Des nombres de Bernoulli à la fonction zêta p-adique

1. Définition et premières propriétés

$1+2+\cdots+n-1 = \frac{n(n-1)}{2}$, $1^2+2^2+\cdots+(n-1)^2 = \frac{n(n-1)(2n-1)}{6}$ $\forall n \geq 1$

$k \geq 1$, $S_k(n) = 1^k + 2^k + \cdots + (n-1)^k$ pb (Jacques Bernoulli 1654-1705) exprimer $S_k(n)$ pol en n d° $k+1$

Déf: (Nb Bernoulli) $(B_k)_{k\geq 0}$ $\quad B(t) = \sum_{k\geq 0} \frac{B_k}{k!} t^k = \frac{t}{e^t - 1} \in \mathbb{Q}[[t]]$

table

$B_0 = 1$, $B_1 = -\frac{1}{2}$, $B_{2n+1} = 0$ $n \neq 0$

$k=$	2	4	6	8	10	12	14	...	32
$B_k=$	$\frac{1}{6}$	$-\frac{1}{30}$	$\frac{1}{42}$	$-\frac{1}{30}$	$\frac{5}{66}$	$-\frac{691}{2730}$	$\frac{-7}{6}$	...	$-\frac{37.208360028141}{510}$

↳ vient de ce que $B(t) - B(-t) = -t$ (exercice).

[J.B $\rightsquigarrow B_{10}, S_{10}$, Euler $\rightsquigarrow B_{30}$ ≃, maintenant jusqu'à B_{107} ~ machine

Théorème (J.B) $S_k(n) = \sum_{i=1}^{k+1} \frac{\binom{k}{i-1}}{i} B_{k+1-i} n^i = B_k n + \frac{k}{2} B_{k-1} n^2 + \cdots + \frac{n^{k+1}}{k+1}$

preuve: $\sum_{k\geq 0} \frac{S_k(n)}{k!} t^k = 1 + e^t + \cdots + e^{(n-1)t} = \frac{e^{nt}-1}{t} \underbrace{\frac{t}{e^t-1}}_{B(t)}$ ∎

$S_0(n) = 1$ $\forall n \geq 1$

Exemple: $S_k(1) = 0 \Rightarrow$ formule pour les B_k récurrence, remplir la table

$B_1 + \frac{1}{2} = 0$, $B_2 + \underbrace{B_1}_{-\frac{1}{6}} + \frac{1}{3} = 0$, $B_4 + 2B_3 + 2B_2 + B_1 + \frac{1}{5} = 0 \Rightarrow B_4 = -\frac{1}{30}$ etc...

Bernoulli

Euler (milieu 18e) $k \geq 2$ pair, $\zeta(k) = (-1)^{\frac{k}{2}+1} \frac{(2\pi)^k}{2 \cdot k!} B_k$ $\rightsquigarrow$ lien entre B_k arithmétique (se prouve plus rapidement avec Kummer)

$\zeta(s) = 1 + \frac{1}{2^s} + \cdots + \frac{1}{n^s} + \cdots$

Une conséquence: $\text{signe}(B_k) = (-1)^{1+\frac{k}{2}}$, $|B_k| \underset{k\to\infty}{\sim} 2\frac{k!}{(2\pi)^k} \to \infty$

suite $\rightsquigarrow$ (19e) Etude plus détaillée des B_k : décomp en facteurs premiers, num, dén, congruences.

théorème (Clausen, Von-Staudt) $\forall k \geq 2$ pair, $B_k + \sum_{p-1 \mid k} \frac{1}{p} \in \mathbb{Z}$ (la somme porte sur des p premiers)

Cela explique les dénominateurs : $30 = 2 \cdot 3 \cdot 5$, $42 = 7 \cdot 3 \cdot 2$, car $B_8 + \frac{1}{2} + \frac{1}{3} + \frac{1}{5} = 1$

(6 tjs dénom. pas de facteur carré)

On verra une preuve plus loin. Les numérateurs sont plus difficiles à expliquer certains s'expliquent facilement, ou par congruences (cf plus loin), d'autres non ~ premiers irréguliers

Définition (Kummer) Si p ne divise aucun de $B_2, B_4, \dots, B_{p-3}$ on dit que p est régulier

Ex: $\forall p < 37$ régulier, $37 \mid B_{32}$ irrégulier, ainsi que 691, 2083, 600211, ...
on sait que $\exists \infty$ d'irréguliers (élémentaire), question $\exists \infty$ de réguliers?

thm Kummer Si p régulier, $x^p + y^p = z^p$ n'a pas de sol non triviale dans $\mathbb{Z}$
(le groupe des classes d'idéaux de $\mathbb{Q}(\mu_p)$ est d'ordre premier à p)

II Digression nombres p-adiques

Fixons pour l'instant $p \geq 2$ un entier (2 "binaire", 10 "décimal", premier "p-adiques")
Si $x \in \mathbb{N}$, il a une décomposition en base p $x = a_k p^k + \dots + a_1 p + a_0$, $0 \leq a_i \leq p-1$
$= \overline{a_k \dots a_1 a_0}$
On veut considérer de telles expressions mais <u>à gauche</u> $= \overline{\dots a_2 a_1 a_0}$

$\mathbb{Z}_p := \{0, 1, \dots, p-1\}^{\mathbb{N}} = \{\overline{\dots a_2 a_1 a_0}, a_i \in \{0, \dots, p-1\}\}$, muni d'une addition $+$, multi $\times$ (avec retenues) ex $\overline{\dots}$
il contient $\mathbb{N}$ ($a_k = 0$ $k \gg 0$)

[On a pour tout $n \geq 1$ une projection $\mathbb{Z}_p \twoheadrightarrow \mathbb{Z}/p^n\mathbb{Z}$, $\overline{\dots a_2 a_1 a_0} \longmapsto a_0 + a_1 p + \dots + p^{n-1} a_{n-1}$
ce qui suggère une autre déf équivalente : $\mathbb{Z}_p = \{(x_n)_{n \geq 1}, x_n \in \mathbb{Z}/p^n\mathbb{Z}, x_{n+1} \equiv x_n \ (p^n)\}$
(ss anneau de $\prod_{n \geq 1} \mathbb{Z}/p^n\mathbb{Z}$)

ex: $x = \overline{\dots 3219910}$, $x_1 = 0$, $x_2 = 10$, $x_3 = 910$, ...
($p=10$)
• $\mathbb{Z}_p$ stable par $-$ (c'est anneau), e.g. $-1 = \overline{999999}$, il est gros ($\sim \mathbb{R}$)
des entiers deviennent inversibles : $-\frac{1}{3} = \overline{\dots 33333}$, $\frac{1}{3} = \overline{\dots 6666667}$ ($p=10$)
• Si p premier, $\mathbb{Z}_p$ intègre et x inversible ssi $x_1 \neq 0$ dans $\mathbb{Z}/p\mathbb{Z}$
par contre $\mathbb{Z}_{10} \simeq \mathbb{Z}_2 \times \mathbb{Z}_5$

De même, on définit $\mathbb{Q}_p$ = suites $\overline{\dots a_2 a_1 a_0, a_{-1} a_{-2} \dots a_{-k}}$ infini à gauche, fini à droite
il contient $\mathbb{Z}_p$ et en fait $\mathbb{Q}_p = \bigcup_{n \geq 0} \frac{1}{p^n}\mathbb{Z}_p$, $\frac{1}{p^n} = \overline{\dots 0, \underbrace{0001}_{n}}$
et $\mathbb{Q}$

Il y a une distance naturelle (ultrametrique non archimédienne) sur $\mathbb{Q}_p$
On pose $v_p(x) = \sup\{i \mid x \text{ finit par } i \text{ zéros}\} \in \mathbb{Z}$: $v_p(\overline{7417000}) = 3$, $v_p(\overline{334,038}) = -2$
$x \in \mathbb{Q}_p$
puis $d(x,y) = \frac{1}{2^{v_p(x-y)}} = |x-y|_p$ (ex $|x|_p \leq 1 \Leftrightarrow x \in \mathbb{Z}_p$)
Typiquement, $p^n \xrightarrow[n \to \infty]{} 0$ dans $\mathbb{Q}_p$, une série converge ssi son tg tend vers 0 ! $\frac{1}{1-p} = \overline{\dots 1111.1}$

Prop $\mathbb{Q}_p$ est un espace métrique complet dans lequel $\mathbb{Q}$ est dense (c'est un cps si p premier)

$\mathbb{Z}_p \subset \mathbb{Q}_p$ sous espace compact dans lequel $\mathbb{N}$ est dense !

III La preuve de Witt du théorème C,V-S

Fixons $k \geq 2$ pair et B_k. Il faut montrer que $\begin{cases} B_k \in \mathbb{Z}_p \text{ ssi } p-1 \nmid k \\ B_k + \frac{1}{p} \in \mathbb{Z}_p \text{ sinon} \end{cases}$

p premier, $\mathbb{Q} \subset \mathbb{Q}_p$

idée formule de Bernoulli $n \to 0$ dans $\mathbb{Z}_p$! $\quad \frac{S_k(n)}{n} \xrightarrow[n \to 0]{} B_k \quad$ (ex. $n = p^{m}$, $m \to \infty$)

Regardons alors (dans $\mathbb{Z}$) $m \geq 0$: $\quad S_k(p^{m+1}) = \sum_{0 \leq j \leq p^{m+1}-1} j^k = \sum_{u=0}^{p-1} \sum_{v=0}^{p^m-1} \underbrace{(p^m u + v)}^{k}$

$$\equiv v^k + k p^m u v^{k-1} \quad (p^{m+1})$$

comme $k \sum_{u=0}^{p-1} u = k \frac{p(p-1)}{2} \equiv 0 \ (p)$, il vient $\boxed{S_k(p^{m+1}) \equiv p\, S_k(p^m) \ (p^{m+1})}$

donc $\quad \frac{S_k(p^{m+1})}{p^{m+1}} - \frac{S_k(p^m)}{p^m} \in \mathbb{Z}$ puis $\cdots$ $\frac{S_k(p^m)}{p^m} - \frac{S_k(p)}{p} \in \mathbb{Z} \quad \forall m \geq 1$

Mais $\quad S_k(p) = \sum_{j=0}^{p-1} j^k \equiv \sum_{x \in (\mathbb{Z}/p\mathbb{Z})^\times} x^k = \begin{cases} -1 & \text{si } p-1 \mid k \\ 0 & \text{sinon} \end{cases} \quad (p)$

donc $\quad \frac{S_k(p^m)}{p^m} \in \begin{cases} \mathbb{Z}_p & \text{si } p-1 \nmid k \\ -\frac{1}{p} + \mathbb{Z}_p & \text{sinon} \end{cases}$, on conclut par $m \to \infty$ ∎

Thm / Ex $k \equiv 0 \ (p-1)$, $\frac{B_k}{k} \in \mathbb{Z}_p$: Cela explique $\operatorname{num}(B_{10})$, $\operatorname{num}(B_{14})$

IV La fonction ζ p-adique

Le résultat d'Euler + eq. fonctionnelle ζ s'écrit aussi $\zeta(1-k) = -\frac{B_k}{k} \in \mathbb{Q}$, $k \geq 2$

$\left(\Gamma\left(\frac{s}{2}\right) \pi^{-\frac{s}{2}} \zeta(s)\right)$

Fixons p et définissons $\zeta^{(p)}(k) := -(1-p^{k-1}) \frac{B_k}{k}$ pour $k \geq 2$ pair (on a enlevé le p-facteur eulerien de ζ)

Par CVS (cf. Ex) $\quad \zeta^{(p)}(k) \in \mathbb{Z}_p$ si $k \neq 0 \ (p-1)$

Théorème (Kummer)

Si $k \equiv k' \ (p-1)p^N$, alors $\zeta^{(p)}(k) \equiv \zeta^{(p)}(k') \ (p^N)$

et $k \not\equiv 0 \ (p-1)$

Ex: En particulier $\frac{B_k}{k} \equiv \frac{B_{k'}}{k'}$ si $k \equiv k' \ (p-1)$, cela justifie la déf de p régulier.

ex: $p=5$ $\quad \frac{B_2}{2} - \frac{B_6}{6} = \frac{5}{63} \equiv 0 \ (5)$ (de plus $\frac{B_{10}}{10} \equiv \frac{B_6}{6} \ (5) \Rightarrow 5 \mid B_{10}$ (cf avec $\frac{B_{10}}{10} \in \mathbb{Z}_5$))

Une preuve assez naturelle a été donnée par Mazur utilisant les mesures p-adiques.
Une preuve directe est assez facile à faire (cf I. Gessen, congruences de Voronoï. Apparemment Kummer $N=0$)

Application Pour $i = 2, 4, \dots, p-3$ regardons

$$\zeta_{p,i} : \mathbb{N} \longrightarrow \mathbb{Z}_p$$
$$n \longmapsto \zeta^{(p)}(i + n(p-1))$$

Alors $\quad |\zeta_{p,i}(n) - \zeta_{p,i}(n')|_p \leq |n-n'|_p$ par le théorème

comme $\mathbb{N}$ dense dans $\mathbb{Z}_p \rightsquigarrow$ $\zeta_{p,i}$ s'étend par continuité en une fonction

$$\mathbb{Z}_p \longrightarrow \mathbb{Z}_p \quad (\zeta_p\text{-adique d'indice } i)$$

Il y a plein de résultats/conjectures sur ces fonctions, notamment sur les zéros.

Ex: p régulier $\Rightarrow$ $\zeta_{p,i}$ ne s'annule pas (car $\zeta_{p,i}(x) \neq 0 \ (p!)$ $\forall x \in \mathbb{Z}_p$)

Par contre $\zeta_{37,32}$ s'annule !

Conjecture $\forall n \in \mathbb{Z}$, $\zeta_{p,i}(n) \neq 0$
$\forall i, p$

Pas connue en général pour $n=-1$, on conjecture même l'irrationalité si $n<0$