N° d'ordre : 01/2012 – $M/M.T$

REPUBLIQUE ALGÉRIENNE DEMOCRATIQUE ET POPULAIRE
MINISTÈRE DE L'ENSEIGNEMENT SUPÉRIEUR ET DE LA RECHERCHE SCIENTIFIQUE

UNIVERSITÉ DES SCIENCES ET DE LA TECHNOLOGIE
HOUARI BOUMEDIENNE-ALGER
FACULTÉ DE MATHÉMATIQUES

MÉMOIRE

Présenté pour l'obtention du diplôme de MAGISTER

En MATHEMATIQUES

Spécialité : Algèbre et Théorie des Nombres.

Par

Rédha CHELLAL

Sujet :

Autour De Certaines Propriétés Arithmétiques des Nombres De Bernoulli

Soutenu publiquement le 23/09/2012 devant le jury composé de :

M. BENSEBAA Boualem	Maître de Conférences A á	L'USTHB	Président
M. BENCHERIF Farid	Maître de Conférences A á	L'USTHB	Directeur de mémoire
Mme. CHERCHEM Leila	Maître de Conférences A á	L'USTHB	Examinatrice
M. DERBAL Abdallah	Maître de Conférences A á	L'ENS Kouba	Examinateur

Remerciements

Je suis heureux de pouvoir exprimer toute ma reconnaissance à mon Professeur et Directeur de mémoire, Monsieur Farid BENCHERIF, pour m'avoir proposé un sujet de recherche captivant et pour avoir patiemment dirigé mes recherches durant toute une année. Sa disponibilité, sa précieuse aide scientifique, ses encouragements et son soutien moral sans réserve ont énormément contribué à l'aboutissement de ce travail.

J'apprécie au plus haut point l'honneur que me fait mon Professeur, Monsieur Boualem BENSEBAA en acceptant de présider le Jury de ma soutenance.

Je remercie infiniment les Professeurs Madame Leïla CHERCHEM et Monsieur Abdallah DERBAL pour s'être intéressé à ce travail et pour l'honneur qu'ils me font en acceptant de faire partie du Jury de soutenance.

Je remercie aussi les Professeurs Monsieur Abdelhafid BERRACHEDI, Monsieur Rachid BOUMAHDI, Monsieur Tarek GARICI, Monsieur Abdelmoumène ZEKIRI et Madame Schéhérazade ZERROUKHAT pour leur aide scientifique et leurs encouragements.

Je remercie particulièrement le laboratoire LA3C (Laboratoire Arithmétique, codage, combinatoire et calcul formel) pour les moyens mis à ma disposition pour mener à bien cette recherche.

Je remercie aussi tous mes amis et tous ceux et celles qui m'ont soutenu de près ou de loin dans la préparation de ce mémoire et que je n'ai pas pu citer nommément ici, mais envers qui, ma reconnaissance est immense.

Dédicaces

Je dédie ce mémoire de Magister - à ma mère, espérant avoir réalisé l'un de ses vœux les plus chères, celui de voir l'un de ses fils accéder à un grade important couronnant des études avancées. Ses encouragements constants, malgré sa maladie, m'ont aidé à persévérer et m'ont été d'une aide morale très précieuse. C'est vraiment à elle que je dois ma réussite dans les études. J'espère de tout cœur qu'elle en sera fière et je prie Dieu aussi de lui apporter la guérison et de la soulager, - à mon père qui m'a toujours aidé chaque fois que je l'ai sollicité et qui a constamment été à mes côtés dans les moments difficiles, - à ma sœur Nassima et à son mari Taher, - à ma sœur Nawel et à son mari Sifeddine, - à ma petite sœur Asma qui m'a souvent réconforté, - à mes frères Samir et Khireddine en priant Dieu de les aider à toujours persévérer dans la vie pour se surpasser, - à mes neveux adorables Ahmed, Abdo, Anis et Abdallah, - à ma petite nièce Marwa, belle et adorable, - à ma grand-mère Khadouja, - à ma grand-mère Baya, - à mon grand père Rézki, - à la mémoire de Mohammed, mon grand père, - à toute ma grande famille, - à mes collègues de travail, - à mes fidèles amis, - à tous ceux qui aiment Rédha, - à tous ceux que Rédha aime !

Notations

$\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ *et* $\mathbb{C}$ *désignent respectivement les ensembles des entiers naturels, des entiers relatifs,des rationnels, des réels et des complexes*

$\mathcal{P}$ *ensemble des nombres premiers*

p *: un nombre premier sauf mention contraire*

D_n *ensemble des diviseurs de l'entier* $n = \{d \in \mathbb{N}^* / d \quad divise \quad n\}$

$|x|$ *valeur absolue du nombre réel* x

$\lfloor x \rfloor$ *ou* $[x]$ *partie entière inférieure du nombre réel* x

$denom(x)$ *:dénominateur du nombre rationnel* x

$num(x)$ *: numérateur du nombre rationnel* x

$H_n = 1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n}$ *: n-ième nombre harmonique*

$H_n^{(r)} = 1 + \frac{1}{2^r} + \frac{1}{3^r} + \cdots + \frac{1}{n^r}$ *: n-ième nombre harmonique d'ordre r.*

$q_p(a)$ *quotient de Fermat définie pour p premier et pour* $a \in \mathbb{Z} - p\mathbb{Z}$
par : $q_p(a) = \frac{a^{p-1}-1}{p}$

w_p *quotient de Wilson définie pour* $p \in \mathbb{Z}$
par $w_p = \frac{(p-1)!+1}{p}$

$\binom{n}{k}$ *coefficient binomial*

$\begin{bmatrix} n \\ k \end{bmatrix}$ *nombre de Stirling de première espèce non signé*

$s(n,k)$ *nombre de Stirling de première espèce signé* $s(n,k) = (-1)^{n-k} \begin{bmatrix} n \\ k \end{bmatrix}$

$\begin{Bmatrix} n \\ k \end{Bmatrix}$ *nombre de Striling de seconde espèce*

B_n *n-ième nombre de Bernoulli*

$B_n(x)$ *n-ième polynôme de Bernoulli*

φ *fonction indicatrice d'Euler*

$[P]$ *symbole d'Iverson valant* 1 *ou* 0 *selon que l'énoncé* P *est vrai ou faux.*

$a \mid b$ *: a divise b*

$\delta_{j,k}$ *: Symbole de Kronecker.* $(\delta_{j,k} = [i = j]$

$\mathbb{Z}_{(n)} = \{x \in \mathbb{Q} / (denom(x), n) = 1\}$ *: sous anneau de* $\mathbb{Q}$.

$\mathbb{Z}_{(p)}$ *anneau des p-entiers. (p premier).*

$S(n,k) = \begin{Bmatrix} n \\ k \end{Bmatrix}$ *autre notation des nombres de Stirling de seconde espèce.*

Table des matières

Introduction

Ce mémoire est consacré à l'étude de certaines propriétés arithmétiques des nombres et polynômes de Bernoulli et à des applications de ces propriétés à l'étude de certaines congruences. Nous nous intéressons plus particulièrement à l'étude de congruences concernant des sommes finies de rationnels comportant des nombres harmoniques. Nous détaillons la preuve récente donnée par Zhi-Wei Sun en 2012 (théorème 1.1, page 416 de [37]) des congruences suivantes :

$$\sum_{k=1}^{p-1} \frac{H_k}{k2^k} \equiv 0 \pmod{p},$$

$$\sum_{k=1}^{p-1} k^2 H_k^2 \equiv -\frac{4}{9} \pmod{p}$$

$$\sum_{k=1}^{p-1} H_k^3 \equiv 6 \pmod{p},$$

$$\sum_{k=1}^{p-1} H_k^2 \equiv 2p - 2 (\mathrm{mod} p^2),$$

$$\sum_{k=1}^{p-1} \frac{H_k^2}{k^2} \equiv 0 \pmod{p}, \quad \textit{pour } p > 5.$$

La compréhension de la preuve de Zhi-Wei Sun a nécessité l'étude de nombreux théorèmes d'arithmétique et de théorèmes concernant plus spécifiquement les nombres et les polynômes de Bernoulli, en autres, le théorème de Von-Staudt et Clausen et un théorème de Kummer concernant des congruences pour les nombres de Bernoulli.

Ce mémoire comporte quatre chapitres que nous allons détailler succintement.

Dans le premier chapitre, nous rappelons de nombreuses définitions et propriétés des coefficients binomiaux, des nombres de Stirling de première et seconde espèce, des nombres harmoniques et des nombres harmoniques généralisés. Nous précisons les notations adoptées ainsi que la similarité de propriétés entre les nombres de Stirling et les coefficients binomiaux. Nous précisons aussi la notion de p-entier et la définition d'une congruence dans l'anneau des p-entiers $\mathbb{Z}_{(p)}$.

Dans le second chapitre, nous nous intéressons à l'étude de la sommation des puissances numériques. Plus précisément, il s'agit de l'étude des sommes de puissances

$$S_m(n) = 1^m + 2^m + \cdots + n^m$$

où n et m sont deux entiers ≥ 1. Il s'agit d'un problème qui a préoccupé des générations de mathématiciens depuis l'antiquité et qui est encore et toujours une source de problèmes, de conjectures et de défis pour le mathématicien. La simple recherche d'une formule générale exprimant $S_m(n)$ en fonction de n et m a retenu l'attention de plusieurs générations de mathématiciens, durant de nombreux siècles. L'aboutissement final et quelque peu satisfaisant de cette recherche a été la découverte par J. Bernoulli de la formule suivante

$$S_m(n) = \frac{1}{m+1}n^{m+1} + \frac{1}{2}n^m + \frac{1}{m+1}\sum_{k=1}^{\left[\frac{m}{2}\right]} \binom{m+1}{2k} B_{2k} n^{m+1-2k}.$$

Dans cette formule, $(B_n)_{n\in\mathbb{N}}$ est une suite de rationnels (appelés nombres de Bernoulli) définie par la relation de récurrence suivante

$$B_0 = 0 \quad et \quad B_n = -\frac{1}{n+1}\sum_{k=0}^{n-1} \binom{n+1}{k} B_k \quad pour\ n \geq 1.$$

La suite de polynômes $(B_n(x))_{n\in\mathbb{N}}$ définie par

$$B_n(x) = \sum_{k=0}^{n} \binom{n}{k} B_{n-k} x^k \ pour\ n \geq 0,$$

est appelée suite de polynômes de Bernoulli. Dans ce chapitre, nous énonçons et prouvons de nombreuses propriétés des nombres et polynômes de Bernoulli. Nous terminons ce chapitre en prouvant la formule explicite précédente exprimant $S_m(n)$. Grâce à D. Knuth qui a réhabilité le mathématicien allemand Johann Faulhaber (1580−1635), cette formule est aujourd'hui connue sous le nom de formule de Faulhaber en hommage à ce mathématicien qui bien avant Jacques Bernoulli avait réussi à exprimer $S_m(n)$ pour $1 \leq m \leq 17$.

Le troisième chapitre de ce mémoire est consacrée à une étude détaillée du théorème de Von Staudt et Clausen. Ce théorème affirme que pour tout entier $n \geq 1$, le $(2n)$-ième nombre de Bernoulli vérifie la remarquable propriété suivante

$$B_{2n} + \sum_{(p-1)|2n} \frac{1}{p} \in \mathbb{Z}$$

La sommation étant étendue à l'ensemble des nombres premiers p tels que $p-1$ soit un diviseur de l'entier $2n$.

Nous donnons deux preuves de cet important théorème en théorie des nombres. L'une est une démonstration par récurrence qui utilise certaines propriétes des p-entiers, l'autre est une démonstration directe qui exploite seulement certaines conguences pour les nombres de Stirling de deuxième espèce ainsi que la formule explicite suivante exprimant B_n en fonction de n :

$$B_n = \sum_{k=0}^{n} (-1)^k \frac{k!}{k+1} \left\{ n \atop k \right\},$$

où $\left\{ n \atop k \right\}$ *est un nombre de Stirling de deuxième espèce qui lui même s'exprime explicitement :*

$$\left\{ n \atop k \right\} = \frac{1}{k!} \sum_{j=0}^{k} \binom{k}{j} (-1)^{k-j} j^n.$$

Dans ce chapitre, nous examinons aussi un théorème datant de 1851*, dû à Kummer. Ce théorème affirme que si* p *est un nombre premier, si* n *et* m *sont deux entiers tels que* $n \equiv m \mod (p-1)$ *et si de plus* $p-1$ *ne divise pas* n*, alors on a la congruence suivante dans l'anneau des* p*-entiers :*

$$\frac{B_n}{n} \equiv \frac{B_m}{m} \pmod{p}.$$

Enfin au quatrième et dernier chapitre de ce mémoire, nous étudions de nombreuses applications des théorèmes précédents pour prouver certaines congruences. Plus précisément, ce chapitre est entièrement consacré à une étude détaillée de la preuve des congruences établies par Zhi-Wei Sun en 2012 *et rappelées au début de cette introduction. Nous nous intéressons plus particulièrement à la congruence*

$$\sum_{k=1}^{p-1} \frac{H_k}{k2^k} \equiv 0 \pmod{p}.$$

Chapitre 1

Nombres de Stirling et nombres harmoniques

Dans ce chapitre, nous rappelons les définitions et certaines propriétés des coefficients binomiaux, des nombres de Stirling de première et seconde espèce, des nombres harmoniques et des nombres harmoniques généralisés. Nous rappelons aussi la définition d'un p-entier et nous étudions certaines propriétés des congruences définies dans l'anneau $\mathbb{Z}_{(p)}$.
Dans tout ce qui suit, nous désignons $\mathbb{K}$ *l'un des trois corps* $\mathbb{Q}$, $\mathbb{R}$ *ou* $\mathbb{C}$ *et par* A *un anneau. De plus, on adopte la convention qu'un produit vide vaut* 1 *et qu'une somme vide vaut* 0.

1.1 Puissances factorielles descendantes et puissances factorielles montantes :

Soit $a \in A$. *Pour tout entier naturel* n, *on définit les éléments* $a^{\underline{n}}$ *et* $a^{\overline{n}}$ *de* A *par les relations :*

$$a^{\underline{n}} = \prod_{j=0}^{n-1}(a-j) \quad et \quad a^{\overline{n}} = \prod_{j=0}^{n-1}(a+j)$$

Ainsi, on a

$$\begin{cases} a^{\underline{0}} = a^{\overline{0}} = 1, \\ a^{\underline{1}} = a^{\overline{1}} = a, \\ a^{\underline{2}} = a(a-1) \quad et \quad a^{\overline{2}} = a(a+1) \end{cases}$$

Plus généralement, pour tout entier $n \geq 1$, *on a :*

$$a^{\underline{n}} = a(a-1)...(a-n+1) \quad et \quad a^{\overline{n}} = a(a+1)...(a+n-1)$$

La quantité $a^{\underline{n}}$ *est appelée "a puissance n descendante" tandis que* $a^{\overline{n}}$ *est appelée "a puissance n montante".* $a^{\underline{n}}$ *et* $a^{\overline{n}}$ *sont aussi appelées les puissances factorielles descendantes et montantes de a respectivement.*

Remarquons que dans le cas où $A = \mathbb{K}[x]$, on a pour tout entier $n \geq 0$:

$$deg x^{\underline{n}} = deg x^{\overline{n}} = n.$$

Il en résulte que $(x^{\underline{n}})_{n\in\mathbb{N}}$ et $(x^{\overline{n}})_{n\in\mathbb{N}}$ sont des bases du $\mathbb{K}$-espace vectoriel $\mathbb{K}[x]$.

1.2 Coefficients binomiaux :

1.2.1 Définition et premières propriétés

Pour tout entier naturel n et pour tout polynôme $P(x)$ de $A[x]$, la notation $[x^n](P(x))$ désigne le coefficient de x^n dans le polynôme $P(x)$.

Ainsi si

$$P(x) = \sum_{m\geq 0} a_m x^m,$$

on a alors :

$$[x^n](P(x)) = a_n.$$

Avec cette notation, on définit le coefficient binomial $\binom{n}{k}$, où n et k sont deux entiers naturels par :

$$\binom{n}{k} = [x^k]((x+1)^n). \tag{1.1}$$

Autrement dit, on a

$$(x+1)^n = \sum_{k\geq 0} \binom{n}{k} x^k. \tag{1.2}$$

Les coefficients binomiaux vérifient les propriétés données dans le théorème suivant :

Théorème 1.1. *Pour tous entiers naturels n et k :*

1) on a

$$\binom{n}{0} = \binom{n}{n} = 1 \quad pour \quad n \geq 0 \quad et \quad \binom{0}{k} = 1 \tag{1.3}$$

2) pour $k > n$, on a

$$\binom{n}{k} = 0. \tag{1.4}$$

3) Pour $n \geq 1$ et $k \geq 1$, on a

$$\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k} \tag{1.5}$$

1.2. Coefficients binomiaux :

4) Pour $0 \leq k \leq n$, *on a*

$$\binom{n}{k} = \binom{n}{n-k} \tag{1.6}$$

5) on a

$$\binom{n}{k} = \frac{n(n-1)...(n-k+1)}{k!} = \frac{n^{\underline{k}}}{k!} \tag{1.7}$$

6) Pour $n \geq k$, *on a*

$$\binom{n}{k} = \frac{n!}{k!(n-k)!} \tag{1.8}$$

Démonstration. 1) On a :

$$\binom{n}{0} = [x^0](x+1)^n = 1 \quad \text{et} \quad \binom{n}{n} = [x^n](x+1)^n = 1. \quad \square$$

2)

$$\binom{n}{k} = [x^k](x+1)^n = 0 \quad \text{pour} \quad k \geq n.$$

3) Pour tout entier $n \geq 1$ et $k \geq 1$, on a

$$\begin{aligned}
\binom{n}{k} &= [x^k](x+1)^n \\
&= [x^k]((x+1)(x+1)^{n-1}) \\
&= [x^k]((x+1)\sum_{k\geq 0}\binom{n-1}{k}x^k) \\
&= [x^k](\sum_{k\geq 1}\binom{n-1}{k}x^{k+1} + \sum_{k\geq 0}\binom{n-1}{k}x^k) \\
&= \binom{n-1}{k-1} + \binom{n-1}{k}. \quad \square
\end{aligned}$$

4) Plaçons nous dans $\mathbb{Q}(x)$, on a

$$(1+\frac{1}{x})^n = \sum_{k=0}^{n}\binom{n}{k}\frac{1}{x^k}$$

On en déduit que :

$$(x+1)^n = \sum_{k=0}^{n}\binom{n}{k}x^{n-k} = \sum_{k=0}^{n}\binom{n}{n-k}x^k$$

Ainsi

$$\binom{n}{k} = [x^k](x+1)^n = \binom{n}{n-k}. \quad \square$$

5) On a

$$\sum_{k=0}^{n} \binom{n}{k} x^k = (x+1)^n$$

En dérivant les deux membres de l'égalité, on obtient :

$$\begin{aligned}
\sum_{k=1}^{n} k\binom{n}{k} x^{k-1} &= n(x+1)^{n-1} \\
&= n\sum_{k=0}^{n} \binom{n-1}{k} x^k \\
&= n\sum_{k=1}^{n} \binom{n-1}{k-1} x^{k-1}
\end{aligned}$$

Par identification des coefficients de x^{k-1} dans chacun des deux membres, on obtient :

$$k\binom{n}{k} = n\binom{n-1}{k-1}$$

Ainsi

$$\begin{aligned}
\binom{n}{k} &= \frac{n}{k}\binom{n-1}{k-1} \\
&= \frac{n}{k}.\frac{n-1}{k-1}...\frac{n-k+1}{1}\binom{n-k}{0} \\
&= \frac{n^{\underline{k}}}{k!}.
\end{aligned}$$

□

On vérifie que cette relation est encore vraie pour $k = 0$ et $n \geq 0$ ainsi que pour $n = 0$ et $k \geq 0$.

1.2.2 Interpétation combinatoire :

On considère $E_n = \{1, 2, ..., n\}$ pour $n \geq 1$ et $E_n = \varnothing$ si $n = 0$,

On a alors pour tout $n \geq 0$ et $k \geq 0$,

$$\binom{n}{k} = Card\{A/ \quad A \subset E_n \quad et \quad CardA = k\}.$$

1.2.3 Formule de binôme :

On suppose que A est un anneau non nécessairement commutatif. On considère deux éléments a et b de A. On suppose que a et b commutent pour le produit de A ($ab=ba$). Alors on a

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k} \tag{1.9}$$

Démonstration. On commence par prouver que a^r et b^s commutent pour tout entier $r \geq 0$ et $s \geq 0$ (i.e $a^r b^s = b^s a^r$). La preuve se fait alors par récurrence sur n.

Remarquons que 1 et -1 commutent pour le produit de A. Car :

$$a.1 = 1.a = a \quad \text{et} \quad a.(-1) = (-1).a = -a$$

On a donc dans tout anneau (commutatif ou non commutatif)

$$(a+1)^n = \sum_{k=0}^{n} \binom{n}{k} a^k \quad \text{et} \quad (a-1)^n = \sum_{k=0}^{n} \binom{n}{k} (-1)^{n-k} a^k.$$

□

1.2.4 Généralisation des coefficients binomiaux

Une généralisation de $\binom{n}{k}$ consiste à remplacer n par un nombre complexe α et à définir $\binom{\alpha}{k}$ en posant $\alpha \in \mathbb{C}$ et $k \in \mathbb{N}$ par :

$$\binom{\alpha}{k} = \frac{\alpha(\alpha-1)...(\alpha-k+1)}{k!}.$$

On a la propriété suivante :

$$\binom{\alpha}{k} = \binom{\alpha-1}{k} + \binom{\alpha-1}{k-1} \quad \textit{pour} \quad \alpha \in \mathbb{C} \quad \textit{et} \quad k \in \mathbb{N}^*.$$

En effet :

$$\binom{\alpha-1}{k} = \frac{(\alpha-1)(\alpha-2)...(\alpha-k)}{k!} = \frac{(\alpha-1)(\alpha-2)...(\alpha-k+1)}{k!}(\alpha-k)$$

et

$$\binom{\alpha-1}{k-1} = \frac{(\alpha-1)(\alpha-2)...(\alpha-k+1)}{(k-1)!} = \frac{k(\alpha-1)(\alpha-2)...(\alpha-k+1)}{k!}$$

d'où

$$\binom{\alpha-1}{k} + \binom{\alpha-1}{k-1} = \frac{\alpha(\alpha-1)(\alpha-2)...(\alpha-k+1)}{k!} = \binom{\alpha}{k}. \quad \square$$

On démontre aussi que l'on a :

$$(1+x)^\alpha = \sum_{k=0}^{\infty} \binom{\alpha}{k} x^k, \quad \textit{pour} \quad \alpha \in \mathbb{R} \quad \textit{et} \quad x \in \mathbb{R}, |x| < 1.$$

1.3 Les endomorphismes $D, \triangle, E, I$ de $\mathbb{K}[x]$

On considère $\mathbb{K}[x]$ comme espace vectoriel sur $\mathbb{K}$. $L(\mathbb{K}[x])$ désigne l'algèbre des endomorphismes du $\mathbb{K}$-espace vectoriel sur $\mathbb{K}$.

Les opérateurs $D, \triangle, E$ et I sont les endomorphismes de $\mathbb{K}[x]$ définies par :

$$\begin{aligned} D(P(x)) &= P'(x) \\ \triangle(P(x)) &= P(x+1) - P(x) \\ E(P(x)) &= P(x+1) \\ I(P(x)) &= P(x) \end{aligned}$$

Avec : $P'(x)$ désignant la dérivée du polynôme $P(x)$ de $\mathbb{K}[x]$.
D est l'opérateur de dérivation, $\triangle$ est de différence finie, E est l'opérateur d'avance et I est l'opérateur identité dans $\mathbb{K}[x]$.

Pour tout opérateur $\Omega \in L(\mathbb{K}[x])$ et pour tout entier naturel n, on pose :

$$\Omega^0 = I \quad et \quad \Omega^n = \Omega \circ \Omega^{n-1}, \quad pour \quad n \geq 1.$$

Autrement dit :

$$\Omega^n = \underbrace{\Omega \circ \Omega \circ ... \circ \Omega}_{n fois} \quad pour \quad n \geq 1.$$

Il est facile de constater que pour tout entier $n \geq 0$, on a

$$E^n(P(x)) = P(x+n)$$

Pour tout entier $n \geq 1$, on sait que l'on a pour $n \geq 1$:

$$\begin{aligned} D(x^n) &= nx^{n-1}. \\ D^k(x^n) &= n(n-1)...(n-k+1)x^{n-k} \quad pour \quad 0 \leq k \leq n. \\ D^k(x^n) &= 0 \quad pour \quad k > n. \end{aligned}$$

On peut aussi écrire que l'on a pour $n \geq 0$ et $k \geq 0$:

$$\frac{D^k(x^n)}{k!} = \binom{n}{k} x^{n-k} \quad et \quad D^n(x^n) = n!.$$

L'opérateur de différence finie $\triangle$ a un comportement analogue à l'opérateur de dérivation quand on l'applique sur un vecteur de la base $(x^{\underline{n}})$ de $\mathbb{K}[x]$. On a alors pour $n \geq 1$:

$$\begin{aligned} \triangle(x^{\underline{n}}) &= nx^{\underline{n-1}}. \\ \triangle^k(x^{\underline{n}}) &= n(n-1)...(n-k+1)x^{\underline{n-k}} \quad pour \quad 0 \leq k \leq n. \\ \triangle^k(x^{\underline{n}}) &= 0 \quad pour \quad k > n. \end{aligned}$$

On peut aussi écrire que l'on a pour $n \geq 0$ et $k \geq 0$:

$$\frac{\triangle^k(x^{\underline{n}})}{k!} = \binom{n}{k} x^{\underline{n-k}} \quad et \quad \triangle^n(x^{\underline{n}}) = n!.$$

On sait aussi que pour tout polynôme $P(x)$ de $\mathbb{K}[x]$, on a la formule suivante appelée "formule de Taylor-Maclaurin" donnée par :

$$P(x) = \sum_{k\geq 0} \frac{D^k P}{k!}(0).x^k$$

On a aussi une formule analogue pour l'opérateur $\triangle$ appelée "formule de Gregory" donnée dans le théorème qui suit :

Théorème 1.2. *Pour tout polynôme $P(x)$ de $\mathbb{K}[x]$, on a*

$$P(x) = \sum_{k\geq 0} \frac{\triangle^k P}{k!}(0).x^{\underline{k}}$$

Démonstration. Soit $P(x) \in \mathbb{K}[x]$, comme $(x^{\underline{k}})_{k\geq 0}$ est une base du $\mathbb{K}-$espace vectoriel, alors il existe une unique suite de coefficients $(a_k)_{k\in\mathbb{N}}$ de $\mathbb{K}$ telle que :

$$P(x) = \sum_{k\geq 0} a_k x^{\underline{k}}$$

On sait qu'il existe $k_0 \in \mathbb{N}$ tel que $a_k = 0$ pour $k \geq k_0$, on a alors :

$$\triangle^j(P(x)) = \sum_{k\geq 0} a_k \triangle^j(x^{\underline{k}})$$

Or :

$$\triangle^j(x^{\underline{k}}) = \begin{cases} \binom{k}{j} x^{\underline{k-j}} & \text{si} \quad 0 \leq j \leq k. \\ 0 \quad \text{si} \quad j > k. \end{cases}$$

En particulier :

$$\triangle^j(x^{\underline{k}})|_{x=0} = \begin{cases} 0 \quad \text{si} \quad 0 \leq j \leq k-1. \\ k! \quad \text{si} \quad j = k. \\ 0 \quad \text{si} \quad j > k. \end{cases}$$

Autrement dit

$$\triangle^j(x^{\underline{k}}) = \delta_{j.k} k!$$

Ainsi

$$a_j = \frac{\triangle^j P(0)}{j!}.$$

Le théorème en découle. □

Expression de l'opérateur $\triangle^n$:
Comme pour tout polynôme $P(x)$ de $\mathbb{K}[x]$, on a :

$$\begin{aligned}\triangle(P(x)) &= P(x+1)-P(x)\\ &= E(P(x))-I(P(x))\\ &= (E-I)P(x)\end{aligned}$$

On en déduit que l'on a :

$$\triangle = E - I$$

Les opérateurs E et $-I$ commutent pour le produit dans l'anneau $L(\mathbb{K}[x])$.

On sait que l'on a :

$$\triangle^n = (E-I)^n = \sum_{k=0}^{n} \binom{n}{k} (-1)^{n-k} E^k$$

Ainsi pour tout polynôme $P(x)$ de $\mathbb{K}[x]$, on a donc :

$$\triangle^n(P(x)) = \sum_{k=0}^{n} \binom{n}{k} (-1)^{n-k} P(x+k)$$

1.4 Les nombres de Stirling :

Nous savons que $(x^{\overline{n}})_{n\geq 0}$, $(x^{\underline{n}})_{n\geq 0}$ et $(x^n)_{n\geq 0}$ sont des bases de $\mathbb{K}[x]$. Chaque vecteur d'une base se décompose d'une manière unique sur toute autre base. Il en résulte qu'il existe des familles de coefficients uniques

$$(\begin{bmatrix} n \\ k \end{bmatrix})_{n,k\in\mathbb{N}}, \quad (s(n,k))_{n,k\in\mathbb{N}} \quad et \quad (\begin{Bmatrix} n \\ k \end{Bmatrix})_{n,k\in\mathbb{N}}$$

telles que pour tout entier $n \geq 0$, on ait :

$$\begin{aligned} x^{\overline{n}} &= \sum_{k\geq 0} \begin{bmatrix} n \\ k \end{bmatrix} x^k.\\ x^{\underline{n}} &= \sum_{k\geq 0} s(n,k) x^k\\ x^n &= \sum_{k\geq 0} \begin{Bmatrix} n \\ k \end{Bmatrix} x^{\underline{k}}\end{aligned}$$

Les nombres $\begin{bmatrix} n \\ k \end{bmatrix}$ sont appelés nombres de Stirling de première espèce non signés. Il est facile de constater que ces nombres sont des entiers naturels.

Les nombres $s(n,k)$ sont liés aux nombres entiers $\begin{bmatrix} n \\ k \end{bmatrix}$ par la relation :

$$s(n,k) = (-1)^{n-k} \begin{bmatrix} n \\ k \end{bmatrix}.$$

Ce sont des entiers relatifs. On les appelle nombres de Stirling de première espèce signés.

On constatera dans ce qui suit que les nombres $\begin{Bmatrix} n \\ k \end{Bmatrix}$ sont aussi des entiers naturels. On note souvent $\begin{Bmatrix} n \\ k \end{Bmatrix}$ par $S(n,k)$. Ces nombres sont appelés nombres de Stirling de seconde espèce.

Nous allons examiner les principales propriétés de ces nombres qui seront utiles dans la suite.

1.4.1 La famille des nombres de Stirling de première espèce non signés

Par définition, on a

$$\begin{bmatrix} n \\ k \end{bmatrix} = [x^k](x^{\overline{n}}) = [x^k](x(x+1)...(x+n-1))$$

La famille des nombres de Stirling $(\begin{bmatrix} n \\ k \end{bmatrix})_{n\geq 0, k\geq 0}$ de première espèce vérifie les propriétés suivantes :

Théorème 1.3. *On a :*

1) Pour $n \geq 0$ et $k \geq 0$, on a

$$\begin{bmatrix} n \\ 0 \end{bmatrix} = [n=0], \quad \begin{bmatrix} n \\ n \end{bmatrix} = 1 \quad et \quad \begin{bmatrix} 0 \\ k \end{bmatrix} = [k=0].$$

2)

$$\begin{bmatrix} n \\ k \end{bmatrix} = 0 \quad pour \quad k > n.$$

3)

$$\begin{bmatrix} n \\ k \end{bmatrix} = \begin{bmatrix} n-1 \\ k-1 \end{bmatrix} + (n-1) \begin{bmatrix} n-1 \\ k \end{bmatrix} \quad pour \quad n \geq 1 \quad et \quad k \geq 1.$$

4)

$$\sum_{n=0}^{\infty} s(n,k) \frac{t^n}{n!} = \frac{\ln^k(1+t)}{k!} \quad pour \quad |t| < 1.$$

Démonstration. Les propriétés 1 et 2 sont immédiates.

3) On a :

$$\begin{aligned}
\begin{bmatrix} n \\ k \end{bmatrix} &= [x^k](x^{\overline{n}}) \\
&= [x^k](x(x+1)...(x+n-1)) \\
&= [x^k](x^{\overline{n-1}}(x+n-1)) \\
&= [x^k](x.x^{\overline{n-1}} + (n-1)x^{\overline{n-1}}) \\
&= [x^k](\sum_{k\geq 0} \begin{bmatrix} n-1 \\ k \end{bmatrix} x^{k+1} + (n-1)\sum_{k\geq 0} \begin{bmatrix} n-1 \\ k \end{bmatrix} x^k \\
&= [x^k](\sum_{k\geq 1} \begin{bmatrix} n-1 \\ k-1 \end{bmatrix} x^k + \sum_{k\geq 0}(n-1) \begin{bmatrix} n-1 \\ k \end{bmatrix} x^k \\
&= \begin{bmatrix} n-1 \\ k-1 \end{bmatrix} + (n-1) \begin{bmatrix} n-1 \\ k \end{bmatrix}
\end{aligned}$$

4) On a d'une part pour x réel et pour $|t| < 1$:

$$\begin{aligned}
(1+t)^x &= \sum_{n=0}^{\infty} \binom{x}{n} t^n \\
&= \sum_{n=0}^{\infty} x^{\underline{n}} \frac{t^n}{n!} \\
&= \sum_{n=0}^{\infty} \frac{t^n}{n!} (\sum_{k=0}^{n} s(n,k)x^k) \\
&= \sum_{k=0}^{\infty} x^k (\sum_{n=k}^{\infty} s(n,k)\frac{t^n}{n!})
\end{aligned}$$

D'autre part :

$$(1+t)^x = e^{x\ln(1+t)} = \sum_{k=0}^{\infty} \ln^k(1+t)\frac{x^k}{k!}.$$

Par identification, on obtient

$$\sum_{n=0}^{\infty} s(n,k)\frac{t^n}{n!} = \frac{\ln^k(1+t)}{k!}.$$

□

Remarque 1.1. *: On constate aussi que pour $n \geq 1$,*

$$\begin{bmatrix} n \\ n-1 \end{bmatrix} = \binom{n}{2}. \quad \textit{En effet :}$$

1.4. Les nombres de Stirling :

$$\begin{aligned}\begin{bmatrix} n \\ n-1 \end{bmatrix} &= [x^{n-1}](x(x+1)...(x+n-1)) \\ &= [x^{n-2}]((x+1)...(x+n-1)) \\ &= 1+2+...+(n-1) = \frac{n(n-1)}{2} \\ &= \frac{n!}{2!(n-2)!} = \binom{n}{2}\end{aligned}$$

On peut déterminer les valeurs des nombres de Stirling de première espèce en développant $x^{\overline{n}}$.

On a :
$x^{\overline{0}} = 1$
$x^{\overline{1}} = 0 + 1x$
$x^{\overline{2}} = x(x+1) = 0 + 1x + 1x^2$
$x^{\overline{3}} = 0 + 2x + 3x^2 + x^3$
$x^{\overline{4}} = 0 + 6x + 11x^2 + 6x^3 + 1x^4$
$x^{\overline{5}} = 0 + 24x + 50x^2 + 35x^3 + 10x^4 + 1x^5$
$x^{\overline{6}} = 0 + 120x + 274x^2 + 225x^3 + 85x^4 + 15x^5 + 1x^6$
$x^{\overline{7}} = 0 + 720x + 1764x^2 + 1624x^3 + 735x^4 + 175x^5 + 21x^6 + 1x^7$

Voici donc une table donnant quelques valeurs des nombres de Stirling de première espèce analogue au triangle de Pascal.

n/k	0	1	2	3	4	5	6	7
0	1							
1	0	1						
2	0	1	1					
3	0	2	3	1				
4	0	6	11	6	1			
5	0	24	50	35	10	1		
6	0	120	274	225	85	15	1	
7	0	720	1764	1624	735	175	21	1

Table 1.1 – Les premières valeurs des nombres de Stirling de première espèce.

Interprétation combinatoire :*([18]).*

Soit S_n *le groupe des permutations de l'ensemble* $\{1, 2, ..., n\}$.

Soit $\sigma \in S_n$, *alors* σ *s'écrit de manière unique à l'ordre près des facteurs :* $\sigma = \sigma_1\sigma_2...\sigma_r$ *où* $\sigma_1, \sigma_2, ..., \sigma_r$ *sont des cycles disjoints deux à deux de longueurs*

resperctives $l_1, l_2, ..., l_r$ *tels que* $l_1 + l_2 + ... + l_r = n$.

r *est le nombre de cycles intervenant dans la décomposition de* σ *en produit de cycles disjoints. Alors*

$\begin{bmatrix} n \\ k \end{bmatrix}$ = *nombre de permutation de* σ_n *s'écrivant comme un produit de* k*-cycles disjoints dont la somme des longueurs est égale à* n.

Ainsi pour $n = 3$, *on a*

$$S_3 = \{I; (1,3,2); (1,2); (1,3); (2,3)\}$$

On a :

$$\begin{aligned}
\begin{bmatrix} 3 \\ 0 \end{bmatrix} &= Card \quad \emptyset = 0 \\
\begin{bmatrix} 3 \\ 1 \end{bmatrix} &= Card\{(1,3,2); (1,2,3)\} = 2 \\
\begin{bmatrix} 3 \\ 2 \end{bmatrix} &= Card\{(1,2); (1,3); (2,3)\} = 3 \\
\begin{bmatrix} 3 \\ 3 \end{bmatrix} &= Card\{I\} = 1 \\
\begin{bmatrix} 3 \\ k \end{bmatrix} &= Card \quad \emptyset = 0 \quad pour \quad k > 4.
\end{aligned}$$

1.4.2 La famille des nombres de Stirling de seconde espèce

Rappelons que par définition on a

$$x^n = \sum_{k \geq 0} \begin{Bmatrix} n \\ k \end{Bmatrix} x^{\underline{k}}$$

La famille des nombres de Stirling de seconde espèce $(\begin{Bmatrix} n \\ k \end{Bmatrix})_{n>0,k>0}$ *vérifie les propriétés suivantes :*

Théorème 1.4. *On a :*

1) Pour $n \geq 0$ *et* $k \geq 0$, *on a*

$$\begin{Bmatrix} n \\ 0 \end{Bmatrix} = [n = 0], \quad \begin{Bmatrix} n \\ n \end{Bmatrix} = 1 \quad et \quad \begin{Bmatrix} 0 \\ k \end{Bmatrix} = [k = 0].$$

2)

$$\begin{Bmatrix} n \\ k \end{Bmatrix} = 0 \quad pour \quad k > n.$$

1.4. Les nombres de Stirling :

3)

$$\left\{ {n \atop k} \right\} = \left\{ {n-1 \atop k-1} \right\} + k \left\{ {n-1 \atop k} \right\} \quad pour \quad n \geq 1 \quad et \quad k \geq 1.$$

4)

$$\left\{ {n \atop k} \right\} = \frac{1}{k!} \sum_{j=0}^{k} \binom{k}{j} (-1)^{k-j} j^n.$$

5)

$$\frac{(e^z - 1)^n}{k!} = \sum_{k=0}^{\infty} \left\{ {n \atop k} \right\} \frac{z^n}{n!}.$$

Démonstration. Les propriétés 1 et 2 sont immédiates.

3) On a :

$$\begin{aligned} x^n = \sum_{k \geq 0} \left\{ {n \atop k} \right\} x^{\underline{k}} &= x.x^{n-1} \\ &= \sum_{k \geq 0} \left\{ {n-1 \atop k} \right\} x^{\underline{k}}.x \end{aligned}$$

Or :

$$\begin{aligned} x^{\underline{k}}.x &= (\prod_{j=0}^{k-1}(x-j)((x-k)+k) \\ &= \prod_{j=0}^{k}(x-j) + k\prod_{j=0}^{k-1}(x-j) \\ &= x^{\underline{k+1}} + kx^{\underline{k}} \end{aligned}$$

et donc :

$$\begin{aligned} x^n &= \sum_{k \geq 0} \left\{ {n-1 \atop k} \right\} (x^{\underline{k+1}} + kx^{\underline{k}}) \\ &= \sum_{k \geq 1} \left\{ {n-1 \atop k-1} \right\} x^{\underline{k}} + \sum_{k \geq 0} k \left\{ {n-1 \atop k} \right\} x^{\underline{k}} \\ &= \sum_{k \geq 1} (\left\{ {n-1 \atop k-1} \right\} + k \left\{ {n-1 \atop k} \right\}) x^{\underline{k}} \end{aligned}$$

Ainsi :

$$\left\{ {n \atop k} \right\} = \left\{ {n-1 \atop k-1} \right\} + k \left\{ {n-1 \atop k} \right\}. \quad \square$$

1.4. Les nombres de Stirling :

4) On a :

$$\left\{ n \atop k \right\} = x^n = P(x) = \sum_{k \geq 0} \frac{\triangle^k P(0)}{k!} x^{\underline{k}}$$

et donc

$$\begin{aligned} \left\{ n \atop k \right\} &= \frac{1}{k!}(\triangle^k P)(0) \\ &= \frac{1}{k!}(\sum_{j=0}^{k} \binom{k}{j}(-1)^{k-j}(x+j)^n)|_{x=0} \\ &= \frac{1}{k!}\sum_{j=0}^{k} \binom{k}{j}(-1)^{k-j} j^n. \quad \square \end{aligned}$$

5) On a

$$\begin{aligned} \frac{(e^z-1)^n}{k!} &= \frac{1}{k!}\sum_{k=0}^{n} \binom{n}{k}(-1)^{n-k} e^{kz} \\ &= \frac{1}{k!}\sum_{k=0}^{n} \binom{n}{k}(-1)^{n-k}(\sum_{n=0}^{\infty} \frac{(kz)^n}{n!} \\ &= \sum_{n=0}^{\infty}(\sum_{k=0}^{n} \frac{1}{k!}\binom{n}{k}(-1)^{n-k} k^m)\frac{z^n}{n!} \\ &= \sum_{k=0}^{\infty} \left\{ n \atop k \right\} \frac{z^n}{n!}. \end{aligned}$$

□

Voici donc une table donnant quelques valeurs des nombres de Stirling de seconde espèce obtenue à l'aide du théorème (1.4)

n/k	0	1	2	3	4	5	6	7
0	1							
1	0	1						
2	0	1	1					
3	0	1	3	1				
4	0	1	7	6	1			
5	0	1	15	25	10	1		
6	0	1	31	90	65	15	1	
7	0	1	63	301	350	140	21	1

Table 1.2 – Les premières valeurs des nombres de Stirling de seconde espèce.

Interprétation combinatoire :

On démontre que $\left\{ {n \atop k} \right\}$ *est exactement le nombre de partitions de l'ensemble* $\{1, 2, ..., n\}$ *ayant* k *éléments.*

Ainsi pour $n = 3$.

1. *Il n'y a qu'une partition de* $\{1, 2, 3\}$ *ayant un élément : c'est la partition* $\{\{1, 2, 3\}\}$, *on a donc :* $\left\{ {3 \atop 1} \right\} = 1$.
2. *Il y a trois partitions de* $\{1, 2, 3\}$ *qui ont deux éléments. Ce sont les partitions suivantes :*
$$\{\{1, 2\}; \{3\}\}, \{\{1, 3\}; \{2\}\}, \{\{2, 3\}; \{1\}\}, \text{ on a donc } \quad \left\{ {3 \atop 2} \right\} = 3.$$
3. *Il n'y a qu'une partition de* $\{1, 2, 3\}$ *ayant trois éléments. C'est la partition* $\{\{1\}, \{2\}, \{3\}\}$, *on a donc* $\left\{ {3 \atop 3} \right\} = 1$.

Relation entre les nombres de Stirling de première et seconde espèce : *les nombres de Stirling de première et seconde espèce sont relies par la relation suivante :*

$$\left[{n \atop m} \right] = \sum_{k=0}^{n-m} (-1)^k \binom{n-1+k}{n-m+k} \binom{2n-m}{n-m-k} \left\{ {n-m+k \atop k} \right\}$$

Démonstration. [19] □

1.5 Les nombres harmoniques et la fonction Zêta de Riemann

Pour $n \geq 1$, *on définit le* n*-ième nombre harmonique* H_n *par :*

$$H_n = \sum_{k=1}^{n} \frac{1}{k}.$$

Pour $s \in \mathbb{C}$ *et pour* $n \geq 1$, *on définit le* $n - ième$ *nombre harmonique d'ordre* s *(nombre harmonique généralisé) par :*

$$H_n^{(s)} = \sum_{k=1}^{n} \frac{1}{k^s}.$$

Pour $\Re e(s) > 1$, *la suite* $(H_n^{(s)})_{n \geq 1}$ *converge dans* $\mathbb{C}$. *Autrement dit : la série* $(\sum_{n \geq 1} \frac{1}{n^s})$ *converge. On définit la fonction zêta de Riemann et on note* $\zeta(s)$ *la somme de cette série*

$$\zeta(s) = \sum_{n \geq 1} \frac{1}{n^s} \quad pour \quad \Re e(s) > 1.$$

On démontre que la fonction ζ se prolonge analytiquement à tout le plan complexe sauf au point 1.

Les nombres de Stirling de première espèce $\begin{bmatrix} n \\ k \end{bmatrix}$ s'expriment à l'étude des nombres harmoniques généralisés.

Théorème 1.5. *Pour $n \geq 1$, on a :*
1)

$$\begin{bmatrix} n \\ 2 \end{bmatrix} = (n-1)!H_{n-1} = (n-1)!\sum_{k=1}^{n-1} \frac{1}{k}. \tag{1.10}$$

2)

$$\begin{aligned} \begin{bmatrix} n \\ 3 \end{bmatrix} &= \frac{1}{2}(n-1)!(H_{p-1}^2 - H_{n-1}^{(2)}) \\ &= \frac{1}{2}(n-1)!((\sum_{k=1}^{n-1} \frac{1}{k})^2 - \sum_{k=1}^{n-1} \frac{1}{k^2}) \end{aligned}$$

Démonstration. 1) On a :

$$\begin{aligned} \begin{bmatrix} n \\ 2 \end{bmatrix} &= [x^2](x(x+1)...(x+(n-1)) \\ &= [x]((x+1)(x+2)...(x+(n-1)) \\ &= \sum_{k=1}^{n-1} \frac{1.2....(n-1)}{k} \\ &= (n-1)!\sum_{k=1}^{n-1} \frac{1}{k} \\ &= (n-1)!H_{n-1} \end{aligned}$$

2) Pour la preuve du (2), on a besoin du lemme suivant :

Lemme 1.1. *Pour tout entier $m \geq 1$ et pour tous nombres réels $x_1, x_2, ..., x_m$, on a*

$$\sum_{1 \leq k < l \leq m} x_k x_l = \frac{1}{2}((\sum_{k=1}^{m} x_k)^2 - \sum_{k=1}^{m} x_k^2)$$

Démonstration. immédiate, en remarquant que :

$$(\sum_{k=1}^{m} x_k)^2 = \sum_{k=1}^{m} x_k^2 + 2 \sum_{1 \leq k < l \leq m} x_k x_l.$$

□

En revenant à la preuve du (2).

$$\begin{aligned}\begin{bmatrix} n \\ 3 \end{bmatrix} &= [x^3](x(x+1)...(x+(n-1))) \\ &= [x^2]((x+1)(x+2)...(x+(n-1))) \\ &= \sum_{1\leq k<l\leq n-1} \frac{1.2.....(n-1)}{k.l} \\ &= (n-1)! \sum_{1\leq k<l\leq n-1} \frac{1}{k.l}\end{aligned}$$

En utilisant le lemme (1.1), posons $m = n-1$, $x_k = \frac{1}{k}$ et $x_l = \frac{1}{l}$, on a :

$$\begin{aligned}\sum_{1\leq k<l\leq n-1} \frac{1}{k.l} &= \frac{1}{2}((\sum_{k=1}^{n-1} \frac{1}{k})^2 - \frac{1}{2}\sum_{k=1}^{n-1} \frac{1}{k^2}) \\ &= \frac{1}{2}H_{n-1}^2 - \frac{1}{2}H_{n-1}^{(2)}.\end{aligned}$$

Par suite

$$\begin{bmatrix} n \\ 3 \end{bmatrix} = (n-1)!(\sum_{1\leq k<l\leq n-1} \frac{1}{k.l}) = \frac{1}{2}(n-1)!(H_{n-1}^2 - H_{n-1}^{(2)})$$

□

1.6 Etude de l'anneau $\mathbb{Z}_{(n)}$

1.6.1 Numérateur et dénominateur d'un nombre rationnel

Soit $x \in \mathbb{Q}$. Considérons l'ensemble P défini comme suit

$$P = \{m \in \mathbb{N} \ / \ m \geq 1 \text{ et } mx \in \mathbb{Z}\}.$$

Alors P est une partie non vide de $\mathbb{N}$. En effet par sa définition même, P est une partie de $\mathbb{N}$. De plus, si $x = \frac{a}{b}$ est une écriture de x avec $a \in \mathbb{Z}$ et $b \in \mathbb{N}^*$, on a alors $bx = a \in \mathbb{Z}$ et par suite $b \in P$ et $P \neq \varnothing$. P admet donc un plus petit élément v qu'on convient d'appeler dénominateur de x et qu'on note $v = denom(x)$. Le nombre entier $u := vx$ est appelé numérateur de x. On le note $u = num(x)$. On constate aisément qu'on alors $x = \frac{u}{v}$, avec $(u, v) = 1$ et aussi que $x = \frac{u}{v}$ est l'unique manière d'écrire x comme un quotient de deux entiers u et v premiers entre eux et tels que $v \geq 1$.

Remarquons que l'on a les propriétés immédiates suivantes

1. $\forall m \in \mathbb{Z}$, $num(m) = m$ et $denom(m) = 1$.
2. $\forall x \in \mathbb{Q}$, $x \in \mathbb{Z} \iff denom(x) = 1$.

1.6.2 Définition et propriétés de l'anneau $\mathbb{Z}_{(n)}$

Soit n un entier naturel non nul. Nous définissons l'ensemble $\mathbb{Z}_{(n)}$ comme suit :

$$\mathbb{Z}_{(n)} = \{x \in \mathbb{Q} \ / \ \ (denom(x), n) = 1\}$$

Autrement dit $\mathbb{Z}_{(n)}$ est constitué par l'ensemble des nombres rationnels dont le dénominateur est premier avec l'entier n. On a bien sûr

$$\mathbb{Z} \subset \mathbb{Z}_{(n)} \subset \mathbb{Q}.$$

Remarquons que pour qu'un nombre rationnel x soit un élément de $\mathbb{Z}_{(n)}$, il faut et il suffit que x puisse s'écrire $x = \frac{a}{b}$, avec $a \in \mathbb{Z}$, $b \in \mathbb{Z}^*$ et $(b, n) = 1$ (sans avoir nécessairement $(a, b) = 1$).

Théorème 1.6. *$\mathbb{Z}_{(n)}$ est un sous anneau de $\mathbb{Q}$.*

Démonstration. En effet $\mathbb{Z}_{(n)}$ est une partie de $\mathbb{Q}$ telle que $-1 \in \mathbb{Z}_{(n)}$ et c'est aussi une partie stable pour l'addition et la multiplication de $\mathbb{Q}$. En effet si $x = \frac{u}{v}$ et $y = \frac{u'}{v'}$ sont deux éléments de $\mathbb{Z}_{(n)}$, avec $(v, n) = 1$ et $(v', n) = 1$. On a alors $x + y = \frac{uv'+u'v}{vv'}$ et $xy = \frac{uu'}{vv'}$. Comme on a $(vv', n) = 1$, car le produit de deux entiers premiers avec n est aussi un entier premier avec n. Il résulte de la remarque précédente que l'on a $x + y \in \mathbb{Z}_{(n)}$ et $xy \in \mathbb{Z}_{(n)}$. Par suite $\mathbb{Z}_{(n)}$ est un sous anneau de $\mathbb{Q}$. □

Remarque 1.2.

1. *Il est facile de constater que le groupe des unités $U(\mathbb{Z}_{(n)})$ est défini par*

$$U(\mathbb{Z}_{(n)}) = \{x \in \mathbb{Q} \ / \ \ (denom(x), n) = 1 \quad et \quad (num(x), n) = 1\}.$$

2. *Tout entier premier avec n est une unité de $\mathbb{Z}_{(n)}$.*
3. *Si $x \in U(\mathbb{Z}_{(n)})$, autrement dit si $x \neq 0$ et si $x \in \mathbb{Z}_{(n)}$ et $\frac{1}{x} \in \mathbb{Z}_{(n)}$, alors on a*

$$x\mathbb{Z}_{(n)} = \mathbb{Z}_{(n)}.$$

4. *Si $n \geq 2$ et si $n = p_1^{\alpha_1} p_2^{\alpha_2} ... p_r^{\alpha_r}$ est la décomposition de n en un produit de nombres premiers distincts ($\alpha_i \geq 1$ pour $1 \leq i \leq r$), alors on a*

$$\mathbb{Z}_{(n)} = \mathbb{Z}_{(p_1^{\alpha_1} p_2^{\alpha_2} ... p_r^{\alpha_r})} = \mathbb{Z}_{(p_1 p_2 ... p_r)}.$$

Théorème 1.7.

$\mathbb{Z}_{(n)}$ est un anneau principal. De plus

1. *Si $n = 1$, alors $\mathbb{Z}_{(1)} = \mathbb{Z}$ et les idéaux de $\mathbb{Z}_{(1)}$ sont les $m\mathbb{Z}$ où $m \in \mathbb{N}$.*

2. *Si $n \geq 2$ et si $n = p_1^{\alpha_1} p_2^{\alpha_2} ... p_r^{\alpha_r}$ est la décomposition de n en un produit de nombres premiers distincts ($\alpha_i \geq 1$ pour $1 \leq i \leq r$), alors les idéaux de $\mathbb{Z}_{(n)}$ distincts de l'idéal nul sont les idéaux principaux de $\mathbb{Z}_{(n)}$ engendré par les éléments s'écrivant $m = p_1^{\beta_1} p_2^{\beta_2} ... p_r^{\beta_r}$ avec $\beta_i \in \mathbb{N}$, pour $1 \leq i \leq r$.*

Démonstration. 1. Soit $n \geq 1$ un entier. Dans le cas où $n = 1$, on a trivialement $\mathbb{Z}_{(1)} = \mathbb{Z}$. Il est bien connu que $\mathbb{Z}$ est un anneau principal et que les idéaux de $\mathbb{Z} = \mathbb{Z}_{(1)}$ sont les $m\mathbb{Z}$ où $m \in \mathbb{N}$. Supposons $n \geq 2$. Soit I un idéal de $\mathbb{Z}_{(n)}$. Posons $J = I \cap \mathbb{Z}$. Il est facile de vérifier que J est un idéal de $\mathbb{Z}$. Il existe donc un entier $m \in \mathbb{N}$ tel que $J = m\mathbb{Z}$. Prouvons que l'on a $I = m\mathbb{Z}_{(n)}$. Pour cela, nous allons prouver qu'on a les deux inclusions suivantes : $I \subset m\mathbb{Z}_{(n)}$ et $m\mathbb{Z}_{(n)} \subset I$.
   - Prouvons que $I \subset m\mathbb{Z}_{(n)}$. Soit $x \in I$, alors x s'écrit $x = \frac{a}{b}$ avec $a \in \mathbb{Z}$, $b \in \mathbb{N}^*$ et $(b, n) = 1$. Comme I est un idéal de $m\mathbb{Z}_{(n)}$ et que $x \in I$ et $b \in \mathbb{Z}_{(n)}$ (car $\mathbb{N}^* \subset \mathbb{Z}$), on a $a = bx \in I$. Comme on a aussi $a \in \mathbb{Z}$, on en déduit que $a \in I \cap \mathbb{Z} = J = m\mathbb{Z}$. Ainsi $a \in m\mathbb{Z}$. Il existe donc un entier $c \in \mathbb{Z}$ tel que $a = mc$. On a alors $x = \frac{a}{b} = m\frac{c}{b}$. Comme $(b, n) = 1$, on a $\frac{c}{b} \in \mathbb{Z}_{(n)}$, par suite $x = m\frac{c}{b} \in m\mathbb{Z}_{(n)}$. On a ainsi prouvé que tout x de I se retrouve dans $m\mathbb{Z}_{(n)}$, autrement dit que $I \subset m\mathbb{Z}_{(n)}$.
   - Prouvons que $m\mathbb{Z}_{(n)} \subset I$. On a $m \in m\mathbb{Z} = I \cap \mathbb{Z}$. On a donc $m \in I$. L'inclusion $m\mathbb{Z}_{(n)} \subset I$ résulte alors du fait que par hypothèse, I est un idéal de $\mathbb{Z}_{(n)}$ et que $m \in I$.

2. Supposons $n \geq 2$ et soit $n = p_1^{\alpha_1} p_2^{\alpha_2} ... p_r^{\alpha_r}$ la décomposition de n en un produit de nombres premiers distincts ($\alpha_i \geq 1$ pour $1 \leq i \leq r$). Soit I un idéal non nul de $\mathbb{Z}_{(n)}$. Alors, d'après ce qui précède, il existe un entier naturel non nul m tel que $I = m\mathbb{Z}_{(n)}$. On peut écrire m de la manière suivante : $m = p_1^{\beta_1} p_2^{\beta_2} ... p_r^{\beta_r} q$ avec $\beta_i = v_{p_i}(m) \in \mathbb{N}$, pour $1 \leq i \leq r$ et $q = \prod_{\substack{p \text{ premier} \\ p \notin \{p_1, p_2, ..., p_r\}}} p^{v_p(m)}$.

   Comme q est une unité de $\mathbb{Z}_{(n)}$, on a $I = m\mathbb{Z}_{(n)} = p_1^{\beta_1} p_2^{\beta_2} ... p_r^{\beta_r} q \ \mathbb{Z}_{(n)} = p_1^{\beta_1} p_2^{\beta_2} ... p_r^{\beta_r} \mathbb{Z}_{(n)}$.

□

1.6.3 L'anneau $\mathbb{Z}_{(p)}$ des p-entiers

Considérons le cas particulier où $n = p$, p étant un nombre premier. Dans ce cas, on a

$$\mathbb{Z}_{(p)} \ = \ \{x \in \mathbb{Q} \ / \ \ p \text{ ne divise pas } denom(x)\}.$$

Les éléments de $\mathbb{Z}_{(p)}$ sont appelés des p-entiers.

Définition 1.1. *Pour tout nombre premier p, on appelle p-entier tout nombre rationnel dont le dénominateur n'est pas divisible par p.*

Remarquons que pour tout entier $m \geq 1$, on a $\mathbb{Z}_{(p^m)} = \mathbb{Z}_{(p)}$. En effet, on a

$$\begin{aligned} \mathbb{Z}_{(p^m)} &= \{x \in \mathbb{Q} \ / \ \ (denom(x), p^m) = 1\} \\ &= \{x \in \mathbb{Q} \ / \ \ (denom(x), p) = 1\} = \mathbb{Z}_{(p)}. \end{aligned}$$

On sait aussi d'après le theorème 1.7 que $\mathbb{Z}_{(p)}$ est un anneau principal et ses idéaux sont les $p^m\mathbb{Z}_{(p)}$ où $m \in \mathbb{N}$.

1.7 Congruences dans un anneau commutatif

Dans tout ce qui suit, A désigne un anneau commutatif, 0_A désigne l'élément neutre de l'addition de A.

Définition 1.2. *On appelle congruence sur l'anneau A toute relation d'équivalence définie sur l'anneau A compatible avec l'addition et la multiplication de l'anneau A.*

Autrement dit, si $\mathcal{R}$ est une relation binaire définie sur A, alors $\mathcal{R}$ est une congruence sur l'anneau A si et seulement si on a

1. *$\mathcal{R}$ est réflexive : $\forall x \in A, \ \ x\mathcal{R}x$,*
2. *$\mathcal{R}$ est symétrique : $\forall x, y \in A, \ \ x\mathcal{R}y \Longrightarrow y\mathcal{R}x$,*
3. *$\mathcal{R}$ est transitive : $\forall x, y, z \in A, \ \ x\mathcal{R}y$ et $y\mathcal{R}z \Longrightarrow x\mathcal{R}z$,*
4. *$\mathcal{R}$ est compatible avec l'addition de l'anneau A :*

$$\forall x, y, x', y' \in A, \ x\mathcal{R}y \ \ \text{et} \ \ x'\mathcal{R}y' \Longrightarrow (x + x')\mathcal{R}(y + y'),$$

5. *$\mathcal{R}$ est compatible avec la multiplication de l'anneau A :*

$$\forall x, y, x', y' \in A, \ x\mathcal{R}y \ \ \text{et} \ \ \ x'\mathcal{R}y' \Longrightarrow xx'\mathcal{R}yy'.$$

Le théorème suivant prouve qu'il y a en fait une bijection entre l'ensemble des congruences définies sur l'anneau A et l'ensemble des idéaux de A.

Théorème 1.8.

1. *Soit $\mathcal{R}$ une conguence définie sur l'anneau A. Alors l'ensemble I constitué par l'ensemble des éléments de A équivalents à 0_A, c'est à dire la classe de 0_A modulo la relation d'équivalence $\mathcal{R}$, est un idéal de A. On a alors l'équivalence suivante*

$$\forall x, y \in A, \ x\mathcal{R}y \iff x - y \in I$$

2. *Soit I un idéal de l'anneau A, alors la relation $\mathcal{T}$ définie par*

$$\forall x, y \in A, \ x\mathcal{T}y \iff x - y \in I$$

est une congruence sur l'anneau A.

Démonstration. 1. Soit $\mathcal{R}$ une conguence définie sur l'anneau A. Posons

$$I = \{x \in A / \quad x\mathcal{R}0_A\}.$$

Alors I est la classe d'équivalence de 0_A. I est donc une partie non vide de A. Si x et y sont deux éléments de I, on a $x\mathcal{R}y$. Comme $\mathcal{R}$ est réfléxive, on a aussi $-y\mathcal{R}-y$. La relation $\mathcal{R}$ étant compatible avec l'addition, les relations $x\mathcal{R}y$ et $-y\mathcal{R}-y$ impliquent que l'on a $(x-y)\mathcal{R}(y-y)$, autrement dit on a $(x-y)\mathcal{R}0_A$ et par conséquent $x-y \in I$. On a ainsi prouvé que I est un sous groupe de $(A,+)$. Soit maintenant $a \in A$ et $x \in I$, on a alors $a\mathcal{R}0_A$ et $x\mathcal{R}0_A$. La relation $\mathcal{R}$ étant compatible avec la multiplication, on en déduit que $ax\mathcal{R}0_A0_A$, c'est à dire $ax\mathcal{R}0_A$ ou encore $ax \in I$. On peut donc conclure que I est un idéal de l'anneau A.

2. Soit I un idéal de l'anneau A et $\mathcal{T}$ la relation définie par

$$\forall x, y \in A,\ x\mathcal{T}y \iff x-y \in I.$$

On vérifie aisément que $\mathcal{T}$ vérifie les 5 propriétes cités plus haut caractérisant une congruence définie sur l'anneau A.

□

Notation 1.1. *La relation $x-y \in I$ où $x, y \in A$ et I est un idéal de A se note*

$$x \equiv y \pmod{I}$$

1.8 Congruences dans $\mathbb{Z}$ et dans $\mathbb{Z}_{(p)}$

1.8.1 Congruences dans $\mathbb{Z}$

Il est bien connu que $\mathbb{Z}$ est un anneau principal. Toute idéal I de $\mathbb{Z}$ est de la forme $I = m\mathbb{Z}$. où m est un entier naturel Toute congruence $\mathfrak{R}$ définie sur $\mathbb{Z}$ est de la forme :

$$x\mathfrak{R}y \ \Leftrightarrow\ x-y \in m\mathbb{Z}.$$

Les congruences correspondantes à $m=0$ et $m=1$ ne présentent aucun intérêt, c'est pourquoi on supposera dans tout ce qui suit que $m \geq 2$. Si $x-y \in m\mathbb{Z}$, autrement si la différence entre les deux entiers x et y est divisible par m.on dit alors que les entiers x et y sont congrus modulo $m\mathbb{Z}$ et on ecrit

$$x \equiv y \ (\mathrm{mod} m\mathbb{Z})$$

Plus couramment, on écrit plus simplement

$$x \equiv y \pmod{m}$$

et on dit que les entiers x et y sont congrus modulo m. On peut alors remarquer les entiers x et y sont congrus modulo m si et seulement si x et y ont même reste dans la division euclidienne par m.

Les propriétes des congruences dans $\mathbb{Z}$ sont bien connues. Nous nous contenterons de rappeller ici les théorèmes classiques et importants suivants : le petit théorème de Fermat, le théorème d'Euler et le théorème de Wilson.

Théorème 1.9. *(Petit théorème de Fermat) Pour tout nombre premier p et pour tout entier $a \in \mathbb{Z} - p\mathbb{Z}$, on a*

$$a^{p-1} \equiv 1 \pmod{p}$$

La relation "$a \in \mathbb{Z} - p\mathbb{Z}$" est équivalente à la relation "a est premier avec p", c'est à dire à la relation "$(a, p) = 1$". Il résulte du petit théorème de Fermat que pour tout nombre premier p et pour tout nombre a premier avec p, on a $\frac{a^{p-1}-1}{p} \in \mathbb{Z}$. Cette constatation nous permet de définir pour tout nombre premier p et pour tout entier $a \in \mathbb{Z} - p\mathbb{Z}$ le quotient de Fermat $q_p(a)$ comme étant l'entier suivant :

$$q_p(a) = \frac{a^{p-1} - 1}{p}.$$

Le théorème d'Euler qui suit est une généralisation du petit théorème de Fermat.

Théorème 1.10. *(Théorème d'Euler). Pour tout nombre entier $n \geq 2$ et pour tout entier a tel que $(a, n) = 1$, on a*

$$a^{\varphi(n)} \equiv 1 \pmod{n}.$$

Dans ce théorème, φ est la fonction indicatrice d'Euler définie pour tout entier naturel $n \geq 1$, par

$$\varphi(n) = card\{k \in \mathbb{N} \ / \ 1 \leq k \leq n \text{ et } (k, n) = 1\}.$$

Il est bien connu que φ est une fonction arithmétique multiplicative, ce qui signifie que l'on a pour tout entier $n \geq 1$ et $m \geq 1$:

$$(n, m) = 1 \Rightarrow \ \varphi(nm) = \varphi(n)\varphi(m).$$

Il est facile de constater que pour tout nombre premier p et pour tout nombre entier $m \geq 1$, on a

$$\varphi(p^m) = p^m - p^{m-1}.$$

En particulier, pour $m = 1$, on a $\varphi(p) = p - 1$ et pour $n = p$, le théorème d'Euler permet d'obtenir le petit théorème de Fermat comme cas particulier. Pour tout entier naturel n non nul, on a

$$\varphi(n) = n \prod_{\substack{p \text{ premier} \\ p \text{ divise } n}} (1 - \frac{1}{p}).$$

Théorème 1.11. *(Théorème de Wilson). Pour tout entier $p \geq 2$, on a l'équivalence*

$$p \text{ est un nombre premier } \Leftrightarrow (p-1)! \equiv -1 \pmod{p}$$

Il résulte du petit théorème de Wilson que pour tout nombre premier p, on a $\frac{(p-1)!+1}{p} \in \mathbb{Z}$. Cette constatation nous permet de définir pour tout nombre premier p le quotient de Wilson w_p comme étant l'entier suivant :

$$w_p = \frac{(p-1)!+1}{p}.$$

Signalons le remarquable résultat suivant concernant les coefficients binomiaux et les nombres de Striling de première espèce et de deuxième espèce.

Théorème 1.12. *Soit p un nombre premier, alors*

1. *pour tout entier k tel que $1 \leq k \leq p-1$,*

$$\binom{p}{k} \equiv 0 \pmod{p},$$

2. *pour tout entier k tel que $2 \leq k \leq p-1$,*

$$\begin{bmatrix} n \\ k \end{bmatrix} \equiv 0 \pmod{p},$$

3. *pour tout entier k tel que $2 \leq k \leq p-1$,*

$$\begin{Bmatrix} n \\ k \end{Bmatrix} \equiv 0 \pmod{p}.$$

Démonstration. 1. Soit k un entier tel que $1 \leq k \leq p-1$, on a

$$k!\binom{p}{k} = p(p-1)...(p-k+1).$$

Le nombre premier p divise $p(p-1)...(p-k+1)$. Comme $(k!, p) = 1$, selon le théorème de Gauss, le nombre premier p doit diviser $\binom{p}{k}$. On a donc

$$\binom{p}{k} \equiv 0 \pmod{p}.$$

2. Considérons le polynôme $P(x) := x^p - x \in \mathbb{Z}/p\mathbb{Z}[x]$. D'après le petit théorème de Fermat, on a $P(\overline{k}) = \overline{0}$ pour $0 \leq k \leq p-1$. Le polynôme P unitaire de degré p admet donc p racines distinctes dans le corps $\mathbb{Z}/p\mathbb{Z}$. Le polynôme $P(x)$ se factorise donc de la manière suivante dans $\mathbb{Z}/p\mathbb{Z}[x]$:

$$x^p - x = x(x-\overline{1})(x-\overline{2})...(x-\overline{p-1}).$$

Or on sait que dans $\mathbb{Z}[x]$, on a l'égalité suivante

$$x(x-1)(x-2)...(x-p-1) = \sum_{k=0}^{p} s(p,k)x^k.$$

On en déduit qu'on a

$$x^p - x = x(x-\overline{1})(x-\overline{2})...(x-\overline{p-1}) = \sum_{k=0}^{p} \overline{s(p,k)}x^k.$$

On obtient ainsi l'égalité suivante entre polynômes de $\mathbb{Z}/p\mathbb{Z}[x]$:

$$x^p - x = \sum_{k=0}^{p} \overline{s(p,k)}x^k.$$

On en déduit que pour $2 \leq k \leq p-1$, on a

$$\overline{s(p,k)} = \overline{0}$$

C'est à dire

$$s(n,k) \equiv 0 \pmod{p}.$$

Comme on a

$$\begin{bmatrix} n \\ k \end{bmatrix} = (-1)^{p-k} s(n,k),$$

on en conclut qu'on a aussi pour $2 \leq k \leq p-1$:

$$\begin{bmatrix} n \\ k \end{bmatrix} \equiv 0 \pmod{p},$$

3. On a d'après la relation 4) du théorème 1.4 :

$$\begin{Bmatrix} n \\ k \end{Bmatrix} = \frac{1}{k!} \sum_{j=0}^{k} \binom{k}{j} (-1)^{k-j} j^n.$$

D'après le petit théorème de Fermat, on a

$$j^p \equiv j \pmod{p},$$

on en déduit que

$$\begin{Bmatrix} n \\ k \end{Bmatrix} \equiv \frac{1}{k!} \sum_{j=0}^{k} \binom{k}{j} (-1)^{k-j} j \pmod{p}$$

Or on a pour $2 \leq k \leq p-1$,

$$\begin{aligned}
\frac{1}{k!}\sum_{j=0}^{k}\binom{k}{j}(-1)^{k-j}j &= \frac{1}{k!}\sum_{j=1}^{k}\binom{k}{j}(-1)^{k-j}j \\
&= \frac{1}{k!}\sum_{j=1}^{k}\frac{k}{j}\binom{k-1}{j-1}(-1)^{k-j}j \\
&= \frac{(-1)^k}{(k-1)!}\sum_{j=1}^{k}\binom{k-1}{j-1}(-1)^{j} \\
&= \frac{(-1)^{k+1}}{(k-1)!}\sum_{s=0}^{k-1}\binom{k-1}{s}(-1)^{s} \\
&= \frac{(-1)^{k+1}}{(k-1)!}(1+(-1))^{k-1} = 0.
\end{aligned}$$

On a donc bien pour tout entier k tel que $2 \leq k \leq p-1$,

$$\left\{ n \atop k \right\} \equiv 0 \pmod{p}.$$

□

1.8.2 Congruences dans $\mathbb{Z}_{(p)}$

Rappelons que $\mathbb{Z}_{(p)}$ désigne l'anneau des p-entiers, c'est à dire l'anneau constitué par les nombres rationnels dont le dénominateur n'est pas divisible par p. Rappelons que pour qu'un nombre rationnel x soit dans $\mathbb{Z}_{(p)}$, il est nécessaire et suffisant qu'on puisse trouver une écriture de x de la forme $x = \frac{a}{b}$ avec $a \in \mathbb{Z}$ et $b \in \mathbb{Z} - p\mathbb{Z}$, cette écriture $\frac{a}{b}$ de x n'étant pas nécessairement la forme réduite de x.

On sait aussi que $\mathbb{Z}_{(p)}$ est un anneau principal et que tout idéal I de $\mathbb{Z}_{(p)}$ peut s'écrire $I = p^m\mathbb{Z}_{(p)}$, où m est un entier naturel. Il en résulte que toute congruence $\mathfrak{R}$ sur $\mathbb{Z}_{(p)}$ est définie par une relation de la forme :

$$x\mathfrak{R}y \Leftrightarrow x - y \in p^m\mathbb{Z}_{(p)}.$$

Autrement dit, si x et y sont deux p- entiers, la relation $x - y \in p^m\mathbb{Z}_{(p)}$ signifie qu'il est possible de trouver une écriture du nombre rationnel $x - y$ de la forme

$$x - y = p^m\frac{a}{b},$$

avec $a \in \mathbb{Z}$ et $b \in \mathbb{Z} - p\mathbb{Z}$, a et b n'étant pas nécessairement premiers entre eux.

Si $x - y \in p^m\mathbb{Z}_{(p)}$,on dit alors que les p-entiers x et y sont congrus modulo l'déal $p^m\mathbb{Z}_{(p)}$. On écrit alors que

$$x \equiv y \ (\mathrm{mod} p^m\mathbb{Z}_{(p)}),$$

Rappelons que $\mathbb{Z} \subset \mathbb{Z}_{(p)}$. Remarquons qu'on a la propriété suivante facile à prouver

$$\forall x \in \mathbb{Z},\ \forall y \in \mathbb{Z} \quad x - y \in p^m\mathbb{Z} \Leftrightarrow x - y \in p^m\mathbb{Z}_{(p)}.$$

Il en résulte que l'on a

$$\forall x \in \mathbb{Z},\ \forall y \in \mathbb{Z} \quad x \equiv y\ (\mathrm{mod} p^m\mathbb{Z}) \Leftrightarrow x \equiv y\ (\mathrm{mod} p^m\mathbb{Z}_{(p)}).$$

Cette équivalence nous permet de noter sans risque de confusion la relation $x \equiv y\ (\mathrm{mod} p^m\mathbb{Z})$ pour $x \in \mathbb{Z}_{(p)}$ et $y \in \mathbb{Z}_{(p)}$ plus simplement par $x \equiv y\ (\mathrm{mod} p^m)$.

Remarques :

1. *Si $x \in \mathbb{Z}_{(p)}$ et $y \in \mathbb{Z}_{(p)}$ sont tels que $\frac{1}{x} \in \mathbb{Z}_{(p)}$ et $\frac{1}{y} \in \mathbb{Z}_{(p)}$, autrement dit si x et y dont des nombres rationnels tels que leur numérareur et leur dénominateur ne sont pas divisibles par le nombre premier p, alors on a*

$$x \equiv y\ (\mathrm{mod} p^m\mathbb{Z}) \Leftrightarrow \frac{1}{x} \equiv \frac{1}{y}\ (\mathrm{mod} p^m\mathbb{Z})$$

   En effet si l'on écrit $x = \frac{a}{b}$ et $y = \frac{c}{d}$, on a $x - y = \frac{ad-bc}{bd}$ et $\frac{1}{x} - \frac{1}{y} = \frac{b}{a} - \frac{d}{c} = \frac{bc-ad}{ac}$, comme aucun des entiers a, b, c et d n'est divisible par p, bd et ac ne sont pas divisibles par p. Il est de plus évident à dire que $ad - bc \in p\mathbb{Z}$ équivaut à dire que $bc - ad \in p\mathbb{Z}$.
2. *Soit p un nombre premier. Supposons que k soit un entier tel que $1 \leq k \leq p-1$, alors k et $p - k$ sont premiers avec p ; k et $p - k$ sont donc des unités de $\mathbb{Z}_{(p)}$. Comme on a : $-k \equiv p - k\ (\mathrm{mod}\ p)$, on en déduit que $-\frac{1}{k} \equiv \frac{1}{p-k}\ (\mathrm{mod}\ p)$ et donc $\frac{1}{p-k} + \frac{1}{k} \equiv 0\ (\mathrm{mod}\ p)$.*

Congruence pour le nombre harmonique d'indice $p - 1$

Le résultat suivant est remarquable. De plus, il est facile à prouver :

Théorème 1.13. *Pour tout nombre premier $p \geq 3$, on a*

$$1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{p-1} \equiv 0 \pmod{p}$$

Démonstration. Soit p un nombre premier impair. On a

$$1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{p-1} = \sum_{k=1}^{p-1} \frac{1}{k} = \sum_{k=1}^{p-1} \frac{1}{p-k}.$$

On en déduit que

$$\begin{aligned} 1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{p-1} &= \frac{1}{2} \sum_{k=1}^{p-1} \left(\frac{1}{k} + \frac{1}{p-k} \right) \\ &= p. \sum_{k=1}^{p-1} \left(\frac{1}{2k(p-k)} \right). \end{aligned}$$

Comme il est facile de constater que $\sum_{k=1}^{p-1}\left(\frac{1}{2k(p-k)}\right) \in \mathbb{Z}_{(p)}$, il en résulte que $1+\frac{1}{2}+\frac{1}{3}+\cdots+\frac{1}{p-1} \in p.\mathbb{Z}_{(p)}$, ce qui est bien la relation qu'on voulait prouver. □

Généralisation

Le théorème suivant est une importante généralisation du théorème précédent.

Théorème 1.14. *Pour tout nombre premier $p \geq 3$ et pour tout entier $m \in \mathbb{Z}$, on a*

$$1^m+2^m+3^m+\cdots+(p-1)^m \equiv \begin{cases} 0 \pmod p & si\ m \notin (p-1)\mathbb{Z} \\ -1 \pmod p & si\ m \in (p-1)\mathbb{Z} \end{cases}$$

Démonstration. Si $m \in (p-1)\mathbb{Z}$, alors d'après le petit théorème de Fermat, on a pour tout entier k tel que $1 \leq k \leq p-1$

$$k^m \equiv 1 \pmod p,$$

il en résulte que l'on a alors

$$\sum_{k=1}^{p-1} k^m \equiv \sum_{k=1}^{p-1} 1 = p-1 \ \equiv -1 \pmod p.$$

Suposons maintenant que $m \notin (p-1)\mathbb{Z}$. Désignons par $\overline{g}$, avec $g \in \{1,2,..,p-1\}$, un générateur du groupe cyclique $(\mathbb{Z}/p\mathbb{Z})^*$. On a alors

$$1^m+2^m+3^m+\cdots+(p-1)^m \equiv \sum_{k=0}^{p-2}(g^k)^m \pmod p.$$

On constate que l'on a

$$\sum_{k=0}^{p-2}(g^k)^m = \sum_{k=0}^{p-2}(g^m)^k = \frac{(g^m)^{p-1}-1}{g^m-1} = \frac{(g^{p-1})^m-1}{g^m-1}.$$

Comme $m \notin (p-1)\mathbb{Z}$, on a $\overline{g^m} = \overline{g}^m \neq \overline{1}$. On a donc $g^m-1 \notin p\mathbb{Z}$ et comme $\overline{g^{p-1}} = \overline{g}^{p-1} = \overline{1}$, on a $(g^{p-1})^m-1 \in p\mathbb{Z}$. On en conclut que $\frac{(g^{p-1})^m-1}{g^m-1} \in p\mathbb{Z}_{(p)}$. Par conséquent, on a bien

$$1^m+2^m+3^m+\cdots+(p-1)^m \equiv 0 \pmod p,$$

pour $m \notin (p-1)\mathbb{Z}$. □

Théorème de Wolstenholme :

En 1862, Joseph Wolstenholme énonça et démontra la remarquable congruence suivante relative au $p-1$-ième nombre harmonique, améliorant pour $p \geq 5$ le théorème 1.13.

Théorème 1.15. *Pour tout nombre premier $p \geq 5$, on a*

$$1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{p-1} \equiv 0 \ (\mathrm{mod} p^2).$$

Démonstration. Soit $p \geq 5$ un nombre premier, on a vu dans la preuve du théorème 1.13 que l'on avait

$$1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{p-1} = p. \sum_{k=1}^{p-1} \left(\frac{1}{2k(p-k)} \right).$$

Comme on a pour $1 \leq k \leq p-1$

$$2k(p-k) \equiv -2k^2 \pmod{p}$$

et que $-2k^2 \notin p\mathbb{Z}_{(p)}$, on a

$$\frac{1}{2k(p-k)} \equiv -\frac{1}{2k^2} \pmod{p}$$

et donc

$$\sum_{k=1}^{p-1} \frac{1}{2k(p-k)} \equiv -\frac{1}{2} \sum_{k=1}^{p-1} \frac{1}{k^2} \ \equiv 0 \pmod{p}$$

Pour $p \geq 5$, $2 \notin (p-1)\mathbb{Z}$. Il en résulte qu'en appliquant le théorème 1.14, on a

$$-\frac{1}{2} \sum_{k=1}^{p-1} \frac{1}{k^2} \ \equiv 0 \pmod{p}.$$

Par suite,

$$1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{p-1} = p. \sum_{k=1}^{p-1} \left(\frac{1}{2k(p-k)} \right) \equiv . - \frac{p}{2} \sum_{k=1}^{p-1} \frac{1}{k^2} \ \equiv 0 \ (\mathrm{mod} p^2).$$

□

Congruences faisant intervenir le quotient de Fermat $q_p(2)$

De nombreuses congruences comportant des nombres harmoniques font intervenir les quotients de Fermat. On a

Théorème 1.16. *Pour tout nombre premier p, on a*

$$\sum_{k=1}^{p-1} \frac{(-1)^{k-1}}{k} = 1 - \frac{1}{2} + \frac{1}{3} + \cdots - \frac{1}{p-1} \equiv 2q_p(2) \pmod{p}$$

Démonstration. En effet, p étant un nombre premier, on a

$$\binom{p}{k} = p\frac{(p-1)(p-2)...(p-(k-1))}{k!} \equiv p\frac{(-1)^{k-1}(k-1)!}{k!} \equiv p\frac{(-1)^{k-1}}{k} \pmod{p^2}.$$

Il en découle que

$$2^p - 2 = \sum_{k=1}^{p-1} \binom{p}{k} \equiv p\sum_{k=1}^{p-1} \frac{(-1)^{k-1}}{k} \pmod{p^2}.$$

Ce qu'on peut écrire

$$p\sum_{k=1}^{p-1} \frac{(-1)^{k-1}}{k} \equiv \frac{2^p - 2}{p} \equiv 2q_p(2) \pmod{p}.$$

□

En exploitant le théorème 1.13 et le théorème précédent, on a

Théorème 1.17. *Pour tout nombre premier p, on a*

$$H_{\frac{p-1}{2}} \equiv -2q_p(2) \pmod{p}$$

Démonstration. Il suffit de remarquer que l'on a

$$2q_p(2) \equiv \sum_{k=1}^{p-1} \frac{(-1)^{k-1}}{k} \equiv H_{p-1} - 2(\frac{1}{2} + \frac{1}{4} + \cdots \frac{1}{p-1}) = H_{p-1} - H_{\frac{p-1}{2}} \equiv -H_{\frac{p-1}{2}} \pmod{p}$$

□

Le théorème d'Einsentein (1850) est un corollaire au théorème précédent.

Théorème 1.18. *(Einsenstein,1850) Pour tout nombre premier impair, on a*

$$1 + \frac{1}{3} + \frac{1}{5} + \cdots \frac{1}{p-2} \equiv q_p(2) \pmod{p}$$

Démonstration. Il suffit de remarquer que

$$1 + \frac{1}{3} + \frac{1}{5} + \cdots \frac{1}{p-2} = H_{p-1} - (\frac{1}{2} + \frac{1}{4} + \cdots \frac{1}{p-1}) = H_{p-1} - \frac{1}{2}H_{\frac{p-1}{2}} \equiv -\frac{1}{2}H_{\frac{p-1}{2}} \equiv q_p(2) \pmod{p}$$

□

Le théorème 1.17 a été amélioré par E. Lehmer en 1938.

Théorème 1.19. *Pour tout nombre premier p impair, on a*

$$H_{\frac{p-1}{2}} \equiv \ -2q_p(2) \ + p(q_p(2))^2 (\mathrm{mod} p^2)$$

Le théorème ci-dessus est exactement la relation (45) figurant en page 358 de l'article "On congruences involving Bernoulli numbers and the quotients of Fermat and Wilson" d'Emma Lehmer, parue dans la revue "Annals of Mathematics", Vol39, N°2, April, 1938. Il s'agit d'un article de référence important contenant de très nombreuses congruences. Cet article se trouve cité régulièrement de nos jours encore (cité dans au moins 95 articles, (ref :Google)). Ce théorème est aussi et surtout essentiel dans la preuve des congruences établies par Zhi Wei Sun. Nous détaillons la preuve de Zhi Wei sun au chapitre 4. La preuve que donne Emma Lehmer de son théorème résulte de plusieurs autres relations établies dans son article. Il serait trés fastidieux de détailler ici la preuve d'Emma Lehmer, cette preuve étant loin d'être courte et simple. De plus la preuve d'Emma Lehmer se base sur des propriétés essentielles des nombres de Bernoulli.

Nous nous proposons dans ce qui suit de donner une preuve simple et directe de ce célèbre théorème. Cette preuve repose sur les lemmes qui suivent.

Lemme 1.2. *Pour tout nombre premier impair p et pour tout entier n tel que $2 \leq n < p-1$, on a la congruence suivante dans $\mathbb{Z}_{(p)}$*

$$\prod_{k=1}^{n} \left(1 - \frac{p}{k}\right) \equiv 1 - pH_n + \frac{1}{2}p^2 \left(H_n^2 - H_n^{(2)}\right) \ (\mathrm{mod} p^3).$$

Démonstration. Soient $x_1, x_2, ..., x_n \in \mathbb{K}$, posons pour tout entier r tel que $1 \leq r \leq n$:

$$\sigma_r = \sum_{1 \leq i_1 \leq i_2 \leq \cdots \leq i_r \leq n} x_{i_1} x_{i_2} ... x_{i_r}.$$

On a alors en particulier

$$\begin{aligned} \sigma_1 &= \sum_{k=1}^{n} x_k, \\ \sigma_2 &= \sum_{1 \leq k < l \leq n} x_k x_l, \\ \sigma_n &= x_1 x_2 ... x_{n.} \end{aligned}$$

Rappelons que dans $K[x]$, on a les égalités suivantes :

$$(x - x_1)(x - x_2)...(x - x_n) = x^n - \sigma_1 x^{n-1} + \sigma_2 x^{n-2} - \cdots + (-1)^n \sigma_n$$

et

$$(1 - x_1 x)(1 - x_2 x)...(1 - x_n x) = 1 - \sigma_1 x + \sigma_2 x^2 - \cdots + (-1)^n \sigma_n x^n.$$

Supposons maintenant que p soit un nombre premier impair et que $x_1, x_2, ..., x_n$ soient des p-entiers, σ_r est alors aussi un p-entier pour $1 \leq r \leq n$. On déduit de l'égalité précédente la congruence suivante dans $\mathbb{Z}_{(p)}$:

$$(1-x_1p)(1-x_2p)...(1-x_np) = 1-\sigma_1p+\sigma_2p^2-\cdots+(-1)^r\sigma_rp^r \pmod{p^{r+1}}. \quad (1.11)$$

Dans le cas particulier où l'on choisit $x_k = \frac{1}{k}$, pour $1 \leq k \leq n$, on a

$$\begin{aligned}\sigma_1 &= \sum_{k=1}^{n} \frac{1}{k} = H_n, \\ \sigma_2 &= \sum_{1\leq k<l\leq n} \frac{1}{kl} = \frac{1}{2}\left(\left(\sum_{k=1}^{n}\frac{1}{k}\right)^2 - \sum_{k=1}^{n}\frac{1}{k^2}\right) = \frac{1}{2}\left(H_n^2 - H_n^{(2)}\right).\end{aligned}$$

Il en résulte que si n est un entier tel que $1 \leq n \leq p-1$, on a $\frac{1}{k} \in \mathbb{Z}_{(p)}$, pour $1 \leq k \leq n$, on obtient à l'aide de la relation 1.11, pour $r = 2$:

$$\prod_{k=1}^{n}\left(1-\frac{p}{k}\right) \equiv 1 - pH_n + \frac{1}{2}p^2\left(H_n^2 - H_n^{(2)}\right) \pmod{p^3}.$$

□

Lemme 1.3. *Pour tout nombre premier $p \geq 5$, on a*

$$\prod_{k=1}^{\frac{p-1}{2}}\left(1-\frac{p}{k}\right) \equiv 1 - pH_{\frac{p-1}{2}} + 2p^2q_p^2(2) \pmod{p^3}.$$

Démonstration. Choisissons $n = \frac{p-1}{2}$, p étant un nombre premier impair. La condition d'application du lemme 1.2, à savoir la condition $2 \leq n < p-1$ nous impose $n = \frac{p-1}{2} \geq 2$, soit $p \geq 5$. Supposons donc $p \geq 5$. Le lemme 1.2 s'applique. On obtient

$$\prod_{k=1}^{\frac{p-1}{2}}\left(1-\frac{p}{k}\right) \equiv 1 - pH_{\frac{p-1}{2}} + \frac{1}{2}p^2\alpha_p \pmod{p^3}.$$

avec

$$\alpha_p = \left(H_{\frac{p-1}{2}}^2 - H_{\frac{p-1}{2}}^{(2)}\right). \quad (1.12)$$

Pour terminer la preuve du lemme 1.3, il nous suffit de prouver que l'on a

$$\alpha_p \equiv 4q_p^2(2) \pmod{p}. \quad (1.13)$$

Pour cela remarquons que d'après le theorème 1.17

$$H_{\frac{p-1}{2}} \equiv -2q_p(2) \pmod{p}.$$

On a donc

$$H^2_{\frac{p-1}{2}} \equiv 4q_p^2(2) \pmod{p}. \tag{1.14}$$

En constatant que pour $1 \leq k \leq p-1$

$$\frac{1}{k^2} \equiv \frac{1}{(p-k)^2} \pmod{p},$$

on obtient en exploitant le théorème 1.14 et en remrquant que $2 \notin (p-1)\mathbb{Z}$:

$$2H^{(2)}_{\frac{p-1}{2}} \equiv \sum_{k=1}^{\frac{p-1}{2}} \frac{1}{k^2} = \sum_{k=1}^{\frac{p-1}{2}} \frac{1}{(p-k)^2} = \sum_{k=1}^{p-1} \frac{1}{k^2} \equiv 0 \pmod{p}.$$

Il en résulte que

$$H^{(2)}_{\frac{p-1}{2}} \equiv 0 \pmod{p} \tag{1.15}$$

On déduit des relations (1.12), (1.14) et (1.15) que

$$\alpha_p = 4q_p^2(2) \pmod{p},$$

ce qui est bien la relation (1.13) qu'on voulait établir. □

Lemme 1.4. *Pour tout nombre premier impair p, on a*

$$\sum_{k=1}^{\frac{p-1}{2}} \frac{1}{(2k-1)^2} \equiv 0 \pmod{p}$$

Démonstration. En effet, on a

$$\begin{aligned}
\sum_{k=1}^{\frac{p-1}{2}} \frac{1}{(2k-1)^2} &= \frac{1}{1^2} + \frac{1}{3^2} + \frac{1}{5^2} + \cdots + \frac{1}{(p-2)^2} \\
&= \left(\frac{1}{1^2} + \frac{1}{2^2} + \frac{1}{3^2} + \cdots + \frac{1}{(p-1)^2}\right) - \left(\frac{1}{2^2} + \frac{1}{4^2} + \frac{1}{6^2} + \cdots + \frac{1}{(p-1)^2}\right) \\
&= H^{(2)}_{p-1} - \frac{1}{4} H^{(2)}_{\frac{p-1}{2}} \equiv 0 \pmod{p}.
\end{aligned}$$

Or en remarquant que $2 \notin (p-1)\mathbb{Z}$, on a d'après le théorème 1.14, et la relation (1.15) :

$$H^{(2)}_{p-1} \equiv 0 \pmod{p} \quad \text{et} \quad H^{(2)}_{\frac{p-1}{2}} \equiv 0 \pmod{p},$$

il s'ensuit que l'on a bien

$$\sum_{k=1}^{\frac{p-1}{2}} \frac{1}{(2k-1)^2} \equiv 0 \pmod{p}.$$

□

Lemme 1.5. *Pour tout entier $n \geq 1$, on a*

$$4^n(2n)! = \prod_{k=1}^{n} \left((2n+1)^2 - (2k+1)^2\right)$$

Démonstration. En remarquant que l'on peut écrire :

$$n! = \prod_{k=1}^{n}(n+1-k),$$

on a

$$\begin{aligned} 4^n(2n)! &= (2^n n!)(2^n \prod_{k=1}^{n}(n+k)) \\ &= \prod_{k=1}^{n}(2n+2-2k) \prod_{k=1}^{n}(2n+2k) \\ &= \prod_{k=1}^{n} \left((2n+1)-(2k-1)\right)\left((2n+1)+(2k-1)\right) \\ &= \prod_{k=1}^{n} \left((2n+1)^2 - (2k-1)^2\right). \end{aligned}$$

□

Lemme 1.6. *Pour tout nombre premier $p \geq 5$, on a*

$$4^{\frac{p-1}{2}}(p-1)! \equiv (-1)^{\frac{p-1}{2}} \prod_{k=1}^{\frac{p-1}{2}}(2k-1)^2 \pmod{p^3}$$

Soit un nombre premier $p \geq 5$. Posons $n = \frac{p-1}{2}$. Alors $n \geq 2$. On a à l'aide du lemme 1.5

$$\begin{aligned} 4^{\frac{p-1}{2}}(p-1)! &= 4^n(2n)! = \prod_{k=1}^{n} \left((2n+1)^2 - (2k-1)^2\right) \\ &= \prod_{k=1}^{n} \left(p^2 - (2k+1)^2\right) \\ &= \left((-1)^{\frac{p-1}{2}} \prod_{k=1}^{n}(2k-1)^2\right) \prod_{k=1}^{n} \left(1 - \frac{p^2}{(2k+1)^2}\right). \end{aligned} \tag{1.16}$$

On a dans la congruence suivante dans $\mathbb{Z}_{(p)}$

$$\prod_{k=1}^{n} \left(1 - \frac{p^2}{(2k+1)^2}\right) \equiv 1 - \left(\sum_{k=1}^{\frac{p-1}{2}} \frac{1}{(2k-1)^2}\right) p^2 \pmod{p^4}. \tag{1.17}$$

Or, on déduit du lemme 1.4 que

$$p^2 \sum_{k=1}^{\frac{p-1}{2}} \frac{1}{(2k-1)^2} \equiv 0 \ (\mathrm{mod} p^3). \tag{1.18}$$

Des relations (1.17) et (1.18), on déduit que l'on a

$$\prod_{k=1}^{n} \left(1 - \frac{p^2}{(2k+1)^2}\right) \equiv 1 \ (\mathrm{mod} p^3). \tag{1.19}$$

A l'aide de cette dernière relation, on déduit de (1.16)

$$4^{\frac{p-1}{2}}(p-1)! = (-1)^{\frac{p-1}{2}} \prod_{k=1}^{n} (2k-1)^2 \ \ (\mathrm{mod} p^3).$$

Lemme 1.7. *Pour tout nombrer premier $p \geq 5$, on a*

$$\prod_{k=1}^{\frac{p-1}{2}} \left(1 - \frac{p}{k}\right) \equiv 4^{p-1} \ \equiv (1 + pq_p(2))^2 \ \ (\mathrm{mod} p^3).$$

Démonstration. En effet, on a avec $p = 2n+1$

$$\begin{aligned}
\prod_{k=1}^{\frac{p-1}{2}} \left(1 - \frac{p}{k}\right) &= (-1)^{\frac{p-1}{2}} \prod_{k=1}^{\frac{p-1}{2}} \left(\frac{p-k}{k}\right) = (-1)^n \prod_{k=1}^{n} \left(\frac{2n+1-k}{k}\right) \\
&= (-1)^n \binom{2n}{n} = (-1)^n \frac{(2n)!}{n!n!} \\
&= 4^n (-1)^n \frac{1}{(2n)!} \left(\frac{(2n)!}{2^n n!}\right)^2 \\
&= 4^n (-1)^n \frac{1}{(2n)!} \left(\frac{1.2.3..(2n)}{2.4...(2n)}\right)^2 \\
&= 4^n (-1)^n \frac{1}{(2n)!} \left(1.3...(2n-1)\right)^2 \\
&= 4^n (-1)^n \frac{1}{(2n)!} \prod_{k=1}^{n} (2k-1)^2 \\
&= 4^{\frac{p-1}{2}} (-1)^{\frac{p-1}{2}} \frac{1}{(p-1)!} \prod_{k=1}^{\frac{p-1}{2}} (2k-1)^2
\end{aligned}$$

Ainsi on a

$$\prod_{k=1}^{\frac{p-1}{2}} \left(1 - \frac{p}{k}\right) = 4^{\frac{p-1}{2}} \frac{1}{(p-1)!} (-1)^{\frac{p-1}{2}} \prod_{k=1}^{\frac{p-1}{2}} (2k-1)^2$$

En exploitant le lemme 1.6, on obtient

$$\prod_{k=1}^{\frac{p-1}{2}}\left(1-\frac{p}{k}\right) \equiv 4^{\frac{p-1}{2}}\frac{1}{(p-1)!}4^{\frac{p-1}{2}}(p-1)! \ \equiv 4^{p-1} \ (\mathrm{mod} p^3).$$

Comme on a aussi $4^{p-1} = \left(2^{p-1}\right)^2 = \left(1+pq_p(2)\right)^2$, la preuve du lemme 1.7 est complète. □

Preuve du théorème d'Emma Lehmer (théorème 1.19) *Les lemmes 1.3 et 1.7 fournissent chacun une expession de* $\prod_{k=1}^{\frac{p-1}{2}}\left(1-\frac{p}{k}\right)$ *modulo* p^3 *dans* $\mathbb{Z}_{(p)}$. *Ces deux expessions sont donc congrues modulo* p^3 *dans* $\mathbb{Z}_{(p)}$. *On peut donc écrire que l'on a*

$$1 - pH_{\frac{p-1}{2}} + 2p^2q_p^2(2) \ \equiv \left(1+pq_p(2)\right)^2 \ (\mathrm{mod} p^3).$$

On en déduit ainsi que l'on a

$$pH_{\frac{p-1}{2}} \equiv -2pq_p(2) + p^2q_p^2(2) (\mathrm{mod} p^3).$$

En simplifiant par p, on obtient la relation

$$H_{\frac{p-1}{2}} \equiv -2q_p(2) + pq_p^2(2) \ (\mathrm{mod} p^2).$$

La preuve du théorème d'Emma Lehmer est complète.

Chapitre 2

Définitions et propriétés des nombres et polynômes de Bernoulli

2.1 Intoduction

L'étude des sommes de puissances

$$S_m(n) = 1^m + 2^m + \cdots + n^m$$

où n et m sont deux entiers ≥ 1 est un problème qui a préoccupé des générations de mathématiciens depuis l'antiquité. C'est encore et toujours une source de problèmes, de conjectures et de défis pour l'esprit humain. Ainsi on sait d'après le petit théorème de Fermat que pour tout nombre premier p, on a

$$\forall k \in \{1, 2, ..., p-1\}, \quad k^{p-1} \equiv 1 \pmod{p}.$$

Il en résulte que l'on a pour tout nombre premier p :

$$S_{p-1}(p-1) = 1^{p-1} + 2^{p-1} + \cdots + (p-1)^{p-1} \equiv -1 \pmod{p}$$

Posons-nous la question de savoir si la réciproque de cette propriété est vraie. Plus précisément, étant donné un entier $n \geq 2$ tel que $1^{n-1} + 2^{n-1} + \cdots + (n-1)^{n-1} \equiv -1 \mod n$, peut-on affirmer que n est premier ? On peut vérifier à l'aide d'un ordinateur que n est effectivement premier pour tous les entiers $n \leq 100$ tels que

$$1^{n-1} + 2^{n-1} + \cdots + (n-1)^{n-1} \equiv -1 \pmod{n}.$$

On peut donc raisonnablement conjecturer que la réciproque est bien vrai. C 'est ce que fit Giuga en 1950. Cette conjecture est d'ailleurs connue sous le nom de "conjecture de Giuga". Malgré de nombreux efforts entrepris depuis 1950 pour prouver ou infirmer cette conjecture, aucune de ces recherches n'a abouti à ce jour. Concernant à la détermination effective des sommes $S_m(n)$. Les grecs dont Archimède ont connu

les formules

$$\begin{aligned} S_1(n) &= \frac{n(n+1)}{2}, \\ S_2(n) &= \frac{n(n+1)(2n+1)}{6}, \\ S_3(n) &= \frac{n^2(n+1)^2}{4} = (S_1(n))^2. \end{aligned}$$

La preuve de ces formules n'était pas connue. Il a fallu attendre l'an 1000 *pour qu'un mathématicien persan Abu Bakr Al Karaji découvre une méthode géométrique justifiant l'égalité*

$$1^3 + 2^3 + \cdots + n^3 = (1 + 2 + + \cdots + n)^3.$$

La détermination d'une formule pour $S_4(n)$*, somme des* n *premiers bicarrés, fut beaucoup plus tardive dans l'histoire (connue) des mathématiques. Selon Edouard Lucas (citation extraite de la page 228 de son ouvrage "Théorie des nombres"), la détermination de* $S_4(n)$ *« a été donnée par le medecin Djamchid Ben Mas'oud, qui prit part à la rédaction des Tables astronomiques d'Ouloug-Beg. On lit dans un manuscrit conservé au British Museum, daté de* 1589 (997 *Hégire),un passage qui a été traduit ainsi : " Si nous désirons connaître la somme des bicarrés, nous retranchons* 1 *de la somme des premiers nombres et nous prenons constamment le cinquième du reste, nous l'ajoutons à la somme des dits nombres et nous multiplions ce qui en provient par la somme des carrés des mêmes nombres." ». On a donc*

$$S_4(n) = (\frac{S_1(n) - 1}{5} + S_1(n))S_2(n),$$

ce que l'on peut aussi écrire

$$5S_4(n) = (6S_1(n) - 1)S_2(n).$$

Cette dernière formule sera retrouvée par Pierre de Fermat $(1601 - 1665)$*. Compte tenu des expressions connues de* $S_1(n)$ *et* $S_2(n)$*, ces deux dernières formules expriment que l'on a*

$$S_4(n) = \frac{n(n+1)(2n+1)(3n^2+3n-1)}{30}.$$

Citons maintenant quelques grands noms connus parmi les nombreux mathématiciens qui se sont intéréssés à la détermination des sommes $S_m(n)$*. En Allemagne, Johann Faulhaber (*$1580 - 1685$*) réussit à déterminer* $S_m(n)$*, pour* $1 \leq m \leq 17$*.*

En France, Blaise Pascal ($1623-1662$*) réussit à trouver une formule de récurrence permettant de calculer* $S_m(n)$*, quand on connait* $S_k(n)$*, pour* $1 \leq k \leq m-1$*.*

En Suisse, Jacques Bernoulli $(1654 - 1705)$ *réussit à écrire une formule générale en mettant en évidence le fait remarquable que la connaissance d'une suite de nombres*

rationnels que l'on appelle aujourd'hui nombre de Bernoulli permet d'établir une formule générale pour la somme $S_m(n)$.

En Suisse aussi, Leonhard Euler (1707−1783) découvre des liens entre les nombres de Bernoulli et la fonction zéta de Riemann. En 1923 parait l'ouvrage du mathématicien danois Niels Nielsen (1865 − 1931). Il s'agit d'un livre [32] entièrement consacré à l'étude des nombres de Bernoulli et intitulé "Traité élémentaire des nombres de Bernoulli". Dans cette ouvrage d'environ 400 pages, Niels Nielsen écrit en page 295 de [32], à propos de la détermination des sommes $S_m(n)$:

« Or le problème susdit, apparemment élémentaire est intimement lié avec les problèmes qui sont à regarder comme les plus difficiles de la Théorie des Nombres, nous le verrons bientôt.».

On trouve dans l'ouvrage trés riche de Nielsen un intéressant historique sur la détermination des sommes $S_m(n)$ et sur des identités concernant les nombres de Bernoulli.

Dans ce chapitre, nous rappelons la définition et les principales propriétés des nombres et polynômes de Bernoulli. En fin de ce chapitre, nous énoncons et prouvons la formule explicite générale exprimant $S_m(n)$ pour tout entier $m \geq 1$ à l'aide des nombres de Bernoulli, appelée formule de Faulhaber et nous signalons la relation entre la fonction zéta de Riemann et les nombres de Bernoulli.

2.2 Définition des nombres et polynômes de Bernoulli

2.2.1 Définition des nombres de Bernoulli

Définition 2.1. *On appelle suite des nombres de Bernoulli la suite de nombres rationnels $(B_n)_{n\in\mathbb{N}}$ définie par la relation de récurrence suivante*

$$B_0 = 1 \quad et \quad B_n = -\frac{1}{n+1}\sum_{k=0}^{n-1}\binom{n+1}{k}B_k \quad pour\ n \geq 1.$$

Pour tout entier naturel n, B_n est appelé n-ième nombre de Bernoulli.

A l'aide de cette définition, nous pouvons calculer les valeurs des nombres de Bernoulli B_n. Pour $0 \leq n \leq 10$. On trouve

$$B_0 = \quad 1,$$

$$B_1 = -\frac{1}{2},$$

$$B_2 = \quad \frac{1}{6},$$

$$B_4 = -\frac{1}{30},$$
$$B_6 = \frac{1}{42},$$
$$B_8 = -\frac{1}{30},$$
$$B_{10} = \frac{5}{66},$$

et

$$B_3 = B_5 = B_7 = B_9 = 0.$$

On constate qu'à part B_1 qui vaut $-\frac{1}{2}$, les nombres de Bernoulli d'indices impairs sont tous nuls pour $n \leq 10$. On prouvera un peu plus loin qu'en fait, tous les nombres de Bernoulli d'indices impairs ≥ 3 sont nuls.

2.2.2 Série génératrice exponentielle des nombres de Bernoulli

Nous allons nous intéresser maintenant à la série génératrice exponentiennelle de la suite des nombres de Bernoulli, c'est à dire de la série formelle $S(z)$ de l'anneau des séries formelles $\mathbb{C}[[z]]$ définie par

$$S(z) = \sum_{n=0}^{\infty} B_n \frac{z^n}{n!}.$$

Rappelons que dans cet anneau, le produit de deux séries formelles $A(z) = \sum_{n=0}^{\infty} a_n \frac{z^n}{n!}$ et $B(z) = \sum_{n=0}^{\infty} b_n \frac{z^n}{n!}$ est égal à la série formelle

$C(z) = \sum_{n=0}^{\infty} c_n \frac{z^n}{n!}$ *avec*

$$c_n = n! \sum_{k=0}^{n} \frac{a_k}{k!} \frac{b_{n-k}}{(n-k)!}, \quad n \in \mathbb{N},$$

relation qu'on peut écrire

$$c_n = \sum_{k=0}^{n} \binom{n}{k} a_k b_{n-k}, \quad n \in \mathbb{N}.$$

Remarquons maintenant que la relation définissant les nombres de Bernoulli peut s'écrire :

$$\forall n \in \mathbb{N}^* \qquad \sum_{k=0}^{n+1} \binom{n+1}{k} B_k = B_{n+1}$$

ou encore, en utilisant le symbole d'Iverson

$$\forall n \in \mathbb{N} \qquad \sum_{k=0}^{n} \binom{n}{k} B_k - B_n = [n = 1].$$

Il en résulte que l'on a

$$\sum_{n=0}^{\infty}(\sum_{k=0}^{n}\binom{n}{k}B_k)\frac{z^n}{n!}-\sum_{n=0}^{\infty}B_n\frac{z^n}{n!}=\sum_{n=0}^{\infty}[n=1]\frac{z^n}{n!}$$

Ce qui peut s'écrire

$$\left(\sum_{n=0}^{\infty}B_n\frac{z^n}{n!}\right)\left(\sum_{n=0}^{\infty}\frac{z^n}{n!}\right)-\sum_{n=0}^{\infty}B_n\frac{z^n}{n!}=z$$

ou encore

$$\left(\sum_{n=0}^{\infty}B_n\frac{z^n}{n!}\right)(e^z-1)=z,$$

d'où l'on déduit.

$$\sum_{n=0}^{\infty}B_n\frac{z^n}{n!}=\frac{z}{e^z-1}.$$

On a ainsi établi le résultat suivant :

Théorème 2.1. *La série génératrice exponentielle des nombres de bernoulli $(B_n)_{n\in\mathbb{N}}$ est donnée par la relation*

$$\sum_{n=0}^{\infty}B_n\frac{z^n}{n!}=\frac{z}{e^z-1}$$

2.2.3 Définition des polynômes de Bernoulli

Définition 2.2. *On appelle suite des polynômes de Bernoulli la suite de polynômes à coefficients rationnels $(B_n(x))_{n\in\mathbb{N}}$ définie par la relation suivante*

$$B_n(x)=\sum_{k=0}^{n}\binom{n}{k}B_{n-k}x^k \text{ pour } n\geq 0. \tag{2.1}$$

Pour tout entier naturel n, $B_n\ (x)$ est appelé n-ième polynôme de Bernoulli.

Signalons que nous désignons par B_n et $B_n(x)$ respectivement le n-ième nombre de Bernoulli et le e n-ième polynôme de Bernoulli. Cet abus de notation que nous avons adopté ici est d'un usage courant dans la littérature scientifique. A l'aide des définitions des nombres et polynômes de Bernoulli, nous pouvons calculer les expressions des polynômes de Bernoulli $B_n(x)$ pour $0\leq n\leq 7$. On trouve

$$B_0(x)=1,$$

$$B_1(x)=x-\frac{1}{2},$$

$$B_2(x)=x^2-x+\frac{1}{6},$$

$$B_3(x) = x^3 - \frac{3}{2}x^2 - \frac{1}{2}x$$
$$B_4(x) = x^4 - 2x^3 + x^2 - \frac{1}{30},$$
$$B_5(x) = x^5 - \frac{5}{2}x^4 + \frac{5}{3}x^3 - \frac{1}{6}x,$$
$$B_6(x) = x^6 - 3x^5 + \frac{5}{2}x^4 - \frac{1}{2}x^2 - \frac{1}{42},$$

Remarquons que par sa définition même, le polynôme de Bernoulli est un polynôme unitaire et que de plus, on a

$$B_n = B_n(0).$$

2.2.4 Série génératrice exponentielle des polynômes de Bernoulli

Théorème 2.2. *La série génératrice exponentielle des polynômes de bernoulli $(B_n)_{n\in\mathbb{N}}$ est donnée par la relation*

$$\sum_{n=0}^{\infty} B_n(x)\frac{z^n}{n!} = \frac{z}{e^z - 1}e^{xz}$$

Démonstration. Pour $n \geq 0$, on a d'après la relation définissant les polynômes de Bernoulli

$$\begin{aligned}\sum_{n=0}^{\infty} B_n(x)\frac{z^n}{n!} &= \sum_{n=0}^{\infty}\left(\sum_{k=0}^{n}\binom{n}{k}B_{n-k}x^k\right)\frac{z^n}{n!} \\ &= \left(\sum_{n=0}^{\infty} B_n\frac{z^n}{n!}\right)\left(\sum_{n=0}^{\infty} x^n\frac{z^n}{n!}\right) \\ &= \frac{z}{e^z-1}e^{xz}\end{aligned}$$

□

2.3 Propriétés des nombres et polynômes de Bernoulli

2.3.1 Propriétés des nombres de Bernoulli

Nullité des nombres de Bernoulli d'indices impairs supérieurs ou égal à 3

Théorème 2.3. *Pour tout entier $n \geq 1$, on a*

$$B_{2n+1} = 0$$

Démonstration. Posons

$$T(z) = 1 + \sum_{n=2}^{\infty} B_n \frac{z^n}{n!}.$$

Comme $B_0 = 1$ et $B_1 = -\frac{1}{2}$, on a

$$\begin{aligned} T(z) &= \frac{z}{e^z - 1} + \frac{z}{2} \\ &= \frac{z}{2}\left(\frac{e^z + 1}{e^z - 1}\right) \\ &= \frac{z}{2}\left(\frac{e^{\frac{z}{2}} + e^{-\frac{z}{2}}}{e^{\frac{z}{2}} - e^{-\frac{z}{2}}}\right). \end{aligned}$$

Il en résulte que l'on a

$$T(-z) = T(z).$$

$T(z)$ est donc une série formelle paire. Les coefficients d'indices impairs de $T(z)$ sont nuls. On a donc $B_n = 0$, pour n impair avec $n \geq 3$. □

Conséquence : L'expression du n-ième polynôme de Bernoulli se simplifie. On a pour $n \geq 1$:

$$B_n(x) = x^n - \frac{n}{2}x^{n-1} + \sum_{j=1}^{\left[\frac{n}{2}\right]} \binom{n}{2j} B_{2j} x^{n-2j}$$

Expression des nombres de Bernoulli à l'aide des nombres de Stirling de seconde espèce

Théorème 2.4. *Pout tout entier $n \geq 1$, on a*

$$B_n = \sum_{k=0}^{n} (-1)^k \frac{k!}{k+1} \left\{ n \atop k \right\}$$

Démonstration. On a

$$\begin{aligned} z &= \ln(1 + (e^z - 1)) \\ &= \sum_{n=0}^{\infty} (-1)^n \frac{(e^z - 1)^{n+1}}{n+1} \end{aligned}$$

On en déduit que

$$\begin{aligned}\sum_{n=0}^{\infty} B_n \frac{z^n}{n!} &= \frac{z}{e^z-1} = \sum_{k=0}^{\infty}(-1)^k \frac{(e^z-1)^k}{k+1} \\ &= \sum_{k=0}^{\infty}(-1)^k \frac{k!}{k+1}\frac{(e^z-1)^k}{k!} \\ &= \sum_{k=0}^{\infty}(-1)^k \frac{k!}{k+1}\sum_{n=0}^{\infty}\left\{ n \atop k \right\}\frac{z^n}{n!} \\ &= \sum_{n=0}^{\infty}\left(\sum_{k=0}^{n}(-1)^k \frac{k!}{k+1}\left\{ n \atop k \right\}\right)\frac{z^n}{n!}\end{aligned}$$

Ainsi

$$\sum_{n=0}^{\infty} B_n \frac{z^n}{n!} = \sum_{n=0}^{\infty}\left(\sum_{k=0}^{n}(-1)^k \frac{k!}{k+1}\left\{ n \atop k \right\}\right)\frac{z^n}{n!}$$

Par identification on en deduit que

$$B_n = \sum_{k=0}^{n}(-1)^k \frac{k!}{k+1}\left\{ n \atop k \right\}.$$

□

Relation entre les nombres de Bernoulli et la fonction zêta de Riemann

Le mathématicien suisse Leonhard Euler $(1707-1783)$ *est parvenu en 1735 à résoudre à l'age de* 28 *ans un célèbre problème en théorie des nombres, posé en 1644 par Pietro Mengoli. Le problème était le suivant : Déterminer la valeur exacte de la série convergente* $\sum_{n\geq 1}\frac{1}{n^2}$*, autrement la valeur exacte de* $\zeta(2n)$*.Euler prouva que l'on avait*

$$\sum_{n=1}^{\infty}\frac{1}{n^2} = \frac{\pi^2}{6}.$$

Ce problème résolu pour la première fois par Euler est connu sous la dénomination "problème de Bâle", Bâle étant la ville natale d'Euler. Euler prouva aussi le résultat suivant :

Théorème 2.5. *(Théorème d'Euler) Pour tour entier* $n \in \mathbb{N}$*, le nombre* $\frac{\zeta(2n)}{\pi^{2n}}$ *est rationnel.*

Pour une preuve de ce théorème [14]. Il existe donc une suite de rationnels $(\alpha_n)_{n\geq 1}$ *telle que pour tout* $n \in \mathbb{N}$ *on ait :*

$$\frac{1}{1^{2n}} + \frac{1}{2^{2n}} + \frac{1}{3^{2n}}\cdots = \alpha_n \pi^{2n}. \tag{2.2}$$

Selon Niels Nielsen, Euler ne s'aperçut pas tout de suite que les nombres ratinnels α_n étaient liés aux nombres de Bernoulli. Il a fallu, toujours selon Niels Nielsen, une dizaine d'années à Euler pour déchiffrer cette énigme et s'apercevoir que

$$\alpha_n = \frac{(-1)^{n-1}B_{2n}}{2(2n)!} \tag{2.3}$$

Aujourd'hui, ce résulat est bien établi, on a

Théorème 2.6. *[2]. Pour tout entier $n \in \mathbb{N}$, on a*

$$\zeta(2n) = \frac{1}{1^{2n}} + \frac{1}{2^{2n}} + \frac{1}{3^{2n}} \cdots = \frac{(-1)^{n-1}B_{2n}}{2(2n)!}\pi^{2n} \tag{2.4}$$

Remarque 2.1.

$$\zeta(-n) = (-1)^n \frac{B_{n+1}}{n+1}.$$

On a donc

$$B_n = -n\zeta(1-n) \qquad \text{pour } n > 1.$$

Comportement asymptotique de $|B_{2n}|$

On a

$$|B_{2n}| = \frac{(2n)!\zeta(2n)}{2^{2n-1}\pi^{2n}}.$$

De la définition de la fonction zêta de Riemann, on déduit que $\zeta(2n) > 1$ pour $n \geq 1$. Par conséquent, on a la minoration suivante

$$|B_{2n}| > \frac{2(2n)!}{(2\pi)^{2n}}.$$

On en déduit que

$$\lim_{n\to\infty}(|B_{2n}|) = +\infty.$$

En utilisant la formule de Stirling pour écrire un équivalent de $(2n)!$, on démontre que quand n tend vers l'infini on a

$$|B_{2n}| \sim 4\sqrt{\pi n}\left(\frac{n}{\pi e}\right)^{2n}$$

B_{2n} est du signe de $(-1)^{n-1}$

Posons pour tout entier $n \geq 1$,

$$C_n = \frac{(-1)^{n-1}B_{2n}}{(2n)!}.$$

Le lemme suivant va nous être utile pour prouver le théorème 2.7 qui suit.

Lemme 2.1. *Pour tout entier $n \geq 2$, on a*

$$(2^{2n}-1)C_n = \sum_{j=1}^{n-1}(2^{2j}-1)C_jC_{n-j}.$$

Démonstration. Les calculs se faisant dans $\mathbb{C}[[z]]$, on a

$$\begin{aligned}
\frac{z}{e^z+1} &= \frac{z}{e^z-1} - \left(\frac{z}{e^z-1} - \frac{z}{e^z+1}\right) \\
&= \frac{z}{e^z-1} - \frac{2z}{e^{2z}-1} \\
&= \sum_{n=0}^{\infty} B_n\frac{z^n}{n!} - \sum_{n=0}^{\infty} 2^nB_n\frac{z^n}{n!} \\
&= \sum_{n=0}^{\infty}(1-2^n)B_n\frac{z^n}{n!}
\end{aligned}$$

Ainsi, on a

$$\frac{z}{e^z+1} = \sum_{n=0}^{\infty}(1-2^n)B_n\frac{z^n}{n!} \tag{2.5}$$

En mutilpiant par $\frac{z}{e^z-1}$ les deux membres de (2.5), on en déduit que :

$$\frac{z^2}{e^{2z}-1} = \left(\sum_{n=0}^{\infty} B_n\frac{z^n}{n!}\right)\left(\sum_{n=0}^{\infty}(1-2^n)B_n\frac{z^n}{n!}\right) \tag{2.6}$$

On peut alors remarquer que le premier membre de (2.6) peut s'écrire comme suit :

$$\begin{aligned}
\frac{z^2}{e^{2z}-1} &= \frac{z}{2}\left(\frac{2z}{e^{2z}-1}\right), \\
&= \frac{z}{2}\sum_{n=0}^{\infty} 2^nB_n\frac{z^n}{n!}, \\
&= \sum_{n=0}^{\infty} 2^{n-1}B_n\frac{z^{n+1}}{n!}.
\end{aligned} \tag{2.7}$$

De (2.6) et (2.7), on déduit que l'on a

$$\sum_{n=0}^{\infty} 2^{n-1}B_n\frac{z^{n+1}}{n!} = \left(\sum_{n=0}^{\infty} B_n\frac{z^n}{n!}\right)\left(\sum_{n=0}^{\infty}(1-2^n)B_n\frac{z^n}{n!}\right)$$

On a donc pour tout entier $m \geq 2$:

$$\left[z^{2m}\right]\sum_{n=0}^{\infty} 2^{n-1}B_n\frac{z^{n+1}}{n!} = \left[z^{2m}\right]\left(\sum_{n=0}^{\infty} B_n\frac{z^n}{n!}\right)\left(\sum_{n=0}^{\infty}(1-2^n)B_n\frac{z^n}{n!}\right),$$

C'est à dire

$$2^{2m-2}\frac{B_{2m-1}}{(2m-1)!}=\sum_{k=0}^{2m}\frac{B_{2m-k}}{(2m-k)!}\frac{(1-2^k)B_k}{k!} \tag{2.8}$$

Remarquons que m étant ≥ 2, $2m-1$ est un nombre impair ≥ 3. Par conséquent $B_{2m-1}=0$. L'égalité (2.8) devient

$$\sum_{k=0}^{2m}a_k=0 \tag{2.9}$$

avec pour $0\leq k\leq 2m$:

$$a_k=\frac{B_{2m-k}}{(2m-k)!}\frac{(1-2^k)B_k}{k!}.$$

Remarquons maintenant que si k est impair, alors $a_k=0$. En effet, supposons k impair et rappelons nous que les nombres de Bernoulli d'indices impairs ≥ 3 sont nuls. Si $k=1$, on a $2m-k=2m-1\geq 3$ (car $m\geq 2$) et dans ce cas $B_{2m-k}=0$ et par suite $a_k=0$. Si $k\geq 3$, dans ce cas $B_k=0$ et on a encore $a_k=0$. Ainsi dans l'égalité (2.9), les termes a_k d'indices impairs figurant au second membre sont tous nuls. On en déduit de (2.10) que l'on a

$$\sum_{j=0}^{m}a_{2j}=0 \tag{2.10}$$

Comme

$$\begin{aligned}a_{2j} &= \frac{B_{2m-2j}}{(2m-2j)!}\frac{(1-2^{2j})B_{2j}}{(2j)!}\\ &= (1-2^{2j})\left((-1)^{m-j-1}C_{m-j}\right)\left((-1)^{j-1}C_j\right)\\ &= (-1)^{m-1}(2^{2j}-1)C_jC_{m-j}.\end{aligned}$$

L'égalité (2.10) devient

$$(-1)^{m-1}\sum_{j=0}^{m}(2^{2j}-1)C_jC_{m-j}=0$$

C'est à dire

$$\sum_{j=0}^{m}(2^{2j}-1)C_jC_{m-j}=0.$$

On en déduit que

$$-(2^{2m}-1)C_mC_0=\sum_{j=0}^{m-1}(2^{2j}-1)C_jC_{m-j}=0.$$

Comme $C_0 = \frac{(-1)^{-1}B_0}{0!} = -1$, on a bien prouvé que

$$(2^{2m}-1)C_m = \sum_{j=0}^{m-1}(2^{2j}-1)C_jC_{m-j} = 0.$$

En changeant m en n dans cette dernière égalité, on obtient l'égalité recherchée. □

Théorème 2.7. *Pour tout entier $n \geq 1$, on a*

$$(-1)^{n-1}B_{2n} > 0$$

Démonstration. Remarquons que le résultat du théorème est immédiat si on exploite les relations (2.2), (2.3), et (2.4).En effet, on a

$$\begin{aligned}(-1)^{n-1}B_{2n} &= 2(2n)!\alpha_n \\ &= 2(2n)!\frac{\zeta(2n)}{\pi^{2n}} > 0.\end{aligned}$$

Nous allons prouver ce même résultat par une autre méthode. Comme $(2n)!C_n = (-1)^nB_{2n}$, pour prouver le théorème il suffit de prouver que $C_n > 0$, pour tout entier $n \geq 1$. La preuve de ce résultat peut se faire par récurrence sur n, grace au lemme précédent. Désignons $\mathcal{P}\ (n)$ par la propriété

$$C_n > 0$$

On commence par constater que $\mathcal{P}\ (1)$ est vraie. On a en effet

$$C_1 = B_2 = \frac{1}{6} > 0.$$

Supposons que la propriété $\mathcal{P}\ (m)$ soit vraie pour tout entier m tel que $1 \leq j \leq n-1$ et prouvons qu'alors $\mathcal{P}\ (n)$ est vraie. La propriété "$\mathcal{P}\ (m)$ vraie pour tout entier j tel que $1 \leq j \leq n-1$" implique que l'on a $C_j > 0$ et $C_{n-j} > 0$ et donc $(2^{2j}-1)C_jC_{n-j} > 0$ pour tout entier m tel que $1 \leq j \leq n-1$. Il en résulte que $C_n > o$. □

2.3.2 Propriétés des polynômes de Bernoulli

Théorème 2.8. *Pour tout entier naturel n, on a*

1. $B_n'(x) = nB_{n-1}(x)$ *pour* $n \geq 1$,

2. $B_n(x+1) - B_n(x) = nx^{n-1}$ *pour* $n \geq 1$,

3. $B_n(1) = B_n(0)$ *pour* $n \geq 2$,

4. $\int_x^{x+1} B_n(t)dt = x^n$,
5. $B_n(1-x) = (-1)^n B_n(x)$
6. *Dans* $\mathbb{Q}[x,y]$, *on a* $B_n(x+y) = \sum_{k=0}^{n} \binom{n}{k} B_{n-k}(x)y^k = \sum_{k=0}^{n} \binom{n}{k} B_{n-k}(y)x^k$

Démonstration. 1. Soit $n \in \mathbb{N}^*$, on a

$$\begin{aligned} B_n'(x) &= \sum_{k=1}^{n} k\binom{n}{k} B_{n-k}x^{k-1} \\ &= n\sum_{k=1}^{n} \binom{n-1}{k-1} B_{n-k}x^{k-1} \\ &= n\sum_{k=0}^{n-1} \binom{n-1}{k} B_{n-1-k}x^{k} \\ &= nB_{n-1}(x) \end{aligned}$$

2. On a

$$\begin{aligned} \sum_{k=1}^{\infty}(B_n(x+1) - B_n(x))\frac{z^n}{n!} &= \sum_{k=1}^{n} B_n(x+1)\frac{z^n}{n!} - \sum_{k=1}^{n} B_n(x)\frac{z^n}{n!} \\ &= \frac{z}{e^z-1}e^{(x+1)z} - \frac{z}{e^z-1}e^{xz} \\ &= \frac{z}{e^z-1}e^{xz}(e^z-1) \\ &= ze^{xz} \\ &= \sum_{n=0}^{\infty} x^n \frac{z^{n+1}}{n!} \\ &= \sum_{n=1}^{\infty} x^{n-1}\frac{z^n}{(n-1)!} \\ &= \sum_{n=1}^{\infty} nx^{n-1}\frac{z^n}{n!} \end{aligned}$$

Ainsi

$$\sum_{k=1}^{\infty}(B_n(x+1) - B_n(x))\frac{z^n}{n!} = \sum_{n=1}^{\infty} nx^{n-1}\frac{z^n}{n!}$$

En identifiant pour $n \geq 1$ les coefficients de $\frac{z^n}{n!}$ dans chacun des deux membres de cette dernière égalité, on obtient la relation cherchée.

3. Pour $n \geq 2$, en remplaçant x par 0 dans l'égalité 2 précédente on obtient :

$$B_n(1) - B_n(0) = n0^{n-1} = 0$$

4. Pour $n \geq 0$, on a

$$\begin{aligned}
\int_x^{x+1} B_n(t)dt &= \int_x^{x+1} \frac{B'_{n+1}(t)}{n+1}dt \\
&= \left[\frac{B_{n+1}(t)}{n+1}\right]_x^{x+1} \\
&= \frac{B_{n+1}(x+1) - B_{n+1}(x)}{n+1} \\
&= x^n
\end{aligned}$$

5.

$$\begin{aligned}
\sum_{n=0}^{\infty} B_n(1-x)\frac{z^n}{n!} &= \frac{z}{e^z-1}e^{(1-x)z} \\
&= \frac{ze^z}{e^z-1}e^{-xz} \\
&= \frac{z}{1-e^{-z}}e^{-xz} \\
&= \frac{-z}{e^{-z}-1}e^{x(-z)} \\
&= \sum_{n=0}^{\infty} B_n(x)\frac{(-z)^n}{n!} \\
&= \sum_{n=0}^{\infty}(-1)^n B_n(x)\frac{z^n}{n!}
\end{aligned}$$

Ainsi on a

$$\sum_{n=0}^{\infty} B_n(1-x)\frac{z^n}{n!} = \sum_{n=0}^{\infty}(-1)^n B_n(x)\frac{z^n}{n!}$$

On en déduit que pour tout entier $n \geq 0$, on a

$$\left[\frac{z^n}{n!}\right]\sum_{m=0}^{\infty} B_m(1-x)\frac{z^m}{m!} = \left[\frac{z^n}{n!}\right]\sum_{n=0}^{\infty}(-1)^n B_n(x)\frac{z^n}{n!},$$

c'est à dire

$$B_n(1-x) = (-1)^n B_n(x).$$

6. Dans $\mathbb{C}[[x,y]]$, on a

$$\begin{aligned}\sum_{n=0}^{\infty} B_n(x+y)\frac{z^n}{n!} &= \frac{z}{e^z-1}e^{(x+y)z} \\ &= \left(\frac{z}{e^z-1}e^{xz}\right)e^{yz}\end{aligned}$$

Ainsi, on a

$$\sum_{n=0}^{\infty} B_n(x+y)\frac{z^n}{n!} = \left(\sum_{n=0}^{\infty} B_n(x)\frac{z^n}{n!}\right)\left(\sum_{n=0}^{\infty} y^n\frac{z^n}{n!}\right).$$

On en déduit que :

$$[z^n]\sum_{m=0}^{\infty} B_m(x+y)\frac{z^m}{m!} = [z^n]\left(\sum_{k=0}^{\infty} B_k(x)\frac{z^k}{k!}\right)\left(\sum_{n=0}^{\infty} y^l\frac{z^l}{l!}\right).$$

C'est à dire :

$$\frac{1}{n!}B_n(x+y) = \sum_{k=0}^{n}\frac{B_k(x)}{k!}\frac{y^{n-k}}{(n-k)!}$$

D'où l'on déduit

$$B_n(x+y) = \sum_{k=0}^{n}\binom{n}{k}B_k(x)y^{n-k}.$$

En échangeant le rôle de x et y, on on obtient aussi

$$B_n(x+y) = \sum_{k=0}^{n}\binom{n}{k}B_k(y)x^{n-k}.$$

□

Théorème 2.9. *Formule de Raabe : Pour tous entier $n \geq 0$ et $m \geq 1$, on a*

$$B_n(x) = m^{n-1}\sum_{k=0}^{m-1} B_n\left(\frac{x+k}{m}\right) \tag{2.11}$$

Démonstration. soit un entier $m \geq 1$, on a

$$\begin{aligned}
\sum_{n=0}^{\infty}\left(\sum_{k=0}^{m-1} B_n(\frac{x+k}{m})\right)\frac{z^n}{n!} &= \sum_{k=0}^{m-1}\left(\sum_{n=0}^{\infty}(B_n(\frac{x+k}{m}))\frac{z^n}{n!}\right) \\
&= \sum_{k=0}^{m-1}\frac{z}{e^z-1}e^{(\frac{x+k}{m})z} \\
&= \frac{z}{e^z-1}e^{\frac{xz}{m}}\sum_{k=0}^{m-1}(e^{\frac{z}{m}})^k \\
&= \frac{z}{e^z-1}e^{\frac{xz}{m}}\frac{e^z-1}{e^{\frac{z}{m}}-1} \\
&= m\frac{\frac{z}{m}}{e^{\frac{z}{m}}-1}e^{\frac{z}{m}x} \\
&= m\sum_{n=0}^{\infty}B_n(x)\frac{z^n}{n!m^n} \\
&= \sum_{n=0}^{\infty}\frac{1}{m^{n-1}}B_n(x)\frac{z^n}{n!}.
\end{aligned}$$

On en déduit par identification que

$$\sum_{k=0}^{m-1} B_n(\frac{x+k}{m}) = \frac{1}{m^{n-1}}B_n(x).$$

Peut s'écrire aussi

$$B_n(x) = m^{n-1}\sum_{k=0}^{m-1} B_n(\frac{x+k}{m}).$$

□

Théorème 2.10. *On a.*

1. $$B_n(1) = B_n + [n=1]$$

Pour n pair, on a

2. $$B_n(\frac{1}{2}) = (2^{1-n}-1)B_n$$

3. $$B_n(\frac{1}{3}) = B_n(\frac{2}{3}) = \frac{1}{2}(3^{1-n}-1)B_n$$

4. $$B_n(\frac{1}{4}) = B_n(\frac{3}{4}) = \frac{1}{2}(4^{1-n}-2^{1-n})B_n$$

5.

$$B_n(\frac{1}{6}) = B_n(\frac{5}{4}) = \frac{1}{2}(6^{1-n} - 3^{1-n} - 2^{1-n} + 1)B_n$$

Démonstration. 1. La relation 2 du théorème 2.8 permet d'affirmer que pour $n \geq 2$

$$B_n(1) = B_n(0)$$

Pour $n = 0$, on a aussi

$$B_0(1) = B_0(0) = 1,$$

alors que pour $n = 1$, on a

$$B_1(1) = \frac{1}{2} = B_1 + 1 = B_1 + [n = 1]\,.$$

La relation est bien vérifiée.

2. Dans tout ce qui suit, on suppose n pair.
3. Appliquons la relation (2.11) pour $m = 2$, on obtient

$$B_n(x) = 2^{n-1}\left(B_n(\frac{x}{2}) + B_n(\frac{x+1}{2})\right).$$

Pour $x = 0$, cette relation devient

$$B_n = 2^{n-1}\left(B_n + B_n(\frac{1}{2})\right).$$

D'où l'on déduit :

$$B_n(\frac{1}{2}) = (2^{1-n} - 1)B_n$$

4. Appliquons la relation (2.11) pour $m = 3$, on obtient

$$B_n(x) = 3^{n-1}\left(B_n(\frac{x}{3}) + B_n(\frac{x+1}{3}) + B_n(\frac{x+2}{3})\right).$$

Pour $x = 0$, cette relation devient

$$B_n = 3^{n-1}\left(B_n + B_n(\frac{1}{3}) + B_n(\frac{2}{3})\right). \tag{2.12}$$

Mais on sait d'après la relation 5 du théorème 2.11 que $B_n(1-x) = (-1)^n B_n(x)$, ce qui permet d'affirmer pour $x = \frac{1}{3}$ et pour n pair que l'on a

$$B_n(\frac{2}{3}) = B_n(\frac{1}{3})$$

La relation (2.12) peut donc s'écrire pour n pair

$$B_n = 3^{n-1}\left(B_n + 2B_n(\frac{1}{3})\right).$$

On en déduit que

$$B_n(\frac{1}{3}) = B_n(\frac{2}{3}) = \frac{1}{2}(3^{1-n} - 1)B_n$$

5. Appliquons la relation (2.11) pour $m = 4$, on obtient

$$B_n(x) = 4^{n-1}\left(B_n(\frac{x}{4}) + B_n(\frac{x+1}{4}) + B_n(\frac{x+2}{4}) + B_n(\frac{x+3}{4})\right).$$

Pour $x = 0$, cette relation devient

$$B_n = 4^{n-1}\left(B_n + B_n(\frac{1}{4}) + B_n(\frac{1}{2}) + B_n(\frac{3}{4})\right).$$

Or on sait que

$$B_n(\frac{3}{4}) = B_n(\frac{1}{4}) \quad \text{et} \quad B_n(\frac{1}{2}) = (2^{1-n} - 1)B_n \ .$$

On a donc

$$B_n = 4^{n-1}\left(B_n + 2B_n(\frac{1}{4}) + (2^{1-n} - 1)B_n \ \right).$$

On en déduit que

$$B_n(\frac{1}{4}) = B_n(\frac{3}{4}) = \frac{1}{2}(4^{1-n} - 2^{1-n})B_n$$

6. Appliquons la relation (2.11) pour $m = 6$, on obtient

$$B_n(x) = 4^{n-1}\left(B_n(\frac{x}{6}) + B_n(\frac{x+1}{6}) + B_n(\frac{x+2}{6}) + B_n(\frac{x+3}{6}) + B_n(\frac{x+4}{6}) + B_n(\frac{x+5}{6})\right).$$

Pour $x = 0$, cette relation devient

$$B_n = 4^{n-1}\left(B_n + B_n(\frac{1}{6}) + B_n(\frac{1}{3}) + B_n(\frac{1}{2}) + B_n(\frac{2}{3}) + B_n(\frac{5}{6})\right). \qquad (2.13)$$

On sait que

$$B_n(\frac{5}{6}) = B_n(\frac{1}{6}) \quad , B_n(\frac{2}{3}) = B_n(\frac{1}{3}) = \frac{1}{2}(3^{1-n} - 1)B_n \quad \text{et} \quad B_n(\frac{1}{2}) = (2^{1-n} - 1)B_n$$

En substituant ces valeurs dans (2.13), on obtient

$$B_n = 4^{n-1}\left(B_n + 2B_n(\frac{1}{6}) + (3^{1-n} - 1)B_n + (2^{1-n} - 1)B_n)\right).$$

On en déduit la relation

$$B_n(\frac{1}{6}) = B_n(\frac{5}{4}) = \frac{1}{2}(6^{1-n} - 3^{1-n} - 2^{1-n} + 1)B_n$$

□

Remarque 2.2. *Pour $n \geq 3$ impair, on a $B_n = 0$ et donc d'après la relation 2 du théorème précédent on a $B_n(\frac{1}{2}) = 0$. Pour $n = 1$, on a aussi $B_n(\frac{1}{2}) = 0$. Il en résulte que pour $n \geq 1$ impair, le polynôme $B_n(x)$ est divisible par $2x-1$.Comme on a aussi $B_n(1) = B_n(0)$ pour $n \geq 3$ impair, il en résulte que le polynôme $B_n(x)$ est divisible par $x(x-1)(2x-1)$ pour $n \geq 3$ impair. On vérifie qu'on a en particulier*

$$B_1(x) = \frac{1}{2}(2x-1)$$

$$B_3(x) = \frac{1}{2}x(x-1)(2x-1)$$

$$B_5(x) = \frac{1}{6}x(x-1)(2x-1)(3x^2-3x-1)$$

$$B_7(x) = \frac{1}{6}x(x-1)(2x-1)(3x^4-6x^3+3x+1)$$

Théorème 2.11. *Formules de Faulhaber*

1.

$$1^m + 2^m + \cdots + (n-1)^m = \frac{1}{m+1}(B_{m+1}(n) - B_{m+1})$$

2.

$$\begin{aligned} 1^m + 2^m + \cdots + (n-1)^m &= \frac{1}{m+1}\sum_{k=0}^{m}\binom{m+1}{k}B_k n^{m+1-k} \\ &= \frac{1}{m+1}\sum_{k=1}^{m+1}\binom{m+1}{k}B_{m+1-k}n^k \\ &= \frac{1}{m+1}n^{m+1} - \frac{1}{2}n^m + \frac{1}{m+1}\sum_{k=1}^{\left[\frac{m}{2}\right]}\binom{m+1}{2k}B_{2k}n^{m+1-2k}. \end{aligned}$$

3.

$$\begin{aligned} 1^m + 2^m + \cdots + n^m &= \frac{1}{m+1}\sum_{k=0}^{m}\binom{m+1}{k}(-1)^k B_k n^{m+1-k} \\ &= \frac{1}{m+1}n^{m+1} + \frac{1}{2}n^m + \frac{1}{m+1}\sum_{k=1}^{\left[\frac{m}{2}\right]}\binom{m+1}{2k}B_{2k}n^{m+1-2k}. \end{aligned}$$

Démonstration. 1. La relation 2 du théorème (2.11) implique que pour tous entier k et m, on a

$$k^m = \frac{1}{m+1}\left(B_{m+1}(k+1) - B_{m+1}(k)\right).$$

Il en résulte que

$$\begin{aligned} 1^m + 2^m + \cdots + (n-1)^m &= \frac{1}{m+1} \sum_{k=0}^{n-1} B_{m+1}(k+1) - B_{m+1}(k) \\ &= \frac{1}{m+1}(B_{m+1}(n) - B_{m+1}). \end{aligned}$$

2. D'après l'expression du n-ième polynôme de Bernoulli, on a

$$\begin{aligned} B_{m+1}(x) &= \sum_{k=0}^{m+1} \binom{m+1}{k} B_{m+1-k} x^k \\ &= \sum_{k=0}^{m+1} \binom{m+1}{k} B_k x^{m+1-k} \end{aligned}$$

3. En remarquant que pour tout entier naturel k,

$$B_k + [k=1] = (-1)^k B_k.$$

On a

$$\begin{aligned} 1^m + 2^m + \cdots + n^m &= 1^m + 2^m + \cdots + (n-1)^m + n^m \\ &= \frac{1}{m+1} \sum_{k=0}^{m} \binom{m+1}{k} B_k n^{m+1-k} + \frac{1}{m+1} \sum_{k=0}^{m} \binom{m+1}{k} B_k . [k=1] . n^{m+1} \\ &= \frac{1}{m+1} \sum_{k=0}^{m} \binom{m+1}{k} (B_k + [k=1]) . n^{m+1-k} \\ &= \frac{1}{m+1} \sum_{k=0}^{m} \binom{m+1}{k} (-1)^k B_k n^{m+1-k} \\ &= \frac{1}{m+1} n^{m+1} + \frac{1}{2} n^m + \frac{1}{m+1} \sum_{k=1}^{\left[\frac{m}{2}\right]} \binom{m+1}{2k} B_{2k} n^{m+1-2k}. \end{aligned}$$

□

Chapitre 3

Théorème de Von-Staudt et Clausen

3.1 Introduction

Rappelons que les nombres de Bernoulli d'indices impairs supérieurs ou égaux à 3 *sont nuls. Intéressons nous donc aux nombres de Bernoulli d'indices pairs. Pour tout entier* $n \geq 1$*, désignons par* $\mathcal{D}_n$ *l'ensemble diviseurs de* n*. dans* $\mathbb{N}$*, par* $\mathcal{D}_n^{+1} = \{d+1 \mid d \in \mathcal{D}_n\}$ *et par* Ω_n*, l'ensemble des diviseurs premiers de l'entier* n*. Un entier* $n \geq 1$ *est dit sans facteur carré s'il n'est divisible par aucun carré d'entier autre que* 1*. Il est facile de constater que les entiers sans facteur carré (appelés aussi entiers libres de carrés ou squarefree) sont les entiers qui sont égaux au produit de leurs diviseurs premiers. Désignons aussi par* $\mathcal{P} = \{2, 3, 5, 7, 11, 13, 17...\}$ *l'ensemble des nombres premier. On peut remarquer que l'on a*

$$B_2 = \frac{1}{6}.$$

Observons que le dénominateur de B_2 *est égal à* 6*, qu'il est sans facteur carré puisque* $6 = 2 \times 3$*, que* $\Omega_6 = \{2, 3\}$ *et que de plus* $\mathcal{D}_2 = \{1, 2\}$*,* $\mathcal{D}_2^{+1} = \{2, 3\}$ *et* $\mathcal{D}_2^{+1} \cap \mathcal{P} = \{2, 3\} = \Omega_6$*. Autrement dit, on a*

$$denom(B_2) = 6 \quad et \quad \Omega_6 = \mathcal{D}_2^{+1} \cap \mathcal{P}.$$

On peut aussi remarquer que l'on a

$$B_4 = -\frac{1}{30}.$$

Le dénominateur de B_4 *est égal à* 30*. On a* $30 = 2 \times 3 \times 5$*. Le dénominateur de* B_4 *est sans facteur carré. On a encore* $\Omega_{30} = \{2, 3, 5\}$*. De plus* $\mathcal{D}_4 = \{1, 2, 4\}$*,* $\mathcal{D}_4^{+1} = \{2, 3, 5\}$*. On a encore* $\mathcal{D}_4^{+1} \cap \mathcal{P} = \{2, 3, 5\} = .\Omega_{30}$

$$denom(B_4) = 30 \quad et \quad \Omega_{30} = \mathcal{D}_4^{+1} \cap \mathcal{P}.$$

La même observation peut-être faite pour les nombres de Bernoulli suivant, on constate que si D_n *désigne le dénominateur de* B_{2n}*, alors* D_n *est un entier sans facteur carré et que de plus*

$$denom(B_{2n}) = D_n \quad et \quad \Omega_{D_n} = \mathcal{D}_{2n}^{+1} \cap \mathcal{P}.$$

Ainsi le dénominateur D_n serait un entier sans facteur carré vérifiant l'égalité suivante

$$denom(B_{2n}) = \prod_{p-1 \ divise \ 2n} p,$$

ce produit étant étendu aux nombres premiers p tels que $p-1$ soit un diviseur de $2n$.

En 1840 Karl Georg Christian von Staudt (1798-1867) et Thomas Clausen (1798-1867) ont indépendamment l'un de l'autre découvert le théorème duquel on peut déduire et donc prouver l'observation précédente.

Théorème 3.1. *Théorème de Von Staudt et Clausen (1840) : Pour tout entier $n \geqslant 1$, on a*

$$(B_{2n} + \sum_{p-1 \ divise \ 2n} \frac{1}{p}) \in \mathbb{Z},$$

la sommation portant sur tous les nombres premiers p tels que $p-1$ soit un diviseur l'entier $2n$.

Posons pour tout entier $n \geq 1$

$$I_{2n} = B_{2n} + \sum_{p-1 \ divise \ 2n} \frac{1}{p}$$

On vérifie que l'on a

$$I_2 = (\frac{1}{6}) + \frac{1}{2} + \frac{1}{3} = 1$$

$$I_4 = (-\frac{1}{30}) + \frac{1}{2} + \frac{1}{3} + \frac{1}{5} = 1$$

$$I_6 = (\frac{1}{42}) + \frac{1}{2} + \frac{1}{3} + \frac{1}{7} = 1$$

$$I_8 = (-\frac{1}{30}) + \frac{1}{2} + \frac{1}{3} + \frac{1}{5} = 1$$

$$I_{10} = (\frac{5}{66}) + \frac{1}{2} + \frac{1}{3} + \frac{1}{11} = 1$$

$$I_{12} = (-\frac{691}{2730}) + \frac{1}{2} + \frac{1}{3} + \frac{1}{5} + \frac{1}{7} + \frac{1}{13} = 1$$

On constate que l'on a $I_2 = I_4 = I_6 = I_8 = I_{10} = I_{12} = 1$. La suite de rationnels $(I_{2n})_{n \geq 1}$ qui selon le théorème de Von staudt et Clausen est une suite d'entiers semble stationnaire. On a déjà une expression simple des nombres de Bernoulli B_{2n} pour $1 \leq n \leq 6$:

$$\forall n \in \{1,2,3,4,5,6\} \qquad B_{2n} = 1 - \sum_{p-1 \ divise \ 2n} \frac{1}{p}.$$

Le calcul de I_{14} et I_{16} donne

$$I_{14} = (\frac{7}{6}) + \frac{1}{2} + \frac{1}{3} = 2$$

$$I_{16} = (-\frac{3617}{510}) + \frac{1}{2} + \frac{1}{3} + \frac{1}{5} + \frac{1}{17} = -6$$

La suite d'entiers $(I_{2n})_{n\geq 1}$ *n'est donc pas stationnaire. On pourrait penser, au vu des résultats précédents, que les valeurs entières de* I_{2n} *sont simples. il n'en est rien car le calcul de* I_{18}, I_{20}, I_{22}, I_{24} , I_{26} *et* I_{28} *donne des résultats surprenants et imprévisibles :*

$$I_{18} = (\frac{43867}{798}) + \frac{1}{2} + \frac{1}{3} + \frac{1}{7} + \frac{1}{19} = 56$$

$$I_{20} = (-\frac{174611}{330}) + \frac{1}{2} + \frac{1}{3} + \frac{1}{5} + \frac{1}{11} = -528$$

$$I_{22} = (\frac{854513}{138}) + \frac{1}{2} + \frac{1}{3} + \frac{1}{23} = 6193$$

$$I_{24} = (-\frac{236364091}{2730}) + \frac{1}{2} + \frac{1}{3} + \frac{1}{5} + \frac{1}{7} + \frac{1}{13} = -86579$$

$$I_{26} = (\frac{8553103}{6}) + \frac{1}{2} + \frac{1}{3} = 1425518$$

$$I_{28} = (-\frac{23749461029}{890}) + \frac{1}{2} + \frac{1}{3} + \frac{1}{5} + \frac{1}{29} = -27298230$$

Le fait que $I_{14} = -86579$ *et que* 86579 *est un nombre premier rend plutôt illusoire la recherche d'une formule simple exprimant* I_{2n} *en fonction de* n. *Signalons qu'en* 1875, *Hermite calcula les nombres* I_{2n} *jusqu'à* I_{18} *et qu'en* 1967, *Donald E. Knuth et Thomas J. Buckholtz ont déterminé des tables pour les nombres* I_{2n}. *La suite* $(I_{2n})_{n\geq 1}$ *est repertoriée dans l'encyclopédie des suites d'entiers Sloane en ligne, sous la référence* A000146.

Dans ce chapitre, nous prouvons le théorème de Von Staudt et Clausen de deux manières différentes. La première est une démonstration par récurrence reposant sur certaines propriétés des p-entiers. La seconde démonstration de ce théorème repose sur des congruences concernant les nombres de Stirling de deuxième espèce $\left\{ {n \atop k} \right\}$ *et sur la formule suivante prouvée au chapitre 2.*

$$B_n = \sum_{k=0}^{n} (-1)^k \frac{k!}{k+1} \left\{ {n \atop k} \right\}.$$

Nous déduisons ensuite du théorème de Von Staudt et Clausen une expression du dénominareur du nombre de Bernoulli B_{2n}. *Nous terminerons ce chapitre par l'énoncé d'un théorème de Kummer concernant des congruences pour les nombres de Bernoulli . Ces deux théorèmes nous permettent alors de prouver d'importantes congruences concernant les sommes* $S_n(p-1)$ *et* $H_{p-1}^{(n)}$*pour* p *premier et* n *entier.*

3.2 Première démonstration du théorème de Von Staudt et Clausen

Cette preuve repose sur les lemmes suivants :

Lemme 3.1. *Pour tout nombre premier p et pout tout entier $m \geq 2$, on a*

1. $p^{m+1} > m+2$
2. $\frac{p^m}{m+2} \in \mathbb{Z}(p)$

Démonstration. 1. Pour tout nombre premier p et pout tout entier $m \geq 2$, on a

$$p^{m+1} \geq 2^{m+1} = (1+1)^{m+1} = \sum_{k=0}^{m+1} \binom{m+1}{k} > \sum_{k=0}^{1} \binom{m+1}{k} = \binom{m+1}{0} + \binom{m+1}{1} = m+2$$

2. Raisonnons par l'absurde. si on avait $\frac{p^m}{m+2} \notin \mathbb{Z}(p)$, on aurait

$$p^{m+1} \mid m+2, \quad \text{ce n'est pas le cas car} \quad p^{m+1} > m+2$$

d'où l'on a

$$\frac{p^m}{m+2} \in \mathbb{Z}(p)$$

□

Lemme 3.2. *Pour tout entier $m \geq 1$, on a*

$$S_m(p-1) + [(p-1) \text{ divise } m] \equiv 0 \pmod{p}$$

Démonstration. Remarquons tout d'abord que grâce au petit théorème de Fermat, on a pour tous entiers m et n

$$m \equiv n (\mathrm{mod}(p-1)) \Longrightarrow S_m(p-1) \equiv S_n(p-1) \pmod{p}.$$

En effet, pour $1 \leq k \leq p-1$, on a k premier avec p et donc si

$$k^{p-1} \equiv 1 \pmod{p}.$$

Si $m \equiv n \pmod{(p-1)}$, on peut supposer sans perte de généralité que $m \geq n$, on a alors

$$m = n + r(p-1),$$

où r est un entier naturel. Alors

$$k^m = k^{n+r(p-1)} = (k^n)(k^{p-1})^r \equiv k^n \pmod{p}.$$

Il en résulte que

$$\sum_{k=1}^{p-1} k^m \equiv \sum_{k=1}^{p-1} k^n \pmod{p},$$

c'est à dire

$$S_m(p-1) \equiv S_n(p-1) \pmod{p}$$

Soit maintenant un entier $m \geq 1$, distinguons deux cas

1. Premier cas : $p-1$ divise m. Dans ce cas, on a $m \equiv 0 \ (\mathrm{mod}(p-1))$ et donc $S_m(p-1) \equiv S_0(p-1) = p-1 \equiv -1 \pmod{p}$ Dans ce cas on a bien

$$S_m(p-1) + [(p-1) \text{ divise } m] \equiv 0 \pmod{p}$$

2. Deuxième cas : $p-1$ ne divise pas m. Dans ce cas, on a $m \equiv n \ (\mathrm{mod}(p-1))$ avec $n \in \{1, 2..p-1\}$ et $S_m(p-1) \equiv S_n(p-1) \pmod{p}$. On a a alors

$$S_n(p-1) = \sum_{k=1}^{p-1} k^n = \sum_{k=0}^{p-1} k^n.$$

On sait que

$$k^n = \sum_{j=0}^{n} \left\{ {n \atop k} \right\} k^{\underline{j}}$$

On a donc

$$\begin{aligned} S_n(p-1) &= \sum_{k=0}^{p-1} \left(\sum_{j=0}^{n} \left\{ {n \atop k} \right\} k^{\underline{j}} \right) \\ &= \sum_{j=0}^{n} \left(\sum_{k=0}^{p-1} \left\{ {n \atop k} \right\} k^{\underline{j}} \right) \\ &= \sum_{j=0}^{n} \left(\left\{ {n \atop k} \right\} \sum_{k=0}^{p-1} k^{\underline{j}} \right) \end{aligned} \tag{3.1}$$

On constate alors que

$$\sum_{k=0}^{p-1} k^{\underline{j}} = \frac{p^{\underline{j+1}}}{j+1}$$

En effet on a

$$\Delta(x^{\underline{j+1}}) = (j+1)x^{\underline{j}}$$

On a donc

$$k^{\underline{j+1}} = \frac{1}{j+1} \left((k+1)^{\underline{j+1}} - k^{\underline{j+1}} \right)$$

et par conséquent

$$\begin{aligned} \sum_{k=0}^{p-1} k^{\underline{j}} &= \frac{1}{j+1} \sum_{k=0}^{p-1} \left((k+1)^{\underline{j+1}} - k^{\underline{j+1}} \right) \\ &= \frac{1}{j+1} \left((p^{\underline{j+1}} - 0^{\underline{j+1}} \right) \\ &= \frac{p^{\underline{j+1}}}{j+1}. \end{aligned}$$

La relation (3.1) devient

$$S_n(p-1) = \sum_{j=0}^{n} \left(\left\{ {n \atop k} \right\} \frac{p^{\underline{j+1}}}{j+1}. \right)$$

Comme $j+1 \in \{1, n+1\}$ et que $\{1, n+1\} \subset \{1, p-2\}$, on a $\frac{1}{j+1} \left\{ {n \atop k} \right\} \in \mathbb{Z}_{(p)}$. En remarquant que $p^{\underline{j+1}} = p(p-1)...(p-j) \equiv 0 \pmod{p}$, on en conclut que

$$S_m(p-1) \equiv S_n(p-1) \equiv 0 \pmod{p}.$$

Dans ce cas on a encore

$$S_m(p-1) + [(p-1) \text{ divise } m] \equiv 0 \pmod{p}.$$

□

Remarque 3.1. *Le lemme 3.2 est aussi une conséquence immédiate du théorème 1.14.*

Lemme 3.3. *Pour tout entier $n \geq 2$, on a*

$$B_{2n} + \frac{[(p-1) \text{ divise } 2n]}{p} - \frac{1}{2}p^{2n-1} + \sum_{k=1}^{2n-2} \frac{p^{2n-k-1}}{2n-2k+1} \binom{2n}{2k} (pB_{2k}) \in \mathbb{Z}.$$

Démonstration. D'après la formule de Faulhaber, on a

$$\begin{aligned}
S_{2n}(p-1) &= \frac{1}{2n+1} \left(B_{2n+1}(p) - B_{2n+1} \right) \\
&= \frac{1}{2n+1} \sum_{k=1}^{2n} \binom{2n+1}{2n+1-k} B_k p^{2n+1-k} \\
&= \frac{1}{2n+1} \binom{2n+1}{1} B_1 p^{2n} + \sum_{k=2}^{2n-2} \frac{1}{2n+1} \binom{2n+1}{2n+1-k} B_k p^{2n+1-k} + \\
&\quad \frac{1}{2n+1} \binom{2n+1}{2} B_{2n-1} p^2 + \frac{1}{2n+1} \binom{2n+1}{1} B_{2n} p \\
&= B_1 p^{2n} + \sum_{k=2}^{2n-2} \frac{1}{2n+1} \binom{2n+1}{2n+1-k} B_k p^{2n+1-k} + n B_{2n-1} p^2 + B_{2n} p \\
&= -\frac{1}{2}p^{2n} + \sum_{k=2}^{2n-2} \frac{1}{2n+1-k} \binom{2n}{2n-k} B_k p^{2n+1-k} + n B_{2n-1} p^2 + B_{2n} p. \quad (3.2)
\end{aligned}$$

Si on suppose $n \geq 2$, on a $B_{2n-1} = 0$, et que $B_k = 0$, pour k impair et $2 \leq k \leq 2n-2$; la formule (3.2) devient

$$S_{2n}(p-1) = B_{2n} p - \frac{1}{2}p^{2n} + \sum_{k=1}^{n-1} \binom{2n}{2k} B_{2k} \frac{p^{2n-2k+1}}{2n-2k+1} \quad (3.3)$$

Remarquons alors que La formule (3.3) peut donc s'écrire

$$S_{2n}(p-1) = p\left(B_{2n} - \frac{1}{2}p^{2n-1} + \sum_{k=1}^{2n-2} \frac{1}{2n-2k+1}\binom{2n}{2k} B_{2k} p^{2n-2k}\right) \tag{3.4}$$

Or on sait d'après le lemme 3.2 que l'on a

$$S_{2n}(p-1) + [(p-1) \text{ divise } 2n] \in p\mathbb{Z}$$

On déduit avec (3.4) que

$$p\left(B_{2n} - \frac{1}{2}p^{2n-1} + \sum_{k=1}^{n-1} \frac{1}{2n-2k+1}\binom{2n}{2k} B_k p^{2n-k}\right) + [(p-1) \text{ divise } 2n] \in p\mathbb{Z}$$

En divisant par p les deux membres de l'égalité précédente, on obtient,

$$B_{2n} - \frac{1}{2}p^{2n-1} + \sum_{k=1}^{n-1} \frac{1}{2n-2k+1}\binom{2n}{2k} B_{2k} p^{2n-2k} + \frac{[(p-1) \text{ divise } 2n]}{p} \in \mathbb{Z}$$

Ce qu'on peut encore écrire

$$B_{2n} + \frac{[(p-1) \text{ divise } 2n]}{p} - \frac{1}{2}p^{2n-1} + \sum_{k=1}^{2n-2} \frac{p^{2n-k-1}}{2n-2k+1}\binom{2n}{2k} (pB_{2k}) \in \mathbb{Z}.$$

ce qui est bien la relation du lemme 3.3. Nous sommes maintenant en mesure de prouver le théorème de Von Staudt et Clausen □

Première démonstration du théorème de Von Staudt et Clausen. *Desi-gnons par $\mathfrak{P}(n)$ la propriété suivante*

$$\textit{Pour tout nombre premier } p, \textit{ on a } B_{2n} + \frac{[(p-1) \textit{ divise } 2n]}{p} \in \mathbb{Z}_{(p)}.$$

Raisonnons par récurrence sur l'entier $n \in \mathbb{N}^*$ pour prouver que pour tout entier $n \in \mathbb{N}^*$, la proriété $\mathfrak{P}(n)$ est vraie. $\mathfrak{P}(1)$ est vraie car en remarquant que les seuls nombres premiers p tels que $p-1$ divise 2 sont 2 et 3, on a

$$B_2 + \frac{[(p-1) \textit{ divise } 2]}{p} = \frac{1}{6} + \frac{[(p-1) \textit{ divise } 2]}{p} = \begin{cases} \frac{1}{6} + \frac{1}{2} = \frac{1}{3} \in \mathbb{Z}_{(p)} = \mathbb{Z}_{(2)} \textit{ si } p = 2 \\ \frac{1}{6} + \frac{1}{3} = \frac{1}{2} \in \mathbb{Z}_{(p)} = \mathbb{Z}_{(3)} \textit{ si } p = 3 \\ \frac{1}{6} \in \mathbb{Z}_{(p)} \textit{ si } p \neq 2 \textit{ et } p \neq 3. \end{cases}.$$

et donc , on a bien

$$\textit{Pour tout nombre premier } p, \textit{ on a } B_2 + \frac{[(p-1) \textit{ divise } 2]}{p} \in \mathbb{Z}_{(p)}.$$

et $\mathfrak{P}(1)$ *est bien vraie.*

Supposons maintenant que $n \geq 2$ *et que* $\mathfrak{P}(k)$ *soit vraie pour tout entier* $k \in \{1, 2, ..., n-1\}$. *Dans ce cas pour tout entier* $k \in \{1, 2, ..., n-1\}$, *on a*

Pour tout nombre premier p, on a $pB_{2k} + [(p-1)\ divise\ 2k] \in p\mathbb{Z}_{(p)}$

et comme $p\mathbb{Z}_{(p)} \subset \mathbb{Z}_{(p)}$ *et que* $[(p-1)\ divise\ 2k] \in \{0, 1\} \subset \mathbb{Z}_{(p)}$, *on en deduit que pour tout nombre premier p, on a d'après une conséquence de l'hypothèse de récurrence :*

$$\forall k \in \{1, 2, ..., n-1\} \quad pB_{2k} \in \mathbb{Z}_{(p)} \tag{3.5}$$

Exploitons maintenant la relation du lemme 3.3

$$B_{2n} + \frac{[(p-1)\ divise\ 2n]}{p} - \frac{1}{2}p^{2n-1} + \sum_{k=1}^{2n-2} \frac{p^{2n-k-1}}{2n-2k+1}\binom{2n}{2k}(pB_{2k}) \in \mathbb{Z}. \tag{3.6}$$

On a pour tout nombre premier p

$$-\frac{1}{2}p^{2n-1} \in \mathbb{Z}_{(p)}. \tag{3.7}$$

Pour $1 \leq k \leq n-1$, *on a d'après le 2 du lemme 3.1*

$$\frac{p^{2n-k-1}}{2n-2k+1} \in \mathbb{Z}_{(p)}. \tag{3.8}$$

En effet, en posant $m = 2n-k-1$, *on a* $m \geq 2$ *pour* $1 \leq k \leq n-1$ *et*

$$\frac{p^{2n-k-1}}{2n-2k+1} = \frac{p^m}{m+2} \in \mathbb{Z}(p).$$

On a aussi du fait que $\mathbb{Z} \subset \mathbb{Z}(p)$.

$$\binom{2n}{2k} \in \mathbb{Z}(p). \tag{3.9}$$

On a vu qu'on avait aussi (3.5)

$$pB_{2k} \in \mathbb{Z}_{(p)} \tag{3.10}$$

Compte tenu des relations (3.7), (3.8),(3.9),(3.10) et de la relation (3.6), on peut affirmer que pour tout nombre premier p, on a dans l'anneau $\mathbb{Z}(p)$,

$$B_{2n} + \frac{[(p-1)\ divise\ 2n]}{p} \in \mathbb{Z}_{(p)}.$$

La relation $\mathfrak{P}(m)$ *est donc vrai pour l'entier* $m = n$. *Elle est donc vrai pour tout entier* $n \geq 1$. *Ainsi, on a pour tout nombre premier p, on a*

$$\forall n \in \mathbb{N}^*, \qquad B_{2n} + \frac{[(p-1)\ divise\ 2n]}{p} \in \mathbb{Z}_{(p)}. \tag{3.11}$$

Le théorème de Von Staudt et Clausen découle aisément de cette dernière relation. En effet, soit n un entier ≥ 1. Désignons par $\{p_1, p_2, ...p_m\}$ l'ensemble des nombres premiers p tels que $p-1$ divise $2n$. Posons

$$I_{2n} = B_{2n} + \sum_{p-1 \ divise \ 2n} \frac{1}{p}.$$

On a

$$I_{2n} = B_{2n} + \sum_{k=1}^{m} \frac{1}{p_k}.$$

Montrons que pour tout nombre premier p, on a

$$I_{2n} \in \mathbb{Z}_{(p)}. \tag{3.12}$$

Il en résultera que

$$I_{2n} \in \cap_{p \in \mathcal{P}} \mathbb{Z}_{(p)} = \mathbb{Z}.$$

Autrement dit, on aura

$$I_{2n} \in \mathbb{Z},$$

ce qui prouvera le théorème de Von Staudt et Clausen.

Soit donc p un nombre premier, pour prouver que $I_{2n} \in \mathbb{Z}_{(p)}$, distinguons deux cas

1. *$p \in \{p_1, p_2, ...p_m\}$. Dans ce cas, il existe un $j \in \{1, 2, ...m\}$ tel que $p = p_j$ et on a*

$$\begin{aligned} I_{2n} &= (B_{2n} + \frac{1}{p_j}) + \sum_{1 \leq k \leq m \ et \ k \neq j} \frac{1}{p}. \\ &= (B_{2n} + \frac{[(p_j - 1) \ divise \ 2n]}{p_j}) + \sum_{1 \leq k \leq m \ et \ k \neq j} \frac{1}{p}. \end{aligned}$$

   On a bien $I_{2n} \in \mathbb{Z}_{(p)}$ car $B_{2n} + \frac{[(p_j - 1) \ divise \ 2n]}{p_j} \in \mathbb{Z}_{(p)}$, d'après la relation (3.11) et $\sum_{1 \leq k \leq m \ et \ k \neq j} \frac{1}{p} \in \mathbb{Z}_{(p)}$ de manière triviale.

2. *$p \notin \{p_1, p_2, ...p_m\}$ Dans ce cas, $[(p-1) \ divise \ 2n] = 0$ et on peut écrire*

$$I_{2n} = (B_{2n} + \frac{[(p-1) \ divise \ 2n]}{p}) + \sum_{1 \leq k \leq m} \frac{1}{p}.$$

   On a encore $I_{2n} \in \mathbb{Z}_{(p)}$ car $B_{2n} + \frac{[(p-1) \ divise \ 2n]}{p} \in \mathbb{Z}_{(p)}$, d'après la relation (3.11) et $\sum_{1 \leq k \leq m} \frac{1}{p} \in \mathbb{Z}_{(p)}$ de manière triviale.

On a bien prouvé que la relation (3.12) est vérifiée pour tout nombre premier p. La démonstration du théorème de Von Staudt et Clausen est complète.

3.3 Deuxième démonstration du théorème de Von Staudt et Clausen

Dans tout ce qui suit n est un entier supérieur ou égal à 1 fixé. On pose pour tout entier $k \in \mathbb{N}$:

$$u_k = (-1)^k \frac{k!}{k+1} \left\{ \begin{matrix} 2n \\ k \end{matrix} \right\}.$$

Cette deuxième demonstration du théorème de Von Staudt et Clausen repose d'une part sur l'expression suivante du n-ième nombre de Bernoulli à l'aide des nombres de Stirling de deuxième espèce :

$$B_{2n} = \sum_{k=0}^{2n} u_k$$

et d'autre part sur les deux lemmes suivants

Lemme 3.4. *Pour tout nombre premier p, on a*

$$\left\{ \begin{matrix} 2n \\ p-1 \end{matrix} \right\} \equiv \begin{cases} 1 \pmod p & \text{si } p-1 \text{ divise } 2n \\ 0 \pmod p & \text{sinon} \end{cases}$$

Lemme 3.5. *Pour tout entier $k \in \mathbb{N}$, on a avec*

$$u_k = (-1)^k \frac{k!}{k+1} \left\{ \begin{matrix} 2n \\ k \end{matrix} \right\}.$$

1. *Si $k+1 \notin \mathcal{P}$ alors $u_k \in \mathbb{Z}$.*
2. *Si $k+1 \in \mathcal{P}$ alors $u_k + \frac{[k \text{ divise } 2n]}{k+1} \in \mathbb{Z}$.*

Voyons tout de suite comment ces deux lemmes permettent de prouver le théorème de Von staudt et Clausen. Nous prouverons les lemmes ensuite.

Deuxième démonstration du théorème de Von Staudt et Clausen *On a*

$$\begin{aligned} I_{2n} \quad : \quad &= B_{2n} + \sum_{p-1 \text{ divise } 2n} \frac{1}{p} = \sum_{k=0}^{2n} u_k + \sum_{\substack{k=0 \\ k+1 \in \mathcal{P}}}^{2n} \frac{[k \text{ divise } 2n]}{k+1} \\ &= \sum_{\substack{k=0 \\ k+1 \notin \mathcal{P}}}^{2n} u_k + \sum_{\substack{k=0 \\ k+1 \in \mathcal{P}}}^{2n} u_k + \sum_{\substack{k=0 \\ k+1 \in \mathcal{P}}}^{2n} \frac{[k \text{ divise } 2n]}{k+1} \\ &= \sum_{\substack{k=0 \\ k+1 \notin \mathcal{P}}}^{2n} u_k + \sum_{\substack{k=0 \\ k+1 \in \mathcal{P}}}^{2n} \left(u_k + \frac{[k \text{ divise } 2n]}{k+1} \right), \end{aligned} \tag{3.13}$$

Il est clair, grâce au lemme (3.5) que $I_{2n} \in \mathbb{Z}$. En effet dans la première sommation du second membre de (3.13), chaque terme $u_k \in \mathbb{Z}$, car $k+1 \notin \mathcal{P}$ et cela en vertu du 1 du lemme (3.5) tandis que dans la seconde sommation du second membre de (3.13), chaque terme $u_k + \frac{[k \text{ divise } 2n]}{k+1} \in \mathbb{Z}$, car $k+1 \in \mathcal{P}$ et cela en vertu du 2 du lemme (3.5). Le théorème de Von Staudt est donc bien prouvé. Pour que cette démonstration soit complète, il nous rest à prouver les lemmes 3.4 et 3.5.

Démonstration des lemmes 3.4 et 3.5

Preuve du lemme 3.4 *On sait d'après la relation 4 du théorème 1.4 du chapitre 1 que l'on a.*

$$\left\{ {2n \atop p-1} \right\} = \frac{1}{(p-1)!} \sum_{j=0}^{p-1} (-1)^{p-1-j} \binom{p-1}{j} j^n.$$

Raisonnons dans $\mathbb{Z}_{(p)}$: On a d'après le theorème de Wilson

$$\frac{1}{(p-1)!} \equiv -1 \pmod{p}$$

et

$$\binom{p-1}{j} = \frac{(p-1)(p-2)...(p-j)}{j!} \equiv \frac{(-1)(-2)...(-j)}{j!} \equiv (-1)^j \pmod{p}.$$

Par suite, on a en vertu d'un résultat du théorème 1.14 du chapitre 1

$$\begin{aligned} \left\{ {2n \atop p-1} \right\} &= -\sum_{j=0}^{p-1} (-1)^{p-1-j} (-1)^j \; j^{2n} \\ &\equiv -\sum_{j=0}^{p-1} (-1)^{p-1-j} (-1)^j \; j^{2n} \equiv -\sum_{j=0}^{p-1} \; j^{2n} \equiv \begin{cases} 1 \pmod{p} & si\ p-1 \ divise\ 2n \\ 0 \pmod{p} & sinon \end{cases} \end{aligned}$$

Preuve du lemme 3.5

1. *Si $k+1 \notin \mathcal{P}$ alors trois cas sont possible, $k=0$ ou $k=3$ ou $k \geq 5$. Montrons que dans chacun de ces cas, on a $u_k \in \mathbb{Z}$.*
   - *si $k=0$, alors $u_k = u_0 = \left\{ {2n \atop 0} \right\} = 0 \in \mathbb{Z}$.*
   - *si $k=3$, alors*

$$\begin{aligned} u_k &= u_3 = -\frac{3}{2} \left\{ {2n \atop 3} \right\} = -\frac{3}{2} \left(\frac{1}{6} \sum_{j=0}^{3} (-1)^{3-j} \binom{3}{j} j^n \right) \\ &= -\frac{1}{4} \left(1\binom{3}{1} - 2^{2n}\binom{3}{2} + \; 3^{2n}\binom{3}{3} \right) \\ &= -\frac{1}{4}(9^n - 3.4^n + 3) \in \mathbb{Z} \end{aligned}$$

   $-\frac{1}{4}(9^n - 3.4^n + 3) \in \mathbb{Z}$ *du fait que* $9^n - 3.4^n + 3 \equiv 1 - 3.0 + 3 \equiv 0 \pmod{4}$.

– *si $k \geq 5$, $k+1$ n'étant pas premier, il existe deux entiers a et b appartenant à l'ensemble $\{2, ...k\}$ tels que $k+1 = ab$ et $a \leq b$. Si $a \neq b$, dans ce cas $k+1 = ab$ divise $k! = 1.2...a...b..k$, on a donc $\frac{k!}{k+1} \in \mathbb{Z}$ et par suite $u_k \in \mathbb{Z}$. Si $a = b$, dans ce cas $k+1 = a^2$, dans ce cas on a $2a \leq k$, c'est à dire $2a \leq a^2 - 1$. En effet .l'inégalité $2a \leq a^2 - 1$ équivaut à $(a-1)^2 \geq 2$ qui est vérifiée quand $k = a^2 \geq 5$ car nécessairement du fait que a est entier, on a $a \geq 3$.*

2. *Si $k+1 \in \mathcal{P}$. Remarquons qu'en utilisant le symbole d'Iverson, la relation du lemme 3.4 peut s'écrire, pour tout nombre premier p :*

$$\left\{ \begin{matrix} 2n \\ p-1 \end{matrix} \right\} - [(p-1) \ divise \ 2n] \ \in p\mathbb{Z}$$

Dans le cas où $k+1 = p \in \mathcal{P}$,on a

$$\begin{aligned} p\left(u_k + \frac{[k \ divise \ 2n]}{k+1}\right) &= pu_{p-1} + [(p-1) \ divise \ 2n] \\ &= (-1)^{p-1}(p-1)! \left\{ \begin{matrix} 2n \\ p-1 \end{matrix} \right\} + [(p-1) \ divise \ 2n] \\ &\equiv -\left(\left\{ \begin{matrix} 2n \\ p-1 \end{matrix} \right\} - [(p-1) \ divise \ 2n] \right) \\ &\equiv 0 \pmod{p}. \end{aligned}$$

Il en résulte que $u_k + \frac{[k \ divise \ 2n]}{k+1} \in \mathbb{Z}$.

3.4 Dénominateur des nombres de Bernoulli

Grâce au théorème de Von Staudt et Clausen, on a la caractérisation suivante du dénominateur du nombre de Bernoulli B_{2n}

Théorème 3.2. *Pour $n \geq 1$, le dénominateur de B_{2n} est*

$$denom(B_{2n}) = \prod_{p-1 \ divise \ 2n} p$$

Démonstration. Soit $n \geq 1$. Désignons par $\{p_1, p_2, ...p_m\}$ l'ensemble des nombres premiers p tels que $p-1$ divise $2n$. Posons

$$I_{2n} = B_{2n} + \sum_{p-1 \text{ divise } 2n} \frac{1}{p}. \tag{3.14}$$

On a alors

$$I_{2n} = B_{2n} + \sum_{i=1}^{m} \frac{1}{p_i}. \tag{3.15}$$

On sait que $I_{2n} \in \mathbb{Z}$, d'après le théorème de Von Staudt et Clausen. Posons

$$u = p_1.p_2...p_m I_{2n} - \sum_{i=1}^{m} \frac{p_1.p_2...p_m}{p_i}$$

et

$$v = p_1.p_2...p_m.$$

On a $u \in \mathbb{Z}$ et $v \in \mathbb{N}^*$. En effet, il est évident que $v \in \mathbb{N}^*$ et on a $u \in \mathbb{Z}$ car $I_{2n} \in \mathbb{Z}$ et on peut écrire :

$$u = vI_{2n} - \sum_{i=1}^{m} \prod_{1 \leq j \leq m \text{ et } j \neq i} p_j.$$

On a aussi , d'après (3.15)

$$B_{2n} = I_{2n} - \sum_{i=1}^{m} \frac{1}{p_i} = \frac{u}{v}$$

Calculons le pgcd de u et v. On a

$$\begin{aligned} (u, v) &= (vI_{2n} - \sum_{i=1}^{m} \prod_{1 \leq j \leq m \text{ et } j \neq i} p_j, v) \\ &= (\sum_{i=1}^{m} \prod_{1 \leq j \leq m \text{ et } j \neq i} p_j, \prod_{1 \leq k \leq m} p_k) = 1 \end{aligned}$$

En effet, on a pour tout $k \in \{1, 2, ..., m\}$

$$\begin{aligned} (\sum_{i=1}^{m} \prod_{1 \leq j \leq m \text{ et } j \neq i} p_j, p_k) &= (\sum_{i=1}^{m} \prod_{1 \leq j \leq m \text{ et } j \neq i} p_j, p_k) \\ &= (\prod_{1 \leq j \leq m \text{ et } j \neq k} p_j, p_k) = 1. \end{aligned}$$

Par suite on a

$$denom(B_{2n}) = v = p_1.p_2...p_m = \prod_{p-1 \text{ divise } 2n} p$$

□

3.5 Théorème de Kummer

Le célèbre et bien connu théorème de Kummer s'énonce ainsi

Théorème 3.3. *Soit p un nombre premier impair. Pour tous entiers $n \geq 1$ et $m \geq 1$ tels que*

$$n \equiv m \pmod{(p-1)}$$

et tels que $n \notin (p-1)\mathbb{Z}$, $\frac{B_n}{n}$ *et* $\frac{B_m}{m}$ *sont des p-entiers et on a*

$$\frac{B_n}{n} \equiv \frac{B_m}{m} \pmod{p}.$$

Une démonstration utilisant les propriétés des p-entiers et des congruences concernant les numérateurs et dénominateurs des nombres de Bernoulli se trouve en pages 234 à 239 de [34].

3.6 Congruences pour les sommes de puissances et pour les sommes harmoniques.

Grâce à la formule de Faulhaber et au théorème de Von-staudt et Clausen, on établit les résultats suivants concernant l'etude des sommes de puissances numériques harmoniques $\sum_{k=1}^{p-1} k^m$, $\sum_{k=1}^{\frac{p-1}{2}} k^m$ *et les sommes harmoniques* $\sum_{k=1}^{p-1} \frac{1}{k^m}$ *et* $\sum_{k=1}^{\frac{p-1}{2}} \frac{1}{k^m}$, *pour* $m \in \mathbb{N}$ *et p premier,* $p > 3$

Théorème 3.4. *Pour tout nombre premier* $p \geq 3$, *et pour tout entier* $m \geq 0$, *on a*

$$1^m + 2^m + 3^m + ... + (p-1)^m \equiv pB_m + \frac{p^2}{2} B_{m-1} (\mathrm{mod} p^2).$$

et

$$1^m + 2^m + 3^m + ... + (\frac{p-1}{2})^m \equiv \begin{cases} (\frac{1}{2^m} - 2)\frac{B_{m+1}}{m+1} \pmod{p}. & si \quad p-1 \nmid m. \\ \frac{-1}{2} \pmod{p}. & si \quad p-1 \mid m. \end{cases}$$

Démonstration. On a
1)

$$\begin{aligned}
\sum_{k=1}^{p-1} k^m &= \frac{B_{m+1}(p) - B_{m+1}}{m+1} \\
&= \frac{1}{m+1} \sum_{r=1}^{m+1} \binom{m+1}{r} B_i p^{m+1-i} \\
&= \frac{1}{m+1} \sum_{r=1}^{m+1} \binom{m+1}{r} B_{m+1-r} p^r \\
&= \frac{1}{m+1} \binom{m+1}{1} B_m p + \frac{1}{m+1} \binom{m+1}{2} p^2 B_{m-1} + \frac{1}{m+1} \sum_{r=3}^{m+1} \binom{m+1}{r} B_{m+1-r} p^r \\
&= pB_m + \frac{p^2}{2} m B_{m-1} + \frac{1}{m+1} \sum_{r=3}^{m+1} \binom{m+1}{r} B_{m+1-r} p^r
\end{aligned}$$

Or

$$\binom{m+1}{r} = \frac{(m+1)!}{r!(m+1-r)!} = \frac{(m+1)m!}{r(r-1)!(m-(r-1))!} = \frac{m+1}{r}\binom{m}{r-1}$$

d'où l'on a

$$\frac{1}{m+1}\sum_{r=3}^{m+1}\binom{m+1}{r}B_{m+1-r}p^r = \sum_{r=3}^{m+1}\binom{m}{r-1}pB_{m+1-r}\frac{p^{r-3}}{r}p^2$$

Par suite :

$$1^m + 2^m + 3^m + ... + (p-1)^m \equiv pB_m + \frac{p^2}{2}B_{m-1}(\mathrm{mod}p^2).$$

2) On a

$$S_m(n) = \frac{B_{m+1}(n+1) - B_{m+1}}{m+1}$$

En remplaçant n par $\frac{p-1}{2}$, on obtient :

$$S_m(\frac{p-1}{2}) = \frac{B_{m+1}(\frac{p-1}{2}+1) - B_{m+1}}{m+1} = \frac{B_{m+1}(\frac{p+1}{2}) - B_{m+1}}{m+1}$$

On a par définition :

$$B_{m+1}(\frac{p+1}{2}) = \sum_{k=0}^{m+1}\binom{m+1}{k}B_{m+1-k}(\frac{p+1}{2})^k$$

D'où

$$S_m(n) = \frac{\sum_{k=0}^{m+1}\binom{m+1}{k}B_{m+1-k}(\frac{p+1}{2})^k - B_{m+1}}{m+1} = \frac{\sum_{k=1}^{m+1}\binom{m+1}{k}B_{m+1-k}(\frac{p+1}{2})^k}{m+1}$$

Comme $\frac{p+1}{2} = \frac{1}{2} + \frac{p}{2} \equiv \frac{1}{2} \pmod p$ alors $(\frac{p+1}{2})^k \equiv (\frac{1}{2})^k \pmod p$.

et comme

$$\binom{m+1}{k} \in \mathbb{N} \subset \mathbb{Z} \subset \mathbb{Z}_{(p)} \quad \text{et} \quad B_{m+1-k} \in \mathbb{Z}_{(p)} \quad \text{alors} \quad \binom{m+1}{k}B_{m+1-k} \in \mathbb{Z}_{(p)}$$

Par suite :

$$B_{m+1}(\frac{p+1}{2}) \equiv B_{m+1}(\frac{1}{2}) \pmod p$$

□

On déduit de ce théorème le corollaire suivant :

Corollaire 3.1. *Pour tout nombre premier $p \geq 3$, et pour tout entier $m \in \mathbb{Z}$, on a*

$$1^m + 2^m + 3^m + ...(p-1)^m \equiv \begin{cases} 0 \pmod{p} & si \quad p-1 \nmid m \\ -1 \pmod{p} & si \quad p-1 \mid m \end{cases}$$

On a aussi :

Corollaire 3.2. *Pour tout nombre premier $p \geq 3$, et pour tout entier $m = 1, ..., p-3$, on a*

$$\frac{1}{1^m} + \frac{1}{2^m} + \frac{1}{3^m} + ... + \frac{1}{(\frac{p-1}{2})^m} \equiv \begin{cases} 0 \pmod{p} & si \quad m \quad est\ pair. \\ (2^m - 2)\frac{B_{p-m}}{p-m} \pmod{p} & si \quad m \quad est\ impair. \end{cases}$$

Ces congruence sont en accord avec les congruences suivantes obtenues en 2000, par Zhi-Hong Sun [36].

Théorème 3.5. *Soit $p > 3$ un nombre premier. Alors pour $p = 1, 2, ..., p-4$, on a*

$$\sum_{k=1}^{p-1} \frac{1}{k^m} \equiv \begin{cases} m(\frac{B_{2p-2-m}}{2p-2-m} - 2\frac{B_{p-2-m}}{p-2-m})p \pmod{p}^3 & si \quad m \quad est\ pair. \\ \binom{k+1}{2}\frac{B_{p-2-m}}{p-2-m}p^2 \pmod{p}^3 & si \quad m \quad est\ impair. \end{cases}$$

En 2000, Zhi-Hong Sun a généralisé ce résultat en prouvant (théorème 5.2, p.208 de [36])

Théorème 3.6. *(Zhi-Hong Sun, 2000). Soit $p > 3$ un nombre premier.*

1) Si $m \in \{2, 4, ..., p-5\}$, alors

$$\sum_{k=1}^{\frac{(p-1)}{2}} \frac{1}{k^m} \equiv \frac{m(2^{m+1}-1}{2}(\frac{B_{2p-2-m}}{2p-2-m} - 2\frac{B_m}{p-2-m})p(\mathrm{mod}p^3).$$

2) Si $m \in \{3, 5, ..., p-4\}$, alors

$$\sum_{k=1}^{\frac{(p-1)}{2}} \frac{1}{k^m} \equiv (2^m - 2)(2\frac{B_{p-m}}{p-m} - 2\frac{B_{2p-1-m}}{2p-1-m})p(\mathrm{mod}p^2)$$

3) Avec $q_p(2) = (2^{p-1} - 1)/p$, on a

$$\sum_{k=1}^{\frac{(p-1)}{2}} \frac{1}{k} \equiv -2q_p(2) + pq_p^2(2) - \frac{2}{3}p^2q_p^3(2) - \frac{7}{12}p^2B_{p-3}(\mathrm{mod}p^3)$$

Chapitre 4

Introduction à la théorie arithmétique des nombres harmoniques

4.1 Introduction

En 2012, *Zhi Wei Sun publie un article intitulé "Arithmetic theory of harmonic numbers dans lequel il souligne le rôle important que joue les sommes harmoniques* $H_k = \sum_{o<j\leq k} \frac{1}{j}$ *en mathématiques. Dans son papier, Zhi Wei Sun développe une "théorie arithmétique" de ces nombres. Il obtient de nombreuses congruences dans* $\mathbb{Z}(p)$, *pour des sommes dans lesquelles interviennent les sommes harmoniques. Ces résultats sont donnés dans le théorème suivant :*

Théorème 4.1. *(Zhi Wei Sun 2012) Soit* p *un nombre premier tel que* $p > 3$. *Alors*

$$\sum_{k=1}^{p-1} \frac{H_k}{k2^k} \equiv 0 \pmod{p},$$

$$\sum_{k=1}^{p-1} k^2 H_k^2 \equiv -\frac{4}{9} \pmod{p}$$

$$\sum_{k=1}^{p-1} H_k^3 \equiv 6 \pmod{p},$$

$$\sum_{k=1}^{p-1} H_k^2 \equiv 2p-2 \pmod{p^2},$$

$$\sum_{k=1}^{p-1} \frac{H_k^2}{k^2} \equiv 0 \pmod{p}, \quad \textit{pour } p > 5.$$

L'obtention de ces résultats nécessite de nombreux calculs et l'emploi des théorèmes de Von Staudt et Clausen et de la formule de Faulhaber entre autres. Dans ce chapitre nous allons particulièrement nous intéresser à la première congruence, les autres pouvant se prouver de la même manière en utilisant les mêmes résultats intermédiaires que pour cette congruence.

4.2 Lemmes préliminaires

La démonstration du théorème de Zhi Wei Sun repose sur les lemmes suivants.

Lemme 4.1. *Soit p un nombre premier. Alors*

1. *Pour tout entier $k \in \{1, 2, ..., p-1\}$ et pour tout nombre premier p*

$$H_{p-k} \equiv H_{k-1} \pmod{p}.$$

2. $$(-1)^k \binom{p-1}{k} \equiv 1 - pH_k + \frac{1}{2}p^2 \left(H_k^2 - H_k^{(2)}\right) (\mathrm{mod} p^3).$$

3. *Pour tout entier $k \in \{1, 2, ..., p-1\}$ et pour tout nombre premier $p > 3$, on a*

$$\sum_{k=1}^{p-1} H_k \equiv 1 - p(\mathrm{mod} p^3).$$

et

$$\sum_{k=1}^{p-1} \frac{H_{k-1}}{k} \equiv 0 \pmod{p}.$$

Démonstration. [37].

1. Comme $k \in \{1, ..., p-1\}$ alors :

$$\begin{aligned} 1 &\leq k \leq p-1 \\ 1-p &\leq -k \leq -1 \\ 1 &\leq p-k \leq p-1 \end{aligned}$$

On a

$$H_{p-1} = \sum_{j=1}^{p-1} \frac{1}{j} = \sum_{j=1}^{p-k} \frac{1}{j} + \sum_{j=1}^{k-1} \frac{1}{p-k+j}.$$

Ce qui implique :

$$H_{p-k} = \sum_{j=1}^{p-k} \frac{1}{j} = H_{p-1} - \sum_{j=1}^{k-1} \frac{1}{p-k+j}$$

D'où :

$$H_{p-k} \equiv \sum_{j=1}^{k-1} \frac{1}{k-j} \pmod{p} \quad (\text{puisque} \quad H_{p-1} \equiv 0 \pmod{p})$$

Or $\displaystyle\sum_{j=1}^{k-1} \frac{1}{k-j} = \frac{1}{k-1} + \frac{1}{k-2} + ... + \frac{1}{2} + 1 = H_{k-1}$, ce qui donne

$$H_{p-k} \equiv H_{k-1} \pmod{p}$$

2. On a

$$\begin{aligned}
\prod_{0<j\leq k}(1-\frac{p}{j}) &= (1-p)(1-\frac{p}{2})(1-\frac{p}{3}...(1-\frac{p}{k}) \\
&= -(p-1).(\frac{-(p-2)}{2}).(\frac{-(p-3)}{3})...(\frac{-(p-k)}{k}) \\
&= (-1)^k\frac{(p-1)(p-2)...(p-k)}{1.2.3....k} \\
&= (-1)^k\frac{(p-1)(p-2)...(p-k)(p-k-1)!}{k!(p-k-1)!} \\
&= (-1)^k\frac{(p-1)!}{k!(p-k-1)!} \\
&= (-1)^k\binom{p-1}{k} \\
&\equiv (1-\sum_{1\leq j\leq k}\frac{p}{j}+\sum_{1<i<j\leq k}\frac{p^2}{ij})(\mathrm{mod}p^3) \\
&\equiv 1-pH_k+\frac{p^2}{2}((\sum_{1\leq j\leq k}\frac{1}{j})^2-\sum_{1\leq j\leq k}\frac{1}{j^2})(\mathrm{mod}p^3)
\end{aligned}$$

D'où l'on a

$$(-1)^k\binom{p-1}{k}\equiv 1-pH_k+\frac{p^2}{2}(H_k^2-H_k^{(2)})(\mathrm{mod}p^3)$$

3. On a :

$$\begin{aligned}
\sum_{k=1}^{p-1}H_k &= \sum_{k=1}^{p-1}\sum_{j=1}^{k}\frac{1}{j}=\sum_{j=1}^{p-1}\frac{1}{j}\sum_{k=j}^{p-1}1 \\
&= \sum_{j=1}^{p-1}\frac{p-j}{j}=p\sum_{j=1}^{p-1}\frac{1}{j}-\sum_{j=1}^{p-1}1 \\
&= pH_{p-1}-(p-1)\equiv 1-p(\mathrm{mod}p^3)
\end{aligned}$$

Puisque :

$$H_{p-1}\equiv 0(\mathrm{mod}p^2)\quad\text{implique}\quad pH_{p-1}\equiv 0(\mathrm{mod}p^3).$$

Voici la preuve de la deuxième congruence. Notons que

$$\sum_{k=1}^{p-1}\frac{p}{k}\binom{p-1}{k-1}(-1)^k=\sum_{k=1}^{p-1}\binom{p}{k}(-1)^k+1+(-1)^p=(1-1)^p=0$$

En effet :

$$\begin{aligned}\sum_{k=1}^{p-1}\frac{p}{k}\binom{p-1}{k-1}(-1)^k &= \sum_{k=1}^{p-1}\frac{p}{k}.\frac{(p-1)!}{(k-1)!(p-k)!}(-1)^k\\ &= \sum_{k=1}^{p-1}\frac{p!}{k!(p-k)!}(-1)^k\\ &= \sum_{k=1}^{p-1}\binom{p}{k}(-1)^k+\underbrace{1+(-1)^p}_{0}\\ &= \sum_{k=1}^{p}\binom{p}{k}(-1)^k=(1-1)^p=0\end{aligned}$$

D'où,

$$-p\sum_{k=1}^{p-1}\frac{(-1)^{k-1}}{k}\binom{p-1}{k-1}=0\Rightarrow 0=\sum_{k=1}^{p-1}\frac{(-1)^{k-1}}{k}\binom{p-1}{k-1}\equiv\sum_{k=1}^{p-1}\frac{1-pH_{k-1}}{k}(\text{ mod } p^2)$$

Or :

$$\sum_{k=1}^{p-1}\frac{1}{k}-p\sum_{k=1}^{p-1}\frac{H_{k-1}}{k}=H_{p-1}-p\sum_{k=1}^{p-1}\frac{H_{k-1}}{k}$$

Comme $H_{p-1}\equiv 0(\text{mod}p^2)$ alors

$$0=\sum_{k=1}^{p-1}\frac{1-pH_{k-1}}{k}(\text{mod}p^2)\equiv -p\sum_{k=1}^{p-1}\frac{H_{k-1}}{k}(\text{mod}p^2)$$

On en déduit que

$$\sum_{k=1}^{p-1}\frac{H_{k-1}}{k}\equiv 0\pmod p.$$

□

Lemme 4.2. *Pour tout entier $k\in\{1,2,...,p-1\}$, on a*

$$(-1)^k\binom{p-1}{k}\equiv 1-pH_k(\text{mod}p^2).$$

et

$$-pH_k\equiv\left((-1)^k\binom{p-1}{k}-1\right)(\text{mod}p^2).$$

Démonstration. D'après 2 du lemme (4.1), on a vu que :

$$(-1)^k\binom{p-1}{k} \equiv 1 - pH_k + \frac{1}{2}p^2\left(H_k^2 - H_k^{(2)}\right)(\mathrm{mod}p^3)$$

Ce qui implique :

$$(-1)^k\binom{p-1}{k} \equiv 1 - pH_k(\mathrm{mod}p^2).$$

D'où l'on a :

$$-pH_k \equiv \left((-1)^k\binom{p-1}{k} - 1\right)(\mathrm{mod}p^2).$$

□

Lemme 4.3. *Pour tout entier $n \geq 1$, on a*

$$\sum_{k=0}^{n-1}\frac{2^k}{k+1} = \sum_{\substack{k=1 \\ 2 \text{ ne divise pas } k}}^{n}\frac{1}{k}\binom{n}{k}$$

Démonstration. On a :

$$\begin{aligned}\sum_{k=0}^{n-1}\frac{2^k}{k+1} &= \sum_{k=0}^{n-1}2^k\int_0^1 x^k dx = \int_0^1\sum_{k=0}^{n-1}(2x)^k dx \\ &= \int_0^1\frac{(2x)^n-1}{2x-1}dx = \int_0^1\sum_{k=1}^{n}\binom{n}{k}(2x-1)^{k-1}dx \\ &= \sum_{k=1}^{n}\binom{n}{k}\frac{(2x-1)^k}{2k}]_0^1 = \sum_{k=1}^{n}\binom{n}{k}\frac{1-(-1)^k}{2k}\end{aligned}$$

Comme 2 ne divise pas k alors : k est impair, d'où l'on a :

$$\sum_{k=0}^{n-1}\frac{2^k}{k+1} = \sum_{k=1}^{n}\frac{1}{k}\binom{n}{k}.$$

□

Lemme 4.4. *Soit $p > 3$ un nombre premier. Alors*

$$H_{\frac{p-1}{2}} \equiv pq_p^2(2) - 2q_p(2)(\mathrm{mod}p^2). \tag{4.1}$$

Démonstration. Ce lemme est exactement le théorème (1.19) démontré dans le premier chapitre. □

Lemme 4.5. *Soit $p > 3$ un nombre premier. Alors*

$$\sum_{\substack{k=1 \\ 2 \text{ divise } k}}^{p-1} \frac{H_k}{k} \equiv \frac{q_p^2(2)}{2} \pmod{p}. \tag{4.2}$$

et

$$\sum_{\substack{k=1 \\ 2 \text{ ne divise pas } k}}^{p-1} \frac{H_k}{k} \equiv -\frac{q_p^2(2)}{2} \pmod{p}. \tag{4.3}$$

Démonstration. (Preuve de 4.2) Comme

$$H_k = H_{k-1} + \frac{1}{k}$$

On en déduit que :

$$\frac{H_k}{k} = \frac{1}{k}(H_{k-1} + \frac{1}{k}).$$

Par suite

$$\sum_{k=1}^{p-1} \frac{H_k}{k} = \sum_{k=1}^{p-1} \frac{1}{k} H_{k-1} + \sum_{k=1}^{p-1} \frac{1}{k^2}.$$

Comme 2 divise k alors k est pair et donc $k-1$ est impair, on a d'après le lemme (4.1), partie (2) :

$$-\binom{p-1}{k-1} \equiv 1 - pH_{k-1} (\mathrm{mod} p^2)$$

On en déduit que :

$$\begin{aligned} p \sum_{\substack{k=1 \\ 2 \text{ divise } k}}^{p-1} \frac{H_{k-1}}{k} &\equiv \sum_{\substack{k=1 \\ 2 \text{ divise } k}}^{p-1} (\frac{1}{k} + \frac{1}{k}\binom{p-1}{k-1}) (\mathrm{mod} p^2) \\ &\equiv (\sum_{\substack{k=1 \\ 2 \text{ divise } k}}^{p-1} \frac{1}{k} + \sum_{\substack{k=1 \\ 2 \text{ divise } k}}^{p-1} \frac{1}{k}\binom{p-1}{k-1}) (\mathrm{mod} p^2) \\ &\equiv (\sum_{\substack{k=1 \\ 2 \text{ divise } k}}^{p-1} \frac{1}{k} + \frac{1}{p}(\sum_{\substack{k=0 \\ 2 \text{ divise } k}}^{p} \binom{p}{k} - 1)) (\mathrm{mod} p^2) \end{aligned}$$

Or :

$$\sum_{\substack{k=1 \\ 2 \text{ divise } k}}^{p-1} \frac{1}{k} = \sum_{j=1}^{\frac{p-1}{2}} \frac{1}{2j} = \frac{1}{2} H_{\frac{p-1}{2}}$$

et

$$\sum_{\substack{k=0 \\ 2 \text{ divise } k}}^{p} \binom{p}{k} = 2^{p-1}.$$

On a pour $n \geq 1$:

$$\begin{aligned} 2^n &= (1+1)^n = \sum_{k=0}^{n} \binom{n}{k} \\ 0 &= (1-1)^n = \sum_{k=0}^{n} (-1)^k \binom{n}{k} \end{aligned}$$

d'où l'on a :

$$\begin{aligned} \sum_{k=0}^{n} (\frac{1+(-1)^k}{2}) \binom{n}{k} &= 2^{n-1} = \sum_{\substack{k=1 \\ 2 \text{ divise } k}}^{n} \binom{n}{k} \\ \sum_{k=0}^{n} (\frac{1-(-1)^k}{2}) \binom{n}{k} &= 2^{n-1} = \sum_{\substack{k=1 \\ 2 \text{ ne divise pas } k}}^{n} \binom{n}{k}. \end{aligned}$$

Par suite :

$$p \sum_{\substack{k=1 \\ 2 \text{ divise } k}}^{p-1} \frac{H_{k-1}}{k} \equiv \frac{p}{2} q_p^2(2) - q_p(2) + \frac{2^{p-1}-1}{p} = \frac{p}{2} q_p^2(2) (\mathrm{mod} p^2).$$

Donc :

$$\begin{aligned} \sum_{\substack{k=1 \\ 2 \text{ divise } k}}^{p-1} \frac{H_k}{k} &= \sum_{\substack{k=1 \\ 2 \text{ divise } k}}^{p-1} \frac{1}{k} H_{k-1} + \sum_{\substack{k=1 \\ 2 \text{ divise } k}}^{p-1} \frac{1}{k^2} \\ &= \frac{q_p^2(2)}{2} + \frac{1}{8} \sum_{k=1}^{\frac{(p-1)}{2}} (\frac{1}{k^2} + \frac{1}{(p-k)^2}) \\ &\equiv \frac{q_p^2(2)}{2} \pmod{p}. \end{aligned}$$

La preuve de (4.3) est tout a fait analogue à celle (4.2). □

4.3 Démonstration du théorème de Zhi-Wei Sun (2012)

Tous les calculs se font dans l'anneau des p-entiers $\mathbb{Z}_{(p)}$. On a d'après le 1 du lemme 4.1 :

$$\textit{Pour} \quad k \in \{1, 2, ..., p-1\} \qquad H_{p-k} \equiv H_{k-1} \pmod{p}.$$

On a aussi

$$-k \equiv p - k \pmod{p}$$

Par suite

$$-\frac{1}{k} \equiv \frac{1}{p-k} \pmod{p}.$$

On a aussi

$$\frac{1}{2^{p-k}} = \frac{2^{k-1}}{2^{p-1}} \equiv 2^{k-1} \pmod{p}\ .$$

On en déduit que

$$\sum_{k=1}^{p-1} \frac{H_k}{k2^k} = \sum_{k=1}^{p-1} \frac{H_{p-k}}{(p-k)2^{p-k}} \equiv \sum_{k=1}^{p-1} \frac{2^{k-1}H_{k-1}}{-k} = -\sum_{k=0}^{p-2} \frac{2^k H_k}{k+1} \pmod{p}\ .$$

Par suite on a

$$p\sum_{k=1}^{p-1} \frac{H_k}{k2^k} \equiv \sum_{k=0}^{p-2} \frac{2^k}{k+1}.(-pH_k) \pmod{p}.$$

En exploitant la deuxième relation du lemme 4.2, on en déduit que

$$p\sum_{k=1}^{p-1} \frac{H_k}{k2^k} \equiv \sum_{k=0}^{p-2} \frac{2^k}{k+1}.\left((-1)^k\binom{p-1}{k}-1\right) \pmod{p}. \tag{4.4}$$

Désignons par S Le deuxième membre de (4.4)

$$S := \sum_{k=0}^{p-2} \frac{2^k}{k+1}.\left((-1)^k\binom{p-1}{k}-1\right)$$

S peut s'écrire :

$$\begin{aligned} S &= \sum_{k=0}^{p-2} \frac{(-2)^k}{k+1}.\binom{p-1}{k} - \sum_{k=0}^{p-2} \frac{2^k}{k+1} \\ &= \frac{1}{p}\sum_{k=0}^{p-2}(-2)^k.\frac{p}{k+1}\binom{p-1}{k} - \sum_{k=0}^{p-2} \frac{2^k}{k+1} \\ &= \frac{1}{-2p}\sum_{k=0}^{p-2}(-2)^{k+1}.\binom{p}{k+1} - \sum_{k=0}^{p-2} \frac{2^k}{k+1} \\ &= \frac{1}{-2p}\sum_{j=1}^{p-1}(-2)^j.\binom{p}{j} - \sum_{k=0}^{p-2} \frac{2^k}{k+1} \end{aligned} \tag{4.5}$$

D'après le lemme 4.3, on a

$$\begin{aligned} \sum_{k=0}^{p-2} \frac{2^k}{k+1} &= \sum_{\substack{k=1 \\ 2 \text{ ne divise pas } k}}^{p-1} \frac{1}{k}\binom{p-1}{k} \\ &= -\sum_{\substack{k=1 \\ 2 \text{ ne divise pas } k}}^{p-1} \frac{(-1)^k}{k}\binom{p-1}{k}. \end{aligned}$$

Compte tenu de cette dernière égalité, la relation (4.5) devient

$$\begin{aligned} S &= \frac{1}{-2p}\sum_{j=1}^{p-1}(-2)^j.\binom{p}{j} - \sum_{k=0}^{p-2}\frac{2^k}{k+1} \\ &= \frac{(1-2)^p - 1 + 2^p}{-2p} + \sum_{\substack{k=1 \\ 2 \text{ ne divise pas } k}}^{p-1} \frac{(-1)^k}{k}\binom{p-1}{k}. \end{aligned}$$

A la lumière des relations(4.1), (4.2) et (4.3), on a

$$\begin{aligned} S + q_p(2) &= \frac{(1-2)^p - 1 + 2^p}{-2p} + \sum_{\substack{k=1 \\ 2 \text{ ne divise pas } k}}^{p-1} \frac{\binom{p-1}{k}(-1)^k}{k} + \frac{2^{p-1}-1}{p} \\ &= \frac{(-1)^p - 1 + 2^p - 2^p + 2}{-2p} + \sum_{\substack{k=1 \\ 2 \text{ ne divise pas } k}}^{p-1} \frac{\binom{p-1}{k}(-1)^k}{k} + \frac{2^{p-1}-1}{p} \\ &= \frac{(-1)^p + 1}{-2p} + \sum_{\substack{k=1 \\ 2 \text{ ne divise pas } k}}^{p-1} \frac{\binom{p-1}{k}(-1)^k}{k} \\ &= \sum_{\substack{k=1 \\ 2 \text{ ne divise pas } k}}^{p-1} \frac{\binom{p-1}{k}(-1)^k}{k}. \quad (puisque \quad \frac{(-1)^p+1}{-2p} = 0, \quad \forall p > 3.) \end{aligned}$$

D'où l'on a :

$$\begin{aligned} S + q_p(2) &\equiv \sum_{\substack{k=1 \\ 2 \text{ ne divise pas } k}}^{p-1} \frac{1 - pH_k}{k} (\mathrm{mod} p^2) \\ &\equiv \sum_{\substack{k=1 \\ 2 \text{ ne divise pas } k}}^{p-1} \frac{1}{k} - p \sum_{\substack{k=1 \\ 2 \text{ ne divise pas } k}}^{p-1} \frac{H_k}{k} (\mathrm{mod} p^2) \end{aligned}$$

Or on peut écrire $\sum_{k=1,2\nmid k}^{p-1}\frac{1}{k}$, *comme suit :*

$$\sum_{\substack{k=1 \\ 2 \text{ ne divise pas } k}}^{p-1} \frac{1}{k} = H_{p-1} - \frac{1}{2}H_{\frac{(p-1)}{2}}. \quad \textit{En effet :}$$

$$\sum_{\substack{k=1\\ 2\ ne\ divise\ pas\ k}}^{p-1}\frac{1}{k} = 1+\frac{1}{3}+\frac{1}{5}+...+\frac{1}{p-2}+(\frac{1}{2}+\frac{1}{4}+...+\frac{1}{p-1})-(\frac{1}{2}+\frac{1}{4}+...+\frac{1}{p-1})$$

$$= \sum_{k=1}^{p-1}\frac{1}{k}-\frac{1}{2}(1+\frac{1}{2}+...+\frac{1}{\frac{p-1}{2}})$$

$$= H_{p-1}-\frac{H_{\frac{(p-1)}{2}}}{2}. \qquad \square$$

Par suite :

$$S+q_p(2) \equiv H_{p-1}-\frac{H_{\frac{(p-1)}{2}}}{2}-p\sum_{\substack{k=1\\ 2\ ne\ divise\ pas\ k}}^{p-1}\frac{H_k}{k}(\mathrm{mod}p^2)$$

$$\equiv \{0-\frac{p}{2}q_p^2(2)+q_p(2)+\frac{p}{2}q_p^2(2)\}(\mathrm{mod}p^2)$$

$$\equiv q_p(2)$$

Ce qui implique :

$$p\sum_{k=1}^{p-1}\frac{H_k}{k2^k}\equiv S\equiv 0(\mathrm{mod}p^2)$$

Ensuite, on aura

$$\sum_{k=1}^{p-1}\frac{H_k}{k2^k}\equiv 0 \pmod{p}. \qquad \square$$

Conclusion

La formule de Faulhaber, le théorème de Von Staudt et Clausen, le théorème de Kummer et les théorèmes classiques de Fermat, d'Euler, de Wilson et les propriétés concernant les congruences dans l'anneau $\mathbb{Z}_{(p)}$ sont des outils essentiels dans l'étude des congruences concernant tout particulièrement des sommes de nombres rationnels, et plus précisément des sommes comportant des sommes harmoniques. Ces outils combinés à certaines techniques combinatoires ont été utilisés par de nombreux auteurs tels que E. Lehmer ou Zhi-Wei Sun pour préciser davantage certaines congruences. Dans ce mémoire, nous nous sommes efforcés de clarifier l'obtention de certains théorèmes. Nous nous sommes particulièrement intéressés à ces techniques calculatoires et combinatoires souvent astucieuses. Nous avons détaillé la preuve que Zhi-Wui Sun a donné de la congruence suivante :

$$\sum_{k=1}^{p-1} \frac{H_k}{k2^k} \equiv 0 \pmod{p}. \tag{4.6}$$

Une question naturelle serait de savoir comment se comporte la somme modulo p^2. Cette question n'a pas échappé à Zhi-Wei Sun. Dans le même article, paru en février 2012, où il démontre la congruence (4.6), Zhi-Wui Sun énonce la conjecture suivante obtenue grâce à des investigations à l'aide du logiciel de calcul formel Mathematica (page 417, Conjecture 1.1)

Conjecture 4.1. *Pour tout nombre premier $p > 3$, nous avons*

$$\sum_{k=1}^{p-1} \frac{H_k}{k2^k} \equiv \frac{7}{24} pB_{p-3} \ (\mathrm{mod} p^2) \tag{4.7}$$

et

$$\sum_{k=1}^{p-1} \frac{H_k^2}{k^2} \equiv \frac{4}{5} pB_{p-5} \ (\mathrm{mod} p^2). \tag{4.8}$$

Bien avant la parution de son article, Zhi-Wei Sun et Li-Lu Zhao ont démontré la première conjecture (4.7) (article sur arXiv daté du 26 octobre 2011). La seconde conjecture (4.8) a finalement été prouvée par Roméo Mestrovic (article sur arXiv daté su 25 mars 2012). Bien que relativement élémentaires, ces deux preuves font appel à des identités combinatoires et des techniques de calculs assez sophistiquées. Ces techniques et les théorèmes classiques permettent ainsi de mieux appréhender la

recherche de la résolution de certaines autres conjectures telles que par exemple les célèbres conjectures de Giuga datant de 1950 ou d'Agoh datant de 1990.

Conjecture 4.2. *(Giuga, 1950) Pour tout entier $n \geq 2$, on a l'équivalence*

$$\sum_{k=1}^{n-1} k^{n-1} \equiv -1 \pmod{n} \quad \Leftrightarrow \quad n \text{ est premier.}$$

Conjecture 4.3. *(Agoh, 1990) Pour tout entier $n \geq 2$, on a l'équivalence*

$$nB_{n-1} \equiv -1 \pmod{n} \quad \Leftrightarrow \quad n \text{ est premier.}$$

En 2004, B.B. Kellner [25] a prouvé que ces deux conjectures étaient équivalentes. A notre connaissance, aucun progrès notable n'a été réalisé depuis. Cela n'empêche pas de continuer cette recherche avec les moyens classiques qui ont si bien réussi jusqu'à présent.

Une autre conjecture célèbre bien connue est la conjecture de Kurepa. Le mathématicien yougoslave Duro Kurapa (1907-1993), bien connue pour ses nombreuses contributions en théorie des ensembles, en logique. Il s'est aussi intéressé à la théorie des graphes et à la théorie des nombres. En 1971, il définit la factorielle à gauche d'un entier $n \geq 1$, qu'il désigne par $!n$ en posant

$$!n = 0! + 1! + \cdots + (n-1)!$$

La conjecture de Kurepa s'énonce alors comme suit

Conjecture 4.4. *(Kurepa) Pour tout entier $n \geq 2$, le plus grand commun diviseur de $!n$ et $n!$ est égal à 2.*

Cette conjecture à fait l'objet de nombreuses recherches. Cette conjecture a été testée par ordinateur jusqu'à $n = 10^6$. Il existe de nombreuses formulations équivalentes de cette conjecture. On a ainsi la formulation suivante équivalente :

Conjecture 4.5. *(Kurepa) Pour tout nombre premier $p \geq 3$, on a*

$$!p \neq 0 \pmod{p}.$$

En 2004, Barsky et Benzaghou publient une preuve de cette conjecture [4]. Malheureusement, cette preuve comportait une erreur qui fut découverte par F. Bencherif en 2008. Malgré de nombreuses tentatives entreprises entre 2008 et 2011 par D. Barsky et F. Bencherif pour essayer d'y remédier, il ne fut pas possible de rectifier la démonstration. L'erreur s'est avéré être irréparable. En 2011 parut un erratum pour signaler l'invalidation de cette preuve [5]. Le problème de la résolution de la conjecture de Kurepa est aujourd'hui de nouveau un problème ouvert.

Ainsi, de nombreuses conjectures en théorie des nombres s'expriment en termes de congruences. Nous avons abordé dans ce mémoire une approche qui permet d'entrevoir la résolution de certaines d'entre elles.

Bibliographie

[1] *M. Abramowitz and I.A. Stegun. Handbook of mathematical Functions : with Formulas, Graphs and Mathematical tables, Dover Publications, 1972.*

[2] *Apostol T.M. Introduction To Analytic Number Theory (Springer, 1976).*

[3] *A. Aïder et F. Bencherif. Some identities for Bernoulli numbers, March 27,2012. Preprint.*

[4] *D. Barsky et B. Benzaghou. Nombes de Bell et somme de factorielles. Journal de théorie des nombres de Bordeaux, 16 :1-17, 2004.*

[5] *D. Barsky et B. Benzaghou. Erratum à l'article Nombres de Bell et somme de factorielles, Journal de théorie des nombres de Bordeaux, 23 no. 2 (2011), p. 527-527.*

[6] *F. Bencherif. Nombres et polynômes de Bernoulli et d'Euler. Cours de P.G, Fac Math USTHB.*

[7] *F. Bencherif, sur une propriété des polynômes de Nörlond, actes des rencontres du CIRM, 2 nř2 : Third international meeting on integr-valued polynomials (2010), p ; 71-77.*

[8] *F. Bencherif et T. Garici. Suite de cesàro et nombres de Bernoulli, pmb.univ-fcomte.fr/2012/1.*

[9] *F. Bencherif et T. Garici. Sur une propriété des polynômes de Stirling, preprint.*

[10] *F. Bencherif et A. Zekiri. On some properties of Nörlond's polynomials, preprint.*

[11] *F. Bencherif et S. Zerroukhat." Généralisation d'une congruence sur les nombres harmoniques ". Fac math N :324/2011.*

[12] *F. Bencherif et S. Zerroukhat. On a generalization of a curious cogruence on harmonic sums. Preprint.*

[13] *B. C. Berndt, Elementary evaluation of $\zeta(2n)$, Math. Mag.,48 (1975), 1067-1086.*

[14] *H. Boualem, R. Brouzet, La planète $\mathbb{R}$, collection universciences, Dunod.*

[15] *D. Borwein and J. M. Borwein, On an intriguing integral and some series related to $\zeta(4)$, Proc. Amer. Math. Soc. 123(1995), 1191-1198.*

[16] *Timothy Simon Caley " A review of the Von Staudt Clausen theorem" thesis Dalhousie-University, 2007.*

[17] *S. W. Coffman, 1240 and Solution : An infinite series with harmonic numbers, Math. Mag. 60(1987), 118-119.*

[18] L. Comtet, Analyse combinatoire, tomes premier et second, Collection Sup "Le Mathématicien", P.U;F. 1970.

[19] Louis Comtet, Advanced Combinatorics : The Art of Finite and Infinite Expansions, D. Reidel Publishing Company, 1974.

[20] R. L. Graham, D. E. Knuth, and O. Patashnik, Concrete Mathematics, 2nd ed., Addison-Wesley Pub1. Co., Reading, MA, 1994.

[21] A. Granville. The square of Fermat quotient. Integers : Electronic J. of Combinatorial Number Theory 4(2004). ‡A22(electronic).

[22] Carl Friedrich Gauss ; Recherche arithmétiques, 1801 Traduction M. Poullet Delisle Ed. Courcier 1807.

[23] G.H. Hardy et E. M. Wright, introduction à la theorie des nombres, traduction de François Sauvagegeot, Vuibert Spinger 2007.

[24] A. Joyal pour le camp mathématique. Les nombres de Bernoulli ; Juillet 2003.

[25] B. C. Kellner, The equivalence of Giuga's and Agoh's Conjectures, arXiv :math/0409259v [math.NT] 15 Sep 2004.

[26] D. Knuth, Johann FAULHABER and sums of powers ; mathematics of computation. Volume 61, number 203. July 1993, 277-294

[27] Emma Lehmer, On congruences involving Bernoulli numbers and the quotients of Fermat and Wilson, Ann. of Math. 39 (1938), no. 2, 350-360.

[28] Emma Lehmer, On congruences involving Bernoulli numbers and the quotients of Fermat and Wilson, Ann. of Math. (2) 39 (1938), no. 2, 350-360.

[29] E. Lucas, Théorie des nombres, Gauthier-Villars 1891, rééd. Jacques Gabay.(1991)

[30] K. Milosevic-Rakocevic, Staudt-Clausenova teorema, Mat. Bibl., 22(1962),71,79.

[31] N. Nielsen, Rechercches sur les polynômes de Bernoulli, Danske Vidensk. Selsk. Skr. (7) 10 (1913),285-366.

[32] N. Nielsen, Traité élémentaire des nombres de Bernoulli, Paris, 1923.,

[33] R. Rado, A new proof of a theorem of Von-Staudt, I. London Math. Soc., 9. (1934). 85-88.

[34] Ireland Rosen. A Classical introduction to number theory,graduate texts in mathematics 84, seconde edition, springer-verlog 2003. 228-241.

[35] N. J. A. Sloane, On-Line Encyclopaedia of integer sequence,http ://oeis.org/

[36] Zhi-Hong Sun, Congruences concerning Bernoulli numbers and Bernoulli polynomials. Discret Applied Mathematics 105 (2000) 193-223

[37] Z-W. Sun and Li-Lu Zhao, Arithmetic Theory Of Harmonic Numbers. Proc. Amer. Math. Soc. 140(2012), no.2,415-428.

[38] Z-W. Sun, Arithmetic Theory Of Harmonic Numbers (II), preprint ar WIV : 0911.4433v7 [math.NT] (2011).

[39] Z-W. Sun, Introduction To Bernoulli and Euler Polynomials.(June 6,2002.)

[40] B. A. Venkov, Elementary Number Theory. Wolters-Noordhoff, Groningen, 1970.

[41] K. G. C. Von Staudt, Beweis eines Lehrattzes die Bernoulli'schen Zahlen betreffend, J. Reine Angrew. Math. 21, (1840), 372-374.

[42] L. C. Washington, Introduction to Cyclotomic Fields, 2nd ed., Graduate Texts in Mathematics, 83. Springer-Vetlag, New York, 1997.

[43] J. Wolstenholme, On certain properties of prime numbers. The Quarterly Journal of Pure and Applied Mathematics, vol. 5, 1862, 35-39.

[44] A. Zekiri and F. Bencherif, A new recursion relationship for Bernoulli numbers, annals mathematicae et informaticae 38 (2011), pp. 123-126.

[45] M. Zuber, Propriétés p-adiques de polynômes classiques. Université de Neuchatel, Institue de Mathématiques Chantemerle 2000. Suisse.