$, l'ensemble $\mathcal{E}(K)$ des points de $\mathcal{E}$ définis sur K est muni d'une structure de groupe abélien de la façon suivante :

(i) le point à l'infini de $\mathcal{E}$ est l'élément neutre ;

(ii) $P_1 + P_2 + P_3 = 0 \iff P_1 , P_2 , P_3$ alignés.

Si $P = P_1 + P_2$ et si, avec le modèle (2), les coordonnées de P (resp. de P_i) sont (x , y) (resp. (x_i , y_i)), alors

$$x = \varphi(x_1 , y_1 , x_2 , y_2) , \quad y = \psi(x_1 , y_1 , x_2 , y_2)$$

où φ et $\psi \in k(X , Y , Z , T)$.

(B) Pour tout K, les points d'ordre fini du groupe $\mathcal{E}(K)$ sont algébriques sur k, donc appartiennent à $\mathcal{E}(\overline{k})$, $\overline{k}$ désignant la clôture algébrique de k. On démontre que, si k est de caractéristique 0, le sous-groupe $\mathcal{E}_N$ des points d'ordre N de $\mathcal{E}(\overline{k})$ est isomorphe à $(\underset{\sim}{Z}/N\underset{\sim}{Z})^2$. A tout couple $(\mathcal{E}, N)$ on associe une extension $k(\mathcal{E}_N)$ en adjoignant à k les coordonnées des points de $\mathcal{E}_N$. On a le théorème :

(i) $k(\mathcal{E}_N)/k$ est galoisienne ;

(ii) $\mathrm{Gal}(k(\mathcal{E}_N)/k) \subseteq \longrightarrow \mathrm{Aut}[(\underset{\sim}{Z}/N\underset{\sim}{Z})^2]$.

3. Rappels sur la théorie du corps de classes.

Soit K une extension finie galoisienne de $\underset{\sim}{Q}$. L'ensemble des nombres premiers ramifiés dans K est fini, et quand p n'est pas ramifié et se prolonge par l'idéal $\mathfrak{p}$ de K, on associe à $\mathfrak{p}$ un élément $\sigma_{\mathfrak{p}}$ de $\mathrm{Gal}(K/\underset{\sim}{Q})$, son "frobenius" défini par la condition que, pour tout entier a de K, $\sigma_{\mathfrak{p}}(a) = a^p \bmod \mathfrak{p}$. La loi de réciprocité consiste à décrire l'application $\mathfrak{p} \longmapsto \sigma_{\mathfrak{p}}$. Quand $\mathfrak{p}$ et $\mathfrak{p}'$ prolongent p dans K, $\sigma_{\mathfrak{p}}$ et $\sigma_{\mathfrak{p}'}$ sont conjugués dans $\mathrm{Gal}(K/\underset{\sim}{Q})$. Si L est une extension galoisienne de K et si P prolonge $\mathfrak{p}$ dans L, la restriction de σ_P à K est $\sigma_{\mathfrak{p}}$.

Si $\mathrm{Gal}(K/\underset{\sim}{Q})$ est abélien, la théorie du corps de classes permet de décrire l'application $\mathfrak{p} \longmapsto \sigma_{\mathfrak{p}}$. En effet, quand $\mathfrak{p}$ et $\mathfrak{p}'$ prolongent p, $\sigma_{\mathfrak{p}} = \sigma_{\mathfrak{p}'}$, et l'application $p \longmapsto \sigma_{\mathfrak{p}}$ est bien définie. On étend cette application à tout entier positif non divisible par un nombre premier ramifié en posant

$$\sigma_{\prod p_i^{\alpha_i}} = \prod (\sigma_{p_i})^{\alpha_i} .$$

Le théorème de la loi de réciprocité d'Artin entraîne que :

(i) l'application $n \longmapsto \sigma_n$ est surjective,

(ii) il existe un entier m divisible seulement par des nombres premiers ramifiés tel que

$$n_1 \equiv n_2 \pmod m \Rightarrow \sigma_{n_1} = \sigma_{n_2}$$

Autrement dit, $n \longmapsto \sigma_n$ est un homomorphisme surjectif de $(\underset{\sim}{Z}/m)^\times$ dans $\mathrm{Gal}(K/\underset{\sim}{Q})$.

4. Interprétation du nombre N_p [3].

Soit $\mathcal{E}$ une courbe elliptique définie sur $\underset{\sim}{Q}$, et soit ℓ un nombre premier. L'extension $k(\mathcal{E}_\ell)/k$ a pour groupe de Galois un sous-groupe de $GL(2, \underset{\sim}{F}_\ell)$ et nous allons donner une description de la loi de réciprocité de cette extension.

D'abord il faut connaître les nombres premiers ramifiés. On démontre que, si p est ramifié, ou bien $p = \ell$, ou bien p est un nombre premier de mauvaise réduc-

tion pour $\mathcal{E}$.

Rappelons qu'on dit qu'un nombre premier est de mauvaise réduction si, pour tout modèle de $\mathcal{E}$ du type (2) à coefficients entiers, la courbe réduite modulo p n'est pas une cubique non singulière. Ces nombres forment un ensemble fini, et il existe un algorithme permettant de les calculer. Dans l'exemple de l'introduction, les nombres premiers de mauvaise réduction sont 5 et 7 .

Maintenant il faut voir ce que donne la loi de réciprocité. Quand p et p' prolongent p , les matrices σ_p et $\sigma_{p'}$ sont conjuguées dans $GL(2 , \underset{\sim}{F}_\ell)$, donc ont le-même polynôme caractéristique :

$$X^2 - \operatorname{tr} \sigma_p \, X + \det \sigma_p \in \underset{\sim}{F}_\ell [X] .$$

On démontre les congruences :

$$(3) \qquad \begin{cases} \det (\sigma_p) \equiv p \pmod{\ell} \\ \operatorname{tr} (\sigma_p) \equiv p - N_p \pmod{\ell} \end{cases}$$

Remarque. - Ce théorème ne donne pas une description complète de l'application $p \longmapsto \sigma_p$, car deux matrices ayant même polynôme caractéristique ne sont pas nécessairement conjuguées (exemple $\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ et $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$).

5. Retour à l'exemple de l'introduction.

Nous prenons pour E la courbe elliptique

$$y^2 + xy + y = x^3 + x^2 - 8x + 6 \quad \text{et} \quad \ell = 37 .$$

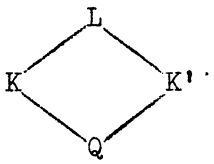
Cette courbe se rencontre dans l'étude de certaines formes modulaires [2], on montre qu'elle a un sous-groupe cyclique à 37 éléments, stable par $\operatorname{Gal}(\overline{\underset{\sim}{Q}}/\underset{\sim}{Q})$, i. e. il existe un point A de $E(\overline{\underset{\sim}{Q}})$ d'ordre 37 tel que $\{0 , A , 2A , \ldots , 36A\}$ soit stable par conjugaison. Si nous prenons ce point A comme premier vecteur de base de l'espace vectoriel E_{37} de dimension 2 sur $\underset{\sim}{F}_{37}$, le groupe

$$\operatorname{Gal}(\underset{\sim}{Q}(E_{37})/\underset{\sim}{Q})$$

est isomorphe à un sous-groupe du groupe des matrices de la forme $\left(\begin{smallmatrix} \alpha & \beta \\ 0 & \alpha' \end{smallmatrix}\right)$. Posons $\underset{\sim}{Q}(E_{37}) = L$ et $\underset{\sim}{Q}(A) = K$; la restriction de $\left(\begin{smallmatrix} \alpha & \beta \\ 0 & \alpha' \end{smallmatrix}\right)$ à K est $A \longmapsto \alpha A$, et le corps K est le corps laissé fixe par le noyau de l'homomorphisme $\left(\begin{smallmatrix} \alpha & \beta \\ 0 & \alpha' \end{smallmatrix}\right) \longmapsto \alpha$. De même, appelons K' le corps laissé fixe par le noyau de l'homomorphisme

$$\left(\begin{smallmatrix} \alpha & \beta \\ 0 & \alpha' \end{smallmatrix}\right) \longmapsto \alpha' .$$

Nous avons :



et

$$\operatorname{Gal}(K/\underset{\sim}{Q}) \subset \underset{\sim}{F}_{37}^{\times} \quad \text{et} \quad \operatorname{Gal}(K'/\underset{\sim}{Q}) \subset \underset{\sim}{F}_{37}^{\times} .$$

Soient P un idéal premier de L, $\mathfrak{p}$ sa restriction à K, $\mathfrak{p}'$ sa restriction à K', p sa restriction à $\underset{\sim}{Q}$. Si $p \neq 5, 7, 37$, le frobenius $\begin{pmatrix} \alpha_p & \beta_p \\ 0 & \alpha'_p \end{pmatrix}$ de P existe, tandis que α_p est le frobenius de $\mathfrak{p}$ et α'_p celui de $\mathfrak{p}'$. Nous pouvons appliquer le théorème d'Artin aux extensions abéliennes K et K', il existe a, b, c (resp. a', b', c') tels que $p \longmapsto \alpha_p$ (resp. $p \longmapsto \alpha'_p$) soit un homomorphisme de $(\underset{\sim}{Z}/5^a.7^b.37^c)^\times$ (resp. $(\underset{\sim}{Z}/5^{a'}.7^{b'}.37^{c'})^\times$) dans $\underset{\sim}{F}_{37}^\times$. Pour obtenir les congruences (1), il n'y a qu'à déterminer ces homomorphismes. Pour chaque valeur de p,

$$\alpha_p + \alpha'_p \equiv p - N_p \pmod{37} \quad \text{et} \quad \alpha_p \alpha'_p \equiv p \pmod{37}.$$

En conséquence, appelons x_p et x'_p les solutions dans $\underset{\sim}{F}_{37}$ de

$$X^2 - (p - N_p) X + p = 0,$$

car on ne sait pas qui est α_p, et qui est β_p. Nous sommes aidés par l'étude de la courbe elliptique sur le corps 37-adique $\underset{\sim}{Q}_{37}$ qui montre que l'une des deux extensions K ou K' n'est pas ramifiée en 37. En fait on pourrait même dire laquelle [4]. Dans ces conditions, appelons χ celui des deux homomorphismes $p \longmapsto \alpha_p$ ou $p \longmapsto \alpha'_p$ qui n'est pas ramifié en 37, l'autre est $\chi' : p \longmapsto p/\chi(p)$. Nous avons

$$\chi : (\underset{\sim}{Z}/5^a\,7^b)^\times \to \underset{\sim}{F}_{37}^\times .$$

Or

$$\begin{aligned}(\underset{\sim}{Z}/5^a.7^b)^\times &\simeq (\underset{\sim}{Z}/5)^\times.\underset{\sim}{Z}/5^{a-1}.(\underset{\sim}{Z}/7)^\times.\underset{\sim}{Z}/7^{b-1} \\ &\simeq \underset{\sim}{Z}/4.\underset{\sim}{Z}/5^{a-1}.\underset{\sim}{Z}/6.\underset{\sim}{Z}/7^{b-1}\end{aligned}$$

et comme $\underset{\sim}{F}_{37}^\times \simeq \underset{\sim}{Z}/36 \simeq \underset{\sim}{Z}/4 * \underset{\sim}{Z}/9$, on a nécessairement $a = b = 1$. Le même raisonnement montre que $a' = b' = c' = 1$. Tout revient donc à trouver le caractère

$$\chi : (\underset{\sim}{Z}/35)^\times \to \underset{\sim}{F}_{37}^\times .$$

Nous remarquons que l'image de χ doit être formée d'éléments d'ordre 12 dans $\underset{\sim}{F}_{37}^\times$ en raison des ordres de $(\underset{\sim}{Z}/35)^\times$ et $\underset{\sim}{F}_{37}^\times$, et que $(\underset{\sim}{Z}/35)^\times \simeq \underset{\sim}{Z}/2 \times \underset{\sim}{Z}/12$; plus précisément, dans $(\underset{\sim}{Z}/35)^\times$, tout élément s'écrit $\pm 2^a$.

Prenons $p = 2$, nous avons $x_2 = 8$, $x'_2 = 28$, seul 8 est d'ordre divisant 12 dans $\underset{\sim}{F}_{37}^\times$, donc nécessairement

$$\chi(2) = 8 \quad \text{et} \quad \chi'(2) = \frac{2}{8} = 28 ;$$

ce qui donne $\chi(2^a) \equiv 8^a \pmod{37}$. Reste à déterminer $\chi(-1)$; pour cela, nous remarquons que $13 \equiv -2^9 \pmod{35}$, donc $\chi(13) = \chi(-1)\,\chi(2)^9$; mais comme $x_{13} = 6$, $x'_{13} = 33$, et que seul 6 est d'ordre divisant 12 dans $\underset{\sim}{F}_{37}^\times$,

$$\chi(13) = 6 \equiv 8^9 \pmod{37},$$

d'où $\chi(-1) = 1$, la détermination de χ et χ' : Si $p \equiv \pm 2^a \pmod{35}$,

$$\chi(p) \equiv 8^a \pmod{37}, \quad \chi'(p) \equiv \frac{p}{8^a} \equiv 14^a\, p \pmod{37},$$

et les congruences (1).

6. Cas général.

Dans le cas où on a une courbe elliptique E munie d'un point A d'ordre ℓ, défini sur $\overline{\mathbb{Q}}$ tel que $\{0, A, 2A, \ldots, (\ell-1)A\}$ soit invariant par conjugaison, une base convenable de E_ℓ permet encore d'écrire $\mathrm{Gal}(\mathbb{Q}(E_\ell)/\mathbb{Q})$ comme sous-groupe du groupe $\begin{pmatrix} \alpha & \beta \\ 0 & \alpha' \end{pmatrix}$. On a encore deux homomorphismes

$$\begin{pmatrix} \alpha & \beta \\ 0 & \alpha' \end{pmatrix} \longmapsto \alpha$$
$$\begin{pmatrix} \alpha & \beta \\ 0 & \alpha' \end{pmatrix} \longmapsto \alpha' ,$$

et on peut encore trouver deux nombres m et m' tels que $p \longmapsto \alpha_p$ et $p \longmapsto \alpha'_p$ soient deux caractères sur $(\mathbb{Z}/m\mathbb{Z})^\times$ et $(\mathbb{Z}/m'\mathbb{Z})^\times$ respectivement, donc en fait trouver un caractère $\chi : (\mathbb{Z}/m\mathbb{Z})^\times \to \mathbb{F}_\ell^\times$ tel que

$$N_p \equiv p - \left[\lambda(p) + \frac{p}{\chi(p)}\right] \pmod{\ell} .$$

SERRE a montré que, réciproquement, de telles congruences entraînent l'existence d'un point A de $E(\overline{\mathbb{Q}})$ ayant les propriétés voulues. On a ainsi un moyen de prouver l'inexistence d'un tel point A, ou que lorsqu'on vérifie de telles congruences pour beaucoup de p, on a des présomptions d'existences de A. Il serait intéressant de rendre ces méthodes effectives, i. e. dire jusqu'à quelle valeur de p il faut les vérifier pour être sûr de l'existence de A.

Faisons une dernière remarque, nous avons expliqué comment calculer dans le frobenius de P, $\begin{pmatrix} \alpha_p & \beta_p \\ 0 & \alpha'_p \end{pmatrix}$, les nombres α_p et α'_p, mais nous n'avons rien dit au sujet de β_p. Dans certains cas particuliers, il est possible de voir que $\beta_p = 0$, ce qui signifie qu'en fait E_ℓ contient deux sous-groupes invariants par $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ mais ce n'est pas toujours le cas, et tant qu'on ne connaît pas β_p, on ne connaît pas l'ordre de $\begin{pmatrix} \alpha_p & \beta_p \\ 0 & \alpha'_p \end{pmatrix}$ et, par conséquent, la décomposition de p.

BIBLIOGRAPHIE

[1] LANG (S.). - Algebraic number theory. - Reading, Addison-Wesley publishing Company, 1968 (Addison-Wesley Series in Mathematics).

[2] MAZUR (B.) and SWINNERTON-DYER (H. P. F.). - Arithmetic of Weil curves (à paraître).

[3] SERRE (J.-P.). - Abelian ℓ-adic representations and elliptic curves. - New York, W. A. Benjamin, 1968.

[4] SERRE (J.-P.). - Propriétés galoisiennes des points d'ordre fini des courbes elliptiques, Invent. Math., Berlin, t. 15, 1972, p. 259-331.

(Texte reçu le 18 décembre 1972)

Jacques VELU
3 Résidence du Parc
91120 PALAISEAU