GROUPE DE TRAVAIL
D'ANALYSE ULTRAMÉTRIQUE

DANIEL BARSKY

Congruences de coefficients de séries de Taylor (Application aux nombres de Bernoulli-Hurwitz)

Groupe de travail d'analyse ultramétrique, tome 3, nº 1 (1975-1976), exp. nº 17, p. 1-9
<http://www.numdam.org/item?id=GAU_1975-1976__3_1_A11_0>

Groupe d'étude d'analyse ultramétrique
(Y. AMICE, P. ROBBA)
3e année, 1975/76, n° 17, 9 p.

26 avril 1976

CONGRUENCES DE COEFFICIENTS DE SÉRIES DE TAYLOR (APPLICATION AUX NOMBRES DE BERNOULLI-HURWITZ)

par Daniel BARSKY

Résumé. - Soit $\wp(z)$ la fonction de Weierstrass vérifiant l'équation différentielle $(\wp')^2 = 4\wp^3 - g_2\wp - g_3$, où g_2 et g_3 sont des entiers rationnels. Si l'on pose

$$\wp(z) = z^{-2} + \sum_{n\geq 1}(2n+2)^{-1}\, BH_{2n+2}\, \frac{z^{2n}}{(2n)!} ,$$

on appellera BH_{2n+2} le $(2n+2)$-ième nombre de Bernoulli-Hurwitz relatif à la courbe elliptique $\mathcal{E}$ d'équation $Y^2 = 4X^3 - g_2 X - g_3$. Soit p un nombre premier tel que la courbe elliptique $\mathcal{E}(g_2, g_3)$ ait bonne réduction $\bmod(p)$ et invariant de Hasse non nul $\bmod(p)$. Nous montrerons en utilisant un résultat de Tate que, si $u \in \mathbb{U}_1 = \{x \in \mathbb{Z}_p ;\ |x-1| \leq p^{-1}\}$,

$$P_u(z) = \sum_{n\geq 1}(2n+2)^{-1}\, BH_{2n+2}(1 - u^{2n+2})\, z^{2n}$$

est un élément analytique au sens de Krasner sur certains quasi-connexes de $\mathbb{C}_p$ contenant strictement son idéal de valuation. Nous étudierons cet élément analytique, et nous montrerons que ce résultat entraîne en particulier que les nombres de Bernoulli-Hurwitz satisfont des congruences du type Kummer et von Staudt - Clausen. Nous retrouverons ainsi des résultats de KATZ et H. LANG. Dans un exposé ultérieur, nous donnerons des propriétés plus fines de ces nombres.

Notations. - Nous utilisons les notations, définitions et théorèmes de [1]. On désigne par p un nombre premier, $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{Z}_p$, $\mathbb{Q}_p$ ont leur signification habituelle, $\mathbb{C}_p$ est le complété de la clôture algébrique de $\mathbb{Q}_p$. La valeur absolue sur $\mathbb{Z}_p$, $\mathbb{Q}_p$, $\mathbb{C}_p$ est normalisée par $|p| = p^{-1}$. On désigne par ρ un nombre réel positif. Si $a \in \mathbb{C}_p$,

$B(a, \rho)^- = \{X \in \mathbb{C}_p ;\ |X - a| < \rho\}$ (resp. $B(a, \rho)^+ = \{X \in \mathbb{C}_p ;\ |X - a| \leq \rho\}$

est la boule ouverte (resp. fermée) de centre a et de rayon ρ. Si $B \subset \mathbb{C}_p$, on note $H(B)$, resp. $H_0(B)$, l'ensemble des éléments analytiques sur B, resp. nuls à l'infini, c'est-à-dire le complété pour la norme de la convergence uniforme sur B, notée $\| \|_B$, de l'espace des fractions rationnelles de $\mathbb{C}_p(X)$ sans pôle dans B (resp. nulles à l'infini si B n'est pas borné) [1]. On note $\mathcal{C}(\mathbb{Z}_p, \mathbb{C}_p)$ l'espace des fonctions continues de $\mathbb{Z}_p$ dans $\mathbb{C}_p$ muni de la norme de la convergence uniforme sur $\mathbb{Z}_p$.

1. Introduction.

Soit $\mathcal{E}$ la courbe elliptique d'invariant g_2 et g_3, définie par l'équation

$Y^2 = 4X^3 - g_2 X - g_3$. On supposera que g_2 et g_3 sont des entiers rationnels. Soit p un nombre premier tel que $\mathcal{E}$ ait bonne réduction $\bar{\mathcal{E}}$ modulo p, et que son invariant de Hasse A ne soit pas nul modulo p. Soit $\wp(z)$ la fonction de Weierstrass, solution de $(\wp')^2 = 4\wp^3 - g_2 \wp - g_3$, considérée comme une série de Laurent formelle en z. On peut écrire

$$\wp(z) = z^{-2} + \sum_{n\geq 1} h_{2n+2} \frac{z^{2n}}{(2n)!} .$$

Suivant KATZ [6], on appelle k-ième nombre de Bernoulli-Hurwitz associé à $\mathcal{E}$ le nombre $BH_k = kh_k$, donc $BH_0 = 0$ et $BH_{2n+1} = 0$ pour $n \in \underset{\sim}{N}$. Nous montrerons que, si

$$P_u(z) = \sum_{n\geq 1} (1 - u^{2n+2}) h_{2n+2} \, z^{2n} \quad \text{où} \quad u \in U_1 = \{x \in \underset{\sim}{Z}_p \; ; \; |x - 1| \leq p^{-1}\} ,$$

alors

$$P_u(z) = \sum_{n\geq 0} b_n(u) \frac{n! \, C^n z^n}{(1 - Cz) \ldots (1 - nCz)}$$

où $b_n(u)$ dépend de $u \in U_1$, et $|b_n(u)| \leq 1$, et où C est une constante dépendant de $\mathcal{E}$ appartenant à l'extension maximale non ramifiée de $\underset{\sim}{Q}_p$, notée K_p, et liée à la fonction zéta de la courbe elliptique [4]. La démonstration repose sur un résultat de TATE [4]. Nous en déduirons, comme $|C| = 1$, que $P_u(z)$ est un élément analytique p-adique au sens de Krasner sur tout partie bornée du quasi-connexe

$$\mathcal{C}_{p,h} = C_p - \bigcup_{n\geq 0} \bigcup_{i=1}^{p-1} \bigcup_{m=0}^{p^h-1} B_{i,m,n} , \text{ où } B_{i,m,n} = B((i + pm)C^{-1} p^{-n} , p^{-h-1+n})^+ .$$

De là on tire aisément que les BH_k vérifient des congruences de type Kummer et von Staudt - Clausen. Soit $\mathcal{O}_p$ l'anneau des entiers de K_p, alors

$$k^{-1} C^{-k+2} BH_k \equiv (k + p - 1)^{-1} C^{-k-p+3} BH_{k+p-1} \mod(p\mathcal{O}_p)$$

si $p - 1$ ne divise pas k ; si $p - 1$ divise k, alors

$$pBH_k \equiv A^{k/(p-1)} \mod(p\mathcal{O}_p) .$$

Nous donnerons aussi une expression de la partie singulière $P_{u,\infty}(z)$ de $P_u(z)$ dans la décomposition de Mittag-Löffler ([1] ou [10]) relativement au trou

$$\underset{\sim}{C}_p - B(0 , 1)^+$$

du quasi-connexe

$$\mathcal{B}_{p,0} = B(0 , 1)^+ - \bigcup_{i=1}^{p-1} B(iC^{-1} , p^{-1})^+ .$$

Ceci nous permettra dans un prochain exposé de trouver une relation fonctionnelle entre $P_{u,\infty}$ et P_u, et d'obtenir ainsi des congruences, pour les nombres de Bernoulli-Hurwitz, très semblables à celles obtenues par KUBOTA et LÉOPOLDT pour les nombres de Bernoulli et de retrouver ainsi des résultats de KATZ [7]. La méthode employée est proche de celle des mesures p-adiques employées par KATZ. Elle nous a déjà servi pour retrouver des résultats sur les nombres de Bell et de Bernoulli.

Cet exposé doit beaucoup à Bernard DWORK qui m'a, en particulier, signalé le résultat de TATE sur lequel repose en fait tout l'exposé. Je le remercie pour l'aide bienveillante qu'il m'a apportée.

2. Fonction génératrice des nombres de Bernoulli-Hurwitz.

Rappelons tout d'abord le théorème de TATE [4].

THÉORÈME (TATE [4]). - Soit $\mathcal{E}$ la courbe elliptique d'équation

$$Y^2 = 4X^3 - g_2 X - g_3 \, ,$$

où g_2 et g_3 appartiennent à un corps k de caractéristique zéro complet pour une valuation discrète, d'anneau de valuation $\mathcal{O}$ et de corps résiduel $\bar{k}$. Si la courbe réduite $\bar{\mathcal{E}}$ sur $\bar{k}$ est non singulière et a un invariant de Hasse A, non nul sur k, alors il existe une unité C, dans l'extension maximale non ramifiée, K de k, telle que, si dz est la différentielle de première espèce sur $\mathcal{E}$, $\exp(Cz)$, considérée comme série de Taylor en $t = X/Y$, ait des coefficients entiers dans K. En outre, si $\bar{k}$ est fini c'est-à-dire si k est un corps p-adique, alors C vérifie la condition $C^{\sigma-1} = \omega$, où ω est la racine de module 1 de la fonction zéta de la courbe elliptique $\bar{\mathcal{E}}$ sur $\bar{k}$, et σ est l'automorphisme de Frobénius de K sur k.

Nous allons utiliser ce théorème en supposant que g_2 et g_3 sont des entiers rationnels, donc contenus dans $\mathbb{Q}_p$ pour tout p. Nous noterons $K_p \subset \mathbb{C}_p$ l'extension maximale non ramifiée de $\mathbb{Q}_p$, et $\mathcal{O}_p$ son anneau des entiers. Il est clair, d'après l'énoncé, que l'hypothèse $g_2, g_3 \in \mathbb{Z}$ peut être facilement affaiblie. Il est bien connu que $\omega \equiv A$ modulo $p\mathbb{Z}_p$ [9]. Posons $X = t^{-2}$ et $Y = t^{-3}$, du théorème précédent on tire que, si $dz = dX/2Y = \alpha_1 + \alpha_2 t + \dots$ avec $\alpha_1 = 1$ et

$$\alpha_i \in \mathbb{Z}_p \quad (p \neq 2) \, ,$$

et donc si $z = \alpha_1 t + \alpha_2 t^2/2 + \dots$, alors il existe C, unité de K_p, définie en fait à un élément de $\mathbb{Z}_p^* = \{x \in \mathbb{Z}_p \; ; \; |x| = 1\}$ près, telle que

$$e^{Cz} = 1 + \beta_1 t + \beta_2 t^2 + \dots \in \mathcal{O}_p[[t]] \, .$$

Mais alors $t = \sum_{j\geq 1} \gamma_j (e^{Cz} - 1)^j$, où $\gamma_1 = \beta_1^{-1}$, la convergence est z-adique.

$$X = t^{-2} = \Big(\sum_{j\geq 1} \gamma_j (e^{Cz} - 1)^j\Big)^{-2} = \wp(z) \, ,$$

or

$$\wp(z) = z^{-2} + \sum_{n\geq 1} h_{2n+2} \frac{z^{2n}}{(2n)!} \, ,$$

on trouve donc par identification $(\gamma_1 C)^2 = 1$, donc γ_1 est une unité de K_p, donc aussi β_1, et par conséquent tous les γ_j sont des entiers de K_p.

PROPOSITION 1. - Soit $\wp(z)$ la fonction de Weierstrass associée à la courbe $\mathcal{E}$ d'équation $Y^2 = 4X^3 - g_2 X - g_3$, g_2 et $g_3 \in \underset{\sim}{Z}$. Sous les hypothèses du théorème de Tate, il existe une unité C de K_p telle que l'on ait formellement (i. e. z-adiquement)

$$\wp(z) = \sum_{i \geqslant -2} a_i (e^{Cz} - 1)^i \text{, où } a_i \in K_p \text{ et } |a_i| \leqslant 1 .$$

En outre, $a_{-2} = C^2$.

La première partie de la proposition est évidente d'après les formules précédentes puisque $\gamma_1 = 1$. le calcul de a_{-2} se fait par identification.

Soit $u \in U_1 = \{x \in Z_p ; |x - 1| \leqslant p^{-1}\}$. Considérons

$$\wp_u(z) = \wp(z) - u^2 \wp(uz) = \sum_{n \geqslant 0} h_{2n+2}(1 - u^{2n+2}) \frac{z^{2n}}{(2n)!} .$$

PROPOSITION 2. - Sous les mêmes hypothèses qu'à la proposition 1,

$$\wp_u(z) = \wp(z) - u^2 \wp(uz) = \sum_{n \geqslant 1} b_n(u)(e^{Cz} - 1)^n ,$$

où $u \in U_1$ et $b_n(u) \in \mathcal{O}_p$.

En effet, on a

$$\begin{aligned} u^2 \wp(uz) &= u^2 \sum_{i \geqslant -2} a_i (e^{Cuz} - 1)^i = u^2 \sum_{i \geqslant -2} a_i (((e^{Cz} - 1) + 1)^u - 1)^i \\ &= u^2 \sum_{i \geqslant -2} a_i \left(\sum_{n \geqslant 1} \binom{u}{n} (e^{Cz} - 1)^n\right)^i \\ &= a_{-2}(e^{Cz} - 1)^{-2} + a_{-1}(e^{Cz} - 1)^{-1} + \sum_{n \geqslant 0} d_n(u)(e^{Cz} - 1)^n \end{aligned}$$

avec $|d_n(u)| \leqslant 1$; donc $\wp_u(z) = \wp(z) - u^2 \wp(uz) = \sum_{n \geqslant 1} b_n(u)(e^{Cz} - 1)^n$, car $\wp_u(0) = 0$.

Nous allons utiliser la transformation formelle $\mathcal{L}$ de $\underset{\sim}{C}_p[[z]]$ dans $\underset{\sim}{C}_p[[z]]$ définie par

$$\tilde{f}(z) = \sum_{n \geqslant 0} a_n z^n (n!)^{-1} \in \underset{\sim}{C}_p[[z]] ,$$

alors

$$\mathcal{L}(\tilde{f})(z) = f(z) = \sum_{n \geqslant 0} a_n z^n \in \underset{\sim}{C}_p[[z]] .$$

On remarque que $\mathcal{L}$ est continue z-adiquement, et que $\mathcal{L}(e^{kz}) = (1 - kz)^{-1}$ pour tout $k \in \underset{\sim}{C}_p$. Posons alors

$$\begin{aligned} P_u(z) &= \mathcal{L}(\wp_u(z)) = \sum_{n \geqslant 0} b_n(u) \mathcal{L}((e^{Cz} - 1)^n) \\ &= \sum_{n \geqslant 0} b_n(u) \sum_{k=0}^{m} (-1)^{n-k} \binom{m}{k} (1 - kCz)^{-1} \\ &= \sum_{n \geqslant 0} b_n(u) \frac{n!\, C^n z^n}{(1 - Cz)(1 - 2Cz) \dots (1 - nCz)} . \end{aligned}$$

Notons $B_{i,m,n}$ la boule fermée $B((i + pm)p^{-n} C^{-1}, p^{-h-1+n})^+$, et appelons $\mathcal{C}_{p,h} = \underset{\sim}{C}_p - \bigcup_{n \geqslant 0} \bigcup_{i=1}^{p-1} \bigcup_{m=1}^{p^h-1} B_{i,m,n}$, un quasi-connexe de $\underset{\sim}{C}_p$.

THÉORÈME 1. - Soit p un nombre premier tel que la courbe elliptique $\mathcal{E}$ d'équation $Y^2 = 4X^3 - g_2 X - g_3$, où g_2, $g_3 \in \underset{\sim}{Z}$, ait bonne réduction modulo p et invariant de Hasse non nul modulo p. Soit $u \in U_1$, alors

$$P_u(z) = \sum_{n\geq 0}(1 - u^{2n+2})\, h_{2n+2}\, z^{2n}$$

$$P_u(z) = \sum_{n\geq 1} b_n(u) \frac{n!\, C^n z^n}{(1 - Cz) \dots (1 - nCz)} \quad \text{avec} \quad b_n(u) \in \mathcal{O}_p \,.$$

De plus, $P_u(z)$ est un élément analytique p-adique sur tout quasi-connexe

$$\mathcal{C}_{p,h} \cap B(0\,,\,\rho) \subset \underset{\sim}{C}_p$$

pour tout entier $h \geq 0$ et tout réel $\rho > 0$.

Remarquons que $(-1)^n \sum_{k=0}^{n}(-1)^k \binom{n}{k}(1 - kCz)^{-1}$ est le n-ième coefficient d'interpolation, sur la base normale de $\mathcal{C}(\underset{\sim}{Z}_p\,,\,\underset{\sim}{C}_{p_1})$ formée des polynômes $\binom{t}{n}$ [2], de la fonction de $\underset{\sim}{Z}_p$ dans $\underset{\sim}{C}_p$: $t \to (1 - tzC)^{-1}$. Si $z \in \mathcal{C}_{p,h} \cap B(0\,,\,\rho)$, la fonction est localement analytique sur $\underset{\sim}{Z}_p$ de rayon d'analyticité locale

$$R = \inf(\rho^{-1}\,,\, p^{-k-1})$$

et donc, d'après des résultats généraux d'AMICE ([2], corollaire 3 du théorème 3)

$$\Big\|\sum_{k=0}^{n}(-1)^k \binom{n}{k}(1 - kCz)^{-1}\Big\|_{B(0,1)^-} \leq M\,|[nR]!|\,,$$

M est un réel > 0. On peut aussi obtenir cette estimation à l'aide des lemmes 1 et 2 de [3].

COROLLAIRE 1. - $P_u \in H(B(0\,,1)^+ - \bigcup_{i=1}^{p-1} B(iC^{-1}\,,\,p^{-1})^+)$.

Il suffit de faire $\rho = 1$ et $h = 0$.

D'après le théorème de Mittag-Löffler p-adique ([1] ou [10]), on peut décomposer de manière unique $P_u(z)$ sous la forme

$$P_u(z) = P_{u,\infty}(z) + \sum_{i=1}^{p-1} P_{u,i}(z)\,, \quad \text{où} \quad P_{u,\infty} \in H(B(0\,,\,1)^+)$$

et

$$P_{u,i} \in H_0(\underset{\sim}{C}_p - B(iC^{-1}\,,\,p^{-1})^+) \quad \text{pour} \quad 1 \leq i \leq p - 1\,,$$

enfin $P_{u,i}$ (resp. $P_{u,\infty}$) est caractérisé par la condition : $P_u - P_{u,i}$ (resp. $P_u - P_{u,\infty}$) se prolonge analytiquement sur

$$B(iC^{-1}\,,\,p^{-1})^+ \quad (\text{resp. sur } \underset{\sim}{C}_p - B(0\,,\,1)^+)\,.$$

Nous allons montrer comment on peut calculer $P_{u,\infty}$.

THÉORÈME 2. - La partie singulière $P_{u,\infty}(z)$ de $P_u(z)$, relative au trou à l'infini du quasi-connexe

$$\mathcal{B}_{p,0} = B(0\,,\,1)^+ \cap \mathcal{C}_{p,0} = B(0\,,\,1)^+ - \bigcup_{i=1}^{p-1} B(iC^{-1}\,,\,p^{-1})^+\,,$$

est donnée par l'expression

$$P_{u,\infty}(z) = \sum_{n\geq 0} b_n(u) \sum_k^* \binom{n}{k} (-1)^{n-k} (1 - kCz)^{-1} ,$$

où $\sum_k^*$ désigne une sommation sur les entiers k tels que $k \equiv 0 \mod(p)$.

En effet, dans la quantité $(-1)^n \sum_k^* (-1)^k \binom{n}{k} (1 - kCz)^{-1}$, on reconnait le n-ième coefficient d'interpolation, sur la base normale de $\mathcal{C}(\underset{\sim}{Z}_p , \underset{\sim}{C}_p)$ formée des polynômes $\binom{t}{n}$, de la fonction de $\underset{\sim}{Z}_p$ dans $\underset{\sim}{C}_p$, $t \to f_z(t) = \psi_0(t)(1 - Ctz)^{-1}$, où $\psi_0(t)$ est la fonction caractéristique de la boule ouverte $B(0 , 1)^-$ de centre zéro et de rayon 1 . Il est clair que $f_z(t)$ est localement analytique sur $\underset{\sim}{Z}_p$ de rayon d'analyticité locale p^{-1} , donc d'après des résultats généraux d'AMICE,

$$\|\sum_k^* (-1)^k \binom{n}{k} (1 - kCz)^{-1}\|_{B(0,1)^-} \leq |[n/p]!| ,$$

puisque

$$\sup_{t \in B(0,1)^+} \sup_{z \in B(0,1)^-} |f_z(t)| = 1$$

(on peut prolonger de manière évidente $f_z(t)$ sur $B(0 , 1)^+$). En fait comme le rayon de convergence de la série de Taylor au voisinage de zéro qui représente $f_z(t)$ est clairement 1^- , on en déduit ([2] corollaire 3 du théorème 3) que

$$\|\sum_k^* (-1)^k \binom{n}{k} (1 - kCz)^{-1}\|_{B(0,1)^-} \leq p^{-(n/p)} |[n/p]!| .$$

D'après les inégalités de Cauchy [1], si

$$\sum_k^* (-1)^k \binom{n}{k} (1 - kCz)^{-1} = \frac{R_n(z)}{S_n(z)} ,$$

alors

$$R_n(z) \in p^{n/p} ([n/p]!) \mathcal{O}_p[z] ,$$

et comme $\|S_n\|_{B(0,1)^+} \leq 1$, on a

$$\lim_{n\to\infty} \|\sum_k^* (-1)^k \binom{n}{k} (1 - kCz)^{-1}\|_{B(0,1)^+} = 0 .$$

Donc

$$g_u(z) = \sum_{n\geq 0} b_n(u) \sum_k^* (-1)^{n-k} \binom{n}{k} (1 - kCz)^{-1} \in H(B(0 , 1)^+) .$$

Montrons maintenant que $P_u(z) - g_u(z)$ est prolongeable analytiquement sur $\underset{\sim}{C}_p - B(0 , 1)^+$. Or

$$P_u(z) - g_u(z) = \sum_{n\geq 0} b_n(u) \sum_k' (-1)^{n-k} \binom{n}{k} (1 - kCz)^{-1} ,$$

où $\sum'$ désigne une sommation sur les entiers premiers à p . On montre que

$$\sum_{n\geq 0} b_n(u) \sum_k' (-1)^{n-k} \binom{n}{k} (1 - kCz)^{-1} \in H_0(\mathcal{D}_{p,0}) ,$$

où $\mathcal{D}_{p,0} = C_p - \bigcup_{i=1}^{p-1} B(iC^{-1} , p^{-1})^+$, en remarquant que, d'après l'inégalité ultramétrique,

$$\|\sum_k' (-1)^k \binom{n}{k} (1 - kCz)^{-1}\|_{B(0,1)^-} \leq \max(|n!| , p^{-(n/p)} |[n/p]!|) .$$

Si $\sum_k'(-1)^{n-k}\binom{n}{k}(1-kCz)^{-1} = \frac{T_n(z)}{V_n(z)}$ alors, d'après les inégalités de Cauchy, $T_n(z) \in p^{n/p}([n/p]!)\,\mathcal{O}_p[z]$. Comme $\|V_n^{-1}\|_{\mathcal{O}_{p,0}} \leq p^{n/p}$, on a le résultat annoncé $P_u - g_u \in H_0(\mathcal{O}_{p,0})$, et donc $g_u(z) = P_{u,\infty}(z)$.

Considérons $\mathcal{L}^{-1}(P_{u,\infty}(z))$, soit Γ_1 le groupe des racines p-ièmes de l'unité. On a

$$\mathcal{L}^{-1}(P_{u,\infty}(z)) = p_{u,\infty}(z) = p^{-1}\sum_{\gamma\in\Gamma_1}\sum_{n\geq 0} b_n(u)(\gamma e^{Cz}-1)^n$$
$$= \sum_{n\geq 0} b_n(u)\sum_k^*(-1)^{n-k}\binom{n}{k} e^{kCz} ,$$

ces formules ont un sens non plus formellement mais (z , p)-adiquement, puisque $|\gamma - 1| = p^{-(p-1)^{-1}} < 1$ ou bien $\gamma - 1 = 0$. En développant cette remarque dans un prochain exposé, nous donnerons une relation fonctionnelle entre $P_{u,\infty}$ et P_u , ce qui nous permettra de retrouver des résultats de KATZ [7]. Nous nous contenterons ici de retrouver les résultats de KATZ contenus dans [6], ainsi que ceux de H. LANG [8].

3. Congruences de type Kummer et von Staudt - Clausen.

On a

$$P_u(z) = \sum_{n=0}^{p-1} b_n(u)\,\frac{(n!)\,C^n z^n}{(1-Cz)\ldots(1-nCz)} \mod p\mathcal{O}_p[[z]] .$$

Donc on a le résultat suivant.

LEMME 1. - *Pour* $n \geq 0$, *on a*

$$|h_n C^{2-n}(1-u^n) - h_{n+p-1} C^{3-n-p}(1-u^{n+p-1})| \leq p^{-1} .$$

En effet,

$$P_u(C^{-1}z) = \sum_{n\geq 0}(1-u^{2n+2})\,C^{-2n} h_{2n+2} z^{2n} = \sum_{n=0}^{p-1} b_n(u)\sum_{k=0}^{n}(-1)^{n-k}\binom{n}{k}(1-kz)^{-1} .$$

On remarque que $(1-kz)^{-1} = \sum_{n\geq 0} k^n z^n$ et que $k^{n+p-1} \equiv k^n \mod(p)$ d'après le théorème de Fermat, si k est premier à p . Le lemme est démontré.

Or $|(1-u^n) - (1-u^{n+p-1})| \leq p^{-1}$, et en outre, si $p - 1$ ne divise pas n , $|1 - u^n| = 1$. Donc

$$h_n/C^{n-2} \equiv h_{n+p-1}/C^{n+p-3} \mod p\mathcal{O}_p$$

si $p - 1$ ne divise pas n . Comme $C^{p-1} \equiv A \mod(p)$, on a $h_n \equiv h_{n+p-1} A \mod p\mathcal{O}_p$ si $p - 1$ ne divise pas n . Si $p - 1$ divise n , choisissons u de telle sorte que $\log(u) = p$ (ici le log est le log p-adique), c'est possible [1].

Donc

$$\frac{1-u^{(p-1)m}}{(p-1)m} \equiv p \mod p\mathcal{O}_p .$$

Remarquons que

$$\lim_{u\to 1}(u-1)^{-1} P_u(z/C) = \sum_{n\geq 1}^{-1} C^{-2n} BH_{2n+2} z^{2n}$$

$$= \lim_{u\to 1} \mathcal{E}((u-1)^{-1}(\wp(z/C) - u^2 \wp(uz/C)) = \mathcal{E}(z/C\wp'(z/C) - 2\wp(z/C)) .$$

Or

$$z/C\wp'(z/C) - 2\wp(z/C) = \sum_{n\geq 0} c_n(e^Z - 1)^n$$

avec

$$c_n = -2a_n + \sum_{k=1}^{n+3} k^{-1} d_{n-k} \quad \text{et} \quad d_{n-k} = (n-k)a_{n-k} + (n-k+1)a_{n-k+1} .$$

Rappelons que $\wp(z) = \sum_{n\geq -2} a_n(e^{Cz} - 1)^n$, ceci est immédiat car

$$z = \log((e^z - 1) + 1) = \sum_{n\geq 1}(-1)^n n^{-1}(e^z - 1)^n .$$

Par conséquent,

$$\sum_{n\geq 1} C^{-2n} BH_{2n+2} z^{2n} = \sum_{n\geq 0} c_n \frac{(n!)z^n}{(1-z)\dots(1-nz)} ,$$

d'où l'on tire en particulier que

$$pC^{p-3} BH_{p-1} \equiv a_{-2} \mod p\mathcal{O}_p ,$$

donc

$$pBH_{p-1} \equiv C^{p-1} \mod p\mathcal{O}_p$$

et, plus généralement, si $p-1$ divise n ,

$$pBH_n \equiv C^n \mod p\mathcal{O}_p$$

puisque $pC^{3-p} BH_{p-1} \equiv pC^{2-n} BH_n \mod p\mathcal{O}_p$. Or $C^{p-1} \equiv A \mod(p\mathcal{O}_p)$, donc

$$pBH_n \equiv A^{n/(p-1)} \mod(p) \quad \text{si} \quad p-1 \quad \text{divise} \quad n .$$

Rassemblons ces résultats.

THÉORÈME 3.(<u>Congruences de Kummer et von Staudt - Clausen pour les nombres de Bernoulli-Hurwitz</u>). - <u>Soit</u> p <u>un nombre premier tel que la courbe elliptique</u> $\mathcal{E}$ <u>d'équation</u>

$$Y^2 = 4X^3 - g_2 X - g_3 \qquad (g_2 , g_3 \in \mathbb{Z})$$

<u>ait bonne réduction</u> modulo p <u>et invariant de Hasse</u> A , <u>non nul</u> modulo p . <u>Les nombres de Bernoulli-Hurwitz</u> BH_n , <u>de la courbe</u> $\mathcal{E}$, <u>définis par</u>

$$\wp(z) = z^{-2} + \sum_{n\geq 2} n^{-1} BH_n z^{n-2}/(n-2)!$$

<u>avec</u> $BH_n = 0$ <u>si</u> n <u>est impair, et</u> $BH_0 = 0$ <u>où</u> $\wp(z)$ <u>est la fonction de Weierstrass, satisfont les congruences suivantes</u> :

(i) <u>Si</u> $p-1$ <u>ne divise pas</u> n ,

$$A \frac{BH_n}{n} \equiv \frac{BH_{n+p-1}}{n+p-1} \mod(p) ;$$

(ii) Si $p-1$ divise n,

$$pBH_n \equiv A^{n/(p-1)} \mod(p) .$$

On pourrait obtenir aussi, par le même moyen, des congruences $\mod(p^h)$ entre les nombres de Bernoulli-Hurwitz.

BIBLIOGRAPHIE

[1] AMICE (Y.). - Nombres p-adiques. - Paris, Presses universitaires de France, 1975 (Collection SUP., "Le Mathématicien", 14).

[2] AMICE (Y.). - Interpolation p-adique, Bull. Soc. math. France, t. 92, 1964, p. 117-180 (Thèse Sc. math. Paris, 1964).

[3] BARSKY (D.). - Fonction génératrice et congruences (Application aux nombres de Bernoulli), Séminaire Delange-Pisot-Poitou : Théorie des nombres, 17e année, 1975/76, n° 21, 16 p.; et C. R. Acad. Sc. Paris (à paraître).

[4] DWORK (B.). - A deformation theory for the zeta function of a hypersurface, "Proceedings of the International Congress of Mathematicians [1962. Stockholm], p. 247-259. - Djursholm, Institut Mittag-Löffler, 1963.

[5] HURWITZ (A.). - Über die Entwicklungscoefficienten der lemmiscatischen Functionen, Math. Annalen, t. 51, 1889, p. 196-226.

[6] KATZ (N.). - The congruences of Clausen - von Staudt and Kummer for Bernoulli-Hurwitz numbers, Math. Annalen, t. 216, 1975, p. 1-4.

[7] KATZ (N.). - Conférence prononcée aux Journées arithmétiques de Caen, mai 1976 (à paraître).

[8] LANG (H.). - Kummersche Kongruenzen für die normierten Entwicklungscoeffi-cienten der Weierstrass p-Funktion, Abh. math. Seminar. Univ. Hamburg, t. 33, 1969, p. 183-196.

[9] LANG (S.). - Elliptic functions. - London, Amsterdam, Addison-Wesley, 1973.

[10] ROBBA (P.). - Fonctions analytiques sur les corps valués complets ultramé-triques, Astérisque n° 10, 1973, p. 109-218.

(Texte reçu le 11 octobre 1976)

Daniel BARSKY
Département de Mathématiques
Université de Paris-7, Tour 45-55
2 place Jussieu
75221 PARIS CEDEX 05