

Certains calculs numériques relatifs à l'interpolation
p-adique des séries de Dirichlet

par P.CARTIER (Bures-sur-Yvette) et Y.ROY (Strasbourg)

Table des Matières

Introduction	270
§1. Sur la théorie des fonctions zêta p-adiques	273
§2. Résultats numériques	280
§3. Calcul numérique des fonctions zêta	289
Bibliographie	306
Tables	309

Introduction

Soient K un corps de nombres, totalelement réel et abélien, et p un nombre premier. Kubota et Leopoldt [12] ont construit une fonction analytique p -adique qui interpole les nombres $\zeta_K^{(p)}(1-k)$ pour $k \equiv 0 \pmod{p}$, $k \geq 1$; on a noté $\zeta_K^{(p)}$ la fonction zêta du corps K débarrassée de son facteur local en p . On renvoie le lecteur à l'excellent petit livre d'Iwasawa [9] pour l'exposé de cette théorie. Lorsque le corps K n'est plus abélien, on savait par Siegel que les nombres $\zeta_K(1-k)$ sont rationnels pour $k \geq 1$ entier; Klingen [10] a étendu ce résultat aux fonctions zêta associées aux classes d'idéaux, en interprétant les nombres $\zeta_K(1-k)$ comme termes constants de certaines formes modulaires. Sa méthode a été approfondie par Serre, et l'on trouvera ses résultats dans ce même volume.

Au début de ses recherches, en février 1971, Serre nous avait suggéré d'étudier numériquement les fonctions zêta de certains corps non abéliens, et d'en inférer la possibilité d'étendre à ce cas les résultats de Kubota-Leopoldt et Iwasawa. A cette époque, Y. Roy venait de mettre au point un système (écrit en langage assembleur) pour traiter des grands entiers ($\leq 10^{600}$) sur ordinateur. Le problème de Serre nous sembla un excellent test de l'efficacité de ce système. Les calculs furent donc entrepris sur l'ordinateur modèle IBM 360/44 du centre de calcul de l'Esplanade à Strasbourg, et durèrent de mars 1971 à avril 1972.

Les premiers résultats sur le corps cubique de discriminant 148 dépassèrent nos espérances, et nous firent entreprendre une étude systématique. Dès juillet 1971, nous disposions de tables étendues sur les corps cubiques. La critique de Weil, exprimée dans une lettre dosant artistiquement le chaud et le froid, nous poussa à sortir franchement du cas abélien en étudiant certains corps de degré 4 ou 5 à groupe de Galois non résoluble. Dans les 80 cas étudiés, les résultats sont frappants; ils

semblent avoir encouragé Serre dans sa recherche, et suggèrent plus que la théorie ne sait établir actuellement.

Le plan de ce rapport est le suivant. La première partie est un résumé des résultats théoriques connus, y compris ceux de Serre. La deuxième partie décrit les résultats et la troisième la méthode de nos calculs. Enfin nous donnons en annexe un extrait de nos tables, qui font environ 600 pages.

Nos remerciements chaleureux vont à J.-P. Serre pour l'enthousiasme avec lequel il a suivi nos efforts, et le soin qu'il a pris à nous instruire de cette théorie. Ils vont aussi à W. Mercuroff qui n'a démantelé le centre de calcul de Strasbourg qu'après l'achèvement de ce travail.

Notations générales.

On note	$\mathbb{Z}$	l'anneau des entiers rationnels
	$\mathbb{Q}$	le corps des nombres rationnels
	$\mathbb{R}$	le corps des nombres réels
	$\mathbb{C}$	le corps des nombres complexes
Re	s	la partie réelle du nombre complexe s
	p	un nombre premier
	$\mathbb{F}_p$	le corps des entiers modulo p
	$\mathbb{Z}_p$	l'anneau des entiers p -adiques
	$\mathbb{Q}_p$	le corps des nombres rationnels p -adiques
	$\mathbb{C}_p$	la complétion d'une clôture algébrique de $\mathbb{Q}_p$
	$\mathcal{O}_p$	l'anneau des entiers de $\mathbb{C}_p$

K un corps de nombres algébriques totalement réel

D le discriminant de K

r le degré de K (sur $\mathbf{Q}$) (supposé fini)

$A[[T]]$ l'algèbre des séries formelles à coefficients dans
l'anneau A .

$A[T]$ l'algèbre des polynômes à coefficients dans l'anneau A .

S1. Sur la théorie des fonctions zêta p-adiques

1. Nombres de Bernoulli.

Ils sont définis par la série génératrice

$$(1) \quad \sum_{n=0}^{\infty} B_n \frac{X^n}{n!} = \frac{X}{e^X - 1},$$

d'où les premiers nombres de la suite

$$(2) \quad B_0 = 1, B_1 = -\frac{1}{2}, B_2 = \frac{1}{6}, B_3 = 0, B_4 = -\frac{1}{30}.$$

D'après un résultat fameux d'Euler, on a

$$(3) \quad \sum_{n=1}^{\infty} \frac{1}{n^{2k}} = (-1)^{k+1} \frac{(2\pi)^{2k}}{2 \cdot (2k)!} B_{2k}$$

pour $k = 1, 2, \dots$ et en particulier $\sum_{n=1}^{\infty} \frac{1}{n^2} = \frac{\pi^2}{6}$. La formule précédente donne le signe et une bonne valeur approchée de B_{2k} : lorsque $k \geq 10$ par exemple, la somme de la série $\sum_{n=1}^{\infty} \frac{1}{n^{2k}}$ diffère de 1 de moins de 10^{-6} . Noter aussi qu'on a $B_{2k+1} = 0$ pour $k \geq 1$.

Le résultat précédent s'explique par la fonction zêta de Riemann, définie par $\zeta(s) = \sum_{n=1}^{\infty} n^{-s}$ lorsque $\operatorname{Re} s > 1$. La formule (3) montre en particulier que $\pi^{-2k} \zeta(2k)$ est un nombre rationnel pour $k \geq 1$. Pour se débarrasser des puissances de π , on utilise le prolongement analytique de $\zeta(s)$ et l'équation fonctionnelle bien connue

$$(4) \quad \zeta(1-s) = 2 \cdot (2\pi)^{-s} \Gamma(s) \cos \frac{\pi s}{2} \zeta(s).$$

Les résultats du premier alinéa sont alors contenus dans la formule d'Euler

$$(5) \quad \zeta(1-k) = -B_k/k \quad \text{pour } k \geq 2 \text{ entier.}$$

Autrement dit, les valeurs de la fonction ζ aux entiers négatifs sont des nombres rationnels, que l'on peut calculer facilement au moyen de rela-

tions de récurrence déduites de la série génératrice des nombres de Bernoulli

Plus généralement, soit χ un caractère primitif de Dirichlet, de conducteur f . La fonction L associée est définie par $L(s; \chi) = \sum_{n=1}^{\infty} \chi(n) n^{-s}$ lorsque $\text{Re } s > 1$. Lorsque $f = 1$, on retrouve la fonction ζ de Riemann; si non, $L(s; \chi)$ se prolonge en une fonction holomorphe sur $\mathbf{C}$, dont la valeur aux entiers négatifs est donnée par la formule de Leopoldt [13]

$$(6) \quad L(1-k; \chi) = -B_{k, \chi} / k, \text{ pour } k \geq 1.$$

Le polynôme de Bernoulli $B_n(X)$ est égal comme d'habitude à $\sum_{j=0}^n \binom{n}{j} B_j X^{n-j}$ et les nombres de Bernoulli généralisés sont définis comme suit

$$(7) \quad B_{k, \chi} = \frac{1}{f} \sum_{a=1}^f \chi(a) f^k B_k\left(\frac{a}{f}\right).$$

2. Interpolation p-adique.

Avant de pouvoir formuler les résultats de Kubota-Leopoldt, Iwasawa et Serre, nous devons rappeler les principes généraux de l'interpolation p-adique.

Choisissons un nombre premier p et notons $\mathbf{C}_p$ la complétion d'une clôture algébrique du corps p-adique $\mathbf{Q}_p$; on normalise la valeur absolue dans $\mathbf{C}_p$ par $|p| = p^{-1}$ et l'on note $\mathcal{O}_p$ l'anneau des éléments x de $\mathbf{C}_p$ tels que $|x| \leq 1$.

Soit par ailleurs $b = (b_0, b_1, \dots)$ une suite d'éléments de $\mathbf{C}_p$. On définit comme d'habitude les différences itérées de cette suite par les formules

$$(8) \quad \Delta^0 b_k = b_k \quad (k \geq 0)$$

$$(9) \quad \Delta^n b_k = \Delta^{n-1} b_{k+1} - \Delta^{n-1} b_k \quad (n \geq 1, k \geq 0)$$

et l'on définit les coefficients d'interpolation $c_n = \Delta^n b_0$, soit plus explicitement

$$(10) \quad c_n = \sum_{j=0}^n (-1)^{n-j} \binom{n}{j} b_j.$$

Pour tout entier $n \geq 0$, on a inversement

$$(11) \quad b_k = \sum_{n=0}^{\infty} c_n \binom{k}{n}.$$

On a alors le critère de Mahler : pour qu'il existe une fonction continue
 $f : \mathbb{Z}_p \rightarrow \mathbb{C}_p$ telle que $f(k) = b_k$ pour tout entier $k \geq 0$, il faut et suffit
 qu'on ait $\lim_{n \rightarrow \infty} |c_n| = 0$. La fonction f est définie par le développement
 binomial

$$(12) \quad f(x) = \sum_{n=0}^{\infty} \frac{c_n}{n!} (x)_n,$$

avec la définition usuelle des "puissances binomiales" (sous la forme "descendante")

$$(13) \quad (x)_n = x(x-1)\dots(x-(n-1)).$$

Pour déduire de là un développement en série de puissances pour $f(x)$, introduisons les nombres de Stirling $S_n^{(m)}$ (pour $0 \leq m \leq n$) par l'identité

$$(14) \quad (X)_n = \sum_{m=0}^n S_n^{(m)} X^m$$

on calcule ces entiers par la formule de récurrence usuelle

$$(15) \quad S_{n+1}^{(m)} = S_n^{(m-1)} - n S_n^{(m)} \quad (1 \leq m \leq n)$$

et les conditions aux limites $S_0^{(0)} = 1$, $S_n^{(0)} = 0$ et $S_n^{(n)} = 1$ pour $n \geq 1$.

Posons alors $q = p$ si $p \neq 2$ et $q = 4$ si $p = 2$; de plus, posons

$R = p^{\frac{p-2}{p-1}}$ si $p \neq 2$ et $R = 2$ si $p = 2$. Supposons que les coefficients d'interpolation c_n satisfassent à la congruence

$$(16) \quad c_n \equiv 0 \pmod{q^n \mathcal{O}_p}.$$

On peut alors définir de nouveaux coefficients a_m par la série convergente

$$(17) \quad a_m = \sum_{n=m}^{\infty} S_n^{(m)} c_n / n!$$

et la fonction f d'interpolation définie par (12) admet le développement en série de Taylor

$$(18) \quad f(x) = \sum_{m=0}^{\infty} a_m x^m$$

de rayon de convergence $\geq R$. Autrement dit, si l'on a $c_n \equiv 0 \pmod{q^n \mathcal{O}_p}$ pour tout $n \geq 0$, il existe une fonction f analytique dans le disque ouvert $\{x \in \mathbf{C}_p \mid \|x\| < R\}$ de $\mathbf{C}_p$ et telle que $f(k) = b_k$ pour $k \geq 0$.

Les méthodes d'Iwasawa [8] suggèrent une notion plus restrictive d'analyticité qui a été étudiée systématiquement par Serre [15]. Notons U_1 le groupe multiplicatif des éléments x de $\mathbf{Z}_p$ tels que $x \equiv 1 \pmod{q}$ $\mathbf{Z}_p$. Choisissons un isomorphisme de groupes topologiques $\phi : \mathbf{Z}_p \rightarrow U_1$, par exemple $\phi(x) = (1+q)^x = \sum_{n=0}^{\infty} \frac{q^n}{n!} (x)_n$ ou $\phi(x) = \exp qx = \sum_{n=0}^{\infty} \frac{q^n}{n!} x^n$. D'après Serre on appelle algèbre d'Iwasawa l'ensemble des fonctions $f : \mathbf{Z}_p \rightarrow \mathbf{C}_p$ de la forme

$$(19) \quad f(x) = F(\phi(x)-1) \quad \text{avec } F \in \mathcal{O}_p[[T]].$$

On voit facilement que l'algèbre d'Iwasawa ne dépend pas du choix de l'isomorphisme ϕ .

On dira par abus de langage que la suite $b = (b_0, b_1, \dots)$ d'éléments de $\mathbf{C}_p$ appartient à l'algèbre d'Iwasawa s'il existe une fonction $f : \mathbf{Z}_p \rightarrow \mathbf{C}_p$

de la forme (19) et telle que $f(k) = b_k$ pour tout entier $k \geq 0$. Il revient au même de dire qu'il existe une série formelle $F \in \mathcal{O}_p[[T]]$ telle que $b_k = F(\gamma^k - 1)$ pour tout $k \geq 0$, le nombre p -adique γ étant choisi de la forme $\gamma = 1 + qu$ avec une unité p -adique u . Par une généralisation facile des résultats de Serre [15], on obtient le critère suivant : la suite b appartient à l'algèbre d'Iwasawa si et seulement si l'on a les congruences $c_n \equiv 0 \pmod{q^n \mathcal{O}_p}$ déjà rencontrées plus haut, et si de plus les éléments $d_n = \sum_{m=0}^n S_n^{(m)} c_m / q^m$ de $\mathcal{O}_p$ sont divisibles par $n!$ dans $\mathcal{O}_p$. En particulier, la classe de $c_n / q^n \pmod{p \mathcal{O}_p}$ ne dépend alors que de la classe de $n \pmod{p-1}$ (pour $n \geq 1$).

3. Les fonctions zêta p -adiques des corps abéliens totalement réels.

Tout repose sur les propriétés arithmétiques des nombres de Bernoulli. Il est bien connu ("congruences de Kummer") que si n n'est pas divisible par $p-1$, le nombre rationnel B_n/n est p -entier (autrement dit, de la forme a/b avec $b \not\equiv 0 \pmod{p}$) et que sa classe modulo p ne dépend que de la classe de n modulo $p-1$. Plus généralement, posons $\zeta^{(p)}(s) = (1 - p^{-s})\zeta(s)$ et considérons les $p-2$ "sous-séries" formées des valeurs de $\zeta^{(p)}(-n)$ sur les progressions arithmétiques de période $p-1$ à l'exception de la progression $-n \equiv 1 \pmod{p-1}$, soit

$$\zeta^{(p)}(0), \zeta^{(p)}(1-p), \zeta^{(p)}(2-2p), \zeta^{(p)}(3-3p), \dots$$

$$\zeta^{(p)}(-1), \zeta^{(p)}(-p), \zeta^{(p)}(1-2p), \zeta^{(p)}(2-3p), \dots$$

$$\zeta^{(p)}(3-p), \zeta^{(p)}(4-2p), \zeta^{(p)}(5-3p), \zeta^{(p)}(6-4p), \dots$$

Iwasawa a prouvé que chacune des sous-séries précédentes appartient à l'algèbre d'Iwasawa. Pour la sous-série restante, il faut une petite modification; c'est la suite des nombres $(\gamma^{(1+k)(p-1)} - 1)\zeta^{(p)}(1 - (k+1)(p-1))$ pour $k \geq 0$ qui appartient à l'algèbre d'Iwasawa.

On peut généraliser ceci aux séries $L(s; \chi)$. Choisissons un isomorphisme $x \mapsto x^\sigma$ du corps $\bar{\mathbb{Q}}$ des nombres algébriques dans le corps algébriquement clos $\mathbb{C}_p$. Il existe alors un unique caractère ω_p , de conducteur q , tel que $\omega_p(x)^\sigma \equiv x \pmod{q \mathcal{O}_p}$ pour tout x entier. De plus, si $L(s) = \sum_{n=1}^{\infty} a_n n^{-s}$ est une série de Dirichlet, on note $L^{(p)}(s)$ la série de Dirichlet $\sum_{(n,p)=1} a_n n^{-s}$ d'où l'on a ôté les termes $a_n n^{-s}$ avec $n \equiv 0 \pmod{p}$. En particulier, on a $\zeta^{(p)}(s) = (1-p^{-s}) \zeta(s)$ comme plus haut et $L^{(p)}(s, \chi) = (1-\chi(p)p^{-s}) L(s; \chi)$. Avec ces notations, Iwasawa a montré que si le caractère χ est distinct de ω_p^{-1} , la suite des nombres $L^{(p)}(-k; \chi \omega_p^{-k})$ pour $k = 0, 1, 2, \dots$ appartient à l'algèbre d'Iwasawa. On en déduit que si χ est distinct du caractère ω_p^{-j} , la suite des éléments $L^{(p)}(1-j-n(p-1); \chi)$ pour $n = 0, 1, 2, \dots$ appartient à l'algèbre d'Iwasawa (pour $j = 1, 2, \dots, p-1$ fixé).

Soit K un corps de nombres totalement réel, abélien et de degré r sur le corps $\mathbb{Q}$ des nombres rationnels et soit ζ_K la fonction zêta du corps K . D'après la théorie du corps de classes, il existe r caractères $\chi_1, \dots, \chi_r$ dont le conducteur divise le discriminant D de K , et tels que $\zeta_K(s) = \prod_{j=1}^r L(s; \chi_j)$. Posons $L(s) = \zeta_K(s)/\zeta(s)$. Ce qui précède montre alors que pour $k \geq 0$, le nombre $L(-k)$ est rationnel et n'a en dénominateur que des nombres premiers divisant le discriminant D de K . De plus si p ne divise pas D , les $p-1$ sous-séries formées des nombres $L^{(p)}(1-j-k(p-1))$ pour $k = 0, 1, 2, \dots$ (on fixe $j = 1, 2, \dots, p-1$) appartiennent à l'algèbre d'Iwasawa.

4. Les résultats de Serre [15].

Serre considère un corps K , totalement réel de degré r sur $\mathbb{Q}$, et les nombres rationnels $\zeta_K(1-k)$ pour $k = 1, 2, \dots$. Les résultats sont de deux ordres.

THÉORÈME D'INTÉGRALITÉ : a) Si $k \geq 1$ est pair et $rk \not\equiv 0 \pmod{p-1}$, alors $\zeta_K(1-k)$ est p-entier.

b) Si $k \geq 1$ est pair et $rk \equiv 0 \pmod{p-1}$, alors $p^{rk} \zeta_K(1-k)$ est p-entier pour $p \neq 2$.

c) Si $k \geq 1$ est pair, le nombre $2^{2-rk} \zeta_K(1-k)$ est 2-entier.

INTERPOLATION p-ADIQUE : Supposons d'abord $p \neq 2$. Choisissons un générateur topologique γ de $U_1 = 1 + \mathfrak{p} \mathbb{Z}_p$, et un entier pair j compris entre 1 et $p-1$.

a) Si $rk \not\equiv 0 \pmod{p-1}$, il existe une série formelle $F_j \in \mathbb{Z}_p[[T]]$ telle que $\zeta_K^{(p)}(1-k) = F_j(\gamma^k - 1)$, pour tout entier $k \geq 2$ tel que $k \equiv j \pmod{p-1}$.

b) Si $rk \equiv 0 \pmod{p-1}$, il existe une série formelle $F_j^* \in \mathbb{Z}_p[[T]]$ telle que $\zeta_K^{(p)}(1-k) = \frac{F_j^*(\gamma^k - 1)}{\gamma^{rk} - 1}$ pour tout entier $k \geq 2$ tel que $k \equiv j \pmod{p-1}$.

Supposons maintenant $p = 2$. Il existe alors une série $F \in \mathbb{Z}_2[[T]]$ telle que $2^{-rk} \zeta_K^{(2)}(1-k) = \frac{F(\gamma^k - 1)}{\gamma^{rk} - 1}$ pour $k \geq 2$ pair.

Avec les notations de Serre, on a dans le cas a) $\zeta_K^*(1-x; 1-u) = F_j(\gamma^x - 1)$ pour $x \in \mathbb{Z}_p$, en notant u la classe de j modulo $p-1$. Il faut remplacer $F_j(T)$ par $\frac{F_j^*(T)}{(1+T)^{r-1}}$ dans le cas b); modification analogue pour $p = 2$.

§2. Résultats numériques5. Description des corps étudiés.

Nous donnons d'abord la description précise des 63 corps totale-
ment réels de degré 3, 4 ou 5 que nous avons étudiés.

A) Corps cycliques de degré 3 et discriminant ≤ 900 .

Si K est un tel corps, son discriminant est un carré $D = d^2$, le corps K est contenu dans le corps cyclotomique $\mathbb{Q}(e^{2\pi i/d})$ et il existe un sous-groupe H du groupe multiplicatif $(\mathbb{Z}/d\mathbb{Z})^\times$ avec les propriétés suivantes :

a) la classe de -1 modulo d appartient à H ;

b) il n'existe aucun diviseur $d' \neq d$ de d tel que H contienne toutes les classes modulo d des entiers a premiers à d et tels que $a \equiv 1 \pmod{d'}$;

c) H est d'indice 3 dans $(\mathbb{Z}/d\mathbb{Z})^\times$;

d) notons $C_0 = H$, C_1 et C_2 les classes de $(\mathbb{Z}/d\mathbb{Z})^\times$ modulo H , et posons $z_j = \sum_{a \in C_j} e^{2\pi i a/d}$ pour $j = 0, 1, 2$. Si d n'est pas divisible par 3, alors (z_0, z_1, z_2) est une base sur $\mathbb{Z}$ de l'anneau des entiers de K .

Les propriétés a), b) et c) montrent que d est de l'une des formes $3^2 p_1 \cdots p_r$ ou $p_1 \cdots p_r$, où $p_1, \dots, p_r$ sont des nombres premiers congrus à 1 modulo 6, et deux à deux distincts. Les nombres premiers $p \equiv 1 \pmod{6}$ au plus égaux à 30 sont 7, 13, 19 et par suite les discriminants $D \leq 900$ sont $3^4 = 81$, $7^2 = 49$, $13^2 = 169$, $19^2 = 361$. Dans chacun de ces cas, le groupe $(\mathbb{Z}/d\mathbb{Z})^\times$ est cyclique et contient donc un seul sous-groupe H d'indice 3; choisissons une racine primitive g modulo d et notons C_j l'ensemble des entiers congrus modulo d à l'un des entiers g^{j+3n} pour $n \geq 0$. On a le tableau suivant (avec $g = 2$ pour $d \neq 7$ et $g = -2$ pour $d = 7$).

D	81	49	169	361
C_0	1	1	1, 5	1, 7, 8
C_1	2	2	2, 3	2, 3, 5
C_2	4	3	4, 6	4, 6, 9

Pour chaque classe C_j , on a donné la liste des éléments a compris entre 1 et $\frac{d-1}{2}$; les autres éléments sont les nombres de la forme $nd \pm a$ avec n entier.

Le tableau précédent donne immédiatement la valeur de $x = z_C$. Nous y avons adjoint l'équation irréductible satisfaite par x .

$$D = 49 \quad x = 2\cos \frac{2\pi}{7} \quad x^3 + x^2 - 2x - 1 = 0$$

$$D = 81 \quad x = 2\cos \frac{2\pi}{9} \quad x^3 - 3x + 1 = 0$$

$$D = 169 \quad x = 2\cos \frac{2\pi}{13} + 2\cos \frac{10\pi}{13} \quad x^3 + x^2 - 4x + 1 = 0$$

$$D = 361 \quad x = 2\cos \frac{2\pi}{19} + 2\cos \frac{14\pi}{19} + 2\cos \frac{16\pi}{19} \quad x^3 + x^2 - 6x - 7 = 0.$$

On peut montrer que $(1, x, x^2)$ est une base des entiers de K .

B) Corps non abéliens de degré 3 et discriminant ≤ 1257 .

Il y a 28 corps de cette classe; la table 1 donne pour chacun d'eux le discriminant et sa décomposition en facteurs premiers, et l'équation irréductible satisfaite par un élément x tel que $K = \mathbb{Q}(x)$. On a choisi x de sorte que les monômes $1, x, x^2$ forment une base sur $\mathbb{Z}$ de l'anneau des entiers de K . La table 1 est copiée de Delone et Faddeev [6].

C) Corps non abéliens de degré 4 ne contenant aucun sous-corps non-trivial, et de discriminant ≤ 8069 .

Il y a 9 corps de cette classe; la table 2 donne pour chacun d'eux le discriminant et sa décomposition en facteurs premiers, et une équation définissant le corps. Si L est la clôture galoisienne de K , le groupe

de Galois de L sur $\mathbb{Q}$ est le groupe symétrique S_4 d'ordre $4!$. Dans chacun des cas, le générateur x de K est tel que $(1, x, x^2, x^3)$ soit une base sur $\mathbb{Z}$ de l'anneau des entiers de K .

D) Corps non abéliens K de degré 4, contenant un sous-corps quadratique E , et de discriminant ≤ 8112 .

Il y a 18 corps de cette catégorie, décrits par la table 3. Dans chaque cas, on a donné le discriminant D de K , le discriminant d de E , un générateur η de E et un générateur x de K . Dans tous les cas, la famille $(1, \eta, x, x\eta)$ est une base sur $\mathbb{Z}$ de l'anneau des entiers du corps K , et la clôture galoisienne L de K est de degré 8 sur $\mathbb{Q}$, de groupe de Galois diédral d'ordre 8.

E) Le corps de degré 5 et discriminant $11^4 = 14641$.

C'est la partie réelle du corps cyclotomique $\mathbb{Q}(e^{2\pi i/11})$. Il est engendré par $x = 2\cos \frac{2\pi}{11}$ dont l'équation irréductible est

$$x^5 + x^4 - 4x^3 - 3x^2 + 3x + 1 = 0.$$

L'anneau des entiers admet $(1, x, x^2, x^3, x^4)$ pour base sur $\mathbb{Z}$.

F) Corps de degré 5 non abéliens.

Il s'agit de 3 corps, dont nous donnons le discriminant et l'équation irréductible satisfaite par un générateur x

$$24217 \quad x^5 - 5x^3 + x^2 + 5x - 1 = 0$$

$$36497 \quad x^5 - 6x^3 - x^2 + 4x - 1 = 0$$

$$38569 \quad x^5 - 5x^3 + 4x - 1 = 0.$$

On a $24217 = 61.397$ et les nombres 36497 et 38569 sont premiers. Comme le discriminant n'est pas divisible par un carré, l'anneau des entiers admet $(1, x, x^2, x^3, x^4)$ pour base sur $\mathbb{Z}$.

Remarque 1 : Les corps de degré 4 ont été pris dans la table de Delone et Faddeev [6] pages 199-200. Cette table comprend trois erreurs d'impression :

- a) Les coefficients s, p, q, n sont tels que l'équation est $x^4 - sx^3 + px^2 - qx + n = 0$ avec $+ px^2$ et non $- px^2$.
- b) Pour le corps de discriminant 2225, lire $\frac{\rho^3 + \rho^2 + \rho}{2}$ et non $\frac{\rho^3 + \rho^2 + \rho^2}{2}$.
- c) Pour le corps de discriminant 7625, l'équation est $x^4 - x^3 - 9x^2 + 4x + 16 = 0$ avec le terme constant 16, et non 1.

Enfin, le corps de discriminant 7260 n'existe pas; l'équation proposée n'est pas irréductible, car on a

$$x^4 - x^3 - 7x^2 + 8x - 2 = (x^2 + 2x - 2)(x^2 - 3x + 1).$$

A titre de contrôle, tous les discriminants des corps de degré 3 et 4 ont été recalculés.

Remarque 2 : Les corps de degré 5 ont été pris dans le travail de H.Cohn [5]. Pour les discriminants indiqués, cet auteur donnent d'autres équations, mais nous avons vérifié qu'elles engendraient le même corps. Nous publierons par ailleurs [3] nos résultats numériques sur les corps de degré 5, et la méthode utilisée.

6. Description des tables.

Pour chacun des 63 corps décrits ci-dessus, nos tables imprimées (dont on trouvera un extrait plus loin) contiennent les renseignements suivants :

a) La loi de décomposition explicite des nombres premiers p en idéaux du corps K , pour $p \leq 2500$ environ. Nous possédons des renseignements analogues pour $p \leq 50000$ environ, stockés sur cartes perforées.

b) Pour chaque corps K , nous avons posé $L(s) = \zeta_K(s)/\zeta(s)$, sauf dans le cas D , où nous avons posé $L(s) = \zeta_K(s)/\zeta_E(s)$. Nous avons calculé les nombres $L(-n)$ dans les limites suivantes :

- pour $1 \leq n \leq 57$ si K est de classe A , sauf pour le plus grand discriminant 361, où nous avons seulement $1 \leq n \leq 53$

- pour $1 \leq n \leq N$ si K est de classe B , l'entier N étant donné par la table 1

- pour $1 \leq n \leq 29$ si K est de classe C

- pour $1 \leq n \leq 39$ si K est de classe D

- pour $1 \leq n \leq 17$ si K est de degré 5 (classes E et F).

Noter qu'on a $L(-n) = 0$ si $n \geq 0$ est pair.

c) Pour chaque entier $L(-n)$, ses facteurs premiers < 10000 avec leur exposant.

d) Coefficients d'interpolation : on forme d'abord des sous-séries comme suit : si $p = 2$, une seule sous-série formée des nombres $L^{(2)}(-1-2n)$ pour $n = 0, 1, 2, \dots$ dans les limites de la table b). Si $p \neq 2$, soit t l'un des nombres $1, 2, \dots, \frac{p-1}{2}$; la t -ième sous-série se compose des nombres $a_n = L^{(p)}(1-2t-n(p-1))$ pour $n = 0, 1, 2, \dots$ dans les limites de la table b). On forme les coefficients d'interpolation $c_n = \sum_{j=0}^n (-1)^{n-j} \binom{n}{j} a_j$, qui sont entiers si K n'est pas abélien. On détermine ensuite la plus grande puissance de p divisant c_n . La suite d'exposants obtenue peut avoir jusqu'à 29 termes pour $p = 2$ et les corps de degré 3 et discriminant assez petit.

e) Valeur extrapolée de $L^{(p)}(1)$: considérons la dernière sous-série définie par $a_{n-1} = L^{(p)}(1-n(p-1))$ pour $n = 1, 2, \dots, N$; définissons les coefficients d'interpolation c_n comme plus haut et soit p^h la plus haute puissance de p divisant c_{N-1} . On a calculé $\ell = \sum_{n=0}^{N-1} c_n \binom{-1}{n}$ modulo p^h . Si les résultats mentionnés en 7, B) ci-dessous sont exacts, la fonction analytique p -adique L^* , telle que $L^*(1-k) = L^{(p)}(1-k)$ pour $k > 0$, $k \equiv 0 \pmod{p-1}$, satisfait à $L^*(1) \equiv \ell \pmod{p^{N-1}}$ pour $p \neq 2$, et à $L^*(1) \equiv \ell \pmod{2^{3(N-1)}}$ pour $p = 2$. Nous n'avons pas interprété les résultats obtenus pour ℓ , mais nous pensons qu'ils pourront servir à tester les conjectures à faire sur le régulateur p -adique dans le cas d'un corps non abélien.

7. Interprétation des résultats.

Les corps cycliques de degré 3 et le corps de degré 5 et de discriminant 11^4 sont abéliens, et la théorie d'Iwasawa fournit tous les renseignements cherchés sur eux. Nous n'avons fait les calculs de tels corps qu'à titre de contrôle de nos méthodes. En particulier, nous avons vérifié que les nombres $L(-n)$ obtenus n'étaient pas toujours entiers, mais n'avaient en dénominateur que les diviseurs premiers du discriminant.

A) Intégralité : Il faut distinguer deux cas.

A₁) Lorsque le corps K ne contient aucun sous-corps abélien $\neq \mathbb{Q}$ (classes B, C et F), les nombres $L(-n) = \zeta_K(-n)/\zeta(-n)$ sont entiers et divisibles par 2^{r-1} pour $n \geq 0$ entier (dans la limite des tables).

A₂) Pour les corps K de classe D, les nombres $\zeta_K(-n)/\zeta(-n)$ ne sont pas toujours entiers, mais par contre les nombres $L(-n) = \zeta_K(-n)/\zeta_E(-n)$, où E est le plus grand sous-corps abélien de K, sont entiers et divisibles par 4 (pour $n \geq 0$).

Dans ces deux cas, la fonction L considérée est une série L d'Artin associée à une représentation irréductible du groupe de Galois $\text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$, de degré $\delta = 2, 3, 2, 4$ pour les classes B, C, D, F respectivement. Ces cas suggèrent l'énoncé suivant : si L est une série d'Artin associée à une représentation du groupe de Galois $\text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$, de degré δ , définie sur $\mathbb{Q}$, et sans composante absolument irréductible de degré 1, alors $L(-n)$ est un entier rationnel divisible par 2^δ (pour tout entier $n \geq 0$). Voir [4] pour des conjectures analogues.

B) Interpolation p-adique : nous nous intéressons aux corps non abéliens (classes B, C, D, F). On peut résumer comme suit les résultats obtenus :

- Supposons $p \neq 2$ et fixons l'entier $t = 1, 2, \dots, \frac{p-1}{2}$; dans la limite

des tables, on a une formule d'interpolation

$$(20) \quad L^{(p)}(1 - 2t - n(p - 1)) = \sum_{j=0}^{\infty} p^j u_j \binom{n}{j}$$

avec $u_0, u_1, \dots$ entiers.

- Supposons $p = 2$; on a une formule d'interpolation

$$(21) \quad L^{(2)}(1 - 2n) = \sum_{j=0}^{\infty} 2^{\delta + 3j} u_j \binom{n}{j}$$

avec $u_0, u_1, \dots$ entiers (dans la limite des tables).

Pour les corps K de la classe C qui contiennent $\mathbb{Q}(\sqrt{2})$, on peut même remplacer $2^{\delta + 3j}$ par $2^{\delta + 4j}$ dans (21); ceci se produit pour les corps de discriminant 2624, 4352, 7168 et 7232.

Pour $p \neq 2$, l'énoncé précédent signifie que les coefficients d'interpolation c_n de la sous-série $L^{(p)}(1 - 2t - k(p - 1))$ (t fixé égal à $1, 2, \dots, \frac{p-1}{2}$, k prenant les valeurs $0, 1, 2, \dots$) satisfont aux conditions $c_n \equiv 0 \pmod{p^n}$. Nous avons vérifié pour le corps cubique de discriminant 148 que les autres congruences de Serre sont satisfaites dans la limite des tables, de sorte que chaque sous-série est le début d'une suite appartenant à l'algèbre d'Iwasawa; nous projetons de vérifier systématiquement de telles propriétés sur nos tables. Il est facile en tout cas de vérifier une des conséquences de l'appartenance à l'algèbre d'Iwasawa, à savoir que si c_n est divisible par p^{n+1} , la propriété analogue a lieu dans la limite des tables pour les entiers $n' \equiv n \pmod{p-1}$ (lorsque $n \geq 1$ et $n' \geq 1$).

8. Séries de Dirichlet tordues.

Si $F(s) = \sum_{n=1}^{\infty} a_n n^{-s}$ est une série de Dirichlet et χ un caractère, on définit la série de Dirichlet $F(s; \chi) = \sum_{n=1}^{\infty} a_n \chi(n) n^{-s}$ et on l'appelle la série F tordue par χ .

Le caractère ω_p est défini comme au n° 3. Serre a démontré le résultat suivant dans [15, thm. 22] ; si a est un entier pair tel que $ra \not\equiv 0 \pmod{p-1}$, la suite des éléments $\zeta_K^{(p)}(-k; \omega_p^{a-k-1})^\sigma$ de $\mathbf{C}_p$ (pour $k = 0, 1, 2, \dots$) appartient à l'algèbre d'Iwasawa. Il en est de même de $(\gamma^{r(k+1)} - 1)\zeta_K^{(p)}(-k; \omega_p^{a-k-1})^\sigma$, si $ra \equiv 0 \pmod{p-1}$. Lorsque $K = \mathbf{Q}$, donc $r = 1$, ceci se réduit à un résultat d'Iwasawa mentionné au n° 3.

Par analogie, nous conjecturons le résultat suivant : soient K un corps de nombres totalement réel, et E le plus grand sous-corps abélien de K . Posons $L(s) = \zeta_K(s)/\zeta_E(s)$. Alors pour tout entier a , la suite des éléments $L^{(p)}(-k; \omega_p^{a-k-1})^\sigma$ de $\mathbf{C}_p$ (pour $k = 0, 1, 2, \dots$) appartient à l'algèbre d'Iwasawa. On pourrait plus généralement considérer des séries L d'Artin (?).

Examinons quelques cas particuliers de cette conjecture. Tout d'abord pour $p = 2$, on trouve que la suite des nombres entiers

$$L^{(p)}(0; \omega_2), L^{(p)}(-1), L^{(p)}(-2; \omega_2), L^{(p)}(-3), \dots$$

appartient à l'algèbre d'Iwasawa. On montre facilement que ceci entraîne que le n -ième coefficient d'interpolation de la suite $L^{(p)}(-1), L^{(p)}(-3), L^{(p)}(-5), \dots$ est divisible par 2^{3n} . Par contre, nous n'avons pas d'explication pour la divisibilité par 2^{4n} lorsque $E = \mathbf{Q}(\sqrt{2})$ et $[K : \mathbf{Q}] = 4$.

Supposons maintenant $p \neq 2$; le caractère $\omega_p^{\frac{p-1}{2}}$ n'est autre que le caractère de Legendre $\chi_p : a \mapsto \left(\frac{a}{p}\right)$, à valeurs dans $\{1, -1\}$. On a donc en particulier l'énoncé conjectural suivant : si $p \equiv 1 \pmod{4}$, pour chacun des nombres $t = 1, 2, \dots, \frac{p-1}{4}$, les suites

$$L^{(p)}(1-2t), L^{(p)}(1-2t-\frac{p-1}{2}; \chi_p), L^{(p)}(1-2t-(p-1)), L^{(p)}(1-2t-3\frac{p-1}{2}; \chi_p), \dots$$

$$L^{(p)}(1-2t; \chi_p), L^{(p)}(1-2t-\frac{p-1}{2}), L^{(p)}(1-2t-(p-1); \chi_p), L^{(p)}(1-2t-3\frac{p-1}{2}), \dots$$

appartiennent à l'algèbre d'Iwasawa; en particulier, le n -ième coefficient d'interpolation de ces suites est divisible par p^n .

Pour tenter de vérifier une telle propriété, nous avons calculé pour certains corps cubiques les nombres $L(-n; \chi_5)$ pour $1 \leq n \leq N$; voici une table des discriminants étudiés

$$\begin{array}{ll} D = 148, 229, 257, 316, 321, 404, 469, 473 & N = 29 \\ D = 564, 568, 621, 697, 733 & N = 23. \end{array}$$

Nous avons vérifié pour ces fonctions $L(s; \chi_5)$ les propriétés usuelles d'intégralité et d'interpolation p -adique (pour $p \neq 5$); de plus, nous avons formé par intercalement les deux suites suivantes (lorsque $N = 29$ par exemple)

$$\begin{aligned} &L^{(5)}(-1), L^{(5)}(-3; \chi_5), L^{(5)}(-5), L^{(5)}(-7; \chi_5), \dots, L^{(5)}(-29) \\ &L^{(5)}(-1; \chi_5), L^{(5)}(-3), L^{(5)}(-5; \chi_5), L^{(5)}(-7), \dots, L^{(5)}(-29; \chi_5) \end{aligned}$$

et vérifié que le n -ième coefficient d'interpolation est divisible par 5^n .

Nous avons aussi calculé les nombres $L(-n; \chi_{13})$ pour $1 \leq n \leq 19$ lorsque K est le corps cubique de l'un des discriminants 148, 229, 257 et 316. Les propriétés d'intégralité et d'interpolation p -adique pour $p \neq 13$ sont comme d'habitude. Nous avons ensuite formé par intercalement les 6 sous-séries

$$\begin{aligned} &L^{(13)}(-1), L^{(13)}(-7; \chi_{13}), L^{(13)}(-13), L^{(13)}(-19; \chi_{13}) \\ &L^{(13)}(-1; \chi_{13}), L^{(13)}(-7), L^{(13)}(-13; \chi_{13}), L^{(13)}(-19) \\ &L^{(13)}(-3), L^{(13)}(-9; \chi_{13}), L^{(13)}(-15) \\ &L^{(13)}(-3; \chi_{13}), L^{(13)}(-9), L^{(13)}(-15; \chi_{13}) \\ &L^{(13)}(-5), L^{(13)}(-11; \chi_{13}), L^{(13)}(-17) \\ &L^{(13)}(-5; \chi_{13}), L^{(13)}(-11), L^{(13)}(-17; \chi_{13}) \end{aligned}$$

et vérifié que dans chacune des sous-séries, le n -ième coefficient d'interpolation est divisible par 13^n .

§3. Calcul numérique des fonctions zêta

9. Méthode générale.

Notons K un corps de nombres totalement réel, de degré r et discriminant D . La fonction zêta de K a été définie par Dedekind au moyen de la formule

$$(22) \quad \zeta_K(s) = \sum_{\mathfrak{a}} (N \mathfrak{a})^{-s} = \prod_p (1 - (N p)^{-s})^{-1}$$

lorsque $\text{Re } s > 1$; la somme est étendue à tous les idéaux entiers $\mathfrak{a}$ de K et le produit à tous les idéaux premiers $\mathfrak{p}$ de K . Il est commode d'écrire le produit infini sous la forme d'un produit étendu aux nombres premiers p

$$(23) \quad \zeta_K(s) = \prod_p H_p(p^{-s})^{-1};$$

pour chaque p , le facteur $H_p(p^{-s})$ est le produit des nombres $1 - (N \mathfrak{p})^{-s}$ pour tous les idéaux premiers $\mathfrak{p}$ de K au-dessus de p . De plus, H_p est un polynôme de degré $\leq r$.

On sait par Hecke que la fonction ζ_K se prolonge en une fonction méromorphe sur $\mathbb{C}$, avec un pôle simple pour $s = 1$, et une équation fonctionnelle

$$(24) \quad \zeta_K(1-s) = D^{s-1/2} C(s)^r \zeta_K(s);$$

on a posé

$$(25) \quad C(s) = 2^{1-s} \pi^{-s} \Gamma(s) \cos \frac{\pi s}{2}.$$

Lorsque $K = \mathbb{Q}$, on retrouve la fonction zêta de Riemann et ses propriétés.

Notre but est le calcul des nombres $L(-1)$, $L(-3)$, $L(-5)$,... pour diverses fonctions L liées étroitement à la fonction ζ_K . La méthode générale est la suivante :

a) Répartition des nombres premiers en classes : dans chaque cas, on peut répartir les nombres premiers p en un nombre fini de classes $D_1, \dots, D_h$ et déterminer des polynômes $M_1, \dots, M_h$ tels que l'on ait

$$(26) \quad L(s) = \prod_{j=1}^h \prod_{p \in D_j} M_j(p^{-s})^{-1} \quad (\text{Re } s > 1).$$

b) Calcul des nombres $L(2)$, $L(4)$,... par le produit infini précédent.

c) Détermination d'une équation fonctionnelle, donnant a priori les nombres $\frac{L(-1)}{L(2)}$, $\frac{L(-3)}{L(4)}$, $\frac{L(-5)}{L(6)}$,... sous une forme ne dépendant que du degré et du discriminant du corps considéré, nombres qu'on peut calculer une fois pour toutes.

10. Le cas des corps abéliens.

Parmi les corps que nous avons étudiés, il y a 4 corps cycliques de degré 3 et un corps cyclique de degré 5. Dans ces cas la loi de réciprocité permet de déterminer les nombres $\zeta_K(-1)$, $\zeta_K(-3)$,... par des calculs faciles, qui permettent le contrôle de nos méthodes.

Considérons un corps K totalement réel, cyclique, de degré 3, et reprenons les notations du n° 5, A. Il y a trois classes de nombres premiers :

a) celle des diviseurs premiers de D , soit D_1 : si $\mathfrak{p}$ est un tel nombre, on a $(\mathfrak{p}) = \mathfrak{p}^3$ où $\mathfrak{p}$ est un idéal premier de K de norme p . Posons $M_1(T) = 1$.

b) La classe $C_0 = H = D_2$: pour p dans C_0 , on a la décomposition $(p) = p_1 p_2 p_3$, avec trois idéaux premiers distincts p_1, p_2, p_3 , de norme p . On pose $M_2(T) = (1-T)^2$.

c) La classe $C_1 \cup C_2 = D_3$: pour p dans $C_1 \cup C_2$, on a $(p) = p$ où p est premier de norme p^3 . On pose $M_3(T) = 1 + T + T^2$.

Posons $L(s) = \zeta_K(s)/\zeta(s)$ et $L_p(s) = M_j(p^{-s})^{-1}$ si $p \in D_j$. On a alors

$$(27) \quad L(s) = \prod_p L_p(s) = L(s; \chi) L(s; \bar{\chi})$$

où χ est le caractère primitif de conducteur $d = D^{1/2}$ défini par $\chi(n) = \rho^{nj}$ pour $n \in C_j$ (on note $\rho \neq 1$ une racine cubique de l'unité).

Soit par ailleurs $r \neq 1$ une racine 11-ième de l'unité et $K = \mathbb{Q}(r + r^{-1})$ (degré 5, discriminant 11^4). On a de même les lois de décomposition :

a) On a $(11) = p^5$ avec $Np = 11$, et le facteur local $L_p(s) = 1$.

b) Si $p \equiv \pm 1 \pmod{11}$, l'idéal (p) est produit de 5 idéaux premiers de norme p , et l'on a le facteur local $L_p(s) = (1-p^{-s})^{-4}$.

c) Dans les autres cas, (p) est premier de norme p^5 dans K , et l'on a le facteur local $L_p(s) = (1 + p^{-s} + p^{-2s} + p^{-3s} + p^{-4s})^{-1}$.

La fonction $L(s) = \zeta_K(s)/\zeta(s)$ admet alors les représentations

$$(28) \quad L(s) = \prod_p L_p(s) = \prod_{j=1}^4 L(s; \chi_j)$$

où $\chi_1, \chi_2, \chi_3, \chi_4$ sont les caractères non triviaux modulo 11 tels que $\chi_j(-1) = 1$.

Il reste à donner une méthode de calcul de $a_k = L(-k; \chi)$ pour tout entier $k \geq 0$ et tout caractère χ non trivial de conducteur f tel que $\chi(-1) = 1$. Le plus commode est d'utiliser la série génératrice

$$(29) \quad \sum_{k=0}^{\infty} a_k X^k/k! = \frac{\sum_{n=1}^f \chi(n) e^{nX}}{1 - e^{fX}}$$

qui fournit les relations $a_0 = a_2 = a_4 = \dots = 0$ et les formules de récurrence

$$\begin{aligned} \binom{2}{1} f a_1 &= - \sum_{n=1}^f \chi(n) n^2 \\ \binom{4}{1} f^3 a_1 + \binom{4}{3} f a_3 &= - \sum_{n=1}^f \chi(n) n^4 \\ \binom{6}{1} f^5 a_1 + \binom{6}{3} f^3 a_3 + \binom{6}{5} f a_5 &= - \sum_{n=1}^f \chi(n) n^6 \\ &\dots\dots\dots \end{aligned}$$

11. Lois de décomposition, facteurs locaux, équation fonctionnelle.

Soient K un corps de nombres, r son degré, D son discriminant et $\mathcal{O}$ l'anneau de ses entiers. La répartition des nombres premiers en classes se fait comme suit :

a) p est ramifié s'il divise D et non ramifié s'il ne divise pas D ;

b) si l'on a dans K la décomposition $(p) = p_1^{e_1} \dots p_n^{e_n}$ avec $e_1 > 1, \dots, e_n > 1$ et des idéaux premiers distincts $p_1, \dots, p_n$ tels que $N p_j = p^{f_j}$, on dit que p appartient à la classe $C(f_1^{e_1}, \dots, f_n^{e_n})$. La classe $C(f_1^{e_1}, \dots, f_n^{e_n})$ est dite non ramifiée si l'on a $e_1 = \dots = e_n = 1$; alors tous les nombres premiers appartenant à cette classe sont non ramifiés. Si au contraire l'un des exposants e_i est différent de 1, la classe $C(f_1^{e_1}, \dots, f_n^{e_n})$ est dite ramifiée, elle ne se compose que de nombres premiers ramifiés.

Une classification plus grossière est fournie par les familles et sous-familles. La sous-famille $F_{s,j}$ est la réunion des classes non-ramifiées $C(f_1, \dots, f_n)$ pour lesquelles le nombre 1 apparaît s fois et le nombre 2 apparaît j fois dans la suite $(f_1, \dots, f_n)$; la famille F_s est la réunion des sous-familles $F_{s,0}, F_{s,1}, \dots$. On définit de manière analogue les familles et sous-familles ramifiées $\bar{F}_s$ et $\bar{F}_{s,j}$.

Dans tous les cas, le corps étudié est donné sous la forme $K = \mathbf{Q}(x)$ où x est un entier algébrique. Notons $F(X) = X^r + c_1 X^{r-1} + \dots + c_r$ le polynôme minimal de x ; ses coefficients $c_1, \dots, c_r$ sont entiers. Posons $N = (0 : \mathbf{Z}[x])$; alors le discriminant du polynôme F est donné par $\Delta = N^2 D$. On dira qu'un nombre premier est exceptionnel (pour x) s'il divise N . Soit p un nombre premier non exceptionnel, et soit F_p la réduction de F modulo p . Alors p appartient à la classe $C(f_1^{e_1}, \dots, f_n^{e_n})$ si et seulement si F_p se décompose dans l'anneau de polynômes $\mathbf{F}_p[X]$ en $F_p = H_1^{e_1} \dots H_n^{e_n}$ où $H_1, \dots, H_n$ sont irréductibles, deux à deux distincts et où H_j est de degré f_j .

Nous examinons maintenant en détail les divers cas.

A) Détermination de $L(s) = \zeta_K(s)/\zeta(s)$. On a l'équation fonctionnelle

$$(30) \quad L(1-s) = D^{s-1/2} C(s)^{r-1} L(s).$$

Le facteur local associé à un nombre premier p de la classe $C(f_1^{e_1}, \dots, f_n^{e_n})$ est

$$(31) \quad L_p(s) = \frac{1-p^{-s}}{(1-p^{-f_1 s}) \dots (1-p^{-f_n s})}.$$

Voir les tables 4 et 5 pour les classes et les facteurs locaux en degré 3, 4 ou 5. On constate qu'en degré 3, il y a au plus une classe par famille. En degré 4, la famille F_0 contient deux classes, qui correspondent chacune à une sous-famille; pour les classes ramifiées, la famille $\bar{F}_1$ se scinde en deux sous-familles comprenant chacune une seule classe; la famille $\bar{F}_2$ contient une seule sous-famille et deux classes, mais celles-ci ont même facteur local. En degré 5, on constate aussi que les sous-familles ramifiées $\bar{F}_{1,0}$, $\bar{F}_{1,1}$, $\bar{F}_{2,0}$ et la famille $\bar{F}_3 = \bar{F}_{3,0}$ contiennent chacune deux classes; ceci n'introduit aucune ambiguïté pour le facteur local, à l'exception de la sous-famille $\bar{F}_{1,0} = C(1^5) \cup C(3,1^2)$. Ce cas se rencontre une seule fois, pour $D = p = 38569$ où p est de classe $C(3,1^2)$; il a requis le calcul du p.g.c.d. de F_p et F_p'' .

Enfin, pour tous les corps étudiés, l'anneau des entiers est $\mathbf{Z}[x]$ et il n'y a donc pas de nombre premier exceptionnel.

En résumé, la connaissance des familles suffit en degré 3, et pour les corps étudiés de degré 4 et 5, la connaissance des sous-familles suffit à une exception près.

B) Séries L tordues.

Comme en A), on pose $L(s) = \zeta_K(s)/\zeta(s)$, et l'on note $L_p(s)$ le facteur local associé à p . Soit par ailleurs d le discriminant d'un corps quadratique réel. Si l'on a $L(s) = \sum_{n=1}^{\infty} c_n n^{-s}$, la série tordue est $L(s; \chi_d) = \sum_{n=1}^{\infty} \left(\frac{d}{n}\right) c_n n^{-s}$ avec le symbole de Jacobi $\left(\frac{d}{n}\right)$. Chaque classe C se décompose en 3 sous-classes C_0, C_+, C_- selon que $\left(\frac{d}{p}\right)$ vaut 0, +1 ou -1; le facteur local est 1 si $p \in C_0$, c'est celui de la classe C si $p \in C_+$ et enfin, il s'obtient en changeant p^{-s} en $-p^{-s}$ si $p \in C_-$. La table 6 donne les sous-classes et les facteurs locaux lorsque K est de degré 3.

Pour obtenir l'équation fonctionnelle, on introduit les corps $K' = \mathbf{Q}(\sqrt{d})$ et $K'' = K(\sqrt{d})$, et l'on utilise la relation

$$(32) \quad L(s; \chi_d) = \frac{\zeta_{K''}(s) \zeta(s)}{\zeta_K(s) \zeta_{K'}(s)}$$

Dans les cas étudiés, d est premier au discriminant D de K ; par suite, le discriminant de K'' est $D^2 d^3$ (et celui de K' est d). On obtient donc l'équation fonctionnelle

$$(33) \quad L(1-s; \chi_d) = (Dd^2)^{s-1/2} C(s)^2 L(s; \chi_d).$$

C) Corps de degré 4 avec sous-corps quadratique.

Soit K un corps totalement réel de degré 4, avec un sous-corps quadratique E ; on note D le discriminant de K et d celui de E , et l'on suppose que K n'est pas abélien sur $\mathbf{Q}$. On pose $L(s) = \zeta_K(s)/\zeta_E(s)$, d'où

l'équation fonctionnelle

$$(34) \quad L(1-s) = (D/d)^{s-1/2} C(s)^2 L(s).$$

La répartition en classes se fait en tenant compte des lois de décomposition d'un nombre premier p à la fois dans E et dans K . On sait que la décomposition dans E est de la forme $C(1^2)$, $C(1,1)$ ou $C(2)$ selon que le symbole de Jacobi $(\frac{d}{p})$ est égal à 0, + 1 ou - 1. On ajoute donc aux symboles de classe dans K un indice 0, + ou - donnant le signe de $(\frac{d}{p})$, indice sous-entendu s'il n'y a pas d'ambiguïté. La table 7 a été déterminée en remarquant qu'un idéal premier p dans E a une décomposition de l'une des formes $p = P^2$, $p = PQ$ ou $p = P$ dans K .

Dans la table 3, on a donné deux nombres x et η tels que $E = Q(\eta)$, $K = Q(x)$ et que $(1, x, \eta, x\eta)$ soit une base sur $\mathbf{Z}$ de l'anneau des entiers de K . Il est alors facile de déterminer les nombre premiers exceptionnels. Comme x et η satisfont à des équations du type

$$(35) \quad \eta^2 = a\eta + b, \quad x^2 = a' + b'x + c'\eta + d'x\eta$$

on a

$$(36) \quad x^3 = (a'b' + bc'd') + (a' + b'^2 + bd'^2)x + (b'c' + a'd' + ac'd')\eta + (2b'd' + c' + ad'^2)x\eta.$$

L'indice du sous-groupe $\mathbf{Z}[x] = \mathbf{Z} + \mathbf{Z}x + \mathbf{Z}x^2 + \mathbf{Z}x^3$ dans l'anneau des entiers $O = \mathbf{Z} + \mathbf{Z}x + \mathbf{Z}\eta + \mathbf{Z}x\eta$ est égal à la valeur absolue du déterminant de la matrice formée des coefficients de η et $x\eta$ dans l'expression de x^2 et x^3 , d'où

$$(37) \quad (0 : \mathbf{Z}[x]) = |d'(a'd' - b'c') - c'^2|.$$

Prenons par exemple le corps K de discriminant 2225, avec $\eta = \frac{1+\sqrt{5}}{2}$

et $x = \frac{\eta + \sqrt{\eta + 9}}{2}$. On a $(2x-\eta)^2 = \eta + 9$, d'où

$$(38) \quad \eta^2 = \eta + 1, \quad x^2 = 2 + x\eta,$$

et la matrice $\begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}$ est égale à $\begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}$. On a alors $(0 : \mathbf{Z}[x]) = 2$ et 2 est le seul nombre premier exceptionnel. Comme 2 ne divise pas le discriminant, il n'est pas ramifié. Comme le polynôme $H^2 - H - 1$ est irréductible modulo 2, et qu'on a $x(x-\eta) \equiv 0 \pmod{2}$ d'après (38), en obtient immédiatement la décomposition $(2) = (x)(x-\eta)$ de (2) en produit de deux idéaux premiers de norme 2^2 . Autrement dit, 2 est dans la classe $C(2,2)$ pour K ; comme on a aussi $\left(\frac{5}{2}\right) = -1$, le nombre premier 2 appartient à la classe $C(2,2)_-$.

Avec un peu de patience, on traite de manière semblable les autres corps de la table 3, et l'on obtient le tableau suivant (il n'y a pas de nombre premier exceptionnel dans les autres cas) :

Discriminant	2225	4525	5225	5725	7232	7625
Nombre premier exceptionnel	2	3	2	3	2	2
Classe	$C(2,2)_-$	$C(2,2)_-$	$C(2,2)_-$	$C(2,2)_-$	$C(1^2,1^2)_0$	$C(2,2)_-$

12. Algorithme de décomposition des polynômes modulo p .

Un tel algorithme, prévoyant tous les cas de décomposition possibles a été mis au point par Y. Roy [14]; il s'agit d'une modification de la méthode de Berlekamp [2] et Knuth [11, p.389], intéressante si le degré est petit et p grand. Comme on l'a noté plus haut, nous n'avons besoin que de la répartition en familles et sous-familles; nous nous contenterons donc d'exposer la partie correspondante de l'algorithme.

Soient p un nombre premier et

$$H(X) = X^r - v_1 X^{r-1} - v_2 X^{r-2} - \dots - v_{r-1} X - v_r$$

un polynôme de degré r à coefficients dans le corps $\mathbf{F}_p$ à p éléments.

Pour tout entier $n \geq 1$, on sait que $X^{p^n} - X$ est le produit des polynômes irréductibles (dans $\mathbf{F}_p[X]$) dont le degré divise n , chacun avec multiplicité 1. Nous voulons déterminer le nombre s de facteurs de degré 1 de $H(X)$ et le nombre j de facteurs irréductibles de degré 2 de $H(X)$ (compte non tenu des multiplicités). Pour tout entier $n \geq 1$, soit $G_n(X)$ le p.g.c.d. de $H(X)$ et $X^{p^n} - X$ dans $\mathbf{F}_p[X]$, et soit g_n son degré. Il est immédiat qu'on a

$$(39) \quad s = g_1, \quad s + 2j = g_2,$$

et tout revient à déterminer g_1 et g_2 . Nous décrivons maintenant les diverses parties de l'algorithme.

A) Algorithme de division modifié.

Il s'agit de la méthode classique, modifiée pour ne pas avoir à faire de division dans le corps $\mathbf{F}_p$. Soient

$$M(X) = m_0 X^\alpha + m_1 X^{\alpha-1} + \dots + m_{\alpha-1} X + m_\alpha$$

$$N(X) = n_0 X^\beta + n_1 X^{\beta-1} + \dots + n_{\beta-1} X + n_\beta \quad (n_0 \neq 0)$$

deux polynômes dans $\mathbf{F}_p[X]$.

Initialisation : $S_0(X) = M(X)$

$$\text{Boucle : } \begin{cases} e_i = \deg S_i - \deg N \\ \text{si } e_i < 0 & \text{fin de procédure} \\ \text{si } e_i \geq 0 & f_i \text{ coefficient dominant de } S_i(X) \\ & S_{i+1}(X) = n_0 S_i(X) - f_i X^{e_i} N(X). \end{cases}$$

La procédure s'arrête pour une valeur q de i et il existe un entier $h \geq 0$ tel que $S_q(X)$ soit le reste de la division euclidienne de $n_0^h M(X)$ par $N(X)$; on a $n_0^h \neq 0$ dans $\mathbf{F}_p$.

B) Calcul du reste $R_1(X)$ de la division de X^p par $H(X)$.

On définit les matrices

$$A = \begin{pmatrix} v_1 & 1 & 0 & 0 & \cdot & \cdot & 0 & 0 \\ v_2 & 0 & 1 & 0 & \cdot & \cdot & 0 & 0 \\ v_3 & 0 & 0 & 1 & \cdot & \cdot & 0 & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ v_{r-1} & 0 & 0 & 0 & \cdot & \cdot & 0 & 1 \\ v_r & 0 & 0 & 0 & \cdot & \cdot & 0 & 0 \end{pmatrix}, \quad v = \begin{pmatrix} v_1 \\ v_2 \\ v_3 \\ \cdot \\ \cdot \\ \cdot \\ v_{r-1} \\ v_r \end{pmatrix}$$

puis l'on effectue le calcul matriciel $w = A^{p-r} v$. Si $w_1, \dots, w_r$ sont les éléments de w , on a

$$(40) \quad R_1(X) = w_1 X^{r-1} + w_2 X^{r-2} + \dots + w_{r-1} X + w_r.$$

Nous avons eu à considérer des nombres premiers p de l'ordre de 45000 et r vaut 3, 4 ou 5. Le calcul par récurrence de la puissance A^{p-r} est très onéreux; voici une méthode qui requiert $O(\log p)$ opérations et qui nous a permis (en degré 5) de traiter en 3 minutes environ les nombres premiers contenus dans chaque tranche de 1000 nombres.

Si $p = r$, on a $w = v$. Sinon, on écrit

$$(41) \quad p - r = \gamma_0 + 2\gamma_1 + 2^2\gamma_2 + \dots + 2^m\gamma_m$$

avec des γ_i égaux à 0 ou 1 et $\gamma_m = 1$. On définit ensuite les matrices $B_1, \dots, B_m$ de type $r \times r$ par

$$B_1 = A, \quad B_2 = B_1^2, \dots, B_m = B_{m-1}^2, \quad B_{m+1} = B_m^2.$$

Les matrices $v_0, v_1, \dots, v_{m+1}$ de type $r \times 1$ sont définies par

$$v_0 = v, \quad v_j = \begin{cases} v_{j-1} & \text{si } \gamma_{j-1} = 0 \\ B_j v_{j-1} & \text{si } \gamma_{j-1} = 1. \end{cases}$$

On a finalement $w = v_{m+1}$.

C) Calcul du reste $R_2(X)$ de la division de $R_1(R_1(X))$ par $H(X)$.

Il s'agit en fait du schéma de Horner appliqué à l'anneau quotient $\mathbf{F}_p[X]/(H(X))$. On définit les polynômes $T_0(X), T_1(X), \dots, T_{r-1}(X)$ de degré $\leq r-1$ par

$$T_0(X) = R_1(X),$$

$T_i(X)$ est le reste de la division de $X T_{i-1}(X)$ par $H(X)$ pour $1 \leq i \leq r-1$.

On pose ensuite, avec les notations de (40),

$$(42) \quad U_1(X) = w_1 R_1(X) + w_2$$

et si

$$(43) \quad U_i(X) = a_1 X^{r-1} + a_2 X^{r-2} + \dots + a_{r-1} X + a_r,$$

on pose

$$(44) \quad U_{i+1}(X) = a_1 T_{r-1}(X) + a_2 T_{r-2}(X) + \dots + a_{r-1} T_1(X) + a_r T_0(X) + w_{i+2}.$$

Il est immédiat que modulo $H(X)$ on a $T_i(X) \equiv X^i R_1(X)$ d'où

$U_{i+1}(X) \equiv U_i(X) R_1(X) + w_{i+2}$ et donc $U_{r-1}(X) \equiv R_1(R_1(X))$. On a par conséquent $R_2 = U_{r-1}$.

D) Calcul de g_1 et g_2 .

Par construction, on a $X^P \equiv R_1(X) \pmod{H(X)}$, d'où

$$(45) \quad G(X^P) \equiv G(R_1(X)) \pmod{H(X)}$$

pour tout polynôme $G(X)$ dans $\mathbf{F}_p[X]$. Remplaçons successivement $G(X)$ par X^P et $R_1(X)$; on obtient

$$(46) \quad X^{P^2} \equiv R_1(X)^P \pmod{H(X)}$$

$$(47) \quad R_1(X^p) \equiv R_1(R_1(X)) \pmod{H(X)},$$

et comme $R_1(X^p) = R_1(X)^p$, on a finalement

$$(48) \quad X^{p^2} \equiv R_1(R_1(X)) \equiv R_2(X) \pmod{H(X)}.$$

Par suite, le p.g.c.d. $G_n(X)$ de $X^{p^n} - X$ et $H(X)$ est aussi celui de $R_n(X) - X$ et $H(X)$ (pour $n = 1, 2$). Pour calculer $G_n(X)$, on utilise l'algorithme classique d'Euclide et l'on voit immédiatement qu'on ne change pas le résultat (à multiplication près par un élément non nul de $\mathbf{F}_p$) si l'on utilise partout l'algorithme de division "modifié" décrit en A).

13. Calcul numérique de $L(1-2n)$.

On note K un corps totalement réel de degré $r = 3, 4$ ou 5 , et de discriminant D , et l'on suppose connue la répartition des nombres premiers en classes; on pose $L(s) = \zeta_K(s)/\zeta(s)$. Les autres cas sont analogues. Le calcul de $L(1-2n)$ se fonde sur les formules suivantes :

$$(49) \quad L(1-2n) = (-1)^{n(r-1)} c_n L(2n)$$

$$(50) \quad L(2n) = \prod_{j=2}^{\infty} L_j(2n)$$

$$(51) \quad L_j(2n) = \begin{cases} (1-p^{-2n}) \prod_{k=1}^t (1-p^{-2n} f_k)^{-1} & \text{si } j \in C(f_1^{e_1}, \dots, f_t^{e_t}) \\ 1 & \text{si } j \text{ n'est pas premier.} \end{cases}$$

$$(52) \quad c_1 = \frac{D \sqrt{D}}{(2\pi^2)^{r-1}}$$

$$(53) \quad c_n = \frac{D^2}{(2\pi^2)^{r-1}} B_n c_{n-1} \quad \text{avec} \quad B_n = [(n-1)(2n-1)]^{r-1}.$$

Enfin, on note $r_p(2n)$ et $s_p(2n)$ le numérateur et le dénominateur du nombre rationnel $L_p(2n)$.

Nos calculs ont été effectués en "arithmétique entière", c'est-à-dire que l'on connaît exactement la valeur de la somme, de la différence ou du produit de deux nombres entiers, et la partie entière $a \div b$ du quotient de l'entier a par l'entier b . Nous pouvions en principe traiter des entiers compris entre -10^{600} et 10^{600} ce qui excédait largement les besoins du calcul.

Détaillons maintenant les calculs et l'estimation de l'erreur. On choisit des entiers strictement positifs P, α, β, γ et l'on pose

$$(54) \quad \varepsilon = \frac{r-1}{(2n-1)P^{2n-1}}, \quad \varepsilon^* = e^\varepsilon - 1.$$

On s'est arrangé pour avoir toujours $\varepsilon \leq \frac{1}{5000}$, ce qui permet de négliger en toute sécurité ε^2 dans les calculs qui suivent. Nous définirons des nombres $F, Z, \dots$ dont les valeurs approchées calculées sont notées $F^*, Z^*, \dots$

a) Calcul de $F = 10^\alpha L(2n)$: on tronque le produit infini en posant $L_1 = \prod_{j=2}^P L_j(2n)$. Si un nombre premier p appartient à la classe $C(f_1^{e_1}, \dots, f_t^{e_t})$ on a $r = \sum_{k=1}^t e_k f_k$, d'où $f_1 + \dots + f_t \leq r$; de plus, on a $0 < p^{-2nf_k} < 1$ et comme $0 < t < 1$ entraîne $1 \leq \frac{1}{1-tf} \leq \frac{1}{1-t}$, on obtient l'estimation suivante du facteur local (voir (51))

$$(55) \quad 1 - p^{-2n} \leq L_p(2n) \leq \left(\frac{1}{1-p^{-2n}} \right)^{r-1}.$$

On a $L(2n)/L_1 = \prod_{p>P} L_p(2n)$, d'où

$$(56) \quad \left[\prod_{p>P} \frac{1}{1-p^{-2n}} \right]^{-1} \leq \frac{L(2n)}{L_1} \leq \left[\prod_{p>P} \frac{1}{1-p^{-2n}} \right]^{r-1};$$

or l'unicité du développement en facteurs premiers entraîne

$$\begin{aligned} \prod_{p>P} \frac{1}{1-p^{-2n}} &= \sum_{a \in S} a^{-2n} \leq 1 + \sum_{a=P+1}^{\infty} a^{-2n} \\ &\leq 1 + \int_P^{\infty} x^{-2n} dx = 1 + \frac{1}{(2n-1)P^{2n-1}} = 1 + \frac{\varepsilon}{r-1} \end{aligned}$$

(on note S l'ensemble des entiers $a \geq 1$ sans facteur premier $\leq P$). En conclusion, on a

$$(57) \quad \left(1 + \frac{\epsilon}{r-1}\right)^{-1} - 1 \leq \frac{L(2n)}{L_1} - 1 \leq \left(1 + \frac{\epsilon}{r-1}\right)^{r-1} - 1.$$

La valeur approchée F^* de $10^\alpha L_1$ est calculée par le schéma

$$\begin{aligned} F_1 &= 10^\alpha \\ F_j &= [F_{j-1} r_j(2n)] \div s_j(2n) \quad \text{pour } j = 2, 3, \dots, P \\ F^* &= F_P. \end{aligned}$$

En ajoutant à l'erreur de troncation donnée par (57) l'erreur d'arrondi due aux divisions, on obtient l'estimation suivante de l'erreur

$$(58) \quad \left| \frac{F^*}{F} - 1 \right| \leq \epsilon^* + (1 + \epsilon^*) \frac{P-1}{10^\alpha} \zeta(2n).$$

b) Calcul de $Z = 10^\beta \sqrt{D}$: soit u la partie entière de $\sqrt{D}$, d'où $D = u^2 + v$ avec $0 \leq v \leq 2u$. On pose

$$(59) \quad T = 10^{\beta+6} \sqrt{D} = 10^{\beta+6} u \sqrt{1 + \frac{v}{u^2}},$$

et l'on développe la racine carrée par la série du binôme. Voici le schéma du calcul

$$\begin{aligned} G_0 &= 10^{\beta+6} u \\ G_k &= [(3-2k)v G_{k-1}] \div 2ku^2 \quad \text{pour } k \geq 1 \\ N &\text{ plus petit entier } k \text{ tel que } G_{k+1} = 0 \\ Z^* &= [G_0 + G_1 + \dots + G_N] \div 10^6. \end{aligned}$$

On a l'erreur

$$(60) \quad \left| \frac{Z^*}{Z} - 1 \right| \leq \frac{1}{10^\beta \sqrt{D}} \left[\frac{7(\beta + \log_{10} u) + 50}{10^6} + 1 \right].$$

c) Calcul de $K = 10^\beta (2\pi^2)^{r-1}$: au moyen d'une table donnant π avec 200 décimales, on définit $U_1 = 10^{\beta+6} \pi$. On calcule successivement

$$\begin{aligned}
 U_2 &= (2U_1^2) \div 10^{\beta+6} \\
 U_3 &= (U_2U_2) \div 10^{\beta+6} \\
 U_4 &= (U_2U_3) \div 10^{\beta+6} \\
 U_5 &= (U_2U_4) \div 10^{\beta+6}
 \end{aligned}$$

et l'on pose $K^* = U_r \div 10^6$ si le degré est égal à r . On a l'erreur

$$(61) \quad \left| \frac{K^*}{K} - 1 \right| \leq \frac{2}{10^{\beta}(2\pi^2)^{r-1}}.$$

Dans les conditions usuelles, ceci signifie que $\sqrt{D}$ et $(2\pi^2)^{r-1}$ ont été calculés à $2 \cdot 10^{-\beta}$ près.

d) Calcul de $C_n = 10^\gamma C_n$: on utilise les formules de récurrence (52) et (53) sous la forme suivante

$$A^* = (10^{2\beta} D^2) \div K^* \quad (\text{valeur approchée de } A = \frac{10^{\beta} D^2}{(2\pi^2)^{r-1}})$$

$$C_1^* = 10^\gamma D Z^* \div K^*$$

$$C_n^* = (A^* B_n C_{n-1}^*) \div 10^\beta.$$

L'erreur se calcule selon la formule

$$(62) \quad \left| \frac{C_n^*}{C_n} - 1 \right| \leq n \left| \frac{K^*}{K} - 1 \right| + \frac{n-1}{A} + \frac{1}{C_1} + \frac{n-1}{C_2} + \left| \frac{Z^*}{Z} - 1 \right|,$$

c'est-à-dire

$$\begin{aligned}
 (63) \quad \left| \frac{C_n^*}{C_n} - 1 \right| &\leq \left\{ \frac{2n}{(2\pi^2)^{r-1}} + \frac{(n-1)(2\pi^2)^{r-1}}{D^2} \right\} 10^{-\beta} \\
 &+ \left\{ \frac{(2\pi^2)^{r-1}}{D^{3/2}} + \frac{(n-1)(2\pi^2)^{2r-2}}{3^{r-1} D^{7/2}} \right\} 10^{-\gamma} + \left\{ \frac{7(\beta + \log_{10} u) + 50}{10^6} + 1 \right\} \frac{10^{-\beta}}{\sqrt{D}}
 \end{aligned}$$

e) Calcul de $L = 10^{10} |L(1-2n)|$: on utilise l'équation fonctionnelle (49), sous la forme de la valeur approchée

$$(64) \quad L^* = (F^* C_n^*) \div 10^{\alpha+\gamma-10}.$$

Dans les cas étudiés, on a $D \geq 49$ d'où $A \geq 6 \cdot 10^6$, $C_1 \geq \frac{3}{4} 10^7$, et l'on n'a considéré que le cas $n \leq 29$. Les nombres α , β , γ de décimales retenues sont définis en fonction de P par

$$\beta = \gamma = \alpha - 6 \quad \text{et} \quad \alpha - 9 = \text{partie entière de } \log_{10} \frac{2n-1}{r-1} + (2n-1) \log_{10} P.$$

Les formules (58) et (63) montrent que dans ces conditions et pour $P \leq 45000$, l'erreur d'arrondi est inférieure au dixième de l'erreur de troncation, d'où l'estimation finale de l'erreur

$$(65) \quad \left| \frac{L^*}{L} - 1 \right| \leq 2\epsilon = \frac{2(r-1)}{(2n-1)P^{2n-1}}.$$

14. Caractère significatif des résultats obtenus.

Les fonctions L considérées ont un développement en série de Dirichlet et

$$(66) \quad L(s) = \sum_{n=1}^{\infty} c_n n^{-s},$$

dont les coefficients c_n sont "petits". Il en résulte que pour $s \geq 10$ par exemple, la série précédente converge très rapidement et a une somme très voisine de $c_1 = 1$. Mais l'équation fonctionnelle introduit un facteur $\Delta^{s-1/2} C(s)^d$ qui croît très rapidement avec s , et ceci d'autant plus que Δ et d sont plus grands. Dans certains des cas étudiés, ce facteur est de l'ordre de 10^{170} , et il nous faut donc sommer la série (66) (ou le produit infini équivalent) avec une erreur inférieure à 10^{-180} ; ceci requiert environ 45000 termes de la série.

Les nombres $L(1-2n)$ ont été calculés avec 10 chiffres après la virgule, et la formule (65) montre qu'avec un P convenable (choisi en fonction de n), on peut faire en sorte que $|L^* - L| \leq 10^{-5}$ (sauf pour $n = 1$, où nous n'avons que $|L^* - L| \leq 10^{-3}$). Par suite, les 5 premiers chiffres après la virgule (sauf pour $n = 1$) sont exacts. Dans tous les cas

étudiés, ces chiffres sont tous égaux à 0 ou tous égaux à 9. Autrement dit, nous avons prouvé que $L(1-2n)$ diffère d'un entier de moins de 10^{-5} . Comme ces nombres sont calculés de manière indépendante, l'existence des congruences très précises sur les différences itérées ne laisse aucun doute sur l'intégralité des nombres $L(1-2n)$.

BIBLIOGRAPHIE

- [1] Y.AMICE et J.FRESNEL, Fonctions zêta p-adiques des corps de nombres abéliens réels, "Acta Arithm." 20 (1972), p.353-384.
- [2] E.R.BERLEKAMP, Factoring polynomials over large finite fields, Math. Comp. 24 (1970), p.713-735.
- [3] P.CARTIER et Y.ROY, On the enumeration of quintic fields with small discriminant, à paraître pour le jubilé de Hasse.
- [4] J.COATES et S.LICHTENBAUM, On l-adic zeta functions, à paraître aux Annals of Mathematics.
- [5] H.COHN, A numerical study of quintics of small discriminant, Comm. Pure Appl. Math. 8, (1955), p.377-385.
- [6] B.N.DELONE et D.K.FADDEEV, The theory of irrationalities of the third degree, Transl. of Math. Monographs, 10, Amer. Math. Soc. Providence, 1964.
- [7] J.FRESNEL, Nombres de Bernoulli et fonctions L p-adiques, Ann. Inst. Fourier, 17 (1967), p.281-333.
- [8] K.IWASAWA, On p-adic L-functions, Annals of Maths, 89 (1969), p.198-200.
- [9] K.IWASAWA, Lectures on p-adic L-functions, Annals Math. Studies, Princeton University Press, 1972.
- [10] H.KLINGEN, Über die Werte der Dedekindschen Zetafunktionen, Math. Annalen, 145 (1962), p.265-272.
- [11] D.E.KNUTH, The art of computer programming, vol.2 : Seminumerical algorithms, Addison-Wesley, Reading, 1969.
- [12] T.KUBOTA et H.W.LEOPOLDT, Eine p-adische Theorie der Zetawerte, Journ. Crelle, 214/215 (1964), p.328-339.
- [13] H.W.LEOPOLDT, Eine Verallgemeinerung der Bernoullischen Zahlen, Abh. Math. Sem. Hamburg, 22 (1958), p.131-140.
- [14] Y.ROY, Algorithmes donnant la structure de la factorisation modulo p d'un polynôme, Séminaire d'informatique de Strasbourg, 1972 (polycopié).
- [15] J.-P.SERRE, Formes modulaires et fonctions zeta p-adiques, dans ce même volume.

- [16] C.L.SIEGEL, Berechnung von Zetafunktionen an ganzzahligen Stellen,
Göttingen Nach. 10 (1969), p.87-102.
- [17] C.L.SIEGEL, Über die Fourierschen Koeffizienten von Modulformen,
Göttingen Nach. 3 (1970), p.15-56.



T A B L E S

TABLE 1
Corps de degré 3 non cycliques

Discriminant	Equation	N
148 = $2^2 \cdot 37$	$x^3 - x^2 - 3x + 1$	57
229	$x^3 - 4x - 1$	55
257	$x^3 - x^2 - 4x + 3$	55
316 = $2^2 \cdot 79$	$x^3 - x^2 - 4x + 2$	53
321 = $3 \cdot 107$	$x^3 - x^2 - 4x + 1$	53
404 = $2^2 \cdot 101$	$x^3 - x^2 - 5x - 1$	53
469 = $7 \cdot 67$	$x^3 - x^2 - 5x + 4$	51
473 = $11 \cdot 43$	$x^3 - 5x - 1$	51
564 = $2^2 \cdot 3 \cdot 47$	$x^3 - x^2 - 5x + 3$	51
568 = $2^3 \cdot 71$	$x^3 - x^2 - 6x - 2$	51
621 = $3^3 \cdot 23$	$x^3 - 6x - 3$	29
697 = $17 \cdot 41$	$x^3 - 7x - 5$	"
733	$x^3 - x^2 - 7x + 8$	"
756 = $2^2 \cdot 3^3 \cdot 7$	$x^3 - 6x - 2$	"
761	$x^3 - x^2 - 6x - 1$	"
785 = $5 \cdot 157$	$x^3 - x^2 - 6x + 5$	"
788 = $2^2 \cdot 197$	$x^3 - x^2 - 7x - 3$	"
837 = $3^3 \cdot 31$	$x^3 - 6x - 1$	"
892 = $2^2 \cdot 223$	$x^3 - x^2 - 8x + 10$	"
940 = $2^2 \cdot 5 \cdot 47$	$x^3 - 7x - 4$	"
985 = $5 \cdot 197$	$x^3 - x^2 - 6x + 1$	"
993 = $3 \cdot 331$	$x^3 - x^2 - 6x + 3$	"
1016 = $2^3 \cdot 127$	$x^3 - x^2 - 6x + 2$	"
1076 = $2^2 \cdot 269$	$x^3 - 8x + 6$	"
1101 = $3 \cdot 367$	$x^3 - x^2 - 9x + 12$	"
1129	$x^3 - 7x - 3$	"
1229	$x^3 - x^2 - 7x + 6$	"
1257 = $3 \cdot 419$	$x^3 - x^2 - 8x + 9$	"

TABLE 2

Corps de degré 4 à groupe de Galois symétrique

Discriminant	Equation
1957 = 19.103	$x^4 - 4x^2 + x + 1$
2777	$x^4 - x^3 - 4x^2 + x + 2$
3981 = 3.1327	$x^4 - x^3 - 4x^2 + 2x + 1$
5744 = $2^4 \cdot 359$	$x^4 - 5x^2 + 2x + 1$
6224 = $2^4 \cdot 389$	$x^4 - 2x^3 - 4x^2 + 2x + 2$
6809 = 11.619	$x^4 - 5x^2 + x + 1$
7053 = 3.2351	$x^4 - 2x^3 - 4x^2 + 3x + 3$
7537	$x^4 - x^3 - 5x^2 + 4x + 3$
8069	$x^4 - x^3 - 5x^2 + 5x + 1$

TABLE 3

Corps de degré 4 contenant un sous-corps quadratique

D	d	η	x	Equation
725	5	$\frac{1 + \sqrt{5}}{2}$	$\frac{\eta + \sqrt{\eta+5}}{2}$	$x^4 - x^3 - 3x^2 + x + 1$
2225	5	$\frac{1 + \sqrt{5}}{2}$	$\frac{\eta + \sqrt{\eta+9}}{2}$	$x^4 - x^3 - 5x^2 + 2x + 4$
2525	5	$\frac{1 + \sqrt{5}}{2}$	$\frac{1 + \sqrt{4\eta+9}}{2}$	$x^4 - 2x^3 - 4x^2 + 5x + 5$
2624	8	$\sqrt{2}$	$\frac{\eta + 1 + \sqrt{2\eta+7}}{2}$	$x^4 - 2x^3 - 3x^2 + 2x + 1$
4205	29	$\frac{1 + \sqrt{29}}{2}$	$\frac{\eta + \sqrt{\eta+3}}{2}$	$x^4 - x^3 - 5x^2 - x + 1$
4352	8	$\sqrt{2}$	$\frac{\eta + \sqrt{-4\eta+10}}{2}$	$x^4 - 6x^2 + 4x + 2$
4400	5	$\frac{1 + \sqrt{5}}{2}$	$\sqrt{\eta + 3}$	$x^4 - 7x^2 + 11$
4525	5	$\frac{1 + \sqrt{5}}{2}$	$\frac{\eta + \sqrt{\eta+13}}{2}$	$x^4 - x^3 - 7x^2 + 3x + 9$
4752	12	$\sqrt{3}$	$\frac{1 + \sqrt{4\eta+9}}{2}$	$x^4 - 2x^3 - 3x^2 + 4x + 1$
5125	5	$\frac{1 + \sqrt{5}}{2}$	$\frac{1 + \sqrt{4\eta+13}}{2}$	$x^4 - 2x^3 - 6x^2 + 7x + 11$
5225	5	$\frac{1 + \sqrt{5}}{2}$	$\frac{\eta + \sqrt{5\eta+13}}{2}$	$x^4 - x^3 - 8x^2 + x + 11$
5725	5	$\frac{1 + \sqrt{5}}{2}$	$\frac{\eta + \sqrt{-3\eta+17}}{2}$	$x^4 - x^3 - 8x^2 + 6x + 11$
7168	8	$\sqrt{2}$	$\sqrt{\eta + 3}$	$x^4 - 6x^2 + 7$
7232	8	$\sqrt{2}$	$\frac{\eta + 1 + \sqrt{2\eta+11}}{2}$	$x^4 - 2x^3 - 5x^2 + 4x + 4$
7488	12	$\sqrt{3}$	$\frac{\eta + 1 + \sqrt{2\eta+8}}{2}$	$x^4 - 2x^3 - 4x^2 + 2x + 1$
7600	5	$\frac{1 + \sqrt{5}}{2}$	$\sqrt{\eta + 4}$	$x^4 - 9x^2 + 19$
7625	5	$\frac{1 + \sqrt{5}}{2}$	$\frac{\eta + \sqrt{\eta+17}}{2}$	$x^4 - x^3 - 9x^2 + 4x + 16$
8112	13	$\frac{1 + \sqrt{13}}{2}$	$\sqrt{\eta + 4}$	$x^4 - 5x^2 + 3$

D discriminant du corps $K = \mathbb{Q}(x)$ d discriminant du corps $E = \mathbb{Q}(\eta)$

TABLE 4
Facteurs locaux associés aux classes non ramifiées

Degré	Classe	Famille	Facteur local
$r = 3$	$C(3)$	F_0	$\frac{p^{2s}}{p^{2s}+p^s+1}$
	$C(2,1)$	F_1	$\frac{p^{2s}}{p^{2s}-1}$
	$C(1,1,1)$	F_3	$\frac{p^{2s}}{p^{2s}-2p^s+1}$
$r = 4$	$C(4)$	$\left. \begin{matrix} F_{0,0} \\ F_{0,2} \end{matrix} \right\} F_0$	$\frac{p^{3s}}{p^{3s}+p^{2s}+p^s+1}$
	$C(2,2)$		$\frac{p^{3s}}{p^{3s}+p^{2s}-p^s-1}$
	$C(3,1)$	F_1	$\frac{p^{3s}}{p^{3s}-1}$
	$C(2,1,1)$	F_2	$\frac{p^{3s}}{p^{3s}-p^{2s}-p^s+1}$
	$C(1,1,1,1)$	F_4	$\frac{p^{3s}}{p^{3s}-3p^{2s}+3p^s-1}$
$r = 5$	$C(5)$	$\left. \begin{matrix} F_{0,0} \\ F_{0,1} \end{matrix} \right\} F_0$	$\frac{p^{4s}}{p^{4s}+p^{3s}+p^{2s}+p^s+1}$
	$C(3,2)$		$\frac{p^{4s}}{p^{4s}+p^{3s}-p^s-1}$
	$C(4,1)$	$\left. \begin{matrix} F_{1,0} \\ F_{1,2} \end{matrix} \right\} F_1$	$\frac{p^{4s}}{p^{4s}-1}$
	$C(2,2,1)$		$\frac{p^{4s}}{p^{4s}-2p^{2s}+1}$
	$C(3,1,1)$	F_2	$\frac{p^{4s}}{p^{4s}-p^{3s}-p^s+1}$
	$C(2,1,1,1)$	F_3	$\frac{p^{4s}}{p^{4s}-2p^{3s}+2p^s-1}$
	$C(1,1,1,1,1)$	F_5	$\frac{p^{4s}}{p^{4s}-4p^{3s}+6p^{2s}-4p^s+1}$

TABLE 5

Facteurs locaux associés aux classes ramifiées

Degré	Classe	Famille	Facteur local
$r = 3$	$C(1^3)$	$\bar{F}_1$	1
	$C(1^2, 1)$	$\bar{F}_2$	$\frac{p^s}{p^s - 1}$
$r = 4$	$C(2^2)$	$\bar{F}_0$	$\frac{p^s}{p^s + 1}$
	$C(2, 1^2)$	$\left. \begin{matrix} \bar{F}_{1,1} \\ \bar{F}_{1,0} \end{matrix} \right\} \bar{F}_1$	$\frac{p^{2s}}{p^{2s} - 1}$
	$C(1^4)$		1
	$C(1^3, 1)$	$\left. \begin{matrix} \\ \end{matrix} \right\} \bar{F}_2$	$\frac{p^s}{p^s - 1}$
	$C(1^2, 1^2)$		$\frac{p^s}{p^s - 1}$
	$C(1^2, 1, 1)$	$\bar{F}_3$	$\frac{p^{2s}}{(p^s - 1)^2}$
$r = 5$	$C(1^5)$	$\left. \begin{matrix} \\ \end{matrix} \right\} \bar{F}_{1,0}$	1
	$C(3, 1^2)$		$\frac{p^{3s}}{p^{3s} - 1}$
	$C(2^2, 1)$	$\left. \begin{matrix} \\ \end{matrix} \right\} \bar{F}_{1,1}$	$\frac{p^{2s}}{p^{2s} - 1}$
	$C(2, 1^3)$		$\frac{p^{2s}}{p^{2s} - 1}$
	$C(1^4, 1)$	$\left. \begin{matrix} \\ \end{matrix} \right\} \bar{F}_{2,0}$	$\frac{p^s}{p^s - 1}$
	$C(1^3, 1^2)$		$\frac{p^s}{p^s - 1}$
	$C(2, 1^2, 1)$	$\bar{F}_{2,1}$	$\frac{p^{3s}}{p^{3s} - p^{2s} - p^s + 1}$

TABLE 5 (suite)

Facteurs locaux associés aux classes ramifiées

Degré	Classe	Famille	Facteur local
$r = 5$	$C(1^3, 1, 1)$	} $\bar{F}_3$	$\frac{p^{2s}}{(p^s - 1)^2}$
	$C(1^2, 1^2, 1)$		$\frac{p^{2s}}{(p^s - 1)^2}$
	$C(1^2, 1, 1, 1)$	$\bar{F}_4$	$\frac{p^{3s}}{(p^s - 1)^3}$

TABLE 6

Facteurs locaux pour $L(s; \chi_d)$ avec $L(s) = \zeta_K(s)/\zeta(s)$

Sous-classes	Facteur local
$C(3)_0$	1
$C(3)_+$	$\frac{p^{2s}}{p^{2s}+p^s+1}$
$C(3)_-$	$\frac{p^{2s}}{p^{2s}-p^s+1}$
$C(2,1)_0$	1
$C(2,1)_+$	$\frac{p^{2s}}{p^{2s}-1}$
$C(2,1)_-$	$\frac{p^{2s}}{p^{2s}-1}$
$C(1,1,1)_0$	1
$C(1,1,1)_+$	$\frac{p^{2s}}{(p^s-1)^2}$
$C(1,1,1)_-$	$\frac{p^{2s}}{(p^s+1)^2}$
$C(1^3)_0$	1
$C(1^3)_+$	1
$C(1^3)_-$	1

TABLE 6 (suite)

Facteurs locaux pour $L(s; \chi_d)$ avec $L(s) = \zeta_K(s)/\zeta(s)$

Sous-classes	Facteur local
$C(1^2, 1)_0$	1
$C(1^2, 1)_+$	$\frac{p^s}{p^s - 1}$
$C(1^2, 1)_-$	$\frac{p^s}{p^s + 1}$

TABLE 7

Facteurs locaux pour $L(s) = \zeta_K(s)/\zeta_E(s)$

Classes non ramifiées	Classe du sous-corps	Facteur local
$C(4)$	$C(2)$	$\frac{p^{2s}}{p^{2s}+1}$
$C(2,2)_+$	$C(1,1)$	$\frac{p^{2s}}{(p^s+1)^2}$
$C(2,2)_-$	$C(2)$	$\frac{p^{2s}}{p^{2s}-1}$
$C(2,1,1)$	$C(1,1)$	$\frac{p^{2s}}{p^{2s}-1}$
$C(1,1,1,1)$	$C(1,1)$	$\frac{p^{2s}}{(p^s-1)^2}$
Classes ramifiées		
$C(2^2)_0$	$C(1^2)$	$\frac{p^s}{p^s+1}$
$C(2^2)_-$	$C(2)$	1
$C(2,1^2)$	$C(1,1)$	$\frac{p^s}{p^s+1}$
$C(1^4)$	$C(1^2)$	1
$C(1^2,1^2)_0$	$C(1^2)$	$\frac{p^s}{p^s-1}$
$C(1^2,1^2)_+$	$C(1,1)$	1
$C(1^2,1,1)$	$C(1,1)$	$\frac{p^s}{p^s-1}$

TABLE 8

FONCTION ZÊTA DU CORPS DE DEGRÉ 3

ET DISCRIMINANT 148

(groupe de Galois non cyclique)

- 1) Répartition en classes des nombres premiers ≤ 2000
- 2) Valeurs de $L(1-2n)$ pour $1 \leq n \leq 29$, avec $L(s) = \zeta_K(s)/\zeta(s)$
- 3) Valuation des différences itérées
- 4) Valeurs extrapolées de $L^{(p)}(1)$
- 5) Valeurs de $L'(1-2n)$ pour $1 \leq n \leq 15$, avec $L'(s) = L(s; \chi_5)$
- 6) Valuation des différences itérées pour $L'(s)$
- 7) Intercalement de $L(s)$ et $L'(s)$

RÉPARTITION EN CLASSES DES NOMBRES PREMIERS INFÉRIEURS A 2000

R= 3 D= 148 .

CLASSE (3) .

3	7	11	41	47	53	71	73	83	101	127	149	157	173	181	197	211
223	229	263	271	307	337	359	373	379	397	419	433	443	509	521	571	593
599	613	617	619	641	659	673	677	719	733	739	743	751	761	773	787	811
821	887	937	953	983	1009	1033	1039	1063	1109	1117	1151	1181	1187	1193	1217	1231
1249	1291	1321	1381	1399	1409	1427	1439	1447	1453	1459	1471	1481	1483	1487	1543	1579
1619	1621	1637	1699	1709	1723	1801	1823	1861	1871	1913	1931	1933	1949	1951	1987	1997
1999																

CLASSE (2 , 1) .

5	13	17	19	23	29	31	43	59	61	79	89	97	103	109	113	131
163	167	179	191	193	199	227	239	241	251	257	277	281	283	311	313	331
347	353	383	389	401	409	421	431	439	449	457	461	463	467	479	487	499
503	523	541	547	557	563	569	577	587	607	631	643	647	653	661	683	701
709	727	757	769	797	809	827	829	853	857	859	883	907	911	919	947	967
977	991	997	1013	1019	1021	1031	1049	1051	1087	1091	1093	1097	1123	1129	1153	1171
1201	1213	1223	1229	1277	1289	1297	1301	1303	1319	1327	1361	1367	1423	1429	1451	1493
1499	1511	1523	1531	1549	1559	1567	1571	1583	1597	1609	1613	1657	1663	1667	1697	1721
1733	1741	1747	1753	1759	1789	1811	1831	1867	1873	1879	1889	1901	1907	1973	1993	

CLASSE (1 , 1 , 1) .

67	107	137	139	151	233	269	293	317	349	367	491	601	691	823	839	863
877	881	929	941	971	1061	1069	1103	1163	1237	1259	1279	1283	1307	1373	1433	1489
1553	1601	1607	1627	1669	1693	1777	1783	1787	1847	1877	1973					

CLASSE (1³)CLASSE (1², 1)

VALEURS DE L(1-2N) .		R= 3 D= 148 .	
-----		-----	
L(-1) =	4	DIVISIBLE PAR	2(2)
L(-3) =	2308	DIVISIBLE PAR	2(2).577
L(-5) =	131 25124	DIVISIBLE PAR	2(2).19.373.463
L(-7) =	32 57915 08228	DIVISIBLE PAR	2(2)
L(-9) =	23 73928 47471 97444	DIVISIBLE PAR	2(2).43.71
L(-11) =	40 37044 12801 87261 30948	DIVISIBLE PAR	2(2).31.37
L(-13) =	138 07573 92562 97487 08699 67364	DIVISIBLE PAR	2(2).23
L(-15) =	855 77580 68859 93637 68688 37359 66468	DIVISIBLE PAR	2(2).6229
L(-17) =	8898 19213 47240 73923 64587 95526 78337 22884	DIVISIBLE PAR	2(2).1889.6763
L(-19) =	1 46270 90535 78676 01466 32391 62984 71198 49198 30788	DIVISIBLE PAR	2(2)
L(-21) =	36 26272 92815 97320 55316 93916 13438 21540 94812 07835 52004	DIVISIBLE PAR	2(2).41.67.4283
L(-23) =	1304 86468 89866 58825 06745 21804 41538 72810 65271 12017 48744 59908	DIVISIBLE PAR	2(2).19.181.587
L(-25) =	66019 45531 93938 22160 12256 45428 55744 87064 46784 87823 32305 96325 42724	DIVISIBLE PAR	2(2).83
L(-27) =	45 72462 14379 91130 75116 96021 93333 96616 66471 58773 49714 24255 36323 65057 09828	DIVISIBLE PAR	2(2).89.109.1471
L(-29) =	4237 07483 35234 88560 60239 03826 30120 36087 01505 32574 18235 66047 77644 09494 00729 83044	DIVISIBLE PAR	2(2).37.41

R= 3 D= 148 .

VALEURS DE L(1-2N) .

L(-31) =	5 15034 10543 47877 15084 06442 27598 66995 93038 51822 53121 17011 03749 39644 95194 81553 44077 56548	DIVISIBLE PAR	2(2).71.193.2203
L(-33) =	807 17514 91498 64882 81700 02476 11362 70182 68786 59779 08725 19242 62665 91972 71461 07874 70957 70035 60964	DIVISIBLE PAR	2(2).157.3499
L(-35) =	1 60644 42661 30456 11048 55548 51331 70802 38773 94424 48288 78615 61944 91707 87547 68629 87677 86978 58580 39702 96068	DIVISIBLE PAR	2(2).23
L(-37) =	400 56967 65819 18056 11233 74816 15911 05807 10144 46491 80133 58431 27712 01122 70607 96275 08493 67564 09075 76491 88525 64484	DIVISIBLE PAR	2(2).479
L(-39) =	1 23645 53397 21319 47860 63045 73607 74984 42144 49034 95981 51703 42700 77018 84152 33670 21162 73676 22199 50506 50394 39379 75737 44388	DIVISIBLE PAR	2(2).113
L(-41) =	467 37996 08783 83635 91371 82314 35417 58555 82989 12207 36886 18764 94131 29854 34914 59872 03228 74098 60921 45309 17036 68903 45213 12770 81604	DIVISIBLE PAR	2(2).19.31.79.107
L(-43) =	2 14244 42871 50149 19068 79719 50096 32736 48788 65445 86124 77201 27016 18343 40777 72540 57072 60857 52037 09601 49023 34694 53323 07843 42507 04324 37508	DIVISIBLE PAR	2(2).137
L(-45) =	1180 43988 48751 59418 21739 63043 11266 81543 81624 95849 46627 08419 89423 37050 04977 79054 19021 55583 86364 76995 17745 56529 57814 54659 35801 58797 07182 00324	DIVISIBLE PAR	2(2).241
L(-47) =	7 75459 66225 78712 01110 46882 70646 68379 13810 70807 74959 71171 43762 99710 51685 60196 45221 60219 40770 91111 33425 20244 24012 70288 91320 29028 50937 26130 38458 31428	DIVISIBLE PAR	2(2).37.79.101

R= 3 D= 148 •

DIFFÉRENCES ITÉRÉES POUR L(s)

* 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28

P= 2 * 2 8 10 12 17 18 28 24 29 30 36 36 41 42 49 48 53 54 60 60 65 66 75 72 77 78 84 84 89

P= 3 * 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28

P= 5 * 0 1 2 3 5 5 6 7 9 9 10 11 13 13 14
* 0 1 2 3 4 5 6 7 8 9 10 11 12 13

P= 7 * 0 1 2 3 4 6 6 7 8 9
* 0 1 2 3 4 5 6 7 8 9
* 0 1 2 3 4 5 6 7 8

P=11 * 0 1 2 3 4 6
* 0 1 2 3 4 5
* 0 2 3 3 4 5
* 0 1 2 3 4 5
* 0 1 2 3 6

P=13 * 0 1 2 3 4
* 0 1 2 3 4
* 0 1 2 3 5
* 0 1 2 3 5
* 0 1 2 3 4
* 0 1 2 3

R= 3 D= 148 .

VALEURS EXTRAPOLÉES DE LP(1)

CES VALEURS SONT ÉCRITES EN BASE P .

P= 2 LP(1) = 110 01110 01100 11001 00100 11110 10101 01011 00011 10000 11110 11110
10101 10000 10101 11110 11000 00100

MODULO 2^{23}

P= 3 LP(1) = 101 01012 12022 21002 01111 01001

MODULO 3^{28}

P= 5 LP(1) = 420 14411 42223

MODULO 5^{13}

P= 7 LP(1) = 13 42235

MODULO 7^8

P=11 LP(1) = 3 45837

MODULO 11^6

P=13 LP(1) = 9A5 (*)

MODULO 13^3

(*) La lettre A désigne "dix" en base 13

VALEURS DE $L'(1-2N)$.		R= 3 D= 148 / R1= 2 D1= 5 .	
-----		-----	
$L'(-1) =$	648	DIVISIBLE PAR	2(3).3(4)
$L'(-3) =$	1849 73064	DIVISIBLE PAR	2(3).3.37.67.3109
$L'(-5) =$	64264 67598 84168	DIVISIBLE PAR	2(3).3.13.1021
$L'(-7) =$	99 45402 46475 42013 04584	DIVISIBLE PAR	2(3).3(2).37.6673
$L'(-9) =$	45280 62626 38921 08663 37283 56488	DIVISIBLE PAR	2(3).3.29.53.181.283.613
$L'(-11) =$	481 25497 35846 70990 44081 84422 73089 89704	DIVISIBLE PAR	2(3).3.661
$L'(-13) =$	10 28744 85398 18135 28523 28635 75289 84245 06733 53608	DIVISIBLE PAR	2(3).3(2).29
$L'(-15) =$	39850 16823 96219 57050 57902 75903 61482 40659 78786 66371 16424	DIVISIBLE PAR	2(3).3.409.907
$L'(-17) =$	2589 71476 59735 24024 83172 65772 33265 48428 24329 11022 40762 69839 31528	DIVISIBLE PAR	2(3).3.13
$L'(-19) =$	266 06522 70456 33541 06271 12777 22880 17329 46159 73250 42979 71541 52813 50459 72744	DIVISIBLE PAR	2(3).3(3)
$L'(-21) =$	41 22595 01944 25925 71724 30641 50074 97982 41340 31384 32485 70604 87193 96606 77616 99294 66248	DIVISIBLE PAR	2(3).3.37
$L'(-23) =$	9 27162 12591 58984 50024 22404 40432 32937 65637 31305 13001 43692 57442 07437 18401 57270 31157 19142 46664	DIVISIBLE PAR	2(3).3
$L'(-25) =$	2 93185 27747 54418 42587 65943 91510 02204 58860 29810 23919 46211 86651 90016 50238 79301 36172 75292 45824 62468 53768	DIVISIBLE PAR	2(3).3(2).37.107

VALEURS DE $L'(1-2N)$.

$L'(-27) =$

1 26911 31878 18280 64747 42672 25427 74265 74096
94663 14918 05784 19657 50248 09561 15035 70439 45882
84922 46001 30700 36222 26184

$L'(-29) =$

73501 53183 18378 87253 54416 04519 11653 51309 45666
91914 35505 66308 71515 66487 08563 91596 52718 90451
14044 46353 06763 32205 84157 10088

R= 3 D= 148 / R1= 2 D1= 5 .

DIVISIBLE PAR

2(3).3.107.443

DIVISIBLE PAR

2(3).3.13.109

R= 3 D= 148 / R1= 2 D1= 5 .

DIFFÉRENCES ITÉRÉES POUR $L'(s)$

[illegible]

INTERCALEMENT DE $L(s)$ ET $L'(s)$

Les différences itérées sont calculées sur les suites

$L^{(5)}(-1), L^{(5)}(-3; X_5), L^{(5)}(-5), L^{(5)}(-7; X_5) \dots$ pour la première ligne
 $L^{(5)}(-1; X_5), L^{(5)}(-3), L^{(5)}(-5, X_5), L^{(5)}(-7), \dots$ pour la seconde ligne.

On a indiqué la plus haute puissance de 5, soit 5^{v_n} (resp. $5^{v'_{11}}$) qui divise la n-ième différence itérée.

n	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
v_n	0	1	2	3	5	5	6	7	9	9	10	11	14	13	14
v'_{11}	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14

Valeurs extrapolées (*) $L^{(5)}(1; X_5) \equiv 9412\ 97769 \pmod{5^{14}}$
 $L^{(5)}(1) \equiv 35194\ 74688 \pmod{5^{14}}$

(*) En écriture décimale

TABLE 9

FONCTION ZÊTA DU CORPS DE DEGRÉ 4
ET DISCRIMINANT 1957

(groupe de Galois symétrique)

- 1) Répartition en classes des nombres premiers ≤ 5000
- 2) Valeurs de $L(1-2n)$ pour $1 \leq n \leq 15$, avec $L(s) = \zeta_K(s)/\zeta(s)$
- 3) Valuation des différences itérées
- 4) Valeurs extrapolées de $L^{(p)}(1)$

R= 4 D= 1957 .

RÉPARTITION EN CLASSES DES NOMBRES PREMIERS INFÉRIEURS A 5000

	421	431	443	457	479	499	509	547	557	577	617	659	677	719	733	773	787
857	881	907	937	941	947	967	967	977	991	1009	1039	1061	1069	1091	1093	1103	1193
1213	1217	1237	1289	1301	1303	1367	1367	1423	1439	1471	1487	1493	1499	1523	1531	1549	1553
1607	1627	1663	1721	1733	1789	1801	1801	1831	1847	1907	1949	1951	2011	2029	2087	2089	2129
2141	2273	2287	2297	2371	2381	2383	2383	2473	2477	2543	2557	2579	2621	2699	2753	2789	2791
2851	2861	2879	2903	2939	2969	3049	3049	3169	3187	3217	3229	3251	3257	3259	3307	3319	3331
3359	3391	3413	3469	3491	3511	3527	3527	3541	3617	3637	3643	3691	3727	3823	3919	3929	4013
4019	4021	4049	4091	4111	4133	4159	4159	4211	4231	4283	4507	4549	4603	4621	4639	4649	4651
4663	4721	4723	4729	4733	4787	4801	4801	4817	4861	4877	4903	4969	4987				

CLASSE

C(1 , 1 , 1 , 1) .

347

487 1283

1409 1987

2239 2633

3079 3347

3533

3803

821 4003 4339 4363

1451 4513

2281 2731

3079 3347

3533

CLASSE C(2 , 1²) .

19

103

VALEURS DE L(1-2N) .		R= 4 D= 1957 .	
-----		-----	
L(-1) = -	8	DIVISIBLE PAR	2(3)
L(-3) =	1 41640	DIVISIBLE PAR	2(3).5.3541
L(-5) = -	7 41765 07128	DIVISIBLE PAR	2(3).11
L(-7) =	346 17448 03732 09480	DIVISIBLE PAR	2(3).5.787.829
L(-9) = -80662 46900 04692 24539 26008		DIVISIBLE PAR	2(3)
L(-11) =	668 76006 54719 97250 78936 28174 30920	DIVISIBLE PAR	2(3).5
L(-13) = -	15 80615 01573 52846 08625 55603 36398 73910 08888	DIVISIBLE PAR	2(3).4639
L(-15) =	91118 44718 51866 66717 33919 94919 80613 75344 00815 17900	DIVISIBLE PAR	2(3).5.11.271
L(-17) = -11413 54179 35192 31575 63220 29316 79065 94667 10041 43836 16554 51768		DIVISIBLE PAR	2(3).31.137.211.229.311
L(-19) =	2841 85840 37088 99787 56194 19479 11127 78384 56427 53295 38176 10124 93903 02600	DIVISIBLE PAR	2(3).5(2)
L(-21) = -	1310 54838 11115 44576 86944 79598 29925 53382 12713 35723 49607 50017 75312 59333 76340 70648	DIVISIBLE PAR	2(3).181.593
L(-23) =	1056 83485 38400 34406 68632 42326 81770 38833 32717 96085 13298 18671 86977 53413 80079 09720 54822 16840	DIVISIBLE PAR	2(3).5.593
L(-25) = -	1420 89942 78219 59418 14999 60563 26591 44038 58463 96658 15579 85865 67198 43898 66361 05352 73628 50810 06980 01528	DIVISIBLE PAR	2(3).11.41
L(-27) =	3059 68764 89801 04245 08897 69288 49491 09670 72572 35046 37056 31403 95109 72336 45379 68699 38395 72646 94113 73629 71756 92680	DIVISIBLE PAR	2(3).5.149

VALEURS DE L(1-2N) .

L(-29) = -10196 41849 10142 77663 59392 65090 32924 88358 86785
 27341 20563 83289 42015 57337 45073 59563 36592 89699
 53694 57879 81280 12621 49755 00408

DIVISIBLE PAR

2(3).251

R= 4 D= 1957 .

DIFFÉRENCES ITÉRÉES

R= 4 D= 1957 •

```

* 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14
*
*****
P= 2 * 3 9 10 13 16 19 22 25 28 31 34 37 40 43 46
*
*****
P= 3 * 0 1 3 3 11 5 7 7 9 9 12 11 13 13 15
*
*****
P= 5 * 0 1 3 3 4 5 8 7
* 1 1 2 3 5 6
*
*****
P= 7 * 0 1 2 4 4
* 0 1 2 3 4
* 0 1 2 3 4
*
*****
P=11 * 0 1 2 2
* 0 2 2 2
* 1 1 2 2
* 0 1 2 2
* 0 1 2 2
*
*****
P=13 * 0 1 2
* 0 1 3 2
* 0 1 1 2
* 0 1 2 2
* 0 2 2
*
*****

```

VALEURS EXTRAPOLÉES DE LP(1)

CES VALEURS SONT ÉCRITES EN BASE P .

P= 2 LP(1) = 1010 11001 01000 00110 11110 11011 10111 01100 01000

P= 3 LP(1) = 11122 22200 01111

P= 5 LP(1) = 3 13100

P= 7 LP(1) = 5132

P=11 LP(1) = 37

P=13 LP(1) = 87

MODULO 2⁴⁶

MODULO 3¹⁵

MODULO 5⁶

MODULO 7⁴

MODULO 11²

MODULO 13²

R= 4 D= 1957 .

TABLE 10

FONCTION ZÊTA DU CORPS DE DEGRÉ 4
ET DISCRIMINANT 725

(groupe de Galois diédral)

- 1) Répartition en classes des nombres premiers ≤ 3000
- 2) Valeurs de $L(1-2n)$ pour $1 \leq n \leq 20$, avec $L(s) = \zeta_K(s)/\zeta_E(s)$
- 3) Valuation des différences itérées
- 4) Valeurs extrapolées de $L^{(p)}(1)$

RÉPARTITION EN CLASSES DES NOMBRES PREMIERS INFÉRIEURS A 3000

R= 4 D= 725

CLASSE	C(4)	17	37	43	47	73	97	113	127	137	157	163	193	263	293	307
2	3	367	433	443	467	503	563	577	607	617	653	677	727	733	743	757
317	797	823	853	887	907	947	947	967	983	997	1013	1033	1063	1087	1117	1123
1163	1187	1237	1303	1307	1373	1423	1423	1433	1447	1453	1487	1493	1523	1583	1597	1607
1613	1627	1663	1693	1697	1723	1777	1777	1783	1787	1867	1873	1877	1933	1987	1993	2003
2027	2143	2207	2273	2293	2347	2357	2357	2393	2417	2447	2467	2473	2477	2593	2647	2657
2683	2687	2707	2753	2767	2803	2857	2897	2903	2917	2927						
CLASSE	C(2 , 2)	23	53	67	83	103	107	167	173	197	223	227	233	257	277	283
7	13	353	373	383	397	457	463	487	523	547	557	587	593	613	643	647
313	347	787	857	863	877	883	937	953	977	1093	1097	1103	1153	1193	1213	1217
673	1277	1283	1327	1367	1427	1483	1543	1553	1567	1637	1657	1733	1747	1753	1823	1847
1223	1913	1973	1997	2017	2053	2063	2083	2087	2113	2137	2153	2203	2213	2237	2267	2287
1907	2333	2377	2383	2423	2437	2503	2543	2557	2617	2633	2663	2677	2693	2713	2777	2797
2297	2837	2843	2887	2953	2957	2963										
CLASSE	C(2 , 2)	151	181	199	239	241	349	401	419	439	661	691	701	719	761	919
59	71	1019	1031	1039	1051	1069	1451	1459	1531	1571	1579	1601	1741	1789	1811	1889
991	1949	1979	2029	2039	2081	2089	2269	2371	2551	2609	2659	2731	2789	2851	2971	
CLASSE	C(2 , 1 , 1)	31	41	61	79	89	101	131	191	211	229	251	269	271	311	331
11	19	389	409	421	449	461	479	491	541	569	599	601	619	641	659	739
359	769	809	829	839	859	881	911	971	1061	1091	1129	1171	1181	1201	1229	1249
1259	1279	1291	1319	1361	1381	1409	1429	1439	1471	1481	1489	1511	1549	1609	1621	1699
1709	1721	1759	1801	1871	1931	1951	1999	2011	2069	2099	2129	2131	2161	2221	2251	2281
2309	2339	2341	2351	2381	2389	2399	2521	2531	2549	2579	2591	2621	2671	2689	2699	2711
2729	2741	2801	2861	2879	2939	2969	2999									
CLASSE	C(1 , 1 , 1)	149	179	281	431	499	509	521	571	631	709	811	821	929	941	1021
109	139	149	179	281	431	499	509	521	571	631	709	811	821	929	941	1021
1049	1109	1151	1231	1289	1301	1321	1399	1499	1559	1619	1669	1831	1861	1879	2111	2141
2179	2239	2311	2411	2441	2459	2539	2719	2749	2791	2819	2909					

R= 4 D= 725 •

RÉPARTITION EN CLASSES DES NOMBRES PREMIERS INFÉRIEURS A 3000

CLASSE $C(2^2)_0$.
5

CLASSE $C(2, 1^2)$.
29

VALEURS DE L(1-2N) .			R= 4 D= 725 .	
-----			-----	
L(-1) =	4		DIVISIBLE PAR	2(2)
L(-3) =	2164		DIVISIBLE PAR	2(2).541
L(-5) =	117 39604		DIVISIBLE PAR	2(2)
L(-7) =	27 94444 17844		DIVISIBLE PAR	2(2).17.317
L(-9) =	19 54268 59225 16884		DIVISIBLE PAR	2(2).17
L(-11) =	31 89969 89772 00455 88724		DIVISIBLE PAR	2(2)
L(-13) =	104 72547 49299 36592 42768 65364		DIVISIBLE PAR	2(2).19.37.239
L(-15) =	623 02785 02010 54439 23709 62168 58804		DIVISIBLE PAR	2(2).109.4909
L(-17) =	6218 15867 04125 53376 30860 78776 76177 61044		DIVISIBLE PAR	2(2).59
L(-19) =	98113 90087 48401 09011 79954 10879 18543 74458 44084		DIVISIBLE PAR	2(2).43.4549
L(-21) =	23 34778 33563 36616 80812 80612 23093 50504 30065 97918 59924		DIVISIBLE PAR	2(2).73.271.379
L(-23) =	806 42358 26208 89424 51072 49831 14989 54692 99779 78519 97494 40564		DIVISIBLE PAR	2(2).17
L(-25) =	39163 56800 00781 55318 37226 76705 55165 44049 65045 61040 68168 31814 98004		DIVISIBLE PAR	2(2).17.3919.4787
L(-27) =	26 03592 46905 01493 12474 29456 11176 12474 78159 59353 56848 78483 39491 50946 24244		DIVISIBLE PAR	2(2).41.1811.5843
L(-29) =	2315 80291 45994 57098 20760 87306 77754 07835 99513 80100 19149 69357 06644 75777 41414 91284		DIVISIBLE PAR	2(2).67.151

VALEURS DE L(1-2N) .

R= 4 D= 725 .

L(-31) =	2 70199 17853 07256 20039 28911 44393 62260 18127	DIVISIBLE PAR	2(2).19
	60258 14759 86773 80144 40704 98187 62418 75712 51124		
L(-33) =	406 46990 10433 11011 34353 71115 62918 41688 90037	DIVISIBLE PAR	2(2).3323
	72690 09068 86113 71368 90729 94780 85764 14503 17479		
	35764		
L(-35) =	77649 53254 37805 87903 10099 43295 50473 56435 47322	DIVISIBLE PAR	2(2)
	17359 93337 81844 91641 62353 05771 19564 73556 72396		
	81568 57204		
L(-37) =	185 85053 95675 59938 44765 12984 13353 38351 66084	DIVISIBLE PAR	2(2)
	81248 02236 85892 97490 69312 21678 22648 14500 54326		
	16249 05849 36190 07444		
L(-39) =	55065 14214 09981 82563 27801 92166 53424 49153 05994	DIVISIBLE PAR	2(2).17.443
	97512 94667 75853 95753 60143 95624 37900 58205 25777		
	44078 86597 29933 62334 58484		

R= 4 D= 725 •

DIFFÉRENCES ITÉRÉES

```

* 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19
*
*****
*
P= 2 * 2 5 8 11 14 17 20 23 26 29 32 35 38 41 44 47 50 53 56 59
*
*****
*
P= 3 * 0 2 2 4 4 6 6 8 8 10 10 12 12 14 14 16 16 18 18 20
*
*****
*
P= 5 * 0 1 2 3 4 5 6 7 8 9
* 0 1 2 3 4 5 6 7 8 9
*
*****
*
P= 7 * 0 1 2 4 4 5 6
* 0 4 2 3 4 5 6
* 0 1 3 4 4 5
*
*****
*
P=11 * 0 1 2 3
* 0 1 2 3
* 0 1 2 3
* 0 1 2 3
* 0 1 2 3
*
*****
*
P=13 * 0 1 2 3
* 0 1 2 3
* 0 1 2 3
* 0 1 2 3
* 0 1 2 3
*
*****
*
*****

```

VALEURS EXTRAPOLÉES DE LP(1)

R= 4 D= 725 •

CES VALEURS SONT ÉCRITES EN BASE P .

P= 2	LP(1) = 1000 00001 00100 10010 11011 01001 10110 11111 00010 01110 01101 10100	MODULO	2 ⁵⁹
P= 3	LP(1) = 12212 22122 02021 22011	MODULO	3 ²⁰
P= 5	LP(1) = 2303 02214	MODULO	5 ⁹
P= 7	LP(1) = 51422	MODULO	7 ⁵
P=11	LP(1) = 246	MODULO	11 ³
P=13	LP(1) = 24	MODULO	13 ²

TABLE 11

FONCTION ZÊTA DU CORPS DE DEGRÉ 5
ET DISCRIMINANT 24217

- 1) Répartition en classes des nombres premiers ≤ 5000
- 2) Valeurs de $L(1-2n)$ pour $1 \leq n \leq 9$, avec $L(s) = \zeta_K(s)/\zeta(s)$
- 3) Valuation des différences itérées
- 4) Valeurs extrapolées de $L^{(p)}(1)$

RÉPARTITION EN CLASSES DES NOMBRES PREMIERS INFÉRIEURS A 5000

R= 5 D= 24217 .

2749	2969	3049	3121	3137	3187	3301	3313	3331	3343	3373	3457	3463	3557	3583	3643	3673
3709	3719	3739	3889	3911	3923	4007	4051	4139	4159	4211	4243	4253	4547	4567	4591	4597
4603	4783	4831	4909													

CLASSE C(2 , 2 , 1) .

47	73	101	107	131	163	193	233	251	293	439	457	569	577	617	641	661
677	751	883	947	953	997	1009	1051	1153	1249	1289	1327	1367	1427	1471	1483	1667
1669	1741	1777	1789	1801	1931	1951	1997	2003	2053	2143	2239	2267	2311	2357	2549	2593
2671	2689	2707	2837	2879	2963	3061	3089	3167	3307	3413	3539	3581	3593	3613	3671	3733
3769	3877	4013	4127	4217	4339	4451	4549	4637	4751	4937	4967					

CLASSE C(2 , 1 , 1 , 1) .

149	557	601	647	691	709	733	761	773	971	991	1019	1091	1193	1229	1259	1277
1283	1523	1579	1759	1861	1933	2161	2251	2371	2683	2797	2909	2957	3191	3203	3217	3251
3389	3467	3517	3607	3767	3917	3967	4003	4019	4111	4561	4639	4691	4919	4943		

CLASSE C(1 , 1 , 1 , 1 , 1) .

3329 4091 4447 4703

CLASSE C(2 , 1², 1) .

61 397

VALEURS DE L(1-2N) .

R= 5 D= 24217 .

L(-1) =	16								DIVISIBLE PAR	2(4)
L(-3) =	71	88208							DIVISIBLE PAR	2(4)
L(-5) =	29495	13678	68656						DIVISIBLE PAR	2(4)
L(-7) =	2245	03358	94871	66394	85808				DIVISIBLE PAR	2(4).9337
L(-9) =	1461	13030	11941	68101	93951	81532	80496		DIVISIBLE PAR	2(4)
L(-11) =	5168	75854	53241	83572	96341	62306	88370	35563	DIVISIBLE PAR	2(4).19
L(-13) =	73920	79607	19345	66145	48012	22364	46192	36939	DIVISIBLE PAR	2(4).257.571
	69033	51536								
L(-15) =	34	71067	10972	64948	51222	84363	94624	87950	DIVISIBLE PAR	2(4).23
	42999	57200	50834	38301	80208					
L(-17) =	4587	20178	62789	28647	76279	52624	46655	79507	DIVISIBLE PAR	2(4).131.1039
	19728	03165	43452	79674	85876	35136	97776			

R= 5 D= 24217 .

DIFFÉRENCES ITÉRÉES

```

* 0 1 2 3 4 5 6 7 8
*
*****
*
p= 2 * 4 7 10 13 16 19 22 25 28
*
*****
*
p= 3 * 0 1 3 3 7 5 7 7 9
*
*****
*
p= 5 * 0 1 2 2 3 4
*
*****
*
p= 7 * 0 1 2 2
*
*****
*
p=11 * 0 1 1 1 1
*
*****
*
p=13 * 0 1 1 1
*
*****
*

```


VALEURS EXTRAPOLÉES DE LP(1)

R= 5 D= 24217 •

CES VALEURS SONT ÉCRITES EN BASE P .

P= 2 LP(1) = 110 01100 00110 01111 01011 10000

MODULO 2²⁸

P= 3 LP(1) = 1200 02111

MODULO 3⁹

P= 5 LP(1) = 13

MODULO 5³

P= 7 LP(1) = 32

MODULO 7²

P=11 LP(1) = 0

MODULO 11

P=13 LP(1) = 0

MODULO 13