

Des nombres de Bernoulli à la fonction zêta p-adique

1. Définition et premières propriétés

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

$$k \geq 1, \quad S_k(m) = 1^k + 2^k + \dots + (m-1)^k \quad \text{pt (Jacques Bernoulli) exprimer } S_k(m) \text{ pol en } m \text{ d' } k+1$$

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

Table

	k=	2	4	6	8	10	12	14	...	32
$B_0=1, B_1=-\frac{1}{2}$ $B_{2m+1}=0 \ m \neq 0$	$B_k =$	$\frac{1}{6}$	$-\frac{1}{30}$	$\frac{1}{42}$	$-\frac{1}{30}$	$\frac{5}{66}$	$-\frac{691}{2730}$	$-\frac{7}{6}$...	$\frac{37.208360028141}{510}$

↳ vient de ce que $B(t) - B(-t) = -t$ (exercice).
 [J.B. $\rightsquigarrow B_{10}, S_{10}$, Euler $\rightsquigarrow B_{30}$, maintenant jusqu'à $B_{107} \sim$ machine]

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

preuve: $\sum_{k \geq 0} \frac{S_k(m)}{k!} t^k = 1 + e^t + \dots + e^{(m-1)t} = \frac{e^{mt} - 1}{t} \frac{B(t)}{e^t - 1}$ ▀

Exemple: $S_k(1) = 0 \Rightarrow$ formule pour les B_k récurrence, remplir la table.
 $B_1 + \frac{1}{2} = 0, \quad B_2 + \frac{B_1 + \frac{1}{3}}{-\frac{1}{6}} = 0, \quad B_4 + 2B_3 + 2B_2 + B_1 + \frac{1}{5} = 0 \Rightarrow B_4 = -\frac{1}{30}$ etc...

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

Une conséquence: signe $(B_k) = (-1)^{1+\frac{k}{2}}$, $|B_k| \sim \frac{2 \cdot k!}{(2\pi)^k} \rightarrow \infty$ (la somme partant sur des p premiers)

suite (19^e) Etude plus détaillée des B_k : décomp. en facteurs premiers, num, dénom, congruences.

Théorème $\forall k \geq 2$ pair, $B_k + \sum_{p|k} \frac{1}{p} \in \mathbb{Z}$ (la somme partant sur des p premiers)
 (Claisen, Von-Staudt)
 Cela explique les dénominateurs : $30 = 2 \cdot 3 \cdot 5, \quad 42 = 7 \cdot 3 \cdot 2$, ex $B_8 + \frac{1}{2} + \frac{1}{3} + \frac{1}{5} = 1$
 (6 too denom. pas de facteur carré)

On verra une preuve plus loin. Les numérateurs sont plus difficiles à expliquer certains s'expliquent ^{supplément, ou} par congruences (cf plus loin), d'autres non ~ premières inégales

Définition (Kummer) Si $p \nmid$ num 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, 208360029141
on sait que 3 cas d'irrégularité (élémentaire), question 300 de régularité?

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

II. Digressions nombres p -adiques

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

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

On a pour tout $n \geq 1$ une projection $\mathbb{Z}_p \rightarrow \mathbb{Z}/p^n \mathbb{Z}, x \mapsto a_0 + a_1 p + \dots + p a_{n-1}$
(ce qui suggère une autre déf équivalente: $\mathbb{Z}_p = \varprojlim_{n \geq 1} \mathbb{Z}/p^n \mathbb{Z}, x_n \in \mathbb{Z}/p^n \mathbb{Z}, x_{n+1} \equiv x_n \pmod{p^n}$)
(= anneau de $\prod_{n \geq 1} \mathbb{Z}/p^n \mathbb{Z}$)

ex: $x = \dots 32109910, x_1=0, x_2=10, x_3=910, \dots$

($p=10$) \mathbb{Z}_p stable par $-$ (c'est anneau), e.g. $-1 = \dots 999999$, il est gros ($\sim \mathbb{R}$)
des entiers deviennent inversibles: $-\frac{1}{3} = \dots 33333, \frac{1}{3} = \dots 66666667$ ($p=10$)

Si p premier, \mathbb{Z}_p intègre et x inversible ssi $x_1 \neq 0$ dans $\mathbb{Z}/p \mathbb{Z}$
par contre $\mathbb{Z}_{10} \cong \mathbb{Z}_2 \times \mathbb{Z}_5$

De même, on définit $\mathbb{Q}_p =$ suites $\dots a_2 a_1 a_0$ infus à gauche, fini à droite
il contient \mathbb{Z}_p et en fait $\mathbb{Q}_p = \bigcup_{m \geq 0} \frac{\mathbb{Z}_p}{p^m}, \frac{1}{p^m} = \dots 0, \overline{0001}^m$

Il y a une distance naturelle (non archimédienne) sur \mathbb{Q}_p
ultramétrique

On pose $v_p(x) = \max \{ i \mid x \text{ fait par } i \text{ zéros} \} \in \mathbb{Z}: v_p(\overline{7917000}) = 3, v_p(\overline{334,08}) = -2$
 $x \in \mathbb{Q}_p$

puis $d(x, y) = \frac{1}{2^{v_p(x-y)}} = |x-y|_p$ (car $|x|_p \leq 1 \Leftrightarrow x \in \mathbb{Z}_p$)
Uniquement, $\frac{1}{p^m} \xrightarrow{m \rightarrow \infty} 0$ dans \mathbb{Q}_p , une série converge si on lg. tend vers 0! $\frac{1}{1-p} = \overline{0,111111}$

Prop: \mathbb{Q}_p est un espace métrique complet dans lequel \mathbb{Q} est dense (c'est un ops v 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 p premier. Il faut montrer que $B_k \in \mathbb{Z}_p$ si $p-1 \nmid k$
 $\mathbb{Q} \subset \mathbb{Q}_p$ $B_k + \frac{1}{p} \in \mathbb{Z}_p$ sinon.

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

Regardons alors $S_k(p^{m+1}) = \sum_{0 \leq j \leq p^{m+1}-1} j^k = \sum_{u=0}^{p-1} \sum_{v=0}^{p^m-1} (p^m u + v)^k$
 $\equiv v^k + k p^m u v^{k-1} \binom{m}{1} \pmod{p^2}$

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

$$S_k(p^{m+1}) \equiv p S_k(p^m) \pmod{p^2}$$

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

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

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

Thm' / Ex $k \not\equiv 0 \pmod{p-1}$, $\frac{B_k}{k} \in \mathbb{Z}_p$: cela explique num(B₀), num(B₄)

IV. La fonction ζ_p -adique

Le résultat d'Euler + eq fonctionnelle ζ_p s'écart aussi $\zeta_p(1-k) = -\frac{B_k}{k} \in \mathbb{Q}$
 $(\Gamma(\frac{s}{2}))^{-1} \zeta_p(s)$ $k \geq 2$

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

Par cvs (cf. Ex) $\zeta_p^{(k)} \in \mathbb{Z}_p$ si $k \neq 0 \pmod{p-1}$

Théorème (Kummer)

Si $k \equiv k' \pmod{(p-1)p^N}$, alors $\sum^{(p)} (k) \equiv \sum^{(p)} (k') \pmod{p^N}$
et $k \not\equiv 0 \pmod{p-1}$

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

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

Une preuve assez naturelle a été donnée par Meiss en utilisant les mesures p -adiques.

Une preuve directe est assez fastidieuse (cf I. Rosen, congruences de Von Staudt. Apparemment Kummer $N=0$)

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

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

Alors $|\sum_{p,i}(m) - \sum_{p,i}(m')|_p \leq |m - m'|_p$ par le théorème

comme \mathbb{N} dense dans $\mathbb{Z}_p \rightsquigarrow \sum_{p,i}$ s'étend par continuité en une fonction
 $\mathbb{Z}_p \longrightarrow \mathbb{Z}_p$ ($\sum_{p,i}$ p -adique d'indice i)

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

Ex p régulier $\Rightarrow \sum_{p,i}$ ne s'annule pas (car $\sum_{p,i}(x) \not\equiv 0 \pmod{p!}$)
 $\forall x \in \mathbb{Z}_p$

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

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

Pas connu en général pour $m = -1$, on conjecture \tilde{m} d'arithmétique si $n < 0$