SÉMINAIRE DE THÉORIE DES NOMBRES DE GRENOBLE

JEAN-RENÉ JOLY

Calcul des nombres de Bernoulli modulo p^m. Application à l'étude des nombres premiers irréguliers

Séminaire de théorie des nombres de Grenoble, tome 9 (1980-1981), exp. nº 4, p. 1-19

<http://www.numdam.org/item?id=STNG_1980-1981__9__A4_0>

Séminaire de Théorie des Nombres
14 mai et 4 juin 1981

Grenoble

CALCUL DES NOMBRES DE BERNOULLI modulo p^m. APPLICATION A L'ETUDE DES NOMBRES PREMIERS IRREGULIERS.

par Jean-René JOLY

1. - INTRODUCTION

Soient p un nombre premier ≥ 5, m un entier ≥ 1, k un entier pair ≥ 2 et non divisible par $p-1$, et B_k le k-ième nombre de Bernoulli ; l'objet de ce papier est de décrire une méthode permettant de programmer et de traiter sur ordinateur le calcul numérique de $\frac{B_k}{k} \pmod{p^m}$, autrement dit, le calcul d'une valeur approchée p-adique du p-entier $\frac{B_k}{k} = -\zeta(1-k)$. Le principe de cette méthode (notée LEM) est expliqué au § 2, sa programmation et sa réalisation en machine sont esquissées au § 3. Des spécimens de résultats, avec les temps de calculs correspondants, sont donnés à la fin de ce § 1. La méthode s'adapte facilement au calcul de $pB_k \pmod{p^m}$ pour k divisible par $p-1$. Pour $m=2$, la méthode LEM se ramène à celle (due à E. Lehmer [9]) employée par Johnson et Wagstaff dans [3], [4], et [13] pour la tabulation des quantités notées a_0 et a_1, et attachées aux couples irréguliers (p,k) avec $p \leq 125\,000$. Notons également que les congruences (mod p) utilisées par Johnson et Wagstaff peuvent s'obtenir par la méthode du § 2, appliquée, non aux sommes $\sum_{a=1}^{p/6} (p-6a)^{k-1}$, mais à des sommes telles que $\sum_{a=1}^{p/6} a^{k-1}$.

Une fois résolu le problème du calcul numérique de $\frac{B_k}{k} \pmod{p^m}$, un certain nombre de questions se traitent facilement ; par exemple :

a) le calcul p-adique approché de $L_p(1,\chi)$, $L_p(0,\chi)$, et plus généralement de $L_p(1-n,\chi)$ (dans cet exposé χ désigne un caractère de Dirichlet pair, non principal, de conducteur p , à valeurs dans $\mathbb{Z}_p$, donc de la forme ω^h , avec ω = le caractère de Teichmüller) ;

b) le calcul p-adique approché des $\frac{B_{n,\chi}}{n}$, toujours avec $\chi = \omega^h$;

c) le calcul p-adique approché des premiers coefficients d'un développement en série d'Iwasawa de $L_p(1-s,\chi)$, $\chi = \omega^h$;

d) l'étude, pour un couple irrégulier (p,h) donné, du (ou des) zéro(s) entier(s) p-adique(s) de $L_p(1-s,\chi)$, $\chi = \omega^h$;

e) la détermination, pour un couple irrégulier (p,h) donné, des entiers $k \equiv h \pmod{p-1}$ tels que

$$\frac{B_k}{k} \equiv 0 \pmod{p^m} , \quad m \text{ donné.}$$

Naturellement, a) et b) sont des problèmes voisins, ainsi que d) et e). Ces divers problèmes sont examinés dans [1]. Bornons-nous ici à indiquer à propos de e) que la congruence $\frac{B_k}{k} \equiv 0 \pmod{p^2}$ a été étudiée systématiquement par Johnson et Wagstaff (loc. cit.). Le prototype d'une telle congruence est

$$(1.1) \qquad \frac{B_{284}}{284} \equiv 0 \pmod{37^2} ,$$

due à Pollaczek, avec $p = 37$ et $h = 32$. En utilisant la méthode LEM et un peu d'Analyse p-adique, on obtient sans difficulté une congruence telle que

$$(1.2) \qquad \frac{B_k}{k} \equiv 0 \pmod{p^m} , \quad p=37 , \quad m=8 ,$$

$$k = 2\,444\,284\,077\,476 ,$$

$$p^m = 3\,512\,479\,553\,921 .$$

La manière d'obtenir k (une fois p , h et m fixés) est expliquée dans [1] (utilisation convenable de diverses séries de Mahler pour $\zeta_p(1-s|h) = L_p(1-s,\omega^h)$) . Pour la congruence particulière ci-dessus, une vérification directe a également été effectuée : voir la fin de ce § 1.

La méthode LEM a été programmée en BASIC et exécutée en machine en trois versions ; version 0 : p quelconque, k petit, exécution lente ; version 1 : p et k petits, exécution rapide ; version 2 : p petit, k éventuellement très grand, exécution assez rapide. On donne en Annexe un listing correspondant à la version 1. On donne également ci-dessous un spécimen de résultats numériques et de temps de calcul obtenus avec les versions 1 et 2. Au préalable, une précision "technique" : dans les versions 1 et 2, m est obligatoirement pair (voir pourquoi au § 2) ; on pose $N = \frac{m-2}{2}$; les données numériques (entiers p-adiques modulo p^m, $m = 2N+2$) sont alors traitées en machine comme suites de $N+1$ chiffres en base $q = p^2$; plus précisément, si $a \in \mathbb{Z}_p$, on peut écrire

$$a = \underbrace{a_o + a_1 q + \ldots + a_N q^N}_{\text{partie "significative"}} + \underbrace{a_{N+1} q^{N+1} + \ldots}_{O(p^m)}$$

et a est "connu" par la machine comme "vecteur" $(a_o, a_1, \ldots, a_N)$. Il est commode de qualifier les a_ν $(0 \leq \nu \leq N)$ de hensimales de a (Hensel + décimales) et d'écrire

$$a = a_o \; ; a_1 \; ; a_2 \; ; \ldots ; a_N \; ; \ldots$$

(de gauche à droite ; les a_ν étant évidemment écrits elles-mêmes normalement en base 10).

Ce point étant précisé, la table I donne une liste de valeurs calculées en machine ; on a partout $p = 37$, $m = 8$ (donc $N = 3$) et $k \equiv 32 \pmod{36}$ (cette table correspond en fait au problème évoqué en (e), ou encore au calcul récurrent d'approximations du zéro dans $\mathbb{Z}_{37}$ de $L_{37}(1-s, \omega^{32})$). La colonne de droite indique le temps de calcul (en minutes et fractions de minute) sur micro-ordinateur (le temps de calcul, dans chaque version, est proportionnel à $pN^2 \log k$). Le micro-ordinateur utilisé (micro-processeur Z 80 : 8 bits, fréquence 2,5 MHz, multiplication non câblée ; travail en BASIC sous interpréteur) est relativement lent. On peut penser que sur un "vrai" ordinateur, la vitesse d'exécution serait multipliée par un facteur de l'ordre de 150 au moins : les temps de calcul indiqués dans la table I (de 2 à 11 minutes pour $p = 37$) seraient alors ramenés à quelques secondes.

Table I (voir en Annexe 3 une table II plus détaillée).

valeur de k	hensimales de $\frac{B_k}{k}$	(*)	T_1 / T_2
32	37 ; 1 139 ; 1 035 ; 383 ;	1	2,1 / 2,3
68	814 ; 1 008 ; 1 201 ; 1 034 ;	1	2,7 / 2,9
284	0 ; 1 077 ; 986 ; 1 001 ;	2	3,1 / 3,4
1 616	0 ; 358 ; 946 ; 989 ;	2	3,6 / 3,9
1 072 544	0 ; 0 ; 665 ; 1 195 ;	4	4,9 / 5,4
2 896 052	0 ; 0 ; 1 315 ; 1 043 ;	4	5,0 / 5,6
(**)	0 ; 0 ; 0 ; 0 ;	8	- / 11,0
...	...	...	...

(*) la valeur figurant dans cette colonne est la valuation p-adique $\mathrm{ord}_p(\frac{B_k}{k})$ (p=37) .

(**) la valeur de k correspondant à cette ligne est le nombre (déjà évoqué) k_8 = 2 444 284 077 476

de hensimales 617 ; 1 042 ; 913 ; 952 .

2. - LA METHODE LEM : PRINCIPE ET EXEMPLE

Pour tout entier $\ell \geq 1$, posons

$$S_{\ell-1} = \sum_{a=1}^{p/6} (p-6a)^{\ell-1} \quad ;$$

$$C_{\ell-1} = 6^{\ell-1} + 3^{\ell-1} + 2^{\ell-1} - 1^{\ell-1}$$

("sommes de Lehmer", "coefficients de Lehmer" : [9]). Notons B_ℓ , $B_\ell(X)$ et $\beta_\ell(x) = B_\ell(\langle x \rangle)$ le nombre, le polynôme et la fonction de Bernoulli d'indice ℓ . Pour ℓ pair, $p \geq 5$ (et donc $p \equiv \pm 1 \pmod 6$), on a

(2.1) $$\beta_\ell(\tfrac{p}{6}) = B_\ell(\tfrac{1}{6}) \quad ;$$

(2.2) $$6^{\ell-1}(B_\ell - B_\ell(\tfrac{1}{6})) = \frac{1}{2} C_{\ell-1} B_\ell$$

(classique : [9]). La formule d'Euler-Maclaurin à l'ordre ℓ , appliquée à $S_{\ell-1}$, donne après quelques manipulations triviales (et compte-tenu de (2.1) et (2.2))

(2.3) $$S_{\ell-1} = \frac{1}{6}\frac{p^\ell}{\ell} - \frac{1}{2}\frac{p^{\ell-1}}{\ell} + \sum_{\lambda=2}^{\ell-1} \binom{\ell-1}{\lambda-1} 6^{\lambda-1} \frac{B_\lambda}{\lambda} p^{\ell-\lambda} + \frac{1}{2} C_{\ell-1} \frac{B_\ell}{\ell} .$$

Dans le second membre, tous les termes sont p-entiers, à l'exception des $\frac{B_\lambda}{\lambda}$ avec $\lambda \equiv 0 \pmod{p-1}$. D'autre part, les B_λ avec λ impair ≥ 3 sont évidemment nuls.

ℓ étant désormais supposé pair, donnons-nous un $n \geq 2$ également pair, et supposons pour simplifier l'exposition que n vérifie les deux conditions suivantes :

$$n \leq \ell - 1 - \mathrm{ord}_p(\ell) \quad ;$$

$$n < \text{reste de } \ell \pmod{p-1}$$

(la première condition sera toujours vérifiée dans la pratique ; la seconde est très peu restrictive, surtout pour l'étude des couples irréguliers ; on y reviendra...) ; l'égalité (2.3) donne alors, avec le changement d'indice $\mu = \ell - \lambda$, la congruence suivante (2.4) :

$$S_{\ell-1} \equiv \frac{1}{2} C_{\ell-1} \frac{B_\ell}{\ell} + \sum_{\substack{\mu=2 \\ \mu \text{ pair}}}^{n-2} \binom{\ell-1}{\mu} 6^{\ell-\mu-1} \frac{B_{\ell-\mu}}{\ell-\mu} p^\mu \qquad (\text{mod } p^n) .$$

Cette congruence, ou plutôt cette famille de congruences (pour ℓ et n variables) donne immédiatement la méthode LEM annoncée (LEM : Lehmer-Euler-Maclaurin) ; expliquons-la sur un exemple :

soit à calculer : $\frac{B_{32}}{32}$ (mod 37^8) ; on a $k = 32$, $m = 8$;

- on calcule S_{25} et C_{25} (mod 37^2) ;

  on inverse C_{25} (mod 37^2) (ça marche !) ; on note C^*_{25} l'inverse obtenu ;

  on pose (pour la généralité : voir plus loin)

  $S^*_{25} = S_{25}$;

  on obtient alors (grâce à (2.4) avec $\ell = 26$ et $n = 2$)

  $\frac{B_{26}}{26} \equiv 2\, C^*_{25} S^*_{25}$ (mod 37^2) ;

- on calcule S_{27} et C_{27} (mod 37^4) ;

  on inverse C_{27} (mod 37^4) (ça marche !) ; on note C^*_{27} l'inverse obtenu ;

  on pose $S^*_{27} \equiv S_{27} - \binom{27}{2} 6^{25} \frac{B_{26}}{26} 37^2$ (mod 37^4)

  (comme $\frac{B_{26}}{26}$ a été calculé précédemment (mod 37^2) , ceci a un sens !) ;

  on obtient alors (grâce à (2.4) avec $\ell = 28$ et $n = 4$)

  $\frac{B_{28}}{28} \equiv 2 C^*_{27} S^*_{27}$ (mod 37^4) ;

- on calcule S_{29} et C_{29} (mod 37^6) ;

  on inverse C_{29} (mod 37^6) (ça marche !) ; on note C^*_{29} l'inverse obtenu ;

on pose $S^*_{29} = S_{29} - \binom{29}{2} 6^{27} \frac{B_{28}}{28} 37^2$

$$- \binom{29}{4} 6^{25} \frac{B_{26}}{26} 37^4 \pmod{37^6}$$

(ce qui a un sens) ;

on obtient alors (grâce à (2.4) avec $\ell = 30$ et $n = 6$)

$$\frac{B_{30}}{30} \equiv 2 C^*_{29} S^*_{29} \pmod{37^6} \quad ;$$

- on calcule S_{31} et C_{31} (mod 37^8) ;

  etc.

  et on obtient finalement (grâce à (2.4) avec $\ell = 32$ et $n = 8$)

$$\frac{B_{32}}{32} \equiv 2C^*_{31} S^*_{31} \pmod{37^8} ,$$

Q.E.C. (quod erat computandum).

Le principe de calcul esquissé sur cet exemple appelle trois remarques.

(a) Le calcul en question (et plus spécialement l'utilisation de (2.4)) suppose vérifiée l'inégalité

$$m \le k - 1 - \mathrm{ord}_p(k) \quad ;$$

cette condition est toujours vérifiée dans la pratique : m intervenant en effet par l'intermédiaire de p^m , il n'est guère concevable de dépasser $m = 20$ ou 30 ; et les B_k pour $k \le 60$ sont connus explicitement depuis Adams. <u>De toute façon</u>, les congruences de Kummer permettent, pour m et k donnés, de remplacer k par

$$k + t(p-1)p^{m-1} \quad , \quad t \ge 1 \ ,$$

sans modifier le problème, et donc de réaliser l'inégalité.

(b) On a également supposé implicitement <u>tous les</u> $C_{\ell-1}$ <u>inversibles</u> (mod p). Si tel n'est pas le cas, il suffit, dans la congruence (2.4) écrite sous la forme

$$S^*_{\ell-1} \equiv \frac{1}{2} C_{\ell-1} \frac{B_\ell}{\ell} \pmod{p^n} ,$$

de "simplifier" par p^{ν_ℓ} , avec $\nu_\ell = \mathrm{ord}_p(C_{\ell-1})$; la congruence finale est alors modulo $p^{m-\sigma}$, avec $\sigma = \sum\limits_\ell \nu_\ell$, et il suffit de recommencer le calcul en augmentant la valeur de m , de manière à compenser la perte de précision due à σ . (Bien entendu, il peut arriver que σ augmente alors également ; mais des considérations "probabilistes" au sens de [8], pp. 18-22, montrent que σ ne dépassera pratiquement jamais la valeur 2).

(c) Enfin, on a aussi supposé implicitement tous les B_ℓ p-entiers, donc tous les ℓ rencontrés <u>non</u> congus à $0 \pmod{p-1}$. Supposons maintenant que tel n'est pas le cas ; on a alors

$$\ell = (p-1)p^v b \quad , \quad b \equiv 0 \pmod p ,$$

$$c^\ell \equiv 1 \pmod{p^{v+1}} \quad \text{pour tout} \quad c \equiv 0 \pmod p ,$$

et par conséquent

$$C_{\ell-1} \equiv 6^{-1} + 3^{-1} + 2^{-1} - 1^{-1} \equiv 0 \pmod{p^{v+1}} \quad ;$$

la congruence (2.4) s'écrit alors

$$S^*_{\ell-1} \equiv \frac{1}{2} \frac{C_{\ell-1}}{p^{v+1}} \frac{1}{(p-1)b} pB_\ell \pmod{p^n} ,$$

et le principe du calcul n'est pas essentiellement modifié, à condition d'avoir calculé $C_{\ell-1}$ modulo p^{n+v+1} (rappel : $pB_\ell \equiv -1 \pmod{p\mathbb{Z}_p}$). De toute façon, si la méthode LEM est appliquée à l'étude d'un couple <u>irrégulier</u> (p,h) , et si $m \leq 10$, ou si $p \neq 691$ et $m \leq 14$, l'accident évoqué ci-dessus ne produira pas, puisque les deux "plus petits" couples irréguliers sont $(691,12)$ et $(3617,16)$.

3. - LA METHODE LEM : PROGRAMMATION

L'exemple explicite traité au § 2 (calcul de $\frac{B_{32}}{32}$ (mod 37^8)) indique l'organisation du calcul :

- calcul, pour $2 \le \mu \le m$, $\ell = k-m+\mu$, $n = \mu$, des $S_{\ell-1}$ et des $C_{\ell-1}$ (mod p^n) ;
- inversion des $C_{\ell-1}$ (mod p^n) , autrement dit, calcul des $C^*_{\ell-1}$ (mod p^n) ; éventuellement, procédure de "rattrapage" pour les $C_{\ell-1}$ non inversibles ;
- calcul récurrent des $S^*_{\ell-1}$ et des $\frac{B_\ell}{\ell}$ (mod p^n) ; éventuellement, procédure de "rattrapage" pour les indices ℓ tel que $\frac{B_\ell}{\ell}$ ne soit pas p-entier ;

et obtention finale de $\frac{B_k}{k}$ (mod p^m) (pour $\mu = m$).

Le calcul en machine fait d'autre part intervenir le facteur <u>précision</u>, et doit donc tenir compte des ordres de grandeur de p^m et de k . En fait, les congruences de Kummer permettent de supposer k réduit (mod $(p-1)p^{m-1}$), donc inférieur à p^m . D'autre part, la structure de la congruence (2.4) incite à mettre un p-entier a (mod p^μ) sous la forme

$$a_o + a_1 q + \ldots + a_\nu q^\nu \pmod{p^\mu}$$

avec $q = p^r$, $\nu = \frac{\mu-2}{2}$, $0 \le a_i < q$ pour $0 \le i \le \nu$, et à calculer sur les hensimales a_i plutôt que sur a . C'est donc en fait l'ordre de grandeur de $q = p^2$ qui est à prendre en compte.

Les programmes "version 1" et "version 2" annoncés dans l'introduction, écrits en fait pour étudier les couples (p,h) irréguliers avec p petit, et avec la restriction (peu gênante : voir § 2) que les $\frac{B_\ell}{\ell}$ rencontrés sont tous p-entiers, peut être décrit de la façon suivante :

(A) <u>Procédures</u>. (Les numéros entre parenthèses renvoient aux lignes du programme BASIC donné en Annexe).

(1) On écrit des procédures de calcul hensimal : développement (8 000),

réduction (8 500), inversion (7 000), multiplication (6 000), exponentiation avec exposant entier ordinaire ou sous forme de développement hensimal (4 000) ;

(2) on écrit également une procédure de calcul des $C_{\ell-1}$ et des $6^{\ell-1}$ (3 000) et des $S_{\ell-1}$ (3 500). (La i-ème hensimale de $S_{\ell-1}$ (resp. $C_{\ell-1}$, $6^{\ell-1}$) pour $\ell = k-m+\mu$, $\mu = 2+2j$, $0 \le j \le N$, $N = \frac{m-2}{2}$, est notée SL(I,J) (resp. CF(I,J), PS(I,J) ; les valeurs de j indexent de 0 à N les $\frac{m}{2} = N+1$ étapes de la récurrence) ;

(3) on introduit d'autre part un premier indicateur IMP à valeurs 1 ou 2. Pour IMP = 1, le programme "fait l'impasse" et laisse la machine inverser les $C_{\ell-1}$ (avec arrêt et message d'erreur si un des $C_{\ell-1}$ n'est pas inversible) ; pour IMP = 2, le programme calcule $\sigma = \Sigma \nu_\ell$ (voir § 2) et agit en conséquence sur m (en fait, sur N) ;

(4) on introduit également un second indicateur VERS à valeurs 1 ou 2. Pour VERS = 1 ("version 1") la machine "connaît" k, ou plutôt

$$\varkappa = k+1-m = k-1-2N$$

comme entier (KAPPA) ; pour VERS = 2 ("version 2") comme développement hensimal (KH(I), $0 \le I \le N$).

(B) <u>Déroulement du calcul</u> (pour IMP = 1).

(1) On introduit (ou on calcule) p, k, N, $q = p^2$, $\varkappa = k-1-2N$, etc. (50 - 250) ;

(2) on calcule les $C_{\ell-1}$ et les $6^{\ell-1}$ (300) ;

(3) on calcule les $S_{\ell-1}$ (400) ;

(4) on calcule les $\frac{1}{(2j)!}$ (500). (La i-ème hensimale de $\frac{1}{(2j)!}$ est notée FC(I,J)) ;

(5) on commence alors une récurrence sur j, pour $0 \le j \le N$, avec

(5a) calcul hensimal de $(\varkappa+2j)(\varkappa+2j-1)$ (800). (La i-ème hensimale de ce produit est notée CD(I,J) ; les CD(I,J) et les FC(I,J) servent à calculer les coefficients binomiaux intervenant dans (2.4).)

(5b) calcul (pour l'indice j , et à partir des résultats obtenus pour les indices $\leq j-1$) du terme correctif

$$T_{\ell-1} = \sum_{\substack{\mu=2 \\ \mu \text{ pair}}} \binom{\ell-1}{\mu} 6^{\ell-\mu-1} \frac{B_{\ell-\mu}}{\ell-\mu} p^{\mu} \quad (\mathrm{mod}\ p^{2j+2}) \tag{3.1}$$

avec, rappelons-le, $\ell = \varkappa+1+2j$ (900) . (La i-ème hensimale de $T_{\ell-1}$ est notée TC(I,J) ; les hensimales HE(I,J) correspondent aux divers termes de la somme de droite dans (3.1).)

(5c) calcul de $SL^{*}_{\ell-1} = S_{\ell-1} - T_{\ell-1}$, inversion de $C_{\ell-1}$, d'où $C^{*}_{\ell-1}$, calcul de $\frac{B_\ell}{\ell}$ $(\mathrm{mod}\ p^{2j+2})$ avec toujours $\ell = \varkappa+1+2j$ (1 200) . (La i-ème hensimale de $\frac{B_\ell}{\ell}$ est notée BERN(I) ; elle est "oubliée" lors de la transition $j \leftarrow j+1$).

En fin de calcul (1 700 - 1 800) , les hensimales de $\frac{B_k}{k}$ $(\mathrm{mod}\ p^{m})$ sont les BERN(I) , $0 \leq I \leq N$.

Remarque. - Le premier programme donné en Annexe correspond en fait <u>uniquement</u> à la version 1 , avec implicitement VERS = 1 , et IMP = 1 (ce qui simplifie la lecture). Indiquons que les KD(I) sont les chiffres de $\varkappa$ en base $D = 256$, rangés en mémoire centrale à l'adresse 49152 + , et utilisés sous cette forme dans la procédure d'exponentiation, <u>via</u> deux petits programmes en langage machine, utilisés en 4 200 et 4 400 , et "implantés" en 10 000 - 10 210 . La version 2 diffère de la version 1 par le fait que k est entré en machine sous forme hensimale (et non en "simple précision"). Le calcul des KD(I) et leur rangement en mémoire centrale sont alors effectués par une "subroutine" en 11 000 , donnée également en Annexe, et qui (pratiquement) convertit l'écriture d'un nombre en base p^2 en son écriture en base $D = 256$.

ANNEXES

L'Annexe 1 est le listing du programme "Version 1" décrit plus haut. L'Annexe 2 donne les principales modifications à apporter à ce listing pour obtenir le programme "Version 1/2" : modification du début du programme (introduction de K) et adjonction d'un sous-programme 11 000 (calcul des KD à partir des KH).

L'Annexe 3 est une table de valeurs plus étendue que la table I mais correspondant au même problème. On y trouve (avec $p = 37$, $h = 32$) les $\frac{B_k}{k} \pmod{p^{12}}$ pour $k = k_r + (p-1)p^{r-1}j$, $j = 0,1,2,\ldots$

et $r = 1$, $k_r = 32$

$r = 2$, $k_r = 284$

$r = 3$, $k_r = 37\,580$

$r = 4$, $k_r = 1\,072\,544$

$r = 6$, $k_r = 325\,656\,968$

$r = 8$, $k_r = 2\,444\,284\,077\,476$

(dans ce dernier cas, le calcul a été fait modulo 37^{16} , ce qui permet en principe de calculer k_{16} ; par définition, k_r est le plus petit k tel que $\frac{B_k}{k} \equiv 0 \pmod{p^r}$).

Cette table permet diverses vérifications ; en particulier :

- les hensimales de $\frac{B_{32}}{32}$ sont celles qu'on calcule directement à partir de la valeur rationnelle connue de $\frac{B_{32}}{32}$;
- toutes les congruences de Kummer imaginables sont vérifiées ; etc.

ANNEXE 1.

```
10 REM ******************************
11 REM *                            *
12 REM *  CALCUL DE  Bk/k (MOD P↑M) *
13 REM *    PROGRAMME "VERSION 1"   *
14 REM *                            *
15 REM ******************************
20 REM
30 REM N = (M-2)/2
50 PRINT "P? K? N?"
60 INPUT P, K, N: Q = P*P: D = 256
70 GOSUB 10000
80 REM
100 PRINT "CALCUL DES KD"
110 KAPPA = K-1-2*N: W = KAPPA
120 FOR I = 0 TO 3
130 KD(I) = FND(W): W = INT(W/D)
140 POKE 49152+I, KD(I)
150 NEXT I
160 N2 = INT(LN(KAPPA)/LN(2))
170 REM
200 PRINT "CALCUL DES KH"
210 NU = N: X8 = KAPPA: GOSUB 8000
220 FOR I = 0 TO N
230 KH(I) = Z8(I)
240 NEXT I
250 REM
300 PRINT "CALCUL DES CF / PS"
310 NU = N: GOSUB 3000
400 PRINT "CALCUL DES SL"
410 NU = N: GOSUB 3500
420 REM
500 PRINT "CALCUL DES FC"
510 NU = N: TC(0) = 1
520 FOR I = 1 TO N
530 TC(I) = 0
540 NEXT I
550 FOR J = 1 TO N
560 J1 = 2*J*(2*J-1)
570 FOR I = 0 TO N
580 X8(I) = J1*TC(I)
590 NEXT I
600 NU = N: GOSUB 8500
610 FOR I = 0 TO N
620 TC(I) = Z8(I): X7(I) = TC(I)
630 NEXT I
640 NU = N: GOSUB 7000
650 FOR I = 0 TO N
660 FC(I,J) = Z7(I)
670 NEXT I
680 NEXT J
690 REM
700 PRINT "": PRINT "RECURRENCE SUR J"
710 FOR J = 0 TO N
720 PRINT "": PRINT "J =";J
750 IF J = 0 GOTO 1200
800 PRINT "CALCUL DES CD"
810 FOR I = 0 TO J
820 X6(I) = KH(I): Y6(I) = KH(I)
830 NEXT I
840 X6(0) = X6(0)+2*J: Y6(0) = X6(0)-1
850 NU = J: GOSUB 6000
860 FOR I = 0 TO J
870 CD(I) = Z6(I)
880 NEXT I
890 REM
900 PRINT "TRANSMISSION DES HE"
910 FOR I = 0 TO N
920 TC(I) = 0
930 NEXT I
940 FOR T = J TO 1 STEP -1
970 X6(0) = CD(0): Y6(0) = 0
980 FOR I = 1 TO J
990 X6(I) = CD(I): Y6(I) = HE(I-1,T-1)
1000 NEXT I
1010 NU = J: GOSUB 6000
1020 FOR I = 0 TO J
1030 HE(I,T) = Z6(I)
1050 X6(I) = FC(I,T): Y6(I) = HE(I,T)
1060 NEXT I
1070 NU = J: GOSUB 6000
1080 FOR I = 0 TO J
1090 TC(I) = TC(I)+Z6(I)
1100 NEXT I
1110 NEXT T
1190 REM
1200 REM CALCUL DES Bk/k SUCCESSIFS
1210 FOR I = 0 TO J
1220 IF J = 0 THEN TC(I) = 0
1230 X8(I) = 2*(SL(I,J)-TC(I))
1240 NEXT I
1250 NU = J: GOSUB 8500
1260 FOR I = 0 TO NU
1270 SL(I,J) = Z8(I)
1280 NEXT I
1300 REM
1500 PRINT "HENSIMALES DE Bk/k"
1510 FOR I = 0 TO J
1520 X7(I) = CF(I,J)
1530 NEXT I
1540 NU = J: GOSUB 7000
1550 FOR I = 0 TO J
1560 X6(I) = Z7(I): Y6(I) = SL(I,J)
1570 NEXT I
1580 NU = J: GOSUB 6000
1590 FOR I = 0 TO J
1600 BERN(I) = Z6(I)
1610 PRINT BERN(I);"  ";
1620 X6(I) = PS(I,J): Y6(I) = BERN(I)
1630 NEXT I
1640 PRINT "": NU = J: GOSUB 6000
```

```
1650 FOR I = 0 TO J
1660 HE(I,0) = Z6(I)
1670 NEXT I
1680 NEXT J
1690 PRINT ""
1700 REM
1710 PRINT "RESULTAT FINAL"
1720 FOR I = 0 TO N
1730 PRINT BERN(I);:PRINT"  ";
1740 NEXT I
1750 PRINT ""
2000 END
3000 PRINT "SUBR 3000"
3010 FOR J3 = 0 TO N
3020 CF(0,J3) = -1
3030 FOR I3 = 1 TO N
3040 CF(I3,J3) = 0
3050 NEXT I3
3060 NEXT J3
3070 FOR X3 = 0 TO 2
3080 X4 = 2+X3*X3: U3 = X4*X4
3170 GOSUB 4000
3180 FOR I3 = 0 TO N
3190 AF(I3) = Z4(I3)
3200 IF X4 = 6 THEN PS(I3,0)=AF(I3)
3210 CF(I3,0) = CF(I3,0)+AF(I3)
3220 NEXT I3
3230 FOR J3 = 1 TO N
3240 FOR I3 = 0 TO N
3250 X8(I3)=U3*AF(I3)
3260 NEXT I3
3270 GOSUB 8500
3280 FOR I3 = 0 TO N
3290 AF(I3) = Z8(I3)
3300 IF X4=6 THEN PS(I3,J3)=AF(I3)
3310 CF(I3,J3) = CF(I3,J3)+AF(I3)
3320 NEXT I3
3330 NEXT J3
3340 NEXT X3
3350 FOR J3 = 0 TO N
3360 FOR I3 = 0 TO N
3370 X8(I3) = CF(I3,J3)
3380 NEXT I3
3390 GOSUB 8500
3400 FOR I3 = 0 TO N
3410 CF(I3,J3) = Z8(I3)
3420 NEXT I3
3430 IF FNP(CF(0,J3)) > 0 GOTO 3480
3440 PRINT "J =";J3;": CF = 0 (MOD P)"
3470 NEXT J3
3480 RETURN
3490 REM
3500 PRINT "SUBR 3500"
3510 R3 = INT(P/6)
3520 FOR J3 = 0 TO N
3530 FOR I3 = 0 TO N
3540 SL(I3,J3) = 0
3550 NEXT I3
3560 NEXT J3
3570 FOR X4 = P-6 TO P-6*R3 STEP -6
3580 U3 = X4*X4
3660 GOSUB 4000
3670 FOR I3 = 0 TO N
3680 AL(I3) = Z4(I3)
3690 SL(I3,0) = SL(I3,0)+AL(I3)
3700 NEXT I3
3710 FOR J3 = 1 TO N
3720 FOR I3 = 0 TO N
3730 X8(I3)=U3*AL(I3)
3740 NEXT I3
3750 GOSUB 8500
3760 FOR I3 = 0 TO N
3770 AL(I3) = Z8(I3)
3780 SL(I3,J3) = SL(I3,J3)+AL(I3)
3790 NEXT I3
3800 NEXT J3
3810 NEXT X4
3820 FOR J3 = 0 TO N
3830 FOR I3 = 0 TO N
3840 X8(I3) = SL(I3,J3)
3850 NEXT I3
3860 GOSUB 8500
3870 FOR I3 = 0 TO N
3880 SL(I3,J3) = Z8(I3)
3890 NEXT I3
3900 NEXT J3
3950 RETURN
3990 REM
4000 PRINT "SUBR 4000": NU = N
4020 FOR I4 = 1 TO N
4030 Z4(I4) = 0: B4(I4) = 0
4040 NEXT I4
4050 Z4(0) = 1: B4(0) = X4
4200 USR(49000)
4300 FOR J4 = 0 TO N2
4310 FOR J4 = 0 TO N2
4400 USR(49012)
4500 IF PEEK(49160) = 0 GOTO 4600
4510 FOR I4 = 0 TO N
4520 X6(I4) = Z4(I4): Y6(I4) = B4(I4)
4530 NEXT I4
4540 GOSUB 6000
4550 FOR I4 = 0 TO N
4560 Z4(I4) = Z6(I4)
4570 NEXT I4
4600 FOR I4 = 0 TO N
4610 X6(I4) = B4(I4): Y6(I4) = B4(I4)
4620 NEXT I4
4630 GOSUB 6000
4640 FOR I4 = 0 TO N
4650 B4(I4) = Z6(I4)
4660 NEXT I4
4700 NEXT J4
4800 RETURN
```

```
6000 REM MULTIPLICATION
6010 FOR I6 = 0 TO NU
6020 A6 = 0
6030 FOR J6 = 0 TO I6
6040 A6 = A6 + X6(J6)*Y6(I6-J6)
6050 NEXT J6
6060 Z6(I6) = A6
6070 NEXT I6
6080 FOR I6 = 0 TO NU
6090 X8(I6) = Z6(I6)
6100 NEXT I6
6110 GOSUB 8500
6120 FOR I6 = 0 TO NU
6130 Z6(I6) = Z8(I6)
6140 NEXT I6
6800 RETURN
6900 REM
7000 REM INVERSION
7010 IF X7(0) = 1 GOTO 7400
7020 IF FNP(X7(0)) > 0 GOTO 7100
7030 PRINT "INCIDENT: P DIVISE X7(0)"
7100 R7(1) = Q: R7(2)=X7(0)
7110 R7(4) = 0: R7(5) = 1
7130 R7(0) = INT(R7(1)/R7(2))
7140 R7(3) = R7(1)-R7(0)*R7(2)
7150 R7(6) = R7(4)-R7(0)*R7(5)
7170 IF R7(3) = 1 GOTO 7220
7180 FOR I7 = 1 TO 5
7190 R7(I7) = R7(I7+1)
7200 NEXT I7
7210 GOTO 7130
7220 Z7(0) = FNQ(R7(6))
7230 GOTO 7500
7400 Z7(0) = 1
7500 A7 = (X7(0)*Z7(0)-1)/Q
7510 FOR I7 = 1 TO NU
7520 FOR J7 = 1 TO I7
7530 A7 = A7+X7(J7)*Z7(I7-J7)
7540 NEXT J7
7550 Z7(I7) = -Z7(0)*A7
7560 Z7(I7) = Z7(I7)-Q*INT(Z7(I7)/Q)
7570 A7 = A7+X7(0)*Z7(I7)
7580 A7 = A7/Q
7590 NEXT I7
7800 RETURN
```

```
8000 REM DEVELOPPEMENT DE HENSEL
8010 FOR I8 = 0 TO NU
8020 A8 = INT(X8/Q)
8030 Z8(I8) = X8-Q*A8
8040 X8 = A8
8050 NEXT I8
8060 RETURN
8500 REM REDUCTION
8510 FOR I8 = 0 TO NU
8520 A8 = INT(X8(I8)/Q)
8530 IF I8 = NU THEN GOTO 8550
8540 X8(I8+1) = X8(I8+1) + A8
8550 Z8(I8) = X8(I8) - Q*A8
8560 NEXT I8
8800 RETURN
8900 REM
10000 REM IMPLANT PROG LANG MACHINE
10100 LIMIT 49000
10110 FOR I = 0 TO 38
10120 READ J: POKE 49000+I,J
10130 NEXT I
10140 DATA 1,4,0,17,4,192,33,0,192
10150 DATA 237,176,201
10160 DATA 221,33,4,192
10170 DATA 221,203,3,30
10180 DATA 221,203,2,30
10190 DATA 221,203,1,30
10200 DATA 221,203,0,30
10210 DATA 62,0,143,50,8,192,201
10300 REM DEF FN ET DIMENSIONS
10310 DEF FND(X) = X-D*INT(X/D)
10320 DEF FNP(X) = X-P*INT(X/P)
10330 DEF FNQ(X) = X-Q*INT(X/Q)
10340 DIM KD(4),R7(6),KH(N)
10350 DIM X6(N),X7(N),X8(N)
10360 DIM U3(N),V3(N),Y6(N)
10370 DIM Z4(N),Z6(N),Z7(N),Z8(N)
10380 DIM A4(N),B4(N),AF(N),AL(N)
10390 DIM CD(N),TC(N),BERN(N)
10400 DIM FC(N,N),HE(N,N),SL(N,N)
10410 DIM CF(N,N),PS(N,N)
10500 RETURN
20000 END
```

ANNEXE 2.

```
15 PRINT "P? N? VERS?"
20 INPUT P, N, VERS:Q = P*P:D = 256
25 GOSUB 10000
30 ON VERS GOTO 80,40
40 PRINT "HENSIMALES DE K?"
45 FOR I = 0 TO N
50 INPUT X8(I)
55 NEXT I
60 GOSUB 11000
65 GOTO 250
80 PRINT "K?"
85 INPUT K: KAPPA = K-1-2*N
90 ND = 1+INT(LN(KAPPA)/LN(2))
100 PRINT "CALCUL DES KD"
110 W = KAPPA
120 FOR I = 0 TO 3
130 KD(I) = FND(W): W = INT(W/D)
140 PRINT KD(I);: POKE 49152+I, KD(I)
150 NEXT I
160 PRINT ""
200 PRINT "CALCUL DES KH"
210 NU = N: Y8 = KAPPA: GOSUB 8000
220 FOR I = 0 TO N
230 KH(I) = Z8(I): PRINT KH(I);
240 NEXT I
250 PRINT""
300 PRINT "CALCUL DES CF ET DES PS"
.....
```

```
11000 REM CHARG DE KD EN MEM CENTRALE
11010 X8(0) = X8(0)-1-2*N
11020 NU = N: GOSUB 8500
11030 FOR I = 0 TO N
11040 KH(I) = Z8(I): X1(I) = KH(I)
11050 NEXT I
11100 X8(0) = D                 :REM D = 256
11110 FOR I = 1 TO N
11120 X8(I) = 0
11130 NEXT I
11140 NU = N: GOSUB 8500
11200 FOR I = 0 TO N
11210 X7(I) = Z8(I)
11220 NEXT I
11230 NU = N: GOSUB 7000
11250 FOR I = 0 TO N
11260 Y6(I) = Z7(I)
11270 NEXT I
11300 Q1 = FND(Q)
11310 NQ = N
11320 IF X1(NQ) > 0 GOTO 11350
11330 NQ = NQ-1: GOTO 11320
11350 ND = INT((NQ+1)*LN(Q)/LN(D))
11360 N2 = INT((NQ+1)*LN(Q)/LN(2))
11400 FOR I1 = 0 TO ND
11410 A1 = 0: R1 = 1
11420 FOR J1 = 0 TO NQ
11430 A1 = A1+R1*X1(J1)
11440 R1 = FND(Q1*R1)
11450 NEXT J1
11460 A1 = FND(A1)
11470 A1 = A1-256*INT(A1/256)
11480 POKE 49152+I1,A1
11500 X6(0) = X1(0)-A1
11510 FOR J1 = 1 TO NQ
11520 X6(J1) = X1(J1)
11530 NEXT J1
11540 NU = N: GOSUB 6000
11550 FOR J1 = 0 TO NQ
11560 X1(J1) = Z6(J1)
11570 NEXT J1
11580 NEXT I1
11700 PRINT "(256)-IMALES DE KH"
11800 FOR I1 = ND TO 0 STEP -1
11810 PRINT PEEK(49152+I1);"   ";
11820 NEXT I1
11830 PRINT ""
11900 RETURN
```

ANNEXE 3.

TABLE DES HENSIMALES DES Bk/k POUR LE COUPLE P = 37, H = 32

** K = 32 **	37	1139	1035	383	1348	846
** K = 68 **	814	1008	1201	1034	1052	783
** K = 104 **	222	989	14	1030	833	982
** K = 140 **	999	451	696	122	830	43
** K = 176 **	407	136	53	1344	1316	595
** K = 212 **	1184	782	1352	1315	963	1116
** K = 248 **	592	393	1188	154	1355	576
** K = 284 **	0	1077	986	1001	190	1222
** K = 320 **	777	835	717	692	621	66
** K = 356 **	185	409	817	466	1269	867

** K = 284 **	0	1077	986	1001	190	1222
** K = 1616 **	0	358	946	989	522	1269
** K = 2948 **	0	1008	1349	739	332	110
** K = 4280 **	0	289	828	235	239	884
** K = 5612 **	0	939	750	828	1328	559
** K = 6944 **	0	220	1117	1132	1046	1161

** K = 37580 **	0	111	666	245	701	650
** K = 86864 **	0	888	535	870	643	505
** K = 136148 **	0	296	405	570	629	739
** K = 185432 **	0	1073	274	714	29	774
** K = 234716 **	0	481	144	1302	952	201
** K = 284000 **	0	1258	13	965	32	1353

```
** K = 1072544 **          0   0   665    1195   265    1106
** K = 2896052 **          0   0   1315   1043   417    1200
** K = 4719560 **          0   0   596    892    1013   1078
** K = 6543068 **          0   0   1246   740    684    741
** K = 8366576 **          0   0   527    589    799    188
** K = 10190084 **         0   0   1177   437    1358   788
** K = 12013592 **         0   0   458    286    992    1173
** K = 13837100 **         0   0   1108   134    1070   1342
** K = 15660608 **         0   0   389    1352   222    1296
** K = 17484116 **         0   0   1039   1200   1188   1033

** K = 325656968 **            0   0   0   235   33     380
** K = 2822039420 **           0   0   0   885   1250   1308
** K = 5318421872 **           0   0   0   166   1099   868
** K = 7814804324 **           0   0   0   816   947    428

** K = 2444284077476 **        0   0   0   0   911   746   9     654
** K = 5861831654264 **        0   0   0   0   192   595   938   131
** K = 9279379231052 **        0   0   0   0   842   443   498   978
** K = 12696926807840 **       0   0   0   0   123   292   58    456
```

BIBLIOGRAPHIE

[1] Compléments à cet exposé : JOLY J.R., Calcul des nombres de Bernoulli modulo p^m et application à l'étude des nombres premiers irréguliers (manuscrit polycopié), Grenoble, Laboratoire de Mathématiques Pures, Nov. 1981.

[2] IWASAWA K. + SIMS C.C., Computation of invariants in the theory of cyclotomic fields, J. Math. Soc. Japan, 18, 1966, pp. 86-96.

[3] JOHNSON W., Irregular prime divisors of the Bernoulli numbers, Math. Comp., 28, 1974, pp. 653-657.

[4] JOHNSON W., Irregular primes and cyclotomic invariants, Math. Comp., 29, 1975, pp. 113-120.

[5] KOBLITZ N., p-adic Numbers, p-adic Analysis and Zeta-Functions, Springer-Verlag.

[6] KOBLITZ N., p-adic Analysis : a Short Course on Recent Work, Cambridge University Press.

[7] LANG S., Cyclotomic Fields I, Springer-Verlag.

[8] LANG S., Cyclotomic Fields II, Springer-Verlag.

[9] LEHMER E., On congruences involving Bernoulli numbers and the quotients of Fermat and Wilson, Ann. of Math. 39, 1938, pp. 350-360.

[10] SIEGEL ("Conjecture de Siegel") : Oeuvres Complètes.

[11] WADA (Calculs mod p^3) . Cité par JOHNSON.

[12] WAGSTAFF S.S., Zeroes of p-adic L-functions, Math. Comp., 29, 1975, pp. 1138-1143.

[13] WAGSTAFF S.S., The irregular primes to 125 000 , Math. Comp., 32, 1978, pp. 583-591.

[14] WASHINGTON L., Sur les zéros des séries L p-adiques, exposés de Séminaire (Paris, Grenoble,... ; 1981).
