SÉMINAIRE N. BOURBAKI

SERGE LANG

Sur la conjecture de Birch-Swinnerton Dyer

Séminaire N. Bourbaki, 1978, exp. n° 503, p. 189-200

<http://www.numdam.org/item?id=SB_1976-1977__19__189_0>

Séminaire BOURBAKI
29e année, 1976/77, n° 503

503-01
Juin 1977

SUR LA CONJECTURE DE BIRCH-SWINNERTON DYER

[d'après J. COATES et A. WILES]

par Serge LANG

§ 1. Résultat de Coates-Wiles

Nous nous proposons de résumer la démonstration de Coates-Wiles du théorème suivant.

> Soit A une courbe elliptique avec multiplication complexe par l'anneau des entiers $\mathfrak{o} = \mathfrak{o}_K$ d'un corps quadratique imaginaire K. Supposons A définie sur K et $\mathfrak{o}$ principal. Soit ζ_A la fonction zêta associée à A. Si A possède un point rationnel sur K d'ordre infini, alors $\zeta_A(1) = 0$.

Comme on sait (Deuring), on peut exprimer ζ_A essentiellement comme fonction L de Hecke, voir par exemple [L], chapitre X, § 4. Nous ne voulons pas entrer dans une discussion de cette question. Par conséquent, nous définirons plutôt la fonction zêta de A comme suit.

Soit $\mathfrak{f}$ le conducteur de A. Soit

$$\exp : \mathbf{C}/\mathfrak{o} \to A_{\mathbf{C}}$$

l'application exponentielle, dont les coordonnées sont les fonctions de Weierstrass $\wp$ et $\wp'$, avec $g_2, g_3 \in \mathfrak{o}$. Si $\mathfrak{a}$ est un idéal, les points d'ordre $\mathfrak{a}$ sur A sont paramétrés par

$$\mathfrak{a}^{-1}\mathfrak{o}/\mathfrak{o} \xrightarrow{\exp} A_{\mathfrak{a}}.$$

Soit $\mathfrak{b}$ premier à $\mathfrak{f}\mathfrak{a}$, et soit $(\mathfrak{b},K)$ le symbole d'Artin sur le corps des points de torsion $K(A_{\mathfrak{a}})$. Il existe une fonction ψ définie sur les idéaux, telle que $\psi(\mathfrak{a})$ soit un générateur de $\mathfrak{a}$, et que le diagramme soit commutatif :

$$\begin{array}{ccc} \mathfrak{a}^{-1}\mathfrak{o} & \longrightarrow & A_{\mathfrak{a}} \\ {\scriptstyle \psi(\mathfrak{b})}\downarrow & & \downarrow{\scriptstyle (\mathfrak{b},K)} \\ \mathfrak{a}^{-1}\mathfrak{o} & \longrightarrow & A_{\mathfrak{a}} \end{array}.$$

La flèche verticale à gauche est la "multiplication par $\psi(\mathfrak{b})$". C'est un théorème que ψ est un caractère de Hecke. On définit

$$L(\psi^k, s) = \sum \frac{\psi^k(\mathfrak{a})}{\mathbf{N}\mathfrak{a}^s}$$

la somme étant prise sur les idéaux $\mathfrak{a}$ premiers à $\mathfrak{f}$.

Nous démontrons le théorème de Coates-Wiles sous la forme :

Si A possède un point rationnel sur K d'ordre infini, alors

$$L(\bar{\psi}, 1) = 0 .$$

Un théorème de Damerell [Da] dit que si Ω est une période engendrant le réseau L de A sur σ , autrement dit, $L = \sigma\Omega$, alors

$$\Omega^{-k} L(\bar{\psi}^k, k)$$

est algébrique, et dans K . On démontrera que ce nombre algébrique (pour $k = 1$) est divisible par une infinité d'idéaux premiers, et est donc égal à 0 . Dans un autre papier à paraître, Coates-Wiles montrent qu'en fait, si A possède r points rationnels sur K linéairement indépendants sur $\mathbb{Z}$, alors la fonction zêta p-adique a un zéro d'ordre r en $s = 1$. Il se trouve que la fonction zêta p-adique fournit des informations complexes (pour le moment) juste dans le cas précédent.

Il est facile de dire de façon plus précise quels sont les idéaux premiers qui diviseront le nombre algébrique en question. Un nombre premier p premier à $6\mathfrak{f}$ est dit normal si :

(i) p se décompose complètement dans K , i.e. $(p) = \mathfrak{p}\bar{\mathfrak{p}}$.

(ii) La complétion $K_{\mathfrak{p}}$ ne contient pas les racines p-ièmes de l'unité μ_p .

On voit facilement qu'il existe un nombre infini d'idéaux premiers normaux, et on démontrera que de tels idéaux premiers (suffisamment grands) divisent $\Omega^{-1} L(\bar{\psi}, 1)$.

C'est un exercice de démontrer la caractérisation suivante, qui ne sera pas employée dans la suite. Posons $\mathfrak{p} = (\pi)$, et

$$p = \pi\bar{\pi} .$$

Alors p est anormal si et seulement si $\pi + \bar{\pi} = 1$. Comme Serre l'a remarqué, la densité des nombres premiers anormaux est 0 .

§ 2. Réduction de la démonstration à un critère Kummérien

Notons A_{π^n} le groupe des points sur A annulés par π^n. Posons

$$K_n = K(A_{\pi^{n+1}}) , \qquad \text{donc} \quad K_o = K(A_\pi) .$$

Soit F_o une complétion de K_o au-dessus de $K_\mathfrak{p}$, donc $F_o = K_\mathfrak{p}(A_\pi)$, et $F_n = K_\mathfrak{p}(A_{\pi^{n+1}})$. Soient U_n les unités $\equiv 1$ (mod idéal maximal) dans F_n. Il existe un groupe d'unités $\mathcal{E}_n$ globales, dans K_n, qui sont les analogues des unités circulaires des corps cyclotomiques, et que nous décrirons plus bas. On note $\bar{\mathcal{E}}_n$ leur clôture dans U_n.

L'extension F_o sur $K_\mathfrak{p} = \mathbb{Q}_p$ est cyclique, de degré $p-1$. Soit w_o un générateur de Kummer, c'est-à-dire que $w_o^{p-1} \in \mathbb{Q}_p$ et $F_o = \mathbb{Q}_p(w_o)$. Le groupe de Galois $G_o = \mathrm{Gal}(F_o/\mathbb{Q}_p)$ opère via un caractère,

$$\sigma w_o = \chi(\sigma) w_o .$$

Si C est un groupe abélien sur lequel G_o opère, notons :

$$C(p) = C/C^p$$
$$C(p,k) = (C/C^p)(\chi^k) = \text{espace propre de } C(p) \text{ pour le caractère } \chi^k .$$

On a alors le critère suivant

Critère Kummérien. $(U_o/\bar{\mathcal{E}}_o)(p,k) \neq 0$ si et seulement si

$$\Omega^{-k} L(\bar{\psi}^k, k) \equiv 0 \mod \mathfrak{p} .$$

(Ici et dans la suite, on a pris $1 \leq k \leq p-2$.)

Le critère Kummérien n'a lui-même rien à voir avec l'existence d'un point d'ordre infini. Razar avait suggéré à Coates-Wiles qu'un tel critère devrait mener à $L(\bar{\psi},1) = 0$ s'il existe un point d'ordre infini. C'est ce qu'ont alors fait Coates-Wiles. En supposant l'existence d'un tel point P, on forme la tour $K_\infty = \bigcup K_n$, et $K_\infty\left(\frac{1}{\pi^{n+1}} P\right)$ qui est abélien sur K_n.

Un argument de théorie de Kummer facile montre que localement

$$\bigcup_n F_\infty\left(\frac{1}{\pi^{n+1}} P\right)$$

est une $\mathbb{Z}_p$-extension (groupe de Galois isomorphe à $\mathbb{Z}_p$) qui est presque totalement ramifiée (le groupe d'inertie est d'indice fini dans le groupe de Galois) au-dessus de $\mathfrak{p}$. Or la théorie du corps de classes relie l'existence d'extensions

abéliennes ramifiées avec la présence d'unités globales comme suit. Si $M_{\mathfrak{p}}(K_n)$ désigne l'extension maximale p-abélienne $\mathfrak{p}$-ramifiée de K_n, on a un isomorphisme

$$\mathrm{Gal}(M_{\mathfrak{p}}(K_n)/H_n) \approx U_{\mathfrak{p}}/\overline{\sigma_{\mathfrak{p}} E}$$

où H_n est le corps de classes de Hilbert, E est le groupe d'unités globales, et $U_{\mathfrak{p}}$ désigne les unités locales, dans $K_{n,\mathfrak{p}} = F_n$.

Un lemme de Nakayama montre que si $(U_o/\bar{\mathcal{E}}_o)(p,1) = 0$ alors $(U_n/\bar{\mathcal{E}}_n)(p,1) = 0$ (Iwasawa se sert de ce genre de lemme constamment dans sa théorie des corps cyclotomiques, e.g. [Iw]). L'existence de l'extension presque totalement ramifiée ci-dessus montre alors que le groupe des unités globales ne peut être trop grand, et en particulier que l'on a

$$(U_n/\bar{\mathcal{E}}_n)(p,1) \neq 0$$

pour n grand, donc $(U_o/\bar{\mathcal{E}}_o)(p,1) \neq 0$. On applique alors le critère de Kummer pour terminer la démonstration.

§ 3. Le cas cyclotomique classique

Le cas elliptique que nous désirons traiter est l'analogue du cas cyclotomique classique, que nous allons rappeler pour aider le lecteur à comprendre. On désire décrire la position des unités globales dans les unités locales. Soit w_o comme précédemment un générateur de Kummer de $Q_p(A_\pi)$, satisfaisant l'équation

$$w_o^p + \pi w_o = 0 ,$$

avec π d'ordre 1 en p. Donc $F_o = Q_p(w_o)$. Soit u une unité dans F_o et $g \in \sigma_p[[W]]$ une série de puissance telle que

$$u = g(w_o) .$$

Soit $\mathfrak{p}_o$ l'idéal premier dans F_o. Il est immédiat que $g'/g(w_o)$ est bien défini modulo $\mathfrak{p}_o^{p-2}$, dans σ_p. En particulier, si on écrit

$$g'/g(w_o) = \sum_{k=1}^{\infty} c_k w_o^{k-1} \quad \text{avec} \quad c_k \in \sigma_p ,$$

alors c_k est bien défini mod p pour $1 \leq k \leq p-2$, et l'on pose

$$\varphi_k(u) = c_k \mod p .$$

Alors $\varphi_k : \sigma_p^* \to \sigma_p/p\sigma_p = \mathbb{Z}_p/p\mathbb{Z}_p$ est un homomorphisme, dit de Kummer.

Les unités

$$1 - w_o^k \qquad \text{avec} \quad k = 1,2,\ldots$$

forment un système de générateurs topologiques des unités $\equiv 1 \mod \mathfrak{p}_o$. On va les orthogonaliser. Soit

$$e_k = \frac{1}{p-1} \sum_{\sigma \in G_o} \chi^{-k}(\sigma)\sigma$$

l'idempotent dans l'anneau du groupe $\mathbb{Z}_p[G_o]$ pour le caractère χ^k . Si u est une unité $\equiv 1 \mod w_o$, on définit u^t avec $t \in \mathbb{Z}_p$ de la manière évidente, à savoir $u^t = \lim u^m$ avec m dans $\mathbb{Z}$, approchant t p-adiquement. Nous poserons

$$\eta_k = (1 - w_o^k)^{e_k} \qquad \text{. pour } k = 1,\dots,p-1 \text{ .}$$

Alors :

(i) $\eta_k \equiv 1 - w_o^k \mod w_o^{k+1}$

(ii) $\sigma\eta_k = \eta_k^{\chi^k(\sigma)}$, c'est-à-dire $\eta_k \in U_o(k)$.

La deuxième propriété est évidente. Pour la première, on forme bêtement le produit

$$\begin{aligned} \eta_k &\equiv \prod (1 - w_o^k)^{-\chi^k(\sigma)\sigma} \mod w_o^{k+1} \\ &\equiv \prod (1 - \chi(\sigma)^k w_o^k)^{-\chi^{-k}(\sigma)} \\ &\equiv (1 + w_o^k)^{p-1} \\ &\equiv 1 - w_o^k \text{ .} \end{aligned}$$

Lemme.- Si j , $k = 1,\dots,p-2$, alors :

(i) $\varphi_k(\eta_j) = 0$ si $k \neq j$.

(ii) $\varphi_k(\eta_k) = -k \mod p$.

Si u est une unité $\equiv 1 \mod \mathfrak{p}_o$ et

$$u \equiv \eta_1^{t_1} \dots \eta_{p-2}^{t_{p-2}} \mod w_o^{p-1} \text{ ,}$$

alors

$$t_k \equiv -\frac{1}{k} \varphi_k(u) \mod p \text{ .}$$

Démonstration. On prend la dérivée logarithmique bêtement $d \log \eta_k / dw_o$, et les formules (i), (ii) en découlent immédiatement. La dernière assertion provient du fait que φ_k est un homomorphisme.

Soient $\mathcal{A} = \{a_i\}$ une famille finie d'entiers premiers à p, et $\mathcal{N} = \{n_i\}$ une famille d'entiers satisfaisant aux conditions

$$\prod a_i^{n_i} \equiv 1 \mod p \quad \text{et} \quad \sum n_i = 0 .$$

Soit

$$u = u(\mathcal{A}, \mathcal{N}) = \prod (\zeta^{a_i} - 1)^{n_i}$$

où ζ est une racine primitive p-ième de l'unité. Alors u est une unité dite cyclotomique. Ecrivons u en fonction des η_k comme dans le lemme.

THÉORÈME 3.1.- Si $u(\mathcal{A}, \mathcal{N}) = \eta_1^{t_1} \ldots \eta_{p-2}^{t_{p-2}} \mod w_o^{p-1}$, alors

$$t_k = -\frac{1}{k!} \frac{1}{k} B_k \sum n_i a_i^k \mod p .$$

Démonstration. Soient G_m le groupe formel multiplicatif et G_a le groupe formel additif. On sait qu'il existe un groupe formel spécial (dit de Lubin-Tate) B tel que si W désigne le paramètre sur B, et Z le paramètre sur G_a, alors

$$Z = \lambda_B(W)$$

est une série de puissances en W (essentiellement le logarithme sur le groupe formel), et

$$\lambda_B(W) \equiv W \mod W^{q-1} .$$

La série de puissances $g_{G_a}(Z) = e^{aZ} - 1$ correspond à la série $g_B(W)$ telle que

$$g_B(w_o) = \zeta^a - 1 .$$

La définition des nombres de Bernoulli par la série

$$\frac{Z}{e^Z - 1} = \sum B_k \frac{Z^k}{k!}$$

donne immédiatement

$$g'_{G_a} / g_{G_a}(Z) = a + \sum_{k=0}^{\infty} \frac{1}{k!} B_k a^k Z^{k-1} .$$

La relation $\lambda_B(W) \equiv W \mod W^{q-1}$ montre que les coefficients dans les séries g'_B/g_B et g'_{G_a}/g_{G_a} coïncident jusqu'en degré $p - 2$. Le théorème en découle en se servant du lemme.

On suivra des arguments semblables dans le cas elliptique, sauf pour la façon de construire des unités qui sera (forcément) plus compliquée. La courbe elliptique donne lieu aussi à un groupe formel de Lubin-Tate, qu'on relie au groupe additif par

le logarithme, et on obtiendra une expression pour des unités globales elliptiques semblable à celle de Kummer-Takagi dans le Théorème 3.1

§ 4. Théorème de Damerell

Soit $\sigma(z,L)$ la fonction sigma de Weierstrass associée au réseau L. Pour toute période ω, on a

$$\sigma(z+\omega, L) = \sigma(z,L) + \eta(\omega,L)$$

où $\eta(z,L)$ est R-linéaire en z, et plus précisément,

$$\eta(z,L) = s_2(L)z + \frac{\pi}{\mathfrak{N}L}\bar{z} .$$

On a posé $s_2(L) = \sum 1/\omega^2$ (qui ne converge pas, mais qu'on définit par prolongement analytique), et $\mathfrak{N}L$ est l'aire du domaine fondamental de L.

On définit la forme de Klein (homogène de degré 1 en (z,L))

$$\mathfrak{k}(z,L) = e^{-\eta(z,L)z/2}\,\sigma(z,L)$$

et pour tout réseau $L' \supset L$,

$$\mathfrak{k}(z,L'/L) = \mathfrak{k}(z,L)^{(L':L)} / \mathfrak{k}(z,L') .$$

Alors on vérifie immédiatement que les termes anti-holomorphes disparaissent de l'expression pour $\mathfrak{k}(z,L'/L)$, et que $\mathfrak{k}(z,L'/L)$ est elliptique pour L. En regardant les zéros et pôles, on trouve en fait :

$$\mathfrak{k}(z,L'/L) = \prod_{\substack{a \in (L'/L)/\pm 1 \\ a \neq 0}} \frac{1}{\wp(z,L) - \wp(a,L)} .$$

Pour le cas de la multiplication complexe, nous prendrons

$$L' = \mathfrak{a}^{-1}L$$

où $\mathfrak{a}$ est un idéal de $\mathfrak{o} = \mathfrak{o}_K$. Notons que dans la littérature, Siegel et Robert se servent plutôt de la fonction thêta

$$\theta(z,L) = e^{-s_2(L)z^2/2}\,\sigma(z,L)$$

alors que Kubert-Lang se servent de la forme de Klein. De toutes façons, on a (avec la notation évidente)

$$\mathfrak{k}(z,L'/L) = \theta(z,L'/L) .$$

Si $\zeta(z,L)$ est la fonction de Weierstrass ($\sigma'/\sigma = \zeta$ et $\zeta' = -\wp$), on trouve

$$\theta'/\theta(z,L) = -s_2(L)z + \zeta(z,L)$$

et pour $\beta \notin L$,

$$\theta'/\theta(z+\beta\,,L) = -s_2(L)(z+\beta) + \zeta(z+\beta\,,L)$$
$$= \sum_{k=1}^{\infty} c_k(\beta,L)z^{k-1}$$

avec des coefficients c_k qui sont donnés par les formules :

$$c_1(\beta,L) = -s_2(L)\beta + \zeta(\beta,L)$$
$$c_2(\beta,L) = -s_2(L) - \wp(\beta,L)$$
$$c_3(\beta,L) = -\frac{1}{(k-1)!}\,\wp^{(k-2)}(\beta,L) \quad \text{pour} \quad k \geq 3 .$$

Si β est un point de torsion par rapport à L , alors les coefficients $c_k(\beta,L)$ sont <u>algébriques</u>. Pour $k \geq 3$, on a

$$c_k(\beta,L) = (-1)^{k+1} \sum_{\omega} \frac{1}{(\beta-\omega)^k} .$$

Rappelons que : $L = \sigma\Omega$, $\mathfrak{f} = (\gamma)$, ψ est le caractère de Hecke. Soit :

$G_{\mathfrak{f}}$ = groupe des idéaux premiers à $\mathfrak{f}$, modulo les idéaux principaux congrus à 1 mod $\mathfrak{f}$.

$\{\mathfrak{b}\}$ = famille finie d'idéaux représentant les éléments de $G_{\mathfrak{f}}$.

$\mathcal{P}_{\mathfrak{b}} = \{\beta\}$ avec $\beta = \psi(\mathfrak{b})\Omega/\gamma$.

THÉORÈME 4.1.- <u>Avec les notations ci-dessus, pour</u> $k \geq 1$ <u>et tout idéal</u> $\mathfrak{a}$ <u>premier à</u> $\mathfrak{f}$, <u>on a</u>

$$\sum_{\beta \in \mathcal{P}_{\mathfrak{b}}} k'/k(z+\beta\,,\mathfrak{a}^{-1}L/L) = \sum c_k(\mathcal{P}_{\mathfrak{b}},\mathfrak{a},L)z^{k-1}$$

<u>où</u>

$$c_k(\mathcal{P}_{\mathfrak{b}},\mathfrak{a},L) = (-1)^{k+1}\,\gamma^k\,\Omega^{-k}L(\bar{\psi}^k,k)(N\mathfrak{a} - \psi^k(\mathfrak{a})) .$$

<u>Démonstration</u>. Supposons d'abord $k \geq 3$. Alors

$$(-1)^{k+1}\sum_{\beta \in \mathcal{P}_{\mathfrak{b}}} c_k(\beta,L) = \sum_{\xi \in \sigma} \frac{1}{(\psi(\mathfrak{b})\frac{\Omega}{\gamma} - \xi\Omega)^k}$$
$$= \Omega^{-k}\,\gamma^k \sum_{\eta \in \mathfrak{f}} \frac{1}{(\psi(\mathfrak{b}) - \eta)^k}$$
$$= \Omega^{-k}\,\gamma^k \sum_{(\mathfrak{a},\mathfrak{f})=1} \frac{1}{\psi(\mathfrak{a})^k} = \Omega^{-k}\,\gamma^k \sum_{(\mathfrak{a}\,,\,\mathfrak{f})=1} \frac{\bar{\psi}(\mathfrak{a})^k}{|\psi(\mathfrak{a})|^{2k}} .$$

On calcule de même la somme $\sum c_k(\beta, \mathfrak{a}^{-1}L)$ où $\mathfrak{a} = (\alpha)$ est principal, et l'assertion voulue en découle immédiatement.

Pour $k = 1$ ou 2, les séries ne convergent plus, et il faut rajouter un s un peu partout, puis par continuation analytique poser $s = 0$. L'argument est tout à fait semblable, et nous l'omettons.

On remarquera que le théorème de Damerell est contenu dans le théorème précédent puisque les coefficients c_k sont algébriques.

Soit $\mathcal{A} = \{\mathfrak{a}_j, n_j\}$ une famille d'idéaux $\mathfrak{a}_j$ premiers à $\mathfrak{p}\bar{\mathfrak{f}}$, et d'entiers n_j satisfaisant à la condition (suivant Robert)

$$\sum n_j(\mathbb{N}\mathfrak{a}_j - 1) = 0 .$$

On peut par exemple prendre $j = 1, 2$ et

$$\mathfrak{a}_1 = (\alpha_1) , \quad \alpha_1 \equiv 1 + 12\gamma\pi$$

$$\mathfrak{a}_2 = (\alpha_2) , \quad \alpha_2 \equiv 1 \mod 12\bar{\mathfrak{f}}\bar{\pi} \quad \text{et} \quad \alpha_2 = \text{générateur de } (\mathfrak{o}/\mathfrak{p})^* .$$

On a alors

$$\sum n_j(\mathbb{N}\mathfrak{a}_j - \psi^k(\mathfrak{a}_j)) \not\equiv 0 \mod \mathfrak{p} .$$

On posera

$$k(z,\mathcal{A}) = k(z,\mathcal{A},L) = \prod_j k(z,\mathfrak{a}_j^{-1}L/L)^{n_j} = \prod_j (k(z,L)^{\mathbb{N}\mathfrak{a}_j} / k(z,\mathfrak{a}_j^{-1}L))^{n_j} .$$

Alors par le théorème 4.1, on trouve

$$\boxed{\sum_\beta k'/k(z+\beta,\mathcal{A},L) = \sum_{k=1}^{\infty} c_k(\mathcal{A},L) z^{k-1}}$$

où

$$c_k(\mathcal{A},L) = (-1)^{k+1} \gamma^k \Omega^{-k} L(\bar{\psi}^k, k) \sum n_j(\mathbb{N}\mathfrak{a}_j - \psi^k(\mathfrak{a}_j)) .$$

§ 5. Connexion avec les unités

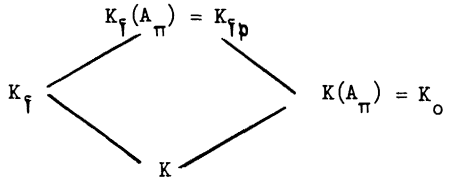
Si on évalue $k(z,\mathcal{A})$ en un point z de torsion par rapport au réseau L, on trouve une unité algébrique selon Robert [Ro 1]. Cela se voit de la manière suivante plus facile à la Kubert-Lang : Faisant varier la courbe elliptique et z comme point de torsion, on trouve une fonction modulaire, qui est une unité dans le corps de fonctions modulaires (on regarde le développement en $q = e^{2\pi i\tau}$ de la fonction et de toutes ses conjuguées, et l'on s'aperçoit que ce développement commence par

une unité circulaire, et que tous ses coefficients sont des entiers cyclotomiques - voir [KL]).

Nous prendrons les valeurs de $k(z,\mathcal{A})$ en des points

$$z = z_o + \frac{\Omega}{\gamma} \quad ,$$

où z_o est un point de π-torsion par rapport à $L = \mathfrak{o}\Omega$. On a le diagramme de corps suivant, où l'on note $K_\mathfrak{f}$ le corps de classes de rayon $\mathfrak{f}$ sur K .



Soit $\mathcal{E}_o = N_{K_{\mathfrak{f}\mathfrak{p}}/K_o}$ (norme) du groupe engendré par les unités

$$k(z_o + \frac{\Omega}{\gamma}, \mathcal{A})$$

avec toutes les familles $\mathcal{A}$ décrites ci-dessus. Le théorème suivant correspond alors au Théorème 3.1.

THÉORÈME 5.1.- Soit $u = N_{K_{\mathfrak{f}\mathfrak{p}}/K_o} k(z_o + \frac{\Omega}{\gamma}, \mathcal{A})$ une telle norme. Ecrivons comme au § 3,

$$u \equiv \prod_{k=1}^{p-2} \eta_k^{t_k} \mod w_o^{p-1} \quad .$$

Alors l'exposant de Kummer-Takagi pour une telle unité est donné par

$$t_k \equiv (-1)^k \Omega^{-k} \gamma^k \frac{1}{k} L(\bar{\psi}^k, k) \sum n_j (\mathbb{N}a_j - \psi^k(a_j)) \mod \mathfrak{p} \quad .$$

Démonstration. Par la théorie de la multiplication complexe, on a

$$(\mathfrak{b}, K_\mathfrak{f}/K) k(z_o + \frac{\Omega}{\gamma}, \mathcal{A}) = k(z_o + \psi(\mathfrak{b})\frac{\Omega}{\gamma}, \mathcal{A}) \quad .$$

Donc la norme de l'unité en question est

$$\prod_{\mathfrak{b}} k(z_o + \psi(\mathfrak{b})\frac{\Omega}{\gamma}, \mathcal{A}) \quad .$$

Si on prend la dérivée logarithmique, on trouve bien l'expression mise en boîte à la fin du numéro précédent.

D'autre part, la courbe elliptique A donne lieu à un groupe formel $\hat{A}$ sur $K_\mathfrak{p}$, de Lubin-Tate, auquel on peut appliquer les considérations du § 3. En particu-

lier, on peut répéter la démonstration du Théorème 3.1 dans le contexte de ce groupe formel, et on peut appliquer comme avant le lemme du § 3, pour démontrer le Théorème 5.1.

Le critère Kummérien en découle immédiatement, et nous avons déjà vu qu'il implique Coates-Wiles, en définissant $\mathfrak{E}_n$ de manière analogue à $\mathfrak{E}_o$ mais en niveau n .

BIBLIOGRAPHIE

[Ar] N. ARTHAUD - On Birch and Swinnerton-Dyer conjecture for elliptic curves with complex multiplication, à paraître.

[C-W 1] J. COATES and A. WILES - On the conjecture of Birch and Swinnerton-Dyer, Invent. Math. 1977.

[C-W 2] J. COATES and A. WILES - Hurwitz numbers and Iwasawa modules, Proc. Int. Conference on Algebraic Number Theory, Kyoto, 1976.

[C-W 3] J. COATES and A. WILES - Kummer's criterion for Hurwitz numbers,

[C-W 4] J. COATES and A. WILES - Explicit reciprocity laws,

[Da] R. DAMERELL - L-functions of elliptic curves with complex multiplication, Acta Arith., 17(1970), 287-301.

[Iw] K. IWASAWA - On some modules in the theory of cyclotomic fields, J. Math. Soc. Japan, 16(1964), 42-82.

[KL] D. KUBERT and S. LANG - Units in the modular function field, survey talk, Modular Functions in one variable, Bonn Conference, 1976.

[L] S. LANG - Elliptic functions, Addison Wesley, 1973.

[Ro 1] G. ROBERT - Unités elliptiques, Bull. Math. Soc. France, Mémoire 36 (1973).

[Ro 2] G. ROBERT - Nombres de Hurwitz et unités elliptiques, à paraître.