N d'ordre : 28/2014-M/MT

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

UNIVERSITE DES SCIENCES ET DE LA TECHNOLOGIE
HOUARI BOUMEDIENE
Faculté de Mathématiques

MÈMOIRE

Présenté pour l'obtention du diplôme de MAGISTER
EN: MATHÉMATIQUES
Spécialité: Arithmétique, codage et combinatoire: théorie des nombres

Abdelkader BENYATTOU

Sujet

ETUDE DE CERTAINES PROPRIETES DES NOMBRES DE BELL

Soutenu publiquement le 15-Juillet-2014 à l'USTHB devant le jury composé de :

M.BENSEBA Boualem,	Maître de Conférences / A,	à l'USTHB	Président
M. BENCHERIF Farid ,	Professeur	à l'USTHB	Directeur de mémoire
M.BOUROUBI Sadek,	Professeur	à l'USTHB	Examinateur
M. MIHOUBI Miloud ,	Maître de Conférences / A ,	à l'USTHB	Examinateur

Etude de certaines propriétés des nombres de Bell

Abdelkader BENYATTOU

Table des matières

Remerciements

Je tiens à remercier avant tout mon Directeur de Mémoire Monsieur le Professeur Farid BENCHERIF, pour m'avoir guidé, et m'avoir permis de mener à bien ce mémoire.

Je suis trés reconnaissant à Messieurs les Professeurs BENSEBA Boualem, BOUROUBI Sadek et MIHOUBI Miloud d'avoir accepté d'être membre du Jury de soutenance. Je suis particulièrement honoré que Monsieur le Professeur BENSEBA ait de plus accepté de présider ce jury.

Je tiens à remercier aussi mes enseigants, Madame et Messieurs les Professeurs BENFERHAT Leila, BENSEBA Boualem,BOUCHENNA Rachid et CHERCHEM Ahmed, pour tous les efforts qu'ils ont consentis pour les étudiants durant ma première année théorique de Magister.

Je remercie les membres du laboratoire d'Arithmétique Codage, Combinatoire et Calcul formel (LA3C) de l'USTHB pour m'avoir fourni de nombreux documents et pour avoir mis à ma disposition tous les moyens du laboratoire pour mener à bien ce travail.

Notations

1. $\mathbb{N} = \{0, 1, 2, \ldots\}$: ensemble des nombres entiers naturels.
2. $\mathbb{N}^* = \{1, 2, \ldots\}$: ensemble des nombres entiers naturels non nuls.
3. $\mathbb{Z}$: ensemble des nombres entiers rationnels.
4. $\mathbb{Q}$: ensemble des nombres rationnels.
5. $\mathbb{R}$: ensemble des nombres réels.
6. S_n : désigne le groupe symétrique de l'ensemble $E_n = \{1, 2, ..., n\}$ (groupe des permutations de l'ensemble $\{1, 2, ..., n\}$).
7. $\mathcal{B}_n$: n-ième nombre de Bell.
8. $A[x]$: anneau des polynômes à une indéterminée x et à coefficients dans l'anneau A.
9. $[n]$ désigne l'ensemble des l premiers nombres entiers, $l \geq 1, [n] = \{1, 2, 3, ..., n\}$
10. $|E|$ désigne le cardinal de l'ensemble E
11. e désigne l'élément neutre de groupe symétrique S_n
12. $\deg(P(x))$: degré du polynôme $P(x)$.
13. $a \mid b$ où a et b sont deux entiers signifie : "a divise b".
14. $a \nmid b$ où a et b sont deux entiers signifie : "a ne divise pas b".
15. (a, b) désigne le plus grand commun diviseur de a et b ($\text{pgcd}(a, b)$), a et b étant des entiers.
16. La lettre p désigne toujours un nombre premier (sauf mention contraire).
17. D_n : désigne le nombre de dérangements
18. $S_{n,k}$: désigne le nombre de surjection de E sur F,tels que $n = \text{card}(E)$ et $k = \text{card}(F)$
19. $\left\{ {n \atop k} \right\}$: désigne le nombre de Stirling de deuxième éspèce
20. $S(n, k)$ autre notation du nombre de stirling de deuxième espèce. On a $S(n, k) = \left\{ {n \atop k} \right\}$.
21. Pour $x \in \mathbb{Q}$, $\text{num}(x)$ et $\text{denom}(x)$ sont respectivement le numérateur et le dénominateur de x. On a $\text{denom}(x) = \min\{n \in \mathbb{N} : \quad nx \in \mathbb{Z}\}$, $x = \frac{\text{num}(x)}{\text{denom}(x)}$ et $(\text{num}(x), \text{denom}(x)) = 1$.

22. $\mathbb{Z}_{(n)}$ désigne l'anneau des n-entiers, $n \geq 1$ étant un entier. Un n-entier est un nombre rationnel dont le dénominateur est premier avec n.
23. Pour $a \in \mathbb{Q}$, $b \in \mathbb{Q}$ et $n \in \mathbb{N}^*$, $a \equiv b \pmod{n} \Leftrightarrow \text{num}(a-b) \equiv 0 \pmod{n}$. On a aussi $a \equiv b \pmod{n} \Leftrightarrow a - b \in n\mathbb{Z}_{(n)}$.
24. Pour $a \in \mathbb{Q}$, $b \in \mathbb{Q}$ et $n \in \mathbb{N}^*$, $a \equiv_n b \Leftrightarrow a \equiv b \pmod{n}$.
25. Pour $a \in \mathbb{Q}$ et $b \in \mathbb{Q}$ et $n \in \mathbb{N}^*$, $n \geq 2$, $a \not\equiv b \pmod{n}$ signifie que $a - b \notin n\mathbb{Z}_{(n)}$ et se lit : a est non congru à b modulo n.
26. Pour deux nombres entiers n et k tels que $0 \leq k \leq n$ on note
$$\binom{n}{k} = \frac{n!}{k!\,(n-k)!}.$$
27. $\delta_{i,j}$ symbole de Kronecker valant 1 su $i = j$ et 0 sinon.
28. Convention : $\sum_{i \in \varnothing} = 0$. Dans tout ce mémoire, on adopte la convention classique qu'une somme portant sur un indice parcourant l'ensemble vide vaut zéro.
29. Pour $x \in \mathbb{Z} - \{0\}$, $v_p(x) := \max\{m \in \mathbb{N} \ / \ p^m | x\}$, $v_p(x)$ est appelé valuation p-adique de x.
30. $w_p = \frac{(p-1)!+1}{p}$ désigne le quotient de Wilson de p.
31. Si $S(z) = \sum_{n=0}^{\infty} a_n z^n \in \mathbb{C}[[z]]$ alors pour tout $k \in \mathbb{N}$, $\left[z^k\right](S(z)) := a_k$
32. Pour tout nombre réel x :
    - $[x]$ désigne la partie entiére de x, c'est à dire l'unique nombre entier k vérifiant $x - 1 < k \leq x$.
    - $\{x\}$ désigne la partie fractionnaire de x , $\{x\} = x - [x]$ $(0 \leq \{x\} < 1)$.

.

« Time makes fools of us all. Our only comfort is that greater shall come after us. »

Eric Temple Bell (1883-1960)

Introduction

Pour tout entier $n \geq 0$, le n-ième nombre de Bell $\mathcal{B}_n$, du nom du mathématicien écossais Eric Temple Bell (1883-1960), est défini comme étant le nombre de partitions d'un ensemble de cardinal n pour $n \geq 1$, avec la convention $\mathcal{B}_0 = 1$. La suite $(\mathcal{B}_n)_{n\geq 0} = (1, 1, 2, 5, 15, 52, 203, 877, ...)$ des nombres de Bell constitue la suite d'entiers répertoriée $A000110$ dans l'encyclopédie en ligne des suites de nombres entiers [19] (OEIS). Cette suite possède de remarquables propriétés arithmétiques qui ont fait et continuent de faire l'objet de nombreuses recherches. Ainsi la congruence établie en 1933 par Touchard [23] affirmant que pour tout nombre premier p, on a

$$\mathcal{B}_{p+n} \equiv \mathcal{B}_n + \mathcal{B}_{n+1} \pmod{p} \quad \text{pour } n = 0, 1, 2...$$

a été de nouveau prouvée de manière élémentaire en 2009 par Greg Hurst et Andrew Schultz. [17]. On peut aussi citer la fameuse conjecture de Kurepa qui affirme que pour tout nombre premier $p \geq 3$, on a

$$\sum_{k=0}^{p-1} k! \not\equiv 0 \pmod{p}.$$

0n montre que l'on a pour tout nombre premier p,

$$\sum_{k=0}^{p-1} k! \equiv \mathcal{B}_{p-1} - 1 \pmod{p}.$$

La conjecture de Kurepa est ainsi équivalente à affirmer que pour tout nombre premier $p \geq 3$, on a

$$\mathcal{B}_{p-1} \not\equiv 1 \pmod{p}.$$

C'est sous cette forme que D. Barsky et B. Benzaghou [3]ont étudié cette conjecture et ont affirmé l'avoir prouvée en 2004. Malheureusement une erreur irréparable signalée par F. Bencherif a invalidé cette preuve [4]. Ainsi La conjecture de Kurepa reste encore, en 2014, une question ouverte.

En explorant exprérimentalement la somme $\sum_{n=0}^{p-1} \frac{\mathcal{B}_n}{(-8)^n}$ modulo un nombre premier, Zhi-Wei Sun constate que pour tout nombre premier $p \neq 2$, on a

$$\sum_{n=0}^{p-1} \frac{\mathcal{B}_n}{(-8)^n} \equiv -1853 \pmod{p}.$$

Il découvre expérimentalement que plus généralement, pour un entier $m \geq 1$ fixé, la somme $\sum_{n=0}^{p-1} \frac{\mathcal{B}_n}{(-m)^n}$ modulo un nombre premier p ne divisant pas m ne dépend pas du nombre premier p. Avec l'aide de Don Zagier, Zhi Wei Sun finit par démontrer un théorème intéressant et surpenant dans un article [25] intitulé "On a curious property of Bell numbers" paru en 2011. Désignons par D_n le nombre de dérangements d'un ensemble à n éléments, c'est à dire le nombre de permutations d'un ensemble à n éléments ne laissant aucun point fixe :

$$D_n = \operatorname{card}\left\{\sigma \in S_n \ / \ \sigma(x) \neq x \ \text{ pour } x \in \{1, 2, ..., n\}\right\}.$$

Le premier théorème remarquable établi par Zhi Wei Sun et Don Zagier dans [25] s'énonce ainsi

Théorème 1 *Pour tout entier $m \geq 1$ et pour tout nombre premier p ne divisant pas m.*

$$\sum_{n=1}^{p-1} \frac{\mathcal{B}_n}{(-m)^n} \equiv (-1)^{m-1} D_{m-1} \pmod{p}.$$

Un autre théorème établi par Zhi Wei Sun et Don Zagier dans [25] faisant intervenir la suite des polynômes de Touchard constitue une extension du théorème précédent. La suite $(T_n(x))_{n\geq 0}$ des polynômes de Touchard (appelé aussi par certains auteurs polynômes de Bell) est définie par

$$T_0(x) = 1, \ T_n(x) = \sum_{k=0}^{n} \left\{ n \atop k \right\} x^k \ , n \geq 1.$$

$\left(\left\{ n \atop k \right\} \right)_{(n,k)\in\mathbb{N}\times\mathbb{N}}$ étant la famille des nombres de Stirling de deuxième éspèce.

Le deuxième théorème remarquable établi par Zhi Wei Sun et Don Zagier dans [25] s'énonce alors ainsi

Théorème 2 *Pour tout entier $m \geq 1$ et pour tout nombre premier p, tels que $p \nmid m$ on a :*

$$(-x)^m \sum_{0<n<p} \frac{T_n(x)}{(-m)^n} \equiv -x^p \sum_{l=0}^{m-1} \frac{(m-1)!}{l!} (-x)^l \left(\operatorname{mod} p\mathbb{Z}_p[x]\right).$$

Ce mémoire est consacré à une étude détaillée de la preuve de chacun de ces deux théorèmes donnée par Zhi Wei Sun et Don Zagier dans [25] . Il comporte quatre chapitres. Le premier chapitre est consacré à une étude de la suite $(D_n)_{n\geq 0}$. Au deuxième chapitre, nous étudirons la famille des nombres de Stirling $\left(\left\{ n \atop k \right\} \right)_{(n,k)\in\mathbb{N}\times\mathbb{N}}$ de deuxième espèce. Nous nous intéresserons aux relations de récurrence, aux formules explicites et aux fonctions génératrices associées à

cette famille d'entiers. Le troisième chapitre est consacré à une étude de la suite $(\mathcal{B}_n)_{n\geq 0}$ des nombres de Bell. Le quatrième et dernier chapitre est consacré à la preuve des deux théorèmes de Zhi-Wei Sun et Don Zagier. Nous conclurons cette étude par les perspectives que ce travail nous permet d'envisager.

Chapitre 1

Congruences dans $\mathbb{Z}$ et nombres de Dérangements

1.1 Introduction

Dans ce chapitre, nous rappelons quelques propriétés concernant les congruences définies sur l'anneau $\mathbb{Z}$ et nous nous intéressons à certaines propriétés arithmétiques de la suite $(D_n)_{n\geq 0}$, D_n étant le nombre de dérangements d'un ensemble de n éléments.

1.2 Congruences dans $\mathbb{Z}$

Soit $x \in \mathbb{Q}$, alors x s'écrit de manière unique sous la forme $x = \frac{u}{v}$ avec $(u, v) \in \mathbb{Z} \times \mathbb{N}^*$ et $(u, v) = 1$. Les entiers u et v sont appelés numérateur et dénominateur de x. On les note respectivement $\text{num}(x)$ et $\text{denom}(x)$. On a

$$\text{denom}(x) = \min\{n \in \mathbb{N}^* / \ nx \in \mathbb{Z}\} \quad \text{et} \quad \text{num}(x) = x\,\text{denom}(x).$$

Désignons par $\mathbb{P} = \{2, 3, 5, 7, 11, 13, 17, ...\}$ l'ensemble des nombres premiers. Le théorème fondamentale de l'arithmétique peut se formuler comme suit : pour tout élément a non nul de $\mathbb{Z}$, il existe une unique famille d'entiers naturels $(\alpha_p(a))_{p\in\mathbb{P}}$ tels que $\{p \in \mathbb{P} / \ \alpha_p(a) \neq 0\}$ est fini (les $\alpha_p(a)$ sont des entiers tous nuls sauf un nombre fini) et tel que

$$a = \pm \prod_{p\in\mathbb{P}} p^{\alpha_p(a)}.$$

Pour tout nombre premier p, l'entier $\alpha_p(a)$ est le plus grand entier positif r tel que $p^r \mid a$. Par convention, on pose $\alpha_p(0) = \infty$, où ∞ est un symbole adjoint à $\mathbb{Z}$ vérifiant $a + \infty = \infty + a = +\infty$ et $a < \infty$, pour tout entier a. La fonction $v_p : \ \mathbb{Q} \longmapsto \mathbb{Z} \cup \{\infty\}$ définie par

$$v_p(x) = \alpha_p(\text{num}(x)) - \alpha_p(\text{denom}(x)) \ \text{ si } x \neq 0 \ \text{ et } v_p(0) = \infty,$$

appelée "valuation p-adique" vérifie les propriétés suivantes, x et y étant des nombres rationnel, on définit une application pour $p \in \mathbb{P}$, la fonction $v_p : \mathbb{Q} \longmapsto \mathbb{Q} \cup \{\infty\}$ est appelée "valuation p-adique" qui prolonge la valuation p-adique définie sur $\mathbb{Z}$ et qui vérifie les propriétés suivantes

1. $v_p(x) = \infty \Longleftrightarrow x = 0$,
2. $v_p(xy) = v_p(x) + v_p(y)$,
3. $v_p(x+y) \geq \min\{v_p(x), v_p(y)\}$.

De plus pour tout nombre rationnel $x \neq 0$, on a

$$x \in \mathbb{Z} \Longleftrightarrow (\forall p \in \mathbb{P} : \ v_p(x) \geq 0)$$

Soit p un nombre premier. On appelle p-entier tout nombre rationnel dont le dénominateur n'est pas divisible par p. Notons $\mathbb{Z}_{(p)}$ l'ensemble des p-entiers. Il est facile de constater que

$$\begin{aligned} \mathbb{Z}_{(p)} &= \{x \in \mathbb{Q} / \ \ p \nmid \operatorname{denom}(x)\} \\ &= \{x \in \mathbb{Q} / \ \ v_p(x) \geq 0\}. \end{aligned}$$

Il est aussi facile de prouver que $\mathbb{Z}_{(p)}$ est un sous-anneau de $\mathbb{Q}$ et que de plus $\mathbb{Z} \subset \mathbb{Z}_{(p)}$.

Le résulat suivant est trés utile

Formule de Legendre

Théorème 3 *Pour tout entier $n \geqslant 1$ et pour tout nombre premier p, on a*

$$v_p(n!) = \sum_{k=1}^{\infty} \left\lfloor \frac{n}{p^k} \right\rfloor \tag{1.1}$$

Preuve. Soit un entier $n \geq 1$ et p un nombre premier, posons pour tout entier naturel k.

$$u_k = v_p\left(\left\lfloor \frac{n}{p^k} \right\rfloor ! \right).$$

On constate tout de suite que

$$u_0 = v_p(n!).$$

De plus si k est tel que $p^k > n$, c'est à dire si $k \geq \left\lfloor \frac{\ln n}{\ln p} \right\rfloor + 1$, alors $\frac{n}{p^k} \in [0,1[$, $\left\lfloor \frac{n}{p^k} \right\rfloor = 0$ et $u_k = v_p(0) = 0$. On a donc en posant $t = \left\lfloor \frac{\ln n}{\ln p} \right\rfloor + 1$

$$\begin{aligned} v_p(n!) &= \sum_{k=1}^{t+1} (u_{k-1} - u_k) \\ &= \sum_{k=1}^{\infty} (u_{k-1} - u_k). \end{aligned}$$

Pour prouver la relation (1.1), il suffit de prouver que pour tout $k \in \mathbb{N}^*$, on a

$$u_{k-1} - u_k = \left\lfloor \frac{n}{p^k} \right\rfloor . \tag{1.2}$$

Pour cela, posons $m = \left\lfloor \frac{n}{p^{k-1}} \right\rfloor$ et calulons $v_p(m!)$. La division euclidienne de m par p s'écrit

$$m = pq + r \quad \text{avec } 0 \leq r < p.$$

En remarquant que $\left\lfloor \frac{1}{p} \lfloor x \rfloor \right\rfloor = \left\lfloor \frac{x}{p} \right\rfloor$ pour tout $x \in \mathbb{R}$, on a

$$q = \left\lfloor \frac{m}{p} \right\rfloor = \left\lfloor \frac{1}{p} \left\lfloor \frac{n}{p^{k-1}} \right\rfloor \right\rfloor . = \left\lfloor \frac{n}{p^k} \right\rfloor .$$

Dans $\mathbb{N}$, comme les seules multiples de p compris entre 1 et m sont les entiers jp avec $1 \leq j \leq q$, on en déduit que pour $k \in \mathbb{N}^*$, on a

$$\begin{aligned} u_{k-1} - u_k &= v_p(m!) - v_p(q!) \\ &= \left(\sum_{j=1}^{q} v_p(jp) \right) - v_p(q!) \\ &= \left(\sum_{j=1}^{q} (1 + v_p(j)) \right) - v_p(q!) \\ &= q + v_p(q!) - v_p(q!) = \left\lfloor \frac{n}{p^k} \right\rfloor . \end{aligned}$$

La relation (1.2) est ainsi bien établie. La preuve du théorème est complète. □

Le théorème suivant précise la valuation p-adique de $\binom{p^m}{k}$, pour $k \in \{1, 2, ..., p^m - 1\}$.

Théorème 4 *Pour tout entier p premier et m un entier ≥ 1, alors on a*

$$v_p\left(\binom{p^m}{k} \right) = m - v_p(k), \text{ pour tout } k \in \{1, 2, ..., p^m - 1\} .$$

Preuve. D'après le théorème 3, on a

$$\begin{aligned} v_p\left(\binom{p^m}{k} \right) &= v_p\left(\frac{p^m!}{k!(p^m - k)!}\right) \\ &= v_p(p^m!) - (v_p(k!) + v_p((p^m - k)!) \\ &= \sum_{j=1}^{\infty} \left\lfloor \frac{p^m}{p^j} \right\rfloor - \left(\sum_{j=1}^{\infty} \left\lfloor \frac{k}{p^j} \right\rfloor + \sum_{j=1}^{\infty} \left\lfloor \frac{p^m - k}{p^j} \right\rfloor \right) \\ &= \sum_{j=1}^{m} p^{m-j} - \left(\sum_{j=1}^{m} \left\lfloor \frac{k}{p^j} \right\rfloor + \sum_{j=1}^{m} \left\lfloor p^{m-j} + \left(\frac{-k}{p^j} \right) \right\rfloor \right) \end{aligned}$$

Comme on sait que pour $x \in \mathbb{R}$ et $n \in \mathbb{Z}$, on a $\lfloor x+n \rfloor = \lfloor x \rfloor + n$, on en déduit que

$$\begin{aligned} v_p(\binom{p^m}{k}) &= \sum_{j=1}^{m} p^{m-j} - \left(\sum_{j=1}^{m} \left\lfloor \frac{k}{p^j} \right\rfloor + \sum_{j=1}^{m} p^{m-j} + \sum_{j=1}^{m} \left\lfloor \frac{-k}{p^j} \right\rfloor \right) \\ &= \sum_{j=1}^{m} \left(- \left\lfloor \frac{k}{p^j} \right\rfloor - \left\lfloor \frac{-k}{p^j} \right\rfloor \right) \end{aligned} \tag{1.3}$$

On vérifie aisément que .

$$- \left\lfloor \frac{k}{p^j} \right\rfloor - \left\lfloor \frac{-k}{p^j} \right\rfloor = \begin{cases} 1 & \text{si } p^j \nmid k, \\ 0 & \text{si } p^j \mid k. \end{cases}$$

On déduit de (1.3) que

$$\begin{aligned} v_p(\binom{p^m}{k}) &= \operatorname{card} \left\{ j \in \{1,2,\ldots,m\} / \ \ p^j \nmid k \right\} \\ &= m - \operatorname{card} \left\{ j \in \{1,2,\ldots,m\} / \ \ p^j \mid k \right\} \\ &= m - v_p(k). \end{aligned}$$

□

Le Théorème 4 a pour corollaire

Corollaire 5 *Pour tout nombre premier p et pour tout entier $m \geq 1$, on a*

$$\binom{p^m}{k} \equiv 0 \mod p, \ \ k \in \{1,2,..p^m - 1\}. \tag{1.4}$$

Preuve. En effet, soit p un nombre premier, $m \geq 1$, un entier et $k \in \{1,2,..p^m-1\}$, on a d'après le théorème 4,

$$v_p(\binom{p^m}{k}) = m - v_p(k).$$

Pour prouver (1.4), il suffit de montrer que $m - v_p(k) \geq 1$. Raisonnons par l'absurde. Si on avait $m - v_p(k) < 1$, on aurait $v_p(k) > m$ et p^m diviserait k. On aurait alors $k \geq p^m$, en contradiction avec l'hypothèse $k < p^m$. On a donc bien $m - v_p(k) \geq 1$. Le corollaire 5 est bien prouvé. □

Le théorème qui suit est connu sous le nom de petit Théorème de Fermat du nom de Pierre de Fermat (1601-1665). Selon Michel Demazure [11] ce théorème a été enoncé par Fermat en 1640 et demontré par Euler en 1736.

Théorème 6 *Soit p un nombre premier. On a alors pour tout entier a*

$$a^p \equiv a \mod p, \ \ \textit{pour tout entier } a \tag{1.5}$$

et si de plus p ne divise pas a, alors on a

$$a^{p-1} \equiv 1 \bmod p, \text{ pour tout entier } a \text{ premier à } p. \tag{1.6}$$

Preuve. Pour tout entier a, on a par la formule du binôme et par le théorème 5

$$(a+1)^p - (a^p+1) = \sum_{k=1}^{p-1} \binom{p}{k} a^k \equiv 0 \bmod p.$$

Comme pour $a = 0$, la relation $a^p - a \equiv 0 \bmod p$, est verifiée. On peut raisonner par récurrence pour l'établir pour tout entier $a \geq 0$. La relation est alors aussi vérifiée pour tout entier $a < 0$, car dans ce cas se ramène au cas où $a \geq 0$ en remarquant qu'on a alors $a^p - a = -(|a|^p - |a|) \equiv 0 \bmod p$, la relation (1.5) est ainsi établie. On a alors $a(a^{p-1} - 1) \equiv 0 \bmod p$, si p ne divise pas a, on en déduit qu'on a $a^{p-1} - 1 \equiv 0 \bmod p$, ce qui prouve (1.6). □

1.3 Nombres de dérangements

Il est bien connu que l'ensemble $S(E)$ des permutations d'un ensemble E, c'est à dire l'ensemble des bijections de E dans lui même muni de la loi de comosition des applications est un groupe appelé groupe symétrique de l'ensemble E, il est facile de prouver que si E et F ont même cardinalité, alors les groupes $S(E)$ et $S(F)$ sont isomorphes. Dans le cas où E et fini et possède n éléménts, on peut choisir pour l'étude du groupe $S(E)$ l'ensemble $E = E_n = \{k \in \mathbb{N} / \ 1 \leq k \leq n\}$. On note alors S_n le groupe $S(E_n)$. On sait alors que S_n est un groupe d'ordre $n!$. Pour $n \geq 1$, on convient souvent de définir un élément $\sigma \in S_n$ l'écrivant

$$\sigma = \begin{pmatrix} 1 & 2 & \dots & i & \dots & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(i) & \dots & \sigma(n) \end{pmatrix}.$$

On appelle **point fixe** de $\sigma \in S_n$ tout entier $k \in \sigma \in S_n$ tel que $\sigma(k) = k$. On appelle **dérangement** toute permutation $\sigma \in S_n$ sans point fixe. On désigne par D_n le nombre de dérangements de l'ensemble E_n. Pour $n = 0$, on a $D_0 = 1$.

Par exemple, si on considère le groupe S_3, on a $S_3 = \{I, \sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5\}$ avec

$$\begin{aligned} I &= \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \ \sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \ \sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \\ \tau_1 &= \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \ \tau_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \ \tau_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}. \end{aligned}$$

Les transpositions τ_1, τ_2 et τ_3 ont chacune un seul point fixe. La permutation I admet trois points fixes par contre les permautions circulaires σ_1 et σ_2 sont des permutaions sans point fixe, ce sont les deux seuls dérangements de l'ensemble $E_3 = \{1, 2, 3\}$. On a donc $D_3 = 2$.

Table de valeurs

Petit table de valeurs de D_n

n	0	1	2	3	4	5	6	7	8
D_n	1	0	1	2	9	44	265	1854	14833

Dans ce chapitre, nous allons étudier quelques propriétés importantes de la suite d'entiers D_n.

1.4 Quelques propriétés du nombre de dérangements

Le théorème suivant donne une relation de récurrence vérifiée par la suite $(D_n)_{n\geq 0}$.

Théorème 7 *Soit n un entier et p un nombre premier. Alors on a*

1. $$n! = \sum_{k=0}^{n} \binom{n}{k} D_k = \sum_{k=0}^{n} \binom{n}{k} D_{n-k}, \quad (n \geq 0), \tag{1.7}$$

2. $$D_{n+1} = (n)(D_n + D_{n-1}), \quad (n \geq 2) \tag{1.8}$$

3. $$D_n = nD_{n-1} + (-1)^n, \quad (n \geq 2) \tag{1.9}$$

4. $$D_n = n!(\sum_{k=0}^{n} \frac{(-1)^k}{k!}), \quad (n \geq 0), \tag{1.10}$$

5. $$D_{n+p} \equiv -D_n \pmod{p}, \quad (n \geq 0). \tag{1.11}$$

6. *Pour tout tout entiers n_1 et n_2, on a*

$$n_1 \equiv n_2 \pmod{p} \implies (-1)^{n_1} D_{n_1} \equiv (-1)^{n_2} D_{n_2} \pmod{p}. \tag{1.12}$$

Preuve.

1. Pour $n = 0$, la relation (1.7) est vérifiée car $D_0 = 1$. Pour $n \geq 1$, désignons par $\mathcal{P}_k$ l'ensemble des permutations de E_n ayant exactement k points fixes. Il est clair que $\{\mathcal{P}_0, \mathcal{P}_1, ..., \mathcal{P}_n\}$ est une partition de S_n,. Comme $|S_n| = n!$, on endéduit que

$$\sum_{k=0}^{n} \text{card}(\mathcal{P}_k) = n!. \tag{1.13}$$

Montrons que pour tout entier k tel que $0 \leq k \leq n$, on a

$$\text{card}(\mathcal{P}_k) = \binom{n}{k} D_{n-k}. \tag{1.14}$$

On a trivialement $D_n = \text{card}(\mathcal{P}_0)$, et $\text{card}(\mathcal{P}_n) = 1 = D_0$. La relation (1.14) est donc vérifiée pour $k = 0$ et pour $k = n$. Si $1 \leq k \leq n-1$, un élément de $\sigma \in \mathcal{P}_k$ est complètement déterminé par le choix de ses k points fixes $\{i_1, i_2, \ldots, i_k\}$ qui constitue une partie à k éléments de E_n, soit $\binom{n}{k}$ possibilités pour ce choix, et par le choix de la permutation induite sur les $n-k$ éléments restants, la restriction de σ à l'ensemble $F = E_n - \{i_1, i_2, \ldots, i_k\}$ étant un dérangement de F, il y a D_{n-k} choix possibles. On a donc exactemant $\binom{n}{k} D_{n-k}$. manières de construire un élément de $\mathcal{P}_k$ La formule (1.14) est ainsi justifiée. De (1.14) et (1.13), on déduit que l'on a

$$n! = \sum_{k=0}^{n} \binom{n}{k} D_{n-k}. \tag{1.15}$$

En changeant k en $n-k$ dans la relation (1.15) et en remarquant que $\binom{n}{n-k} = \binom{n}{k}$, on obtient

$$n! = \sum_{k=0}^{n} \binom{n}{k} D_k. \tag{1.16}$$

La relation (1.7) résulte alors de (1.15) et (1.16).

2. On notra $\mathcal{D}_n$ l'ensemble des dérangements de $E_n = \{1, 2, ..., n\}$. Si $\sigma \in \mathcal{D}_{n+1}$, l'image de $n+1$ par σ est dans E_n. Pour tout $k \in E_n$, notons F_k l'ensemble des éléments σ de D_{n+1} tels que $\sigma(n+1) = k$. Les F_k partitionnent $\mathcal{D}_{n+1}$. Nous allons prouver que le cardinal de F_k est égal à $D_n + D_{n-1}$ quel que soit l'entier k. On fixe donc k et on partitionne F_k en deux : G_k désigne l'ensemble des $\sigma \in F_k$ tels que $\sigma(k) = n+1$ et H_k désigne le complémentaire de G_k dans F_k. Il est clair qu'un élément de G_k est parfaitement déterminé par sa restriction à l'ensemble $\{1, ..., k-1, k+1, ..., n\}$, cette restriction devant être un dérangement. Il en résulte que $\text{card}(G_k) = D_{n-1}$. Cherchons maintenant le cardinal de H_k. Soit $\sigma \in H_k$. Alors $\sigma^{-1}(n+1) \neq k$. Considérons le dérangement $\widetilde{\sigma}$ de E_n défini par $\widetilde{\sigma}(i) = \sigma(i)$ pour $i \neq \sigma^{-1}(n+1)$, et $\widetilde{\sigma}(\sigma^{-1}(n+1)) = k$ (on a simplement ≪court-circuité≫ $n+1$). Il est clair quez l'application de H_k dans $\mathcal{D}_n$ qui à σ associe $\widetilde{\sigma}$ est bijective de sort que $\text{card}(G_k) = D_n$. On obtient donc $\text{card}(F_k) = D_n + D_{n-1}$, pour tout k, ce qui donne la relation de récurrence $D_{n+1} = (n)(D_n + D_{n-1})$

3. On effectue une récurrence sur n, le rrésultat étant vrai pour $n = 2$ puisque $D_2 = 1$ et $D_1 = 0$. Supposons la formule vraie au rang n. On a alors

$$\begin{aligned} D_{n+1} &= n(D_n + D_{n-1}) = nD_n + nD_{n-1} \\ &= nD_n + D_n - (-1)^n = (n+1)D_n + (-1)^{n+1}, \end{aligned}$$

ce qui est la formule au rang $n+1$.

4.
$$\frac{D_k}{k!} - \frac{D_{k-1}}{(k-1)!} = \frac{(-1)^k}{k!}$$
$$\sum_{k=1}^{n}\left(\frac{D_k}{k!} - \frac{D_{k-1}}{(k-1)!}\right) = \sum_{k=1}^{n}\frac{(-1)^k}{k!}$$
$$\frac{D_n}{n!} - \frac{D_0}{0!} = \sum_{k=1}^{n}\frac{(-1)^k}{k!}$$
$$D_n = n!\sum_{k=0}^{n}\frac{(-1)^k}{k!}$$

5.
$$\begin{aligned}
(-1)^n D_n &= (-1)^n \sum_{k=0}^{n}\frac{n!(-1)^k}{k!} \\
&= \sum_{k=0}^{n}(-1)^{n+k}\prod_{0\le s<n-k}(n-s) \\
&= \sum_{k=0}^{n}(-1)^{n-k}\prod_{0\le s<n-k}(n-s)\,,\ n-k=r \\
&= \sum_{r=0}^{n}(-1)^{r}\prod_{0\le s<r}(n-s)\,,\ \text{ce qui implique} \\
D_n &= \sum_{r=0}^{n}(-1)^{r+n}\prod_{0\le s<r}(n-s)
\end{aligned}$$

avec
$$T_k(x) = \prod_{0\le s<k}(x-s) = x(x-1)\dots(x-k+1).$$

On constate que $T_k(n+p) \equiv T_k(n) \pmod p$ et $T_k(n) = 0$ pour $k > n$. On en déduit que $D_{n+p} \equiv -D_n \pmod p$

6. Pour tout nombre premier p et pour tous entiers n_1 et n_2, on a
$$n_1 \equiv n_2 \pmod p \quad \Longrightarrow (-1)^{n_1} D_{n_1} \equiv (-1)^{n_2} D_{n_2} \pmod p\,. \tag{1.17}$$

Cette relation se déduit aisémént de la précédente.

□

1.5 Identité d'Abel et relation de Ping Sun

Afin de prouver une célèbre identité du au mathématicien Abel et d'en déduire ensuite une formulation de D_n due au mathématicien Ping Sun, nous allons établir un lemme qui nous sera utile. Dans ce qui suit $(A_n(x))_{n\geq 0}$ est la suite de polynômes de $\mathbb{C}[x]$ définie par

$$A_n(x) = \frac{1}{n!}x\,(x-n\alpha)^{n-1}, \tag{1.18}$$

α étant un nombre complexe donné.

Lemme 8 .

1. *Pour tout entier $n \geq 0$, on a*

$$\deg(A_n(x)) = n \text{ et } A_n(0) = \delta_{n,0}.$$

2. *La suite de polynômes $(A_n(x))_{n\geq 0}$ est une base du $\mathbb{C}$ espace vectoriel $\mathbb{C}[x]$.*
3. *Pour tour entier $n \geq 1$, on a*

$$A_n^{'}(x) = A_{n-1}(x-\alpha). \tag{1.19}$$

4. *Pour tous entiers n et k tels que $0 \leq k \leq n$, on a*

$$A_n^{(k)}(x) = A_{n-k}(x-k\alpha). \tag{1.20}$$

Preuve.

1. A l'aide de la définition (1.18), on constate que $A_n(x)$ est un polynôme de $\mathbb{C}[x]$, de degré n avec $A_0(x) = 1$ et de coefficient dominant $\frac{1}{n!}$ pour $n \geq 1$, on constate aussi que $A_n(0) = 0$ pour $n \geq 1$. Par conséquent, on a $A_n(0) = \delta_{n,0}$ pour tout entier $n \geq 0$.
2. Ainsi la suite de polynômes $(A_k(x))_{k\geq 0}$ est un système échelonné de $\mathbb{C}[x]$, c'est donc une base du $\mathbb{C}$ espace vectoriel $\mathbb{C}[x]$
3. Pour $1 \leq k \leq n$, on a

$$\begin{aligned} A_n^{'}(x) &= \frac{1}{n!}\left((x-n\alpha)^{n-1} + (n-1)x\,(x-n\alpha)^{n-2}\right) \\ &= \frac{1}{(n-1)!}(x-\alpha)\,(x-n\alpha)^{n-2} = A_{n-1}^{'}(x-\alpha) \end{aligned}$$

4. On obtient (1.20) à l'aide d'une récurrence finie, en exploitant la relation (1.19).

□

La formule du binôme affirme que pour tout entier $n \geq 0$, on a pour tous nombres complexes x et y

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

L'identité d'Abel, donnée dans le théorème suivant est une généralisation de cette formule.

Théorème 9 *[9] Soit x, y, α des nombres complexes quelconque on a*

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x\,(x-k\alpha)^{k-1}\,(y+k\alpha)^{n-k} \qquad (\textit{Identité d'Abel}) \tag{1.21}$$

Preuve. La famille de polynômes $(A_k(x))_{0\leq k\leq n}$ de $\mathbb{C}_n[x]$ constitue une base de ce $\mathbb{C}$ espace vectoriel. $\mathbb{C}_n[x]$ étant le sous-espace vectoriel de $\mathbb{C}[x]$ constitué par les polynômes de $\mathbb{C}[x]$ de degré inférieur ou égal à n. Soit $\beta \in \mathbb{C}$, on a $(x+\beta)^n \in \mathbb{C}_n[x]$. On en déduit qu'il existe des constantes λ_0,λ_1, ...,λ_n telles que

$$(x+\beta)^n = \sum_{j=0}^{n} \lambda_j A_j(x). \tag{1.22}$$

Pour $k \in \{0, 1, ...n\}$, égalons les dérivées d'ordre k de chacun des membres de l'égalité (1.22), comme $A_j^{(k)}(x) = 0$ pour $k > j$, on obtient à l'aide de (1.20)

$$\begin{aligned} k!\binom{n}{k}(x+\beta)^{n-k} &= \sum_{j=k}^{n} \lambda_j A_j^{(k)}(x) \\ &= \sum_{j=k}^{n} \lambda_j A_{j-k}(x-k\alpha) \end{aligned} \tag{1.23}$$

Pour $x = k\alpha$, la relation (1.23) devient

$$\begin{aligned} k!\binom{n}{k}(\beta+k\alpha)^{n-k} &= \sum_{j=k}^{n} \lambda_j A_{j-k}(0) \\ &= \sum_{j=k}^{n} \lambda_j \delta_{j-k,0} \\ &= \lambda_k. \end{aligned} \tag{1.24}$$

De (1.24), (1.22) et (1.18), on déduit que l'on a

$$\begin{aligned}(x+\beta)^n &= \sum_{k=0}^{n}\lambda_k A_k(x)\\ &= \sum_{k=0}^{n}\binom{n}{k}(\beta+k\alpha)^{n-k}x\,(x-k\alpha)^{n-1}\\ &= \sum_{k=0}^{n}\binom{n}{k}x\,(x-k\alpha)^{k-1}\,(\beta+k\alpha)^{n-k}\,. \qquad (1.25)\end{aligned}$$

La relation (1.25) étant vérifiée pour tout $\beta \in \mathbb{C}$, (1.21) en résulte. □

Corollaire 10 *Pour tout entier $n \geq 0$, on a*

$$\sum_{k=0}^{n}\binom{n}{k}(-1)^{n-k}\,x\,(x+k)^{k-1}\,(x+k+1)^{n-k} = (-1)^n \qquad (1.26)$$

Preuve. En choisissant $\alpha = -1$ et $y = -x-1$ dans l'identité d'Abel, on obtient la relation (1.26). □

Pour tout entier $n \geq 0$, posons

$$d_n(x) = \sum_{k=0}^{n}\binom{n}{k}(-1)^{n-k}\,(x+k)^k\,(x+k+1)^{n-k}\,. \qquad (1.27)$$

Nous allons prouver que la suite de polynômes $(d_n(x))_{n\geq 0}$ est une suite constante. Pour cela, le corollaire 10 va nous permettre d'établir aisément le lemme suivant.

Lemme 11 *Pour tout entier $n \geq 1$, on a*

$$d_n(x) - nd_{n-1}(x+1) = (-1)^n. \qquad (1.28)$$

Preuve. Pour tout entier $n \geq 1$, on a

$$\begin{aligned}nd_{n-1}(x+1) &= \sum_{k=0}^{n-1} n\binom{n-1}{k}(-1)^{n-1-k}\,(x+k+1)^k\,(x+k+2)^{n-1-k}\\ &= \sum_{k=1}^{n} n\binom{n-1}{k-1}(-1)^{n-k}\,(x+k)^{k-1}\,(x+k+1)^{n-k}\\ &= \sum_{k=0}^{n} k\binom{n}{k}(-1)^{n-k}\,(x+k)^{k-1}\,(x+k+1)^{n-k}\,. \qquad (1.29)\end{aligned}$$

Des relations (1.29), (1.27) et (1.26) on déduit que l'on a

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

On a ainsi prouvé la relation (1.28) □

L'identité suivante a été établie par Ping Sun en 2004 [20].

Théorème 12 *[20] Pour tout entier $n \geq 0$, on a*

$$D_n = \sum_{k=0}^{n} \binom{n}{k} (-1)^{n-k} (x+k)^k (x+k+1)^{n-k}. \tag{1.30}$$

Preuve. Avec la défintion (1.27), la realtion (1.30) à prouvé s'écrit

$$d_n(x) = D_n. \tag{1.31}$$

De la relation (1.28), on déduit que pour tout entier $n \geq 1$, on a

$$\frac{d_n(x)}{n!} - \frac{d_{n-1}(x+1)}{(n-1)!} = \frac{(-1)^n}{n!}. \tag{1.32}$$

Soit $n \in \mathbb{N}$. Pour $0 \leq k \leq n$, posons

$$u_k = \frac{d_{n-k}(x+k)}{(n-k)!}.$$

On déduit de la relation (1.32) que l'on a pour $0 \leq k \leq n-1$ □

$$u_k - u_{k+1} = \frac{(-1)^{n-k}}{(n-k)!}$$

Par suite, on a pour $n \geq 0$

$$\sum_{k=0}^{n-1} (u_k - u_{k+1}) = \sum_{k=0}^{n-1} \frac{(-1)^{n-k}}{(n-k)!},$$

c'est à dire

$$u_0 - u_n = \sum_{k=1}^{n} \frac{(-1)^k}{k!}$$

$$\frac{d_n(x)}{n!} - \frac{d_0(x+n)}{0!} = \sum_{k=1}^{n} \frac{(-1)^k}{k!}$$

Comme on a $d_0(x+n) = 1$, on en déduit que pour tout entier $n \geq 0$, on a

$$d_n(x) = n! \sum_{k=0}^{n} \frac{(-1)^k}{k!} = D_n.$$

La relation (1.31) est établie. La preuve du théorème 12 est complète.

Chapitre 2

Congruences dans $\mathbb{Q}$ et nombres de Stirling

2.1 Introduction

Dans ce chapitre nous définirons le nombre de Stirling de deuxième éspèce et nous présenterons quelques unes de ses propriétés.

Définition 13 *On appelle nombre de stirling de deuxième espèce le nombre de partitions,de l'ensemble* $X = \{1, 2, ...n\}, n \in \mathbb{N}$, *en* k *partie non vides*

Notation 14 *le nombre de stirling de deuxiéme espèce noté :* $S(n,k)$ *ou* $S_n^{(k)}$ *ou* $\left\{ {n \atop k} \right\}$.

2.2 Relation de récurrence pour les nombres de Stirling de deuxième éspèce et Formule explicite pour les nombres de Stirling de deuxième espèce

Le théorème suivant donne une relation de récurrence verifiée par la famille des nombres de Stirling $\left(\left\{ {n \atop k} \right\} \right)_{(n,k)\in\mathbb{N}\times\mathbb{N}}$.

Théorème 15 *Pour tout* $n \in \mathbb{N}^*$ *et* $k \in \mathbb{N}^*$, *tels que* $0 < k \leq n$ *on a la relation de récurrence*

$$\forall k > 0,\ \left\{ {n+1 \atop k} \right\} = \left\{ {n \atop k-1} \right\} + k\left\{ {n \atop k} \right\},\ \text{avec } \left\{ {0 \atop 0} \right\} = 1 \text{ et } \forall n > 0, \left\{ {n \atop 0} \right\} = 0, \left\{ {n \atop n} \right\} = 1 \quad (2.1)$$

Preuve. Notons $n = \text{card}(E)$ et $k = \text{card}(F)$ et $S_{n,k}$ le nombre de surjection de E sur F, si $k > n$, il est clair que $S_{n,k} = 0$, si $n \geq k$ que vaut $S_{n,k}$?.Pour définir une surjection de E sur F, il suffit de se donner une partition de E en k sous ensembles non vides, puis une bijection de l'ensemble de ces k sous ensembles sur F.D'aprés le principe multiplicatif, on a

$$S_{n,k} = \left\{ n \atop k \right\} k!. \tag{2.2}$$

Considérons un ensemble X de cardinal $n+1$, $X = \{x_1, x_2, ...x_n, x_{n+1}\}$,le nombre de k-partition de X se répartissent en deux catégories, celle qui contiennent le singleton $\{x_{n+1}\}$, il ya en a $\left\{ n \atop k-1 \right\}$, (nombre de$k-1$ partitions de $X = \{x_1, x_2, ...x_n\}$), et celle qui ne contiennent pas le singleton $\{x_{n+1}\}$, il ya $\left\{ n \atop k \right\}$, k-partition de $\{x_1, x_2, ...x_n\}$ et k possibilités d'yadjoindre l'élément x_{n+1}, soit au total $k\left\{ n \atop k \right\}$.D'aprés le principe de la somme on a bien

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

□

Théorème 16 *[13] Pour tout $n \in \mathbb{N}^*$ et $k \in \mathbb{N}^*$, tels que $0 < k < n$ on a*

$$\left\{ n \atop k \right\} = \frac{1}{k!} \sum_{n_1+.....n_k=n} \frac{n!}{n_1!.....n_k!}, \text{ avec } \left\{ 0 \atop 0 \right\} = 1 \text{ et } \forall n > 0, \ \left\{ n \atop 0 \right\} = 0, \ \left\{ n \atop n \right\} = 1 \tag{2.3}$$

Preuve. Soient $E = \{x_1, ..., x_n\}$ et P le sous ensemble formé des éléments $(A_1, ..., A_k) \in E^k$, tels que $\{A_1, ..., A_k\}$ soit une partition de E, on cherche le cardinal de P.Pour obtenir $\{A_1, ...A_k\}$ pour tout i avec $\text{card}\, A_i = n_i$ il ya

$$\begin{aligned}
&\binom{n}{n_1} \text{ façons de choisir } A_1 \\
&\binom{n-n_1}{n_2} \text{ façons de choisir } A_2 \\
&\vdots \\
&\binom{n-(n_1+n_2+.....n_{k-1})}{n_k} \text{ façons de choisir } A_k,
\end{aligned}$$

alors le nombre de façons de choisir $\{A_1, ...A_k\}$, avec $\text{card}\, A_i = n_i$ pour tout i est

$$\binom{n}{n_1}\binom{n-n_1}{n_2}....\binom{n-(n_1+...+n_{k-1})}{n_k} = \frac{n!}{n_1!.....n_k!}.$$

Donc

$$\operatorname{card} P = \sum_{\substack{n_1 + ...n_k = n \\ n_i > 0}} \frac{n!}{n_1!.....n_k!},$$

or l'application $\prod$ qui à $(A_1, A_2, ...A_k)$ associe $\{A_1, A_2, ...A_k\}$ est une application tels que $\left\{ {n \atop k} \right\} = \operatorname{card} \prod(P)$ et puisque il ya $k!$ éléments de P donnant le mème élément de $\prod(P)$ on obtient

$$\left\{ {n \atop k} \right\} = \operatorname{card} \prod(P) = \frac{1}{k!} \operatorname{card}(P) = \frac{1}{k!} \sum_{\substack{n_1 + ...n_k = n \\ n_i > 0}} \frac{n!}{n_1!.....n_k!}.$$

□

Théorème 17 *Soient n, k deux entiers tels que $0 \leq k \leq n$ on a*

$$\left\{ {n \atop k} \right\} = \sum_{j=0}^{k} (-1)^{k-j} \frac{j^n}{j!(k-j)!}. \tag{2.4}$$

Nous avons besoin de démontrer le théorème18

Théorème 18 *Soient E_n, et E_k deux ensembles tels que $|E_n| = n$, $|E_k| = k$, pour tout entier $j \in \{1, 2, ...k\}$ le nombre d'applications de E_n dans E_k ayant un ensemble image à j éléments est égal à*

$$\binom{k}{j} S_{n,j}, \text{ aussi on a } k^n = \sum_{j=0}^{k} \binom{k}{j} S_{n,j} \tag{2.5}$$

Preuve. (1) Pour construire $f : E_n \to E_k$ dont l'ensemble image contienne exactement j éléments, il faut choisir ces j éléments dans E_k, ce qui offre $\binom{k}{j}$ possibilités différentes. Il faut ensuite construire une surjection de E_n sur $\operatorname{Im}(f)$ donc d'un ensemble de cardinal n vers un ensemble de cardinal j, il ya donc $\binom{k}{j} S_{n,j}$ application $f : E_n \to E_k$ dont l'ensemble image a j éléments. (2) il ya k^n application de E_n dans E_k qu'on peut grouper suivant le cardinal j de leur ensemble image, alors l'entier j pouvant varier de $j = 1$ à $j = k$. Pour chaque valeur de j, on sait qu'il ya $\binom{k}{j} S_{n,j}$ applications possibles, ce dénombrement permet donc d'écrire

$$k^n = \sum_{j=0}^{k} \binom{k}{j} S_{n,j}.$$

□

Démonstration du théorème17

On a d'après la relation (2.5) on a $k^n = \sum_{j=0}^{k} \binom{k}{j} S_{n,j}$.On applique la formule d'inversion de Pascal, pour cela on a besoin de donné une rapelle de la Formule d'inversion de Pascal

Théorème 19 *Soient $(a_i)_{0\leq i\leq n}$, $(b_i)_{0\leq i\leq n}$ des familles d'éléments d'un anneau commutatif A,*

$$a_p = \sum_{k=0}^{p} \binom{p}{k} b_k \quad , \forall p \in \{0,1,2,....,n\}, \text{ alors } b_p = \sum_{k=0}^{p} (-1)^{p-k} \binom{p}{k} a_k \quad , \forall p \in \{0,1,....n\}. \tag{2.6}$$

On applique la relation (2.6), tels que $a_k = k^n, b_k = S_{n,k}$, on trouve

$$S_{n,k} = \sum_{j=0}^{k} (-1)^{k-j} \binom{k}{j} j^n,$$

comme $\left\{ {n \atop k} \right\} = \frac{S_{n,k}}{k!}$(d'aprés(2.2)) on a donc

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

On déduit que

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

2.3 Fonction génératrice exponentielle

La Fonction génératrice éxponentielle donner par le théorème suivant

Théorème 20 ***[13]*** *Pour tout z complexe et tout entier $k \geq 0$ on a*

$$\sum_{n=0}^{\infty} \left\{ {n \atop k} \right\} \frac{z^n}{n!} = \frac{(e^z - 1)^k}{k!}, \tag{2.7}$$

On sait que si $n < k$ alors $\left\{ {n \atop k} \right\} = 0$ alors c'est équvaut à dire que

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

Preuve. On sait que si $n \neq o$ on a $\left\{ {n \atop 0} \right\} = 0$ et $\left\{ {0 \atop 0} \right\} = 1$, alors pour $k = 0$ on a $\sum_{n=0}^{\infty} \left\{ {n \atop 0} \right\} \frac{z^n}{n!} = 1$ et $\frac{(e^z-1)^k}{k!} = 1$, pour $k \geq 1$, le produit de séries de rayon infini, $(e^z-1)^k = \left(\sum_{n=1}^{\infty} \frac{z^n}{n!} \right)^k$ se développe en

$$(e^z-1)^k = \sum_{n=k}^{\infty} \left(\sum_{\substack{n_1+\ldots+n_k=n \\ n_i \in \mathbb{N}^*}} \frac{1}{n_1!....n_k!} \right) z^n.$$

Mais d'après la relation (2.3) on sait que $\left\{ {n \atop k} \right\} = \frac{1}{k!} \sum_{n_1+.....n_k} \frac{n!}{n_1!.....n_k!}$ on déduit que

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

□

On donne une autre définition pour les nombres de Stirling de deuxième éspèce.

Polynome de Pochammer (la factorielle décroissante)

Définition 21 *[14] Pour $x \in \mathbb{R}$ et $n \in \mathbb{N}$, on définit le Polynome de Pochammer par*

$$(x)_n = x\,(x-1)\,(x-2)\ldots(x-n+1)\,,\ \ (x)_0 = 1.$$

Remarque 22 *Le polynome $(x)_n$ unitaire de degré n.*

Théorème 23 *Pour tout $x \in \mathbb{R}$ et $n \in \mathbb{N}$ on a l'égalité*

$$x^n = \sum_{k=0}^{n} \left\{ {n \atop k} \right\} (x)_k\,.$$

On a deux méthodes pour démontrer le théorème 23

Méthode 1

Preuve. On a $(x)_{n+1} = (x-n)(x)_n$, on fixe la valeur de x dans $\mathbb{R}$ et on procède par récurence sur n. La propriété est évidente pour $n=0$ puisque $\sum_{k=0}^{n} \left\{ {n \atop k} \right\} x^k = \left\{ {0 \atop 0} \right\} x^0 = 1 = x^0$. Supposons

$$x^n = \sum_{k=0}^{n} \left\{ {n \atop k} \right\} x^k,$$

et montrons que

$$x^{n+1} = \sum_{k=0}^{n+1} \left\{ {n+1 \atop k} \right\} x^k.$$

On utilise $(x)_{k+1} = (x-k)(x)_k$ donc $x(x)_k = k(x)_k + (x)_{k+1}$, ainsi

$$\begin{aligned} x^{n+1} &= xx^n = x\sum_{k=0}^{n} \left\{ {n \atop k} \right\} (x)_k = \sum_{k=0}^{n} \left\{ {n \atop k} \right\} \left(k(x)_k + (x)_{k+1} \right) \\ &= \sum_{k=0}^{n} k \left\{ {n \atop k} \right\} (x)_k + \sum_{k=0}^{n} \left\{ {n \atop k} \right\} (x)_{k+1}, \end{aligned}$$

on isole le dernier tèrme de la deuxiéme somme , après changement d'indice on trouve

$$x^{n+1} = \sum_{k=1}^{n} k \left\{ {n \atop k} \right\} (x)_k + \sum_{k=1}^{n+1} \left\{ {n \atop k-1} \right\} (x)_k = \sum_{k=0}^{n} k \left\{ {n \atop k} \right\} (x)_k + \sum_{k=1}^{n} \left\{ {n \atop k-1} \right\} (x)_k + \left\{ {n \atop n} \right\} (x)_{n+1},$$

on regroupe les sommes, et on utilise la relation

$$k \left\{ {n \atop k} \right\} + \left\{ {n \atop k-1} \right\} = \left\{ {n+1 \atop k} \right\}, et \left\{ {n \atop n} \right\} = \left\{ {n+1 \atop n+1} \right\} = 1,$$

on verra

$$\begin{aligned} x^{n+1} &= \sum_{k=1}^{n} \left(k \left\{ {n \atop k} \right\} + \left\{ {n \atop k-1} \right\} \right) (x)_k + \left\{ {n \atop n} \right\} (x)_{n+1} \\ &= \sum_{k=1}^{n} \left\{ {n+1 \atop k} \right\} (x)_k + \left\{ {n+1 \atop n+1} \right\} (x)_{n+1} = \sum_{k=0}^{n+1} \left\{ {n+1 \atop k} \right\} (x)_k \text{ car } \left\{ {n+1 \atop 0} \right\} = 0. \end{aligned}$$

Ce résultat prouve la propriété au rang $n+1$ et achève la récurrence. □

Méthode 2 [10]

La suite de polynomes $(x)_k$ constituant une base de $\mathbb{R}[X]$, il existera , pour tout $n \in \mathbb{N}^*$, une suite double réelle $(T(n,k))$, unique, telle que

$$x^n = \sum_{k=0}^{n} F(n,k)(x)_k.$$

On observe d'abord que $F(n,k)$, $\begin{Bmatrix} n \\ k \end{Bmatrix}$, ont même socle initial, c'est-à-dire

$$\begin{Bmatrix} 0 \\ 0 \end{Bmatrix} = F(0,0) = 1, \text{ et } \begin{Bmatrix} 0 \\ 0 \end{Bmatrix} = F(0,0) = 0, \text{ si } k \geq 1.$$

Alors pour prouver que $\begin{Bmatrix} n \\ k \end{Bmatrix} = F(n,k)$, il suffit de montrer qu'elle satisfont à la mème relation de récurrence (2.1). Pour cela,on écrit X^{n+1} selon les deux manières suivantes

$$\begin{aligned} x^{n+1} &= \sum_{k=0}^{n+1} F(n+1,k)(x)_k \\ x^{n+1} &= xx^n = x\sum_{k=0}^{n} F(n,k)(x)_k = \sum_{k=0}^{n} F(n,k)(x)_k (x-k+k) \\ &= \sum_{k=0}^{n} F(n,k)(x)_{k+1} + \sum_{k=0}^{n} kF(n,k)(x)_k . \end{aligned}$$

Maintenant en identifiant le coefficient du polynome $(x)_k$, dans ces deux expressions de x^{n+1}, on trouve

$$F(n+1,k) = F(n,k-1) + kF(n,k),$$

ce qui donne $F(n,k) = \begin{Bmatrix} n \\ k \end{Bmatrix}$, on déduit que

$$x^n = \sum_{k=0}^{n} \begin{Bmatrix} n \\ k \end{Bmatrix} (x)_k .$$

2.4 Congruences

Etant donnés un entier naturel $n \geq 2$ et deux nombres rationnels x et y, on convient de dire que x est congru à y modulo n si et seulement si le numérateur du nombre rationnel $x-y$ est divisible par n dans $\mathbb{Z}$. On écrit alors $x \equiv y \pmod n$. Ainsi

$$\forall x \in \mathbb{Q}, \forall y \in \mathbb{Q}, \quad x \equiv y (\mathrm{mod}\, n) \Longleftrightarrow \quad \mathrm{num}(x-y) \in n\mathbb{Z}_{(n)}.$$

La realtion de congruence modulo n ainsi définie sur $\mathbb{Q}$ est une relation d'équivalence compatible avec l'addition de $\mathbb{Q}$. On a

$$\begin{aligned} x &\equiv x \pmod n, \\ x &\equiv y \pmod n \Longrightarrow y \equiv x \pmod n, \\ x &\equiv y \pmod n \text{ et } y \equiv z \pmod n \Longrightarrow x \equiv z \pmod n. \end{aligned}$$

Soient $A(x)$ et $B(x)$ deux polynômes de $\mathbb{Z}_{(p)}[[x]]$ et p un nombre premier. On covient de dire que le polynôme $A(x)$ est congru modulo p au polynôme $B(x)$ si et seulement si on a $A(x)-B(x) \in p\mathbb{Z}_{(p)}[[x]]$. On écrit alors

$$A(x) \equiv B(x) \pmod{n\mathbb{Z}_{(n)}[[x]]}.$$

Dans ce paragraphe nous donons la définition d'un $p-entier$ et aussi la congruence dans $\mathbb{Z}_{(p)}$.

Définition 24 *[24] Soient p un nombre premier,et $A = \frac{a}{b}, a \in \mathbb{Z}, b \in \mathbb{Z}^*$ un nombre rationnel A est appellé $p-entier$ ou ratinonnel $p-adique$ entier si et seulement $(b,p)=1$.*

Notation 25 *L'ensemble des nombres $p-entier$ notée $\mathbb{Z}_{(p)}$, $\mathbb{Z}_{(p)}$ est un sous anneau de l'anneau des entiers $p-adique$ $\mathbb{Z}_p$.*

Définition 26 *Soit $A = \frac{a}{b}$,un $p-entier$, si $\frac{a}{b} = c + p^n q$, $c \in \mathbb{Z}, n \in \mathbb{N}$, pour un certain $q \in \mathbb{Z}_{(p)}$ (équivaut à $a \equiv bc \pmod{p^n}$) on écrit*

$$\frac{a}{b} \equiv c \pmod{p^n}.$$

Exemple 27 *pour $p=3$ on a $\frac{1}{2} \equiv -4 \bmod(3^2)$ puisque $\frac{1}{2} \equiv c \bmod(3^2) \Longleftrightarrow 1 \equiv 2c \bmod(3^2)$on sait que*

$$\begin{aligned} 1 &\equiv -8 \bmod(9) \\ &\equiv 2(-4) \bmod(3^2) \text{ alors } c=-4, \text{ donc } \frac{1}{2} \equiv -4 \bmod(3^2). \end{aligned}$$

2.5 Nombre de Stirling modulo un nombre premier

La famille des nombres de stirling $\left(\left\{ n \atop k \right\}\right)_{(n,k)\in\mathbb{N}\times\mathbb{N}}$ vérifiée la congruence suivante

Théorème 28 *Soient p un nombre premier et k un entier entier tels que $1<k<p$ on a*

$$\left\{ p \atop k \right\} \equiv 0 \pmod{p}. \tag{2.8}$$

Preuve. 0n sait d'aprés la formule explicite pour les nombres de Stirling 2.4

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

pour $n = p$ premier et $1 < k < p$ on a $\left\{ {p \atop k} \right\} = \sum_{j=1}^{k} (-1)^{k-j} \binom{k}{j} j^p$, pour $1 \leq j \leq k \leq p-1$ on sait d'aprés le petit théorème de Fermat que

$$j^p \equiv j (\mathrm{mod}\, p),$$

on a

$$\begin{aligned} \left\{ {p \atop k} \right\} &= \frac{1}{k!}\sum_{j=1}^{k} (-1)^{k-j} \binom{k}{j} j^p \\ &\equiv \frac{1}{k!}\sum_{j=1}^{k} (-1)^{k-j} \binom{k}{j} j (\mathrm{mod}\, p), \end{aligned}$$

on sait que

$$\binom{k}{j} = \frac{k}{j}\binom{k-1}{j-1}.$$

Donc

$$\begin{aligned} \frac{1}{k!}\sum_{j=1}^{k} (-1)^{k-j} \binom{k}{j} j &\equiv \frac{1}{k!}\sum_{j=1}^{k-1} (-1)^{k-j} \frac{k}{j}\binom{k-1}{j-1} j \\ &\equiv \frac{k}{k!}\sum_{j=1}^{k-1} (-1)^{k-j} \binom{k-1}{j-1} \\ &\equiv \frac{1}{(k-1)!}\sum_{j=1}^{k-1} (-1)^{k-j} \binom{k-1}{j-1} (\mathrm{mod}\, p). \end{aligned}$$

On pose $j^{'} = j - 1$

$$\begin{aligned} \frac{1}{(k-1)!}\sum_{j=1}^{k-1} (-1)^{k-j} \binom{k-1}{j-1} (\mathrm{mod}\, p) &= \frac{1}{(k-1)!}\sum_{j=0}^{k} (-1)^{k-j'-1} \binom{k-1}{j'} (\mathrm{mod}\, p) \\ &\equiv \frac{1}{(k-1)!} (1-1)^{k-1} (\mathrm{mod}\, p) \\ &\equiv 0 (\mathrm{mod}\, p). \end{aligned}$$

□

Chapitre 3

Nombres de Bell et polynômes de Touchard

« En mathématiques, "évident" est le mot le plus dangereux.»

Eric Temple Bell (1883-1960)

3.1 Introduction

Dans ce chapitre, nous rappelons la définition des nombres de Bell, et nous étudions quelques unes de ses propriétés.

3.2 Partitions d'un ensemble et défintion des nombres de Bell

Définition 29 *Soit X un ensemble quelconque . On dit que $\mathcal{P}$ est une partition de X si $\mathcal{P}$ est un ensemble de sous ensemble de X tels que*

1. *Aucun élément de $\mathcal{P}$ est vide.*
2. *L'union des éléments de $\mathcal{P}$ égale a X.*
3. *Les éléments de $\mathcal{P}$ sont deux a deux disjoints .*

Dans tout ce qui suit, on suppose que l'ensemble X est un ensemble fini. L'ensemble des partitions de X est alors aussi un ensemble fini. Toute partition $\mathcal{P}$ de X, constituée de n éléments, peut s'écrire $\mathcal{P} = \{P_1, P_2, ..., P_n\}$ avec $P_i \subset X$ pour $1 \leq i \leq n$ avec les conditions suivantes

1. $\forall i \in \{1, 2, ..., n\}, \quad P_i \neq \varnothing$
2. $\cup_{1 \leq i \leq n} P_i = X$
3. $\forall i, j \in \{1, 2, ..., n\}, \ i \neq j \Longrightarrow P_i \cap P_j = \varnothing.$

Remarquons que définir une partition d'un ensemble est équivalent à définir une relation d'équivalence sur cette ensemble. En effet, si une relation d'équivalence est donnée sur l'ensemble X, alors l'ensemble de toutes les classes d'equvalence forme une partition de X. Inversement, si une partition $\mathcal{P}$ de X est donnée, alors nous pouvons définir une relation d'equIvalence sur X notée $\sim$ par $x \sim y$ si et seulement s'il existe un élément de $\mathcal{P}$ qui contient à la fois x et y . Les notions de relation d'equivalence et de partition sont donc deux notions fondamentalement équvalentes. Nous allons maintenant nous intéresser au nombre de partitions définie sur un ensemble de cardinal n, ce nombre est aussi égal au nombre de relations d'équivalence définie sur un ensemble de cardinal n. Nous sommes amenés à la définition suivante :

Définition 30 *Pour tout entier $n \geq 1$, on appelle n-ième nombre de Bell et on note $\mathcal{B}_n$ le nombre de partition d'un ensemble de cardinal n. On convient de poser $\mathcal{B}_0 = 1$.*

$\mathcal{B}_n$ est aussi le nombre de relations d'équivalence défini sur un ensemble à n éléments.

Exemple 31 *L'ensemble des partitions de l'ensemble $X = \{a, b, c\}$ constitué de trois éléments est*

$$\{P_1, P_2, P_3, P_4, P_5\},$$

avec

$$\begin{aligned} P_1 &= \{\{a\}, \{b\}, \{c\}\}, \\ P_2 &= \{\{a, b\}, \{c\}\}, \\ P_3 &= \{\{a; c\}, \{b\}\}, \\ P_4 &= \{\{b, c\}, \{a\}\}, \\ P_5 &= \{a, b, c\}. \end{aligned}$$

Nous constatons que l'ensemble X considéré possède 5 partitions.On peut montrer que le nombre de partitions de l'ensemble $X = \{a, b, c, d\}$ constitué de quatre éléments est égal à 15. Pour prouver cela, on peut énumérer toutes les partitions de cette ensemble.

Table de valeurs

Petit table de valeurs de $\mathcal{B}_n$

n	0	1	2	3	4	5	6	7	8
$\mathcal{B}_n$	1	1	2	5	15	52	203	877	4140

3.3 Relation de récurrence pour les nombres de Bell

Le théorème suivant donne une relation de récurrence vérifiée par la suite des nombres de Bell.

Théorème 32 *Pour tout entier $n \geqslant 0$, on a*

$$\mathcal{B}_{n+1} = \sum_{k=0}^{n} \binom{n}{k} \mathcal{B}_{n-k} = \sum_{k=0}^{n} \binom{n}{k} \mathcal{B}_k. \tag{3.1}$$

Preuve. Soit $\mathcal{B}_n$ le nombre de partition de l'ensemble $X = \{1, 2, 3, ..., n\}$.Considérons une partition de l'ensemble $X' = \{1, 2, 3, ..., n+1\}$, soit $k \in \mathbb{N}^*$, $1 \leq k \leq n+1$, et soit E_k une partition de X', notons π la partie contenant l'élément $n+1$ son cardinal k, pour construire une telle partition il ya $\binom{n}{k-1}$ façons de choisir les $k-1$ éléments autre que $n+1$ dans π, le complémentaire de π contient $n+1-k$ éléments, il ya $\mathcal{B}_{n+1-k}$ façons de le partitionner. Alors card $E_k = \binom{n}{n-k} \mathcal{B}_{n+1-k}$, il est clair que $\{E_1, E_2, ..., E_{n+1}\}$ est une partition de l'ensemble de partition de X'.Donc

$$\mathcal{B}_{n+1} = \sum_{k=1}^{n+1} \binom{n}{k-1} \mathcal{B}_{n+1-k} = \sum_{k=0}^{n} \binom{n}{k} \mathcal{B}_{n-k} = \sum_{k=0}^{n} \binom{n}{k} \mathcal{B}_k$$

puisque $\binom{n}{k} = \binom{n}{n-k}$ □

Exemple 33 *On applique la relation (3.1) pour calculé $\mathcal{B}_{11}$, on trouve $\mathcal{B}_{11} = \sum_{k=0}^{k=10} \binom{10}{k} \mathcal{B}_k =$* 678570

3.4 Formule de Dobinski.

la suite des nombres de Bell vérifiée la formule de Dobinski

Théorème 34 *Pour tout $k \in \mathbb{N}$ on a*

$$B_k = \frac{1}{e} \sum_{n=0}^{\infty} \frac{n^k}{n!}$$

Preuve. Remarquons tout d'abord que la série $\sum_{k=0}^{\infty}\frac{k^n}{k!}$ est bien convergente d'aprés le test de D'Alembert on a

$$\forall k \in \mathbb{N}^* : \lim_{k\to+\infty}\frac{(k+1)^n}{(k+1)!}\times\frac{k!}{k^n} = \lim_{k\to+\infty}\frac{1}{k+1}(1+\frac{1}{k})^n = 0,$$

posons pour tout $n \in \mathbb{N}$ $S_n = \frac{1}{e}\sum_{k=0}^{\infty}\frac{k^n}{k!}$, on a $S_0 = B_0 = 1$, et pour tout $n \in \mathbb{N}$

$$\begin{aligned}\sum_{k=0}^{n}\binom{n}{k}S_k &= \sum_{k=0}^{n}\binom{n}{k}\frac{1}{e}\sum_{p=0}^{\infty}\frac{p^k}{p!} = \frac{1}{e}\sum_{p=0}^{\infty}\frac{1}{p!}\sum_{k=0}^{n}\binom{n}{k}p^k \\ &= \frac{1}{e}\sum_{p=0}^{\infty}\frac{(1+p)^n}{p!} = \frac{1}{e}\sum_{p=0}^{\infty}\frac{(p+1)^{n+1}}{(p+1)!} = S_{n+1}.\end{aligned}$$

La suite (B_n) et (S_n) sont initialsees pour la mème constante et vérifiant la mème relation de recurrence elle sont donc égales, on déduit que

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

□

3.5 Fonction génératrice exponentielle pour les nombres de Bell

Le théorème suivant donne la fonction exponentielle pour les nombres de Bell

Théorème 35 *[16] pour $n \in \mathbb{N}$, et $z \in \mathbb{C}$ on a*

(1) *la série entière* $\sum_{n=0}^{\infty}\frac{B_n z^n}{n!}$ *a un rayon de convergence $R > 0$ et* $\forall z \in [-R, R]$ $\sum_{n=0}^{\infty}\frac{B_n z^n}{n!} = e^{e^z-1}$,

et

(2) *pour tout $k \in \mathbb{N}$ on a* $B_k = \frac{1}{e}\sum_{n=0}^{\infty}\frac{n^k}{n!}$ *(Formule de Dobinski)*

Preuve. (1) Démontrons par récurrence sur $n \geq 0$, que $\forall n \in \mathbb{N}$, $B_n \leq n!$, pour $n = 0$ trivial, supposons $B_n \leq n!$, on a

$$B_{n+1} = \sum_{k=0}^{n}\binom{n}{k}B_k \leq \sum_{k=0}^{n}\binom{n}{k}k! = n!\sum_{k=0}^{n}\frac{1}{(n-k)!} \leq n!(n+1) = (n+1)!, \text{ puisque } \frac{1}{(n-k)!} \leq 1$$

Alors pour tout $n \in \mathbb{N}$, $z \in \mathbb{C}$ on a $0 \leq \frac{B_n}{n!}|z|^n \leq |z|^n$, donc R est supèrieur ou égal au rayon de la série géométrique qui égale à 1, en particulier R est strictement positif.Soit $z \in\in [-R, R]$, alors par un changemment d'indice on trouve

$$\sum_{n=0}^{\infty} \frac{B_n}{n!} z^n = 1 + \sum_{n=1}^{\infty} \frac{B_n}{n!} z^n = 1 + \sum_{n=0}^{\infty} \frac{B_{n+1}}{(n+1)!} z^{n+1}.$$

Posons $f(z) = 1 + \sum_{n=0}^{\infty} \frac{B_{n+1}}{(n+1)!} z^{n+1}$ par le théorème de dérivation terme à terme pour les séries entières on obtient

$$f'(z) = \sum_{n=0}^{\infty} \frac{B_{n+1}}{n!} z^n = \sum_{n=0}^{\infty} \frac{1}{n!} (\sum_{k=0}^{n} \binom{n}{k} B_k) z^n = \sum_{n=0}^{\infty} (z^n \sum_{k=0}^{n} \frac{B_k}{k!(n-k)!}),$$

on reconnait dans cette dernière expression le produit de cauchy des séries $\sum \frac{z^n}{n!}$, $\sum \frac{B_n}{n!} z^n$, toutes deux de rayon de convergence supérieur ou égal à R, donc

$$\forall z \in [-R, R] \ : f'(z) = f(z) \sum_{n=0}^{\infty} \frac{z^n}{n!} = f(z) e^z, \tag{3.2}$$

en résolvant (3.2) on trouve que :$\exists c \in \mathbb{R} \quad , \quad \forall z \in [-R, R],\ f(z) = c e^{e^z}$,or $f(0) = 1$ donc $c = e^{-1}$ d'ou

$$f(z) = \frac{1}{e} e^{e^z} = e^{e^z - 1}.$$

(2) Soit $z \in \mathbb{C}$ on sait que

$$e^{e^z} = \sum_{n=0}^{\infty} \frac{e^{nz}}{n!} = \sum_{n=0}^{\infty} \frac{1}{n!} (\sum_{k=0}^{\infty} \frac{(nz)^k}{k!}).$$

On considère donc la série double $\sum_{(n,k)} u_{n;k}$ ou $\forall n, k \in \mathbb{N} : u_{n,k} = \frac{(nz)^k}{n!k!}$ alors pour tout $n \geq 0$, la série $\sum_{(k)} |u_{n,k}|$ converge et

$$\sum_{k=0}^{\infty} |u_{n,k}| = \sum_{k=0}^{\infty} \frac{n^k |z|^k}{n!k!} = \frac{e^{n|z|}}{n!},$$

aussi la série $\sum_{(n)} |u_{n,k}|$, converge , par le théorème de Fubini pour les séries doubles, $\sum_{(n,k)} u_{n,k}$ converge et

$$\sum_{n=0}^{\infty} \sum_{k=0}^{\infty} u_{n,k} = \sum_{k=0}^{\infty} \sum_{n=0}^{\infty} u_{n,k}$$

On a

$$f(z) = \frac{1}{e}e^{e^z} = \frac{1}{e}\sum_{n=0}^{\infty}\sum_{k=0}^{\infty}\frac{(nz)^k}{n!k!} = \frac{1}{e}\sum_{k=0}^{\infty}\sum_{n=0}^{\infty}\frac{(nz)^k}{n!k!} = \sum_{k=0}^{\infty}\frac{1}{e}(\sum_{n=0}^{\infty}\frac{n^k}{n!})\frac{z^k}{k!}.$$

et donc , par unicité du développement en séries entières de f sur $[-R, R]$ on déduit que

$$\forall k \in \mathbb{N} \quad B_k = \frac{1}{e}\sum_{n=0}^{\infty}\frac{n^k}{n!}$$

□

3.6 Nombres de Bell modulo un nombre premier

Le nombre de Bell,est trés grand lorsque n augmente, on regarde le nombre de Bell modulo un nombre premier.

Table des valeurs de B_n modulo $2, 3, 5$

n	0	1	2	3	4	5	6	7	8	9	10
$\mathcal{B}_n$	1	1	2	5	15	52	203	877	4140	21147	115975
$\mathcal{B}_n \pmod 2$	1	1	0	1	1	0	1	1	0	1	1
$\mathcal{B}_n \pmod 3$	1	1	2	2	0	1	2	1	0	0	1
$\mathcal{B}_n \pmod 5$	1	1	2	0	0	2	3	2	0	2	0

.

Remarque 36 *[21] (1). La suite de résidu de B_n modulo 2 est periodique,la période est 3*

. la suite de résidu de B_n modulo 3 est periodque,la période est 13

. la suite de réidu de B_n modulo 5 est periodique, la période est 781

(2) on général le nombre de Bell modulo un nombre premier p est périodique , et la période divise le nombre $N_p = \frac{p^p - 1}{p - 1}$.donc

$$B_{n+N_p} \equiv B_n (\mathrm{mod}\, p).$$

3.7 Quelques propriétés de nombres de Bell

Comme $\left\{ {n \atop k} \right\}$ est le nombre de partition à k élément de l'ensemble $X = \{1, 2, ...n\}$, $n \in \mathbb{N}$, alors on a immédiatement

$$B_n = \sum_{k=0}^{n}\left\{ {n \atop k} \right\}. \tag{3.3}$$

La conjecture de Kurepa fait intervenier la fonction factorielle à gauche de Kurepa qui définit comme suit.

La fonction factorielle à gauche de Kuerepa est la fonction

$$K : \mathbb{N} \to \mathbb{N}, \text{définie par } K(0) = 0 \text{ et } K(n) = \sum_{k=0}^{n-1} k!, \text{ pour } n \geq 1.$$

Pour $n \in \mathbb{N}$, $K(n)$ est aussi noté $!n$. La conjecture de Kurepa s'énonce comme suit :

Conjecture 37 *Pour tout entier $n \geq 2$, on a $p\gcd(!n, n!) = 2$.*

La conjecture est bien vérifiée pour les premieres valeurs de n. Ainsi

$$\begin{aligned} p\gcd(!2, 2!) &= (2, 2) = 2 \\ p\gcd(!3, 3!) &= (4, 6) = 2 \\ p\gcd(!4, 4!) &= (10, 24) = 2 \end{aligned}$$

Théorème 38 *Les relations suivantes sont équivalentes :*

$$\begin{aligned} (1) &: (K(n), n!) = 2, \ n \geq 2 \\ (2) &: K(n) \not\equiv 0 (\mathrm{mod}\, p), \ \textit{pour } n \geq 2 \textit{ pour } p \textit{ premier } p \geq 3. \\ (3) &: K(p) \not\equiv 0 (\mathrm{mod}\, p), \ n \geq 2, \ \textit{pour } p \textit{ premier } p \geq 3. \\ (4) &: \mathcal{B}_{p-1} \not\equiv 1 (\mathrm{mod}\, p). \end{aligned}$$

Nous allons prouver l'équivalence entre (3) et (4), pour cela le lemme suivant nous sera utile.

Lemme 39 *Poure tout nombre premier $p \geq 3$ on a*

$$D_{p-1} \equiv K(p) (\mathrm{mod}\, p).$$

Preuve. On sait d'aprés la relation 1.9 que

$$\begin{aligned} D_{p-1} &= (p-1)!\sum_{k=0}^{p-1}\frac{(-1)^k}{k!} \\ &= \sum_{k=0}^{p-1}(-1)^k(p-1)\times ...\times(k+1) \\ &= \sum_{k=0}^{p-1}(-1)^k\prod_{1\leq s\leq p-k-1}(p-s) \\ &\equiv \sum_{k=0}^{p-1}(-1)^k(-1)^{p-k-1}\prod_{1\leq s\leq p-k-1}s \\ &\equiv \sum_{k=0}^{p-1}(-1)^{p-1}\prod_{1\leq s\leq p-k-1}(s) \end{aligned}$$

$$\begin{aligned} &\equiv (p-1)!+(p-2)!+...+1\,(\mathrm{mod}\,p) \\ &\equiv K(p)\,(\mathrm{mod}\,p)\,. \end{aligned}$$

□

On démontrera au corollaire 55 qu'on a

$$\mathcal{B}_{p-1}\equiv D_{p-1}+1\,(\mathrm{mod}\,p)\,.$$

Par suite

$$\begin{aligned} K(p) &\equiv D_{p-1}\,(\mathrm{mod}\,p) \\ &\equiv \mathcal{B}_{p-1}-1\,(\mathrm{mod}\,p)\,. \end{aligned}$$

Ainsi

$$(3)\Longleftrightarrow \mathcal{B}_{p-1}\not\equiv 1(\mathrm{mod}\,p).$$

3.8 Une remarquable congruence pour le p-ième nombre de Bell

Dans ce paragraphe, nous allons prouver une remarquable congruence des nombres de Bell $\mathcal{B}_p$, p étant un nombre premier. Désignons par p_n le n-ième nombre premier. On a

$$(p_n)_{n\geq 1} = (2, 3, 5, 7, 11, 13, 17, ...).$$

Alors on a

$$\begin{aligned}(\mathcal{B}_{p_n})_{n\geq 1} &= (\mathcal{B}_2, \mathcal{B}_3, \mathcal{B}_5, \mathcal{B}_7, \mathcal{B}_{11}, \mathcal{B}_{13}, \mathcal{B}_{17}, ...).\\ &= (2, 5, 52, 877, 678570, 27644437, 82864869804, ...)\end{aligned}$$

On a alors

$$(\mathcal{B}_{p_n} \bmod p_n)_{n\geq 1} = (0, 2, 2, 2, 2, 2, 2, 2, 2, ...)$$

A l'aide de Maple, il est facile de constater que $(\mathcal{B}_{p_n} \bmod p_n)_{2\leq n\leq 100}$ est une suite (finie) constante et que $\mathcal{B}_{p_n} \bmod p_n = 2$, pour $2 \leq n \leq 100$. Nous allons prouver que plus génralemnt on a le résultat suivant :

Théorème 40 *[14]Pour tout nombre premier le p-ième nombre de Bell $\mathcal{B}_p$ vérifie la congruence suivante*

$$\mathcal{B}_p \equiv 2 \pmod p.$$

Les lemmes suivants vont nous être utiles pour prouver le théorème 40.

Lemme 41 *Pour tout nombre premier p et*

1. *Pour tout entier r tel que $2 \leq r \leq p-1$, on a*

$$[x^p] \frac{(e^x-1)^r}{r!} \in \mathbb{Z}_{(p)}.$$

2. $$[x^p] \frac{(e^x-1)^p}{p!} = \frac{1}{p!}.$$

3. *Pour tout entier r tel que $r \geq p+1$*

$$[x^p] \frac{(e^x-1)^r}{r!} = 0.$$

Preuve.

1. Rappelons qu'étant donné $S(x) = \sum_{n=0}^{\infty} a_n x^n \in \mathbb{C}[[x]]$, $[x^m](S(x))$ désigne le coefficient de x^m dans l'écriture développée de $S(x)$. Autrement dit :

$$[x^m]\left(\sum_{n=0}^{\infty} a_n x^n\right) = a_m.$$

Pour tout nombre premier p et pour tout entier r tel que $1 \leq r \leq p-1$, on a alors

$$\begin{aligned}[x^p]\,\frac{(e^x-1)^r}{r!} &= \frac{1}{r!}\left(\sum_{n=0}^{\infty}\frac{x^n}{n!}\right)^r \\ &= \sum_{\substack{n_1+n_2+\cdots n_r=p \\ n_1,n_2,\ldots,n_r\geq 1}} \frac{1}{r!n_1!n_2!\ldots n_r!}. \end{aligned} \tag{3.4}$$

On constate que si des entiers $n_1, n_2, \ldots, n_r$ supérieurs ou égaux à 1 vérifient la relation $n_1 + n_2 + \cdots n_r = p$, alors aucun de ces entiers n_j ne peut être divisible par p puisque nécessairement, on a alors $1 \leq n_j \leq p-(r-1) \leq p-1$ pour $1 \leq j \leq r$, car on a $r \geq 2$. Il en résulte qu'on alors pour ces entiers $\frac{1}{r!n_1!n_2!\ldots n_r!} \in \mathbb{Z}_{(p)}$. Le second membre de la relation (3.4) est donc une somme de p-entiers, c'est donc un p-entier puisque $\mathbb{Z}_{(p)}$ est un anneau. Il en resule alors clairement que $[x^p]\,\frac{(e^x-1)^r}{r!} \in \mathbb{Z}_{(p)}$.

2. On a

$$\begin{aligned}(e^x-1)^p &= \left(\sum_{n=0}^{\infty}\frac{x^{n+1}}{(n+1)!}\right)^p \\ &= x^p\left(\sum_{n=0}^{\infty}\frac{x^n}{(n+1)!}\right)^p \\ &= x^p\left(1+\frac{x}{2!}+\frac{x^2}{3!}+\cdots\right)^p\end{aligned}$$

Il en résulte que l'on a

$$[x^p]\,(e^x-1)^p = 1$$

et donc on a bien

$$[x^p]\,\frac{(e^x-1)^p}{p!} = \frac{1}{p!}.$$

3. Pour $r \geq p+1$, on a

$$\begin{aligned}(e^x-1)^r &= \left(\sum_{n=0}^{\infty}\frac{x^{n+1}}{(n+1)!}\right)^r \\ &= x^r\left(\sum_{n=0}^{\infty}\frac{x^n}{(n+1)!}\right)^r \\ &= x^r\left(1+\frac{x}{2!}+\frac{x^2}{3!}+\cdots\right)^r.\end{aligned}$$

Il est alors clair que la valuation de la série formelle $(e^x-1)^r$ est égale à 1. Comme on a supposé que $r \geq p+1$, il en résulte qu'on a bien :

$$[x^p]\,\frac{(e^x-1)^r}{r!} = 0.$$

□

Nous sommes maintenant en mesure de prouver le théorème 40.

Preuve. Soit p un nombre premier, nous allons prouver que

$$\frac{B_p}{p!} - \frac{2}{p!} \in \mathbb{Z}_{(p)}$$

Il en résultera alors $B_p - 2 \in p\mathbb{Z}_{(p)}$.

Pour cela, on commence par remarquer que l'on a

$$\frac{\mathcal{B}_p}{p!} = [x^p]\left(\sum_{n=0}^{\infty}\mathcal{B}_n\frac{x^n}{n!}\right).$$

Or, on sait que la série génératrice exponentielle de la suite des nombres de Bell vérifie la relation

$$\sum_{n=0}^{\infty}\mathcal{B}_n\frac{x^n}{n!} = e^{e^x-1}.$$

On a donc aussi

$$\begin{aligned}\frac{\mathcal{B}_p}{p!} &= [x^p]\,e^{e^x-1}\\ &= [x^p]\left(\sum_{r=0}^{\infty}\frac{(e^x-1)^r}{r!}\right).\end{aligned}$$

on constate qu'on peut écrire

$$\begin{aligned}\sum_{n=0}^{\infty}\frac{(e^x-1)^n}{n!} &= e^x + \sum_{r=2}^{p-1}\frac{(e^x-1)^r}{r!} + \frac{(e^x-1)^p}{p!} + \sum_{r=p+1}^{\infty}\frac{(e^x-1)^r}{r!}\\ &= S_1 + S_2 + S_3 + S_4,\end{aligned}$$

avec

$$\begin{aligned}S_1 &= e^x,\\ S_2 &= \sum_{r=2}^{p-1}\frac{(e^x-1)^r}{r!},\\ S_3 &= \frac{(e^x-1)^p}{p!},\\ S_4 &= \sum_{r=p+1}^{\infty}\frac{(e^x-1)^r}{r!}\end{aligned}$$

On a donc

$$\begin{aligned}\frac{\mathcal{B}_p}{p!} &= [x^p]\,(S_1+S_2+S_3+S_4)\\ &= [x^p]\,(S_1)+[x^p]\,(S_2)+[x^p]\,(S_3)+[x^p]\,(S_4).\end{aligned}$$

On a

$$\begin{aligned}[x^p]\,(S_1) &= [x^p]\,e^x\\ &= \frac{1}{p!}.\end{aligned}$$

$$[x^p]\,(S_2) = [x^p]\,(\sum_{r=2}^{p-1}\frac{(e^x-1)^r}{r!}) \in \mathbb{Z}_{(p)}.$$

$$\begin{aligned}[x^p]\,(S_3) &= [x^p]\,\frac{(e^x-1)^p}{p!}\\ &= \frac{1}{p!}\end{aligned}$$

$$\begin{aligned}[x^p]\,(S_4) &= [x^p]\sum_{r=p+1}^{\infty}\frac{(e^x-1)^r}{r!}\\ &= 0\end{aligned}$$

Ainsi

$$\frac{B_p}{p!}-\frac{2}{p!}\in\mathbb{Z}_{(p).}$$

Il en résulte alors qu'on bien$B_p-2\in p\mathbb{Z}_{(p)}$, c'est à dire

$$\mathcal{B}_p \equiv 2 \pmod p\,.$$

□

3.9 Polynômes de Touchard

La suite des polynômes de Touchard $(T_n(x))_{n\geq 0}$ du nom du mathématicien français Jacques Touchard (1885 – 1968) est définie par

$$T_n(x)=\sum_{k=0}^{n}\left\{{n \atop k}\right\}x^k,\quad (n\geq 0). \tag{3.5}$$

Remarquons que l'on a, d'aprés (3.3)

$$T_n(1) = \sum_{k=0}^{n} \left\{ n \atop k \right\} = \mathcal{B}_n, \quad (n \geq 0).$$

Les premiers polynômes de Touchard sont

$$\begin{aligned} T_0(x) &= 1 \\ T_1(x) &= x \\ T_2(x) &= x^2 + x \\ T_3(x) &= x^3 + 3x^2 + x \\ T_4(x) &= x^4 + 6x^3 + 7x^2 + x \end{aligned}$$

D'après la définition (3.5), le n-ième polynôme de Touchard $T_n(x)$ est un polynôme de $\mathbb{Z}[x]$, à coefficients entiers positifs, de degré n, de coefficient dominant égale à 1. On a aussi

$$T_n(0) = 0, \quad (n \geq 0).$$

Les polynômes de Touchard vérifient de remarquables relations données dans les théorèmes qui suivent.

Théorème 42 *Pour tout entier $n \geq 0$, on a*

$$T_{n+1}(x) = x\left(T_n'(x) + T_n(x)\right). \tag{3.6}$$

Preuve. En effet, on a

$$\begin{aligned} T_{n+1}(x) &= \sum_{k=1}^{n+1} k \left\{ n+1 \atop k \right\} x^{k-1} \\ &= \sum_{k=0}^{n} (k+1) \left\{ n+1 \atop k+1 \right\} x^k \\ &= x\left(\sum_{k=1}^{n} k \left\{ n \atop k \right\} x^{k-1} + \sum_{k=1}^{n} \left\{ n \atop k \right\} x^k \right) \\ &= x\left(T_n'(x) + T_n(x)\right). \end{aligned}$$

□

Corollaire 43 *Pour tout entier $n \geq 0$, on a*

$$\sum_{k=0}^{n} k \left\{ n \atop k \right\} = \mathcal{B}_{n+1} - \mathcal{B}_n. \tag{3.7}$$

Preuve. Pour $x = 1$, on déduit de la relation (3.6)

$$\begin{aligned}\sum_{k=1}^{n} k\left\{{n \atop k}\right\} &= T_n'(1)\\ &= T_{n+1}(1) - T_{n+1}(1)\\ &= \mathcal{B}_{n+1} - \mathcal{B}_n.\end{aligned}$$

□

Théorème 44 *Soit $S(z) = \sum_{k=0}^{\infty} \mathcal{B}_k \frac{z^k}{k!}$ la série généraratrice exponentielle des nombres de Bell, pour tout entier $n \geq 0$, la dérivée n-ième $S^{(n)}(z)$ de cette série formelle vérifie les relations*

$$S^{(n)}(z) = \sum_{k=0}^{\infty} \mathcal{B}_{k+n} \frac{z^k}{k!} \tag{3.8}$$

$$S^{(n)}(z) = T_n(e^z)S(z), \tag{3.9}$$

$$S^{(n)}(z) = \sum_{k=0}^{n} \left\{{n \atop k}\right\} e^{kz} S(z). \tag{3.10}$$

Preuve. On a

$$\begin{aligned}S'(z) &= \sum_{n=1}^{\infty} n\mathcal{B}_n \frac{z^{n-1}}{n!}\\ &= \sum_{n=1}^{\infty} \mathcal{B}_n \frac{z^{n-1}}{(n-1)!}\\ &= \sum_{n=0}^{\infty} \mathcal{B}_{n+1} \frac{z^n}{n!}.\end{aligned}$$

Ainsi, la dérivée de la serie formelle $S(z)$ n'est rien d'autre que la série génératrice exponentielle de la suite $(\mathcal{B}_{n+1})_{n\geq 0}$des nombres de Bell décalée d'un rang Par un raisonnement par récurrence immédiat, on obtient alors la relation (3.8).

Désignons par $\mathfrak{P}(m)$ la propriété " $S^{(m)}(z) = T_m(e^z)S(z)$ ". Le théorème 44 affirme que $\mathfrak{P}(n)$ est vraie pour tout entier $n \in \mathbb{N}$. Prouvons cette propriété à l'aide d'un raisonnement par récurence. Rappelons que la dérivée d'ordre 0 de $S(z)$ est égale à $S(z)$. Comme $T_0(e^z) = 1$, $\mathfrak{P}(0)$ est vraie. Supposons $\mathfrak{P}(n)$ vraie pour un entier $n \geq 0$. On a alors

$$S^{(n)}(z) = T_n(e^z)S(z). \tag{3.11}$$

En égalant les dérivées de chacun des deux membres de (3.11), on obtient

$$\begin{aligned}S^{(n+1)}(z) &= e^z T_n'(e^z)S(z) + T_n(e^z)S'(z)\\ &= e^z T_n'(e^z)S(z) + T_n(e^z)e^z S(z)\\ &= \left(e^z \left(T_n'(e^z) + T_n(e^z)\right)\right) S(z).\end{aligned} \tag{3.12}$$

Avec (3.6), la relation (3.12) peut s'écrire

$$S^{(n+1)}(z) = T_{n+1}(e^z)S(z).$$

$\mathfrak{P}(n+1)$ est vraie. La propriété $\mathfrak{P}(n)$ est donc vraie pour tout entier $n \geq 0$ et la relation (3.9) est ainsi établie. En utilisant la définition du polynôme $T_n(x)$, on en déduit (3.10). □

Théorème 45 *Pour tout entier $n \geq 0$, on a :*

$$T_{n+1}(x) = x\sum_{k=0}^{n}\binom{n}{k}T_k\left(x\right).$$

Preuve. On sait d'après la relation (2.7) que $\sum_{n=0}^{\infty}\left\{ n \atop k \right\}\frac{z^n}{n!} = \frac{(e^z-1)^k}{k!}$, alors la série génératrice exponentielle de la suite de polynome de Touchard est

$$\begin{aligned}
\sum_{n=0}^{\infty}T_n\left(x\right)\frac{z^n}{n!} &= \sum_{n=0}^{\infty}\left(\sum_{k=0}^{n}\left\{ n \atop k \right\}x^k\right)\frac{z^n}{n!}, \text{ d'aprés (3.5)} \\
&= \sum_{k=0}^{n}\left(\sum_{n=0}^{\infty}\left\{ n \atop k \right\}\frac{z^n}{n!}\right)x^k \\
&= \sum_{k=0}^{n}\left(\frac{(e^z-1)^k}{k!}\right)x^k \\
&= \sum_{k=0}^{n}\frac{\left((e^z-1)x\right)^k}{k!} = e^{(e^z-1)x}.
\end{aligned}$$

On a donc

$$\sum_{n=0}^{\infty}T_n\left(x\right)\frac{z^n}{n!} = e^{(e^z-1)x}. \tag{3.13}$$

En dérivant formellement (3.13) (par rapport à z), on obtient

$$\begin{aligned}
\sum_{n=0}^{\infty}T_{n+1}\left(x\right)\frac{z^n}{n!} &= xe^ze^{(e^z-1)x} \\
&= x\sum_{n=0}^{\infty}\frac{z^k}{k!}\sum_{n=0}^{\infty}T_n\left(x\right)\frac{z^n}{n!}, \text{ preduit de deux séries} \\
&= x\sum_{n=0}^{\infty}\left(\sum_{k=0}^{n}\frac{T_n\left(x\right)}{k!\left(n-k\right)!}\right)z^n \qquad (3.14)
\end{aligned}$$

En identifiant les coefficients de z^n dans chacun des deux mombres de (3.14), en trouve

$$\begin{aligned}
\frac{T_{n+1}\left(x\right)}{n!} &= x\sum_{k=0}^{n}\frac{T_{n+1}\left(x\right)}{k!\left(n-k\right)!}, \text{ alors} \\
T_{n+1}\left(x\right) &= x\sum_{k=0}^{n}\frac{n!T_n\left(x\right)}{k!\left(n-k\right)!} = x\sum_{k=0}^{n}\binom{n}{k}T_n\left(x\right), \text{ Ce qui achève la démonstration}
\end{aligned}$$

□

3.10 Congruences de Touchard

En 1933, Jacques Touchard découvre la remarquable congruence vérifiée par les nombres de Bell, donnée dans le théorème suivant.

Théorème 46 *Pour tout nombre premier p et pour tous entiers naturels n et m, on a*

$$\mathcal{B}_{n+p^m} \equiv m\mathcal{B}_n + \mathcal{B}_{n+1} \pmod{p}. \tag{3.15}$$

Ce résulat a été prouvé dernièrement par Gerg Hurst et Andrew Schulte [17] et aussi par Anne Gertsch et Alain M Robert [14]. Nous allons le prouver ici en exploitant les remarquables propriétés des polynômes de Touchard. Nous commencerons par prouver le résulat suivant, qui est un cas particulier de la relation (3.15).

Lemme 47 *Pour tout nombre premier p, on a*

$$\mathcal{B}_p - 2 \equiv 0 \pmod{p}. \tag{3.16}$$

Preuve. On sait d'aprés le théorème (28) que $\left\{ {p \atop k} \right\} \equiv 0 \pmod{p}$ pour $1 < k \leq p-1$, on en déduit que

$$\mathcal{B}_p - 2 = \sum_{k=2}^{p-1} \left\{ {p \atop k} \right\} \equiv 0 \pmod{p}.$$

□

Le lemme suivant est aussi un cas particulier de la relation (3.15) est une généralisation du lemme précédent.

Lemme 48 *Pour tout nombre premier p et pour tout entier naturel n, on a*

$$\mathcal{B}_{n+p} \equiv \mathcal{B}_{n+1} + \mathcal{B}_n \pmod{p}. \tag{3.17}$$

Nous allons maintenant prouver le lemme (48).

Preuve. Soient n un entier naturel et p un nombre premier. En dérivant p fois la série formelle $S^{(n)}(z)$ en partant de la relation (3.10), on obtient

$$\begin{aligned} S^{(n+p)}(z) &= \sum_{k=0}^{n} \left\{ n \atop k \right\} \left(e^{kz} S(z)\right)^{(p)} \\ &= \sum_{k=0}^{n} \left\{ n \atop k \right\} \left(\sum_{\ell=0}^{p} \binom{p}{\ell} (e^{kz})^{(p-l)} S^{(\ell)}(z) \right) \\ &= \sum_{k=0}^{n} \left\{ n \atop k \right\} \left(\sum_{\ell=0}^{p} \binom{p}{\ell} S^{(\ell)}(z) k^{p-\ell} e^{kz} \right). \end{aligned} \tag{3.18}$$

On obtient ainsi

$$\sum_{m=0}^{\infty} \mathcal{B}_{n+p+m} \frac{z^m}{m!} = \sum_{k=0}^{n} \left\{ n \atop k \right\} \left(\sum_{\ell=0}^{p} \binom{p}{\ell} S^{(\ell)}(z) k^{p-\ell} e^{kz} \right)$$

Le coefficient de z dans chacun le membre de gauche de l'égalité (3.18) est

$$\left[z^0\right] \left(S^{(n+p)}(z)\right) = \mathcal{B}_{n+p}.$$

Le coefficient constante dans chacun le membre de droite de l'égalité (3.18) est

$$\left[z^0\right] \left(\sum_{k=0}^{n} \left\{ n \atop k \right\} \left(\sum_{\ell=0}^{p} \binom{p}{\ell} S^{(\ell)}(z) k^{p-\ell} e^{kz} \right) \right) = \sum_{k=0}^{n} \left\{ n \atop k \right\} \left(\sum_{\ell=0}^{p} \binom{p}{\ell} \mathcal{B}_{\ell} k^{p-\ell} \right).$$

On a donc

$$\begin{aligned} \mathcal{B}_{n+p} &= \sum_{k=0}^{n} \left\{ n \atop k \right\} \left(\sum_{\ell=0}^{p} \binom{p}{\ell} \mathcal{B}_{\ell} k^{p-\ell} \right) \\ &= \sum_{k=0}^{n} \left\{ n \atop k \right\} \left(k^p + \mathcal{B}_p + \sum_{\ell=1}^{p-1} \binom{p}{\ell} \mathcal{B}_{\ell} k^{p-\ell} \right) \end{aligned} \tag{3.19}$$

Or on sait que $\binom{p}{\ell}$ est divisible par p pour ℓ compris entre 1 et $p-1$, on déduit de (3.19) que

$$\begin{aligned} \mathcal{B}_{n+p} &\equiv \sum_{k=0}^{n} \left\{ n \atop k \right\} \left(k^p + \mathcal{B}_p\right) \\ &\equiv \sum_{k=0}^{n} \left\{ n \atop k \right\} (k^p + 2) + \sum_{k=0}^{n} \left\{ n \atop k \right\} \left(\mathcal{B}_p - 2\right) \pmod{p}. \end{aligned} \tag{3.20}$$

Or on sait d'après le petit théorème de Fermat que k^p est congru à k modulo p. D'autre part, on sait d'après (3.16)que $\mathcal{B}_p - 2$ est divisible par p. Compte tenu de cela, on déduit de (3.20)

que

$$\begin{aligned}\mathcal{B}_{n+p} &\equiv \sum_{k=0}^{n} \left\{ {n \atop k} \right\} (k+2) \\ &\equiv \sum_{k=0}^{n} k \left\{ {n \atop k} \right\} + 2 \sum_{k=0}^{n} \left\{ {n \atop k} \right\} \pmod{p}. \end{aligned} \tag{3.21}$$

Or, on sait d'après la relation (3.7) que

$$\sum_{k=0}^{n} k \left\{ {n \atop k} \right\} = \mathcal{B}_{n+1} - \mathcal{B}_n.$$

La relation(3.21) peut donc s'écrire

$$\begin{aligned}\mathcal{B}_{n+p} &\equiv \mathcal{B}_{n+1} - \mathcal{B}_n + 2\mathcal{B}_n \\ &\equiv \mathcal{B}_{n+1} + \mathcal{B}_n \pmod{p}. \end{aligned}$$

La relation (3.17) est établie. □

Nous allons généraliser le lemme précédent en prouvant

Lemme 49 *Pour tout nombre premier p et pour tous entiers naturels n et k, on a*

$$\mathcal{B}_{n+kp} \equiv \sum_{r=0}^{k} \binom{k}{r} \mathcal{B}_{n+r} \pmod{p}$$

Preuve. L'ensemble A des applications de $\mathbb{C}^{\mathbb{N}}$ dans $\mathbb{C}^{\mathbb{N}}$ muni de l'addition et de la composition des applications est un anneau non commutatif. Désignons par E l'opérateur "Shift" qui à toute suite $(u_n)_{n\geq 0}$ de $\mathbb{C}^{\mathbb{N}}$ associe la suite $(u_{n+1})_{n\geq 0}$ de $\mathbb{C}^{\mathbb{N}}$ et par I l'application identitée dans $\mathbb{C}^{\mathbb{N}}$. Il est facile de constater que E et I sont deux éléments de A qui commutent $(E \circ I = I \circ E = E)$. On peut donc appliquer la formule du binôme pour calculer dans cet anneau $(E+I)^k$, pour tout entier naturel k. On a

$$(E+I)^k = \sum_{r=0}^{k} \binom{k}{r} E^r.$$

On sait que

$$\mathcal{B}_{n+p} \equiv \mathcal{B}_{n+1} + \mathcal{B}_n \pmod{p}.$$

Il en résulte que

$$\mathcal{B}_{n+p} \equiv (E+I)(\mathcal{B}_n) \pmod{p}.$$

Plus généralement

$$\begin{aligned}
\mathcal{B}_{n+kp} &\equiv (E+I)(\mathcal{B}_{n+(k-1)p}) \\
&\equiv (E+I)^2(\mathcal{B}_{n+(k-2)p}) \\
&\equiv \dots \\
&\equiv (E+I)^k(\mathcal{B}_n) \\
&\equiv \left(\sum_{r=0}^{k}\binom{k}{r}E^r\right)\ \mathcal{B}_n \pmod p \\
&\equiv \sum_{r=0}^{k}\binom{k}{r}\mathcal{B}_{n+r} \pmod p .
\end{aligned}$$

Le lemme 49 est ainsi établi. □

Nous sommes maintenant en mesure de prouver le théorème (46). En effet dans le cas particulier où $k = p^m$, le lemme

$$\begin{aligned}
\mathcal{B}_{n+p^{m+1}} &\equiv \sum_{r=0}^{p^m}\binom{p^m}{r}\mathcal{B}_{n+r} \\
&\equiv \mathcal{B}_n + \mathcal{B}_{n+p^m} + \sum_{r=1}^{p^m-1}\binom{p^m}{r}\mathcal{B}_{n+r} \pmod p .
\end{aligned}$$

Mais, on sait que $\binom{p^m}{r}$ est divisible par p, si r est compris entre 1 et $p^m - 1$. On en déduit que

$$\mathcal{B}_{n+p^{m+1}} - \mathcal{B}_{n+p^m} \equiv \mathcal{B}_n \pmod p .$$

$$\begin{aligned}
\mathcal{B}_{n+p^m} &= \mathcal{B}_{n+1} + \sum_{r=0}^{m-1}(\mathcal{B}_{n+p^{r+1}} - \mathcal{B}_{n+p^r}) \\
&\equiv \mathcal{B}_{n+1} + m\mathcal{B}_n \pmod p .
\end{aligned}$$

La preuve du théorème 46 est complète.

Chapitre 4

Théorèmes de Zhi-Wei Sun et Don Zagier

4.1 Introduction

Dans ce chapitre, nous démontrons minutieusement le théorème principal de l'article de Zhi-Wei Sun et Don Zagier intitulé "On a curious property of Bell numbers" [25]. Nous prouvons ensuite deux corollaires de ce théorème. Nous terminons ce chapitre par la preuve détaillée d'une extension de ce théorème que Zhi-Wei Sun et Don Zagier ont donné dans le même article [25].

4.2 Théorème principal de Zhi-Wei Sun et Don Zagier

Le théorème qui suit fournit pour tout nombre premier et pour un choix arbitraire d'un entier naturel m non divisible par p une congruence modulo p entre une somme finie faisant intervenir les nombres de Bell $\mathcal{B}_k$ pour $1 \leq k \leq p-1$ et le nombre de dérangement D_{m-1}.

Théorème 50 *Pour tout entier $m \geq 1$, et pour tout nombre premier p ne divisant pas m, on a :*

$$\sum_{k=1}^{p-1} \frac{\mathcal{B}_k}{(-m)^k} \equiv (-1)^{m-1} D_{m-1} (\mathrm{mod}\, p). \tag{4.1}$$

Pour tout entier naturel m non nul, posons

$$f(m) = (-1)^{m-1} D_{m-1} - \sum_{k=1}^{p-1} \frac{\mathcal{B}_k}{(-m)^k}.$$

Le théorème 50 équivaut alors à affirmer que l'on a $f(m) \equiv 0 \pmod p$ pour tout nombre premier p ne divisant pas m. Pour prouver ce théorème, nous allons commencer par démontrer le lemme suivant :

Lemme 51 *Pour tout nombre premier p et pour tous entiers m_1 et m_2, on a*

$$p \nmid m_1 \quad et \quad m_2 \equiv m_1 \pmod p \Longrightarrow p \nmid m_2 \quad et \quad f(m_2) \equiv f(m_1) \pmod p. \tag{4.2}$$

Preuve. Soient p un nombre premier et m_1 et m_2 deux entiers tels que $m_2 \equiv m_1 \pmod p$. Dans la relation (4.2), m_1 et m_2 ont des rôles symétriques. Sans nuire à la généralité du problème, on peut donc supposer que $m_2 \geq m_1$. Si $p \nmid m_1$, on alors $m_1 \not\equiv 0 \pmod p$ et comme $m_2 \equiv m_1 \pmod p$, on en déduit que l'on a aussi $m_2 \not\equiv 0 \pmod p$. Il en résulte que $f(m_2)$ et $f(m_1)$ sont des p-entiers. Posons

$$n_1 = m_1 - 1 \text{ et } n_2 = m_2 - 1.$$

On a alors

$$n_2 \equiv n_1 (\mathrm{mod}\, p).$$

On a d'après la propriété (1.12),

$$(-1)^{n_2} D_{n_2} \equiv (-1)^{n_1} D_{n_1} \pmod p,$$

c'est à dire

$$(-1)^{m_2-1} D_{m_2-1} \equiv (-1)^{m_1-1} D_{m_1-1} \pmod p. \tag{4.3}$$

D'autre part, comme on a $m_2 \equiv m_1 \pmod p$, on en déduit que pour $k \in \{1, 2, \ldots, p-1\}$, on a

$$(-m_2)^k \equiv (-m_1)^k \pmod p. \tag{4.4}$$

Comme p ne divise ni m_1, ni m_2, les entiers $(-m_2)^k$ et $(-m_1)^k$ sont des unités de $\mathbb{Z}_{(p)}$, on déduit alors de (4.4) que pour $k \in \{1, 2, \ldots, p-1\}$, on a

$$\frac{1}{(-m_2)^k} \equiv \frac{1}{(-m_1)^k} (\mathrm{mod}\, p).$$

Par sommation, on obtient alors

$$-\sum_{k=1}^{p-1} \frac{\mathcal{B}_k}{(-m_2)^k} \equiv -\sum_{k=1}^{p-1} \frac{\mathcal{B}_k}{(-m_1)^k} \pmod p. \tag{4.5}$$

En sommant membre à membre les relations (4.3) et (4.5), on déduit que l'on a

$$(-1)^{m_2-1} D_{m_2-1} - \sum_{k=1}^{p-1} \frac{\mathcal{B}_k}{(-m_2)^k} \equiv (-1)^{m-1} D_{m_1-1} - \sum_{k=1}^{p-1} \frac{\mathcal{B}_k}{(-m_1)^k} \pmod p.$$

Ainsi on a prouvé que $f(m_2) \equiv f(m_1) \pmod p$. La preuve du lemme est complète. □

Lemme 52 *Avec* $f(m) = (-1)^{m-1}D_{m-1} - \sum_{k=1}^{p-1} \frac{\mathcal{B}_k}{(-m)^k}$, *on a pour* $1 \leq m \leq p-2$ *:*

$$f(m+1) \equiv -mf(m) \pmod{p}$$

$$f(1) \equiv 0 \pmod{p}$$

Preuve. Posons

$$S_m = \sum_{k=1}^{p-1} \frac{\mathcal{B}_k}{(-m)^k}.$$

On a alors

$$\begin{aligned} -mS_m &= \sum_{k=1}^{p-1} (-m)^{1-k}\mathcal{B}_k \\ &= \sum_{n=0}^{p-2} (-m)^{-n}\mathcal{B}_{n+1}. \end{aligned} \tag{4.6}$$

On sait d'après le petit théorème de Fermant que $m^{p-1} \equiv 1 \pmod{p}$ et que $\mathcal{B}_{n+1} = \sum_{k=0}^{n} \binom{n}{k}\mathcal{B}_k$. La relation (4.6) peut donc s'écrire

$$\begin{aligned} -mS_m &\equiv \sum_{n=0}^{p-2} (-m)^{p-1-n} \sum_{k=0}^{n} \binom{n}{k}\mathcal{B}_k \\ &\equiv \sum_{0 \leq k \leq n \leq p-2} (-m)^{p-1-n}\binom{n}{k}\mathcal{B}_k \\ &\equiv \sum_{k=0}^{p-2} \sum_{r=0}^{p-k-2} (-m)^{p-1-n}\binom{n}{k}\mathcal{B}_k \pmod{p}. \end{aligned} \tag{4.7}$$

En faisant le changement de variable $r = n - k$, la relation (4.7) devient

$$-mS_m = \sum_{k=0}^{p-2} \sum_{r=0}^{p-k-2} (-1)^{p-1-k-r} m^{p-1-k-r} \binom{k+r}{k} \mathcal{B}_k. \tag{4.8}$$

En remarquant que l'on a $(-1)^{p-1} \equiv 1 \pmod{p}$, (4.8) s'écrit

$$-mS_m = \sum_{k=0}^{p-2} (-1)^k \mathcal{B}_k \sum_{r=0}^{p-k-2} m^{p-k-1-r}(-1)^r \binom{k+r}{k}. \tag{4.9}$$

On a

$$\begin{aligned}(-1)^r\binom{k+r}{k} &= (-1)^r\binom{k+r}{r} = (-1)^r\prod_{j=1}^{r}\frac{k+j}{j}\\ &\equiv \prod_{j=1}^{r}\frac{p-k-j}{j}\\ &= \binom{p-k-1}{r} \pmod p.\end{aligned}$$

Compte tenu de cette dernière relation, on déduit de (4.8)

$$\begin{aligned}-mS_m &\equiv \sum_{k=0}^{p-2}(-1)^k\mathcal{B}_k\sum_{r=0}^{p-k-2}m^{p-k-1-r}\binom{p-k-1}{r}\\ &\equiv \sum_{k=0}^{p-2}(-1)^k\mathcal{B}_k\left((m+1)^{p-1-k}-1\right)\\ &\equiv \sum_{k=0}^{p-1}(-1)^k\mathcal{B}_k\left((m+1)^{p-1-k}-1\right)\\ &\equiv \sum_{k=0}^{p-1}(-1)^k\mathcal{B}_k(m+1)^{p-1-k}-\sum_{k=0}^{p-1}(-1)^k\mathcal{B}_k\\ &\equiv \sum_{k=0}^{p-1}(-1)^k\frac{\mathcal{B}_k}{(m+1)^k}-\sum_{k=0}^{p-1}\frac{\mathcal{B}_k}{(-1)^k}\\ &\equiv S_{m+1}-S_1\\ &\equiv S_{m+1}-1 \pmod p\end{aligned}$$

On sait aussi que

$$(-1)^mD_m = (-1)^mmD_{m-1}+1.$$

On en déduit que$(-1)^{m-1}D_{m-1}-\sum_{k=1}^{p-1}\frac{\mathcal{B}_k}{(-m)^k}$

$$\begin{aligned}f(m+1) &= (-1)^mD_m - S_{m+1}\\ &\equiv (-1)^mmD_{m-1}+1-(-mS_m+1)\\ &\equiv -m\left((-1)^{m-1}D_{m-1}-S_m\right)\\ &\equiv -mf(m) \pmod p.\end{aligned}$$

□

Nous avons vu que La relation du théorème 50 est équivalente à $f(m) \equiv 0 \pmod p$ pour p ne divisant pas m. $1 \leq m \leq p-1$, on a

$$\begin{aligned} f(m) &\equiv -(m-1)f(m-1) \\ &\equiv (-1)^2(m-1)(m-2)f(m-2) \\ &\equiv (-1)^{m-1}(m-1)(m-2)\dots 1 f(1) \\ &\equiv 0 \pmod p. \end{aligned}$$

Il reste à, prouver que

$$f(1) \equiv 0 \pmod p.$$

On a

$$f(1) = (-1)^0 D_0 - \sum_{k=1}^{p-1} (-1)^k \mathcal{B}_k.$$

On montre que

$$\sum_{k=0}^{p-1} (-1)^k \mathcal{B}_k \equiv 2 (\mathrm{mod}\, p),$$

$$\binom{p-1}{k} = \frac{(p-1)\dots(p-k)}{k!} \equiv (-1)^k \pmod p, \tag{4.10}$$

en exploitant (4.10) et (3.1) (congruence de Touchard)

$$\begin{aligned} \sum_{k=0}^{p-1} (-1)^k \mathcal{B}_k &\equiv \sum_{k=0}^{p-1} \binom{p-1}{k} \mathcal{B}_k \\ &\equiv \mathcal{B}_p \quad \text{(d'après la relation (3.1)).} \\ &\equiv \mathcal{B}_0 + \mathcal{B}_1 \\ &\equiv 2 (\mathrm{mod}\, p) \end{aligned}$$

Comme

$$\sum_{k=1}^{p-1} (-1)^k \mathcal{B}_k = \sum_{k=0}^{p-1} (-1)^k \mathcal{B}_k - 1,$$

on déduit que

$$\sum_{k=1}^{p-1} (-1)^k \mathcal{B}_k \equiv 1 \,\mathrm{mod}(p),$$

ce qui implique que

$$\begin{aligned} f(1) &= 1 - \sum_{k=1}^{p-1} (-1)^k \mathcal{B}_k. \\ &\equiv 0 \,\mathrm{mod}(p). \end{aligned}$$

Exemple 53 *On sait qu'il existe un unique entier* $a(m)$ *tel que*

$$\sum_{k=0}^{p-1}\frac{\mathcal{B}_k}{(-m)^k}\equiv a(m)\,(\mathrm{mod}\,p)\,,\ p\nmid m$$

Comme $\sum_{k=1}^{p-1}\frac{\mathcal{B}_k}{(-m)^k}=\sum_{k=0}^{p-1}\frac{\mathcal{B}_k}{(-m)^k}-1$, *et comme* $\sum_{k=1}^{p-1}\frac{\mathcal{B}_k}{(-m)^k}\equiv(-1)^{m-1}D_{m-1}(\mathrm{mod}\,p)$, *on a*

$$a(m)\equiv 1+(-1)^{m-1}D_{m-1}(\mathrm{mod}\,p)\ ,\text{tel que } p\nmid m \tag{4.11}$$

On applique la relation (4.11) pour $m\in\{2,3,4,5,6,7,8,9,10\}$ *on trouve*

m	2	3	4	5	6	7	8	9	10
D_{m-1}	0	1	2	9	44	265	1854	14833	133496
$a(m)$	1	2	-1	10	-43	266	-1853	14834	-133495

Dans [25], Zhi-Wei Sun et Don Zagier donnent deux corollaires.

Dans ce paragraphe, nous montrons comment les corollaires 54 et 55 peuvent être déduit simplement du théorème 50.

Corollaire 54 *Soit* p *un nombre premier. Alors pour tout entier* $n\in\{1,...,p-1\}$, *on a*

$$(-1)^n\mathcal{B}_n\equiv\sum_{m=1}^{p-1}(-1)^m m^n D_{m-1}(\mathrm{mod}\,p). \tag{4.12}$$

Preuve. (1) On montre que $\sum_{m=1}^{p-1}(-m)^{n-k}\equiv-\delta_{n,k}(\mathrm{mod}\,p)$ pour $n,k\in\{1,....p-1\}$, $\left(\delta_{n,k}=\{\begin{array}{l}1,si,n=k\\0,si\ n\neq k\end{array}\right.$

posons $S_{n-k}^{p-1}=\sum_{m=1}^{p-1}(-m)^{n-k}$, alors

$$\sum_{m=1}^{p-1}(-m)^{n-k}=(-1)^{n-k}\sum_{m=1}^{p-1}m^{n-k},$$

on a deux cas :

(1) si $n=k$ alors $S_0^{p-1}=\sum_{m=1}^{p-1}1=p-1\equiv-1(\mathrm{mod}\,p)$

(2) Si $n\neq k$ et $p-1\nmid n-k$,soit g un élément primitif du groupe F_p^*, alors

$$\begin{aligned}S_{n-k}^{p-k} &= (-1)^{n-k}\sum_{m=1}^{p-1}m^{n-k}\equiv(-1)^{n-k}\sum_{m=0}^{p-2}g^{(n-k)m}(\mathrm{mod}\,p)\\ &\equiv (-1)^{n-k}\frac{g^{(n-k)(p-1)}-1}{g^{(n-k)}-1}(\mathrm{mod}\,p).\end{aligned}$$

Donc

$$\begin{aligned}(g^{(n-k)}-1)S_{n-k}^{p-k} &\equiv (-1)^{n-k}((g^{(p-1)})^{n-k}-1)(\mathrm{mod}\, p)\\ &\equiv 0(\mathrm{mod}\, p).\end{aligned}$$

Si $n \neq k$ et $p-1 \backslash n-k$ on a d'après le petit théoréme de Fermat

$$m^{n-k} = m^{\alpha(p-1)} = (m^{p-1})^{\alpha} \equiv 1(\mathrm{mod}\, p),$$

on remarque si $n, k \in \{1, 2, ..., P-1\}$ alors $p-1 \nmid n-k$.

$$\text{On conclut que} \sum_{m=1}^{p-1}(-m)^{n-k} \equiv -\delta_{n,k}(\mathrm{mod}\, p) \ (\delta_{nk} = 1 \text{ si } n = k \text{ et } 0 \text{ si } n \neq k).$$

On a $-\mathcal{B}_n \equiv \sum_{k=1}^{p-1}\mathcal{B}_k \sum_{m=1}^{p-1}(-m)^{n-k}(\mathrm{mod}\, p)$, puisque : $\sum_{m=1}^{p-1}(-m)^{n-k} \equiv -\delta_{nk} \,\mathrm{mod}\, p$, alors.si $n = k$ on a

$$\begin{aligned}\sum_{k=1}^{p-1}\mathcal{B}_k \sum_{m=1}^{p-1}(-m)^{n-k}(\mathrm{mod}\, p) &\equiv \mathcal{B}_n(-1)\\ &\equiv -\mathcal{B}_n \,\mathrm{mod}\, p.\end{aligned}$$

Alors

$$-\mathcal{B}_n \equiv \sum_{k=1}^{p-1}\mathcal{B}_k \sum_{m=1}^{p-1}(-m)^{n-k} \equiv \sum_{m=1}^{p-1}(-m)^{n} \sum_{k=1}^{p-1}\frac{\mathcal{B}_k}{(-m)^k},$$

on applique (4.1) on trouve

$$-\mathcal{B}_n \equiv \sum_{m=1}^{p-1}(-m)^{n}(-1)^{m-1}D_{m-1}(\mathrm{mod}\, p).$$

Donc

$$(-1)^n\mathcal{B}_n \equiv \sum_{m=1}^{p-1} m^n(-1)^m D_{m-1}$$

□

Corollaire 55 *Pour tout nombre premier p, on a*

$$\mathcal{B}_{p-1} \equiv D_{p-1} + 1(\mathrm{mod}\, p).$$

Preuve. On a d'après la relation (4.12) :pour $n = p-1$ on trouve

$$\begin{aligned}\mathcal{B}_{p-1} &\equiv \sum_{m=1}^{p-1}(-1)^m m^{p-1} D_{m-1} (\mathrm{mod}\, p) \\ &\equiv \sum_{m=1}^{p-1}(-1)^m D_{m-1} (\mathrm{mod}\, p) \quad (\text{puisque } m^{p-1} \equiv (1 \,\mathrm{mod}\, p).\end{aligned}$$

On pose $M = m-1$ alors

$$\mathcal{B}_{p-1} \equiv \sum_{m=0}^{p-2}(-1)^{M+1} D_M (\mathrm{mod}\, p).$$

Comme

$$\sum_{M=0}^{p-1}(-1)^M D_M \equiv \sum_{M=0}^{p-1}\binom{p-1}{M} D_M = (p-1)! \equiv -1 \,\mathrm{mod}\, p,$$

puisque d'après la relation (4.10) on a $\binom{p-1}{M} \equiv (-1)^M \,\mathrm{mod}(p)$ et aussi d'après la relation (1.7) on a

$$n! = \sum_{k=0}^{n}\binom{n}{k} D_k,$$

on déduit que

$$\begin{aligned}\mathcal{B}_{p-1} &= \sum_{M=0}^{p-1}(-1)^{M+1} D_M (\mathrm{mod}\, p) - (-1)^p D_{p-1} (\mathrm{mod}\, p) \\ &\equiv 1 + D_{p-1} (\mathrm{mod}\, p).\end{aligned}$$

□

4.3 Extension du théorème de Zhi-Wei Sun et Don Zagier

Dans [25], Zhi-Wei Sun et Don Zagier prouvent l'extension suivante au théorème 50.

Théorème 56 *Pour tout nombre premier p et pour tout entier $m \geq 1$ tels que $p \nmid m$ on a*

$$(-x)^m \sum_{n=1}^{p-1} \frac{T_n(x)}{(-m)^n} \equiv -x^p \sum_{\ell=0}^{m-1} \frac{(m-1)!}{\ell!}(-x)^\ell \pmod{p\mathbb{Z}_p[x]}. \tag{4.13}$$

Dans ce qui suit, nous adoptons la notation $S(n,k)$ pour désigner le nombre de Stirling de deuxième espèce $\left\{ {n \atop k} \right\}$. Dans le théorème (56), rappelons que $T_n(x)$ désigne le n-ième polynôme de Touchard (3.5) défini par

$$T_n(x) = \sum_{k=0}^{n} S(n,k) x^k.$$

Soient p un nombre premier p et $m \geq 1$ un entier tels que $p \nmid m$. Posons

$$A(x) := (-x)^m \sum_{n=1}^{p-1} \frac{T_n(x)}{(-m)^n} \tag{4.14}$$

et

$$B(x) = -x^p \sum_{\ell=0}^{m-1} \frac{(m-1)!}{\ell!} (-x)^\ell . \tag{4.15}$$

La relation (4.13) du théorème 56 s'énonce ainsi

$$A(x) \equiv B(x) \pmod{p\mathbb{Z}_p[x]}. \tag{4.16}$$

On constate que $A(x)$ et $B(x)$ sont bien des polynômes à coefficients dans $\mathbb{Z}_{(p)}$, du fait que $T_n(x) \in \mathbb{Z}[x]$, $\frac{1}{(-m)^n} \in \mathbb{Z}_{(p)}$ pour car $p \nmid m$ et que $\frac{(m-1)!}{l!} \in \mathbb{Z}$ pour $0 \leq \ell \leq m-1$. De plus, il est facile de constater aussi que $A(x)$ et $B(x)$ sont tous les deux des polynômes de degré $m+p-1$. Le coefficient dominant de $A(x)$ est égale à

$$\left[x^{m+p-1}\right](A(x)) = (-1)^m \frac{1}{(-m)^{p-1}}. \tag{4.17}$$

Le coefficient dominant de $B(x)$ est égale à

$$\left[x^{m+p-1}\right](B(x)) = (-1)(-1)^{m-1} = (-1)^m. \tag{4.18}$$

Le théorème équivaut à affirmer que l'on a les congruences suivantes pour $0 \leq k \leq m+p-1$

$$\left[x^k\right](A(x)) \equiv \left[x^k\right](B(x)) \pmod{p\mathbb{Z}_p[x]} \tag{4.19}$$

On peut remarquer que la relation (4.19) est bien vérifiée pour $k = m+p-1$, il suffit pour cela d'exploiter les relations (4.17) et (4.18) et le petit théorème de Fermat. Pour prouver ces congruences, nous allons dans une première étape montrer que le polynôme $B(x)$ vérifie la congruence suivante :

$$B(x) \equiv (-1)^m \sum_{k=1}^{p-1} \left(\prod_{s=1}^{p-k-1} (s-m) \right) x^{m+k} \pmod{p\mathbb{Z}_p[x]}. \tag{4.20}$$

Pour cela, on commence par écrire

$$\begin{aligned} B(x) &= -x^p \sum_{\ell=0}^{m-1} \frac{(m-1)!}{\ell!} (-x)^\ell \\ &= -x^p \sum_{\ell=0}^{m-1} (m-1-\ell)! \binom{m-1}{\ell} (-x)^\ell \end{aligned} \tag{4.21}$$

En faisant le changement de variable $r = m-1-\ell$, la relation (4.21) devient

$$B(x) = -x^p \sum_{r=0}^{m-1} r! \binom{m-1}{r} (-x)^{m-1-r} \tag{4.22}$$

Remarquons alors que l'on a

$$-x^p \sum_{r=0}^{m-1} r! \binom{m-1}{r} (-x)^{m-1-r} \equiv -x^p \sum_{r=0}^{p-1} r! \binom{m-1}{r} (-x)^{m-1-r} \pmod{p\mathbb{Z}_p[x]}. \tag{4.23}$$

En effet, si on a $m > p$, on a alors $r!\binom{m-1}{r} \equiv 0 \pmod{p}$ pour $p < r \leq m-1$ et la relation (4.23) est vérifiée. Autrement on a $m \leq p-1$ et dans ce cas, on a $r!\binom{m-1}{r} = 0$ pour $m \leq r \leq p-1$ et la relation (4.23) est encore vérifiée.Des relations (4.23) et (4.22), on déduit que l'on a

$$B(x) \equiv (-1)^m \sum_{r=0}^{p-1} r! \binom{m-1}{r} (-1)^r x^{m+p-1-r}. \tag{4.24}$$

Remarquons alors que

$$r! \binom{m-1}{r} (-1)^r = \prod_{s=1}^{r} (s-m).$$

La congruence (4.24) s'ecrit donc

$$B(x) \equiv (-1)^m \sum_{r=0}^{p-1} \left(\prod_{s=1}^{r} (s-m) \right) x^{m+p-1-r} \pmod{p\mathbb{Z}_p[x]} \tag{4.25}$$

Par le changement de variable $k = p-1-r$, la relation (4.25) devient

$$B(x) \equiv (-1)^m \sum_{k=0}^{p-1} \left(\prod_{s=1}^{p-1-k} (s-m) \right) x^{m+k} \pmod{p\mathbb{Z}_p[x]} \tag{4.26}$$

Le coefficient de x^m dans le second membre de (4.26) est

$$[x^m] \left((-1)^m \sum_{k=0}^{p-1} \left(\prod_{s=1}^{p-1-k} (s-m) \right) x^{m+k} \right) = (-1)^m \prod_{s=1}^{p-1} (s-m) \tag{4.27}$$

Comme par hypothèse, on a $p \nmid m$, m est congru modulo p à un entier $t \in \{1, 2, \ldots p-1\}$. Par conséquent, on a

$$(-1)^m \prod_{s=1}^{p-1}(s-m) \equiv 0 \pmod{p}.$$

On en déduit que

$$[x^m]\left((-1)^m \sum_{k=0}^{p-1}\left(\prod_{s=1}^{p-1-k}(s-m)\right)x^{m+k}\right) \equiv 0 \pmod{p}. \tag{4.28}$$

De (4.26) et (4.28), on déduit que l'on a

$$B(x) \equiv (-1)^m \sum_{k=1}^{p-1}\left(\prod_{s=1}^{p-1-k}(s-m)\right)x^{m+k} \pmod{p\mathbb{Z}_p[x]}. \tag{4.29}$$

La relation (4.20) est ainsi bien établie.

Compte tenu des relations (4.14), (4.29) et (4.16), la relation 4.13 du théorème (56) est équivalente à

$$(-x)^m \sum_{n=1}^{p-1}\frac{T_n(x)}{(-m)^n} \equiv (-1)^m \sum_{k=1}^{p-1}\left(\prod_{s=1}^{p-1-k}(s-m)\right)x^{m+k} \pmod{p\mathbb{Z}_p[x]}.$$

Cette dernière relation est encore équivalente à

$$\sum_{n=1}^{p-1}\frac{T_n(x)}{(-m)^n} \equiv \sum_{k=1}^{p-1}\left(\prod_{s=1}^{p-1-k}(s-m)\right)x^{k} \pmod{p\mathbb{Z}_p[x]}.$$

Ainsi pour prouver le théorème (56, il faut prouver que l'on a pour $1 \leq k \leq p-1$

$$\left[x^k\right]\left(\sum_{n=1}^{p-1}\frac{T_n(x)}{(-m)^n}\right) \equiv \left[x^k\right]\left(\sum_{k=1}^{p-1}\left(\prod_{s=1}^{p-1-k}(s-m)\right)x^k\right) \pmod{p}.$$

Autrement dit, en désignant par $\mathfrak{P}(k)$ la propriété suivante

$$\mathfrak{P}(k): \qquad \sum_{n=1}^{p-1}\frac{S(n,k)}{(-m)^n} \equiv \prod_{s=1}^{p-1-k}(s-m) \pmod{p}, \tag{4.30}$$

on doit prouver que $\mathfrak{P}(k)$ est vraie pour $1 \leq k \leq p-1$. Nous allons établir ce résulat en raisonnant par récurrence descendante finie. On commce par vérifier que $\mathfrak{P}(p-1)$ est vraie. Pour $k = p-1$, les deux membres de (4.30) sont égaux à 1 modulo p. Supposons donc la relation $\mathfrak{P}(k)$ vraie pour un entier $k \in \{2, 3, \ldots p-1\}$ (hypothèse de recurrence) et prouvons qu'alors $\mathfrak{P}(k-1)$ est vraie. On a d'après la relation

$$S(n, k-1) = S(n+1, k) - kS(n, k).$$

On en déduit que

$$\begin{aligned}\sum_{n=1}^{p-1}\frac{S(n,k-1)}{(-m)^n} &= \sum_{n=1}^{p-1}\frac{S(n+1,k)}{(-m)^n}-k\sum_{n=1}^{p-1}\frac{S(n,k)}{(-m)^n}\\ &= \sum_{n=2}^{p}\frac{S(n,k)}{(-m)^{n-1}}-k\sum_{n=1}^{p-1}\frac{S(n,k)}{(-m)^n}\\ &= \left((-m-k)\sum_{n=1}^{p-1}\frac{S(n,k)}{(-m)^n}\right)+\frac{S(p,k)}{(-m)^{p-1}}-S(1,k) \qquad (4.31)\end{aligned}$$

Or comme $k \geq 2$, on a $S(1,k) = 0$. D'autre part on sait que pour $2 \leq k \leq p-1$, on a $\frac{S(p,k)}{(-m)^{p-1}} \equiv 0 \pmod p$ .On déduit alors de (4.31) que

$$\sum_{n=1}^{p-1}\frac{S(n,k-1)}{(-m)^n} \equiv (-m-k)\sum_{n=1}^{p-1}\frac{S(n,k)}{(-m)^n}. \qquad (4.32)$$

Or par hypothèse de récurrence, on a

$$\sum_{n=1}^{p-1}\frac{S(n,k)}{(-m)^n} \equiv \prod_{s=1}^{p-1-k}(s-m) \pmod p. \qquad (4.33)$$

Des relations (4.32) et (4.33), on obtient

$$\begin{aligned}\sum_{n=1}^{p-1}\frac{S(n,k-1)}{(-m)^n} &\equiv (-m-k)\prod_{s=1}^{p-1-k}(s-m)\\ &\equiv (p-m-k)\prod_{s=1}^{p-1-k}(s-m)\\ &\equiv \prod_{s=1}^{p-k}(s-m) \pmod p \qquad (4.34)\end{aligned}$$

La relation (4.34) n'est rien d'autre que la propriété $\mathfrak{P}(k-1)$ Ainsi l'hypothèse de récurrence implique que la propriété $\mathfrak{P}(k-1)$ est vraie. La propriété $\mathfrak{P}(k)$ est donc vraie pour $1 \leq k \leq p-1$. La preuve du théorème 56 est complète

On remarque que cette congruence de polynome, pour $x \in \mathbb{Z}_{(p)}$, et $p \nmid x$ implique cette congruence

$$\sum_{0<n<p}\frac{T_n(x)}{(-m)^n} \equiv \frac{1}{(-x)^{m-1}}\sum_{l=0}^{m-1}\frac{(m-1)!}{l!}(-x)^l \pmod p,$$

en effet, on a d'après (4.13)

$$(-x)^m\sum_{0<n<p}\frac{T_n(x)}{(-m)^n} \equiv -x^p\sum_{l=0}^{m-1}\frac{(m-1)!}{l!}(-x)^l \pmod{p\mathbb{Z}_p[x]},$$

alors

$$\sum_{0<n<p}\frac{T_n(x)}{(-m)^n}\equiv\frac{1}{(-x)^{m+1-p-1}}\sum_{l=0}^{m-1}\frac{(m-1)!}{l!}(-x)^l\,(\mathrm{mod}\,p\mathbb{Z}_p[x])\,.$$

Comme $(-x)\in\mathbb{Z}_{(p)}$ alors $(-x)^{p-1}\equiv 1\,(\mathrm{mod}\,p)$ (d'après le petit théorème de Fermat), donc

$$\sum_{0<n<p}\frac{T_n(x)}{(-m)^n}\equiv\frac{1}{(-x)^{m-1}}\sum_{l=0}^{m-1}\frac{(m-1)!}{l!}(-x)^l\,(\mathrm{mod}\,p)$$

Cas particuiliers

Pour $m\in\{2,3,4\}$,tel que $p\nmid m$ on trouve

$$(1)\ \sum_{0<n<p}\frac{T_n(x)}{(-2)^n}\equiv\frac{1}{(-x)}\sum_{l=0}^{1}\frac{1}{l!}(-x)^l\,(\mathrm{mod}\,p)\equiv\frac{1}{(-x)}(1-x)\,(\mathrm{mod}\,p)\equiv\frac{x-1}{x}\,(\mathrm{mod}\,p)$$

$$(2)\ \sum_{0<n<p}\frac{T_n(x)}{(-3)^n}\equiv\frac{1}{(-x)^2}\sum_{l=0}^{2}\frac{2!}{l!}(-x)^l\,(\mathrm{mod}\,p)\equiv\frac{1}{(-x)^2}(2-2x+x^2)\,(\mathrm{mod}\,p)$$

$$\equiv\frac{x^2-2x+2}{x^2}\,(\mathrm{mod}\,p)$$

$$(3)\ \sum_{0<n<p}\frac{T_n(x)}{(-4)^n}\equiv\frac{1}{(-x)^3}\sum_{l=0}^{3}\frac{3!}{l!}(-x)^l\,(\mathrm{mod}\,p)\equiv\frac{1}{(-x)^3}(6-6x+3x^2-x^3)\,(\mathrm{mod}\,p)$$

$$\equiv\frac{x^3-3x^2+6x-6}{x^3}\,(\mathrm{mod}\,p)$$

Si on remplace x par 1 dans la congruence

$$\sum_{0<n<p}\frac{T_n(x)}{(-m)^n}\equiv\frac{1}{(-x)^{m-1}}\sum_{l=0}^{m-1}\frac{(m-1)!}{l!}(-x)^l\,(\mathrm{mod}\,p)\,,$$

on trouve

$$\sum_{0<n<p}\frac{T_n(1)}{(-m)^n}\equiv\frac{1}{(-1)^{m-1}}\sum_{l=0}^{m-1}\frac{(m-1)!}{l!}(-1)^l\,(\mathrm{mod}\,p)\,,$$

comme $T_n(1)=\mathcal{B}_n$, on a, alors

$$\begin{aligned}\sum_{0<n<p}\frac{\mathcal{B}_n}{(-m)^n} &\equiv \frac{1}{(-1)^{m-1}}\sum_{l=0}^{m-1}\frac{(m-1)!}{l!}(-1)^l\,(\mathrm{mod}\,p)\\ &\equiv (-1)^{m-1}(m-1)!\sum_{l=0}^{m-1}\frac{(-1)^l}{l!}\,(\mathrm{mod}\,p)\end{aligned}$$

Mais on sait que

$$D_{m-1}=(m-1)!\sum_{l=0}^{m-1}\frac{(-1)^l}{l!}(\text{d'après la relation(1.9)},$$

on obtient immediatement

$$\sum_{0<n<p} \frac{\mathcal{B}_n}{(-m)^n} \equiv (-1)^{m-1} D_{m-1} \,(\mathrm{mod}\, p) \text{ c'est le cas de théorème 50}$$

Conclusion

Notre conclusions cette étude par les perspectives que ce travail nous permet d'envisager.

Recemment, en 2013, dans un aricle intitulé "Congruences on the Bell polynomials and the derangement polynomials" paru dans la revue Journal of Number Theory, Yidong Sun , Xiaojuan Wu et Jujuan Zhuang ont généralisé le théorème de Sun et Zagier en prouvant que pour tous entiers $n \geq 0$, $m \geq 1$ et pour tout nombre premier $p \nmid m$ on a

$$x^m \sum_{k=1}^{p-1} \frac{\mathcal{B}_{n+k}(x)}{(-m)^k} \equiv x^p \sum_{k=0}^{n} S(n,k)(-1)^{m+k-1}\mathcal{D}_{m+k-1}(1-x) \pmod p.$$

Pour démontrer ce résutat, ces auteurs utilisent le calcul ombral.

Un conjecture bien connue est la conjecture de Kurepa. En définissant la factorielle à gauche d'un entier $n \geq 1$ par

$$!n = 0! + 1! + \cdots + (n-1)!,$$

La célèbre conjecture de Kurepa s'énonce ainsi

Conjecture 57 *(Kurepa) Pour tout entier $n \geq 2$, le pgcd de $!n$ et $n!$ est égal à 2.*

Cette conjecture a été testée jusqu'à $n = 10^6$. Cette conjecture est équivalente à une conjecture sur les nombres de Bell. En effet, on montre que l'on a pour tout nombre premier p,

$$\sum_{k=0}^{p-1} k! \equiv \mathcal{B}_{p-1} - 1 \pmod p.$$

La conjecture de Kurepa est alos équivalente à affirmer que pour tout nombre premier $p \geq 3$, on a

$$\mathcal{B}_{p-1} \not\equiv 1 \pmod p.$$

C'est sous cette forme que D. Barsky et B. Benzaghou [3]ont étudié cette conjecture et ont affirmé l'avoir prouvée en 2004. Malheureusement une erreur irréparable signalée par F. Bencherif a invalidé cette preuve [4]. Ainsi La conjecture de Kurepa reste encore, en 2014, une question ouverte.

Annexe 1 : Quelques commandes MAPLE

On trouvera dans cette annexe quelques commandes MAPLE qui nous ont été utiles pour vérifier les relations données dans ce mémoire.

Calcul des nombres de Bell :

$> with(combinat);$

$> seq(bell(n), n = 0..15);$

$1, 1, 2, 5, 15, 52, 203, 877, 4140, 21147, 115975, 678570, 4213597, 27644437, 190899322, 1382958545$

Calcul des nombres de dérengements :

$> with(combinat);$

$f := (n) \rightarrow n! \sum_{k=0}^{n} \frac{(-1)^k}{k!}$

$seq(f(n), n = 0..15);$

$1, 0, 1, 2, 9, 44, 265, 1854, 14833, 133496, 1334961, 14684570,$

$176214841, 2290792932, 32071101049,$

Calcul des nombres de Stirling de deuxiéme éspèce :

$> with(combinat);$

$> seq(seq(stirling2(n, k), k = 0..n), n = 0..6)$

$1, 0, 1, 0, 1, 1, 0, 1, 3, 1, 0, 1, 7, 6, 1, 0, 1, 15, 25, 10, 1, 0, 1, 31, 90, 65, 15, 1$

Annexe 2 : Auteurs cités

1-**Eric Tample Bell**

Eric Tample Bell nait le 7 février 1883 à Peterhead (Scotland).La famille déménage pour San José,Californie alors qu'il est agé de 15 mois.La famille retourne à Bedford (Angleterre) apré la mort de son père.En 1902,Bell retourne aux Etats-Unis.

Bell étudie à l'université Stanford età l'unversité Colombia.puis à l'université de Washington etplus tard au California (Institute of Technology).

Ses recherches portent sur la théoriedes nombres,en particulier les séries de Bell.Il a essayé, bien que sans succès, de donner une rigueur logique au traditionnel calcul ombral. Il travaille aussi beaucoup sur les fonctions génératrices,traitées comme des séries entièrs, sans se soucier de leur convergence.Il est à l'origine des polynomes deBell et de nombres de Bell en combinatoire.

Eric Tampel Bell meurt le 21 décembre 1960 à Watsonville,Etats-Unis.

Les travaux de Eric Tampel Bell

1- Fiction et poésie

Au début des années 1920,Bell a écrit quelques long poèmes. Il a aussi écrit qulque romans de sience-fiction.

2- Ecrits sur les mathématiques

Les Grands mathématiciens, un livre de biographies, a poussé beaucoup de personnes vers les mathématiques.

Développement des mathématiques, son dernier livre , a eu moins de succès.Constance Reib pense pourtant qu'il a moins de faiblesses.

Le dernier problème, de publication posthume,et un hybride entre histoire sociale et histoire des mathématiques

3-Publications mathématiques

.*The Cyclotomic Quinary Quintitc (sa thése) 1912*

.An Arithmetical Theory of Certain Numerical Function 1915

.Algebraic Arithmetic 1927

4-Livers sur les mathématiques

.Dobunking Science.

The Search for Truth

.Man and His Lifebelts

.Men of Mathématics

.The Development of Mathématics

The Magic of Numbers

.Mathématics :Queen and Servant of Science

.The Last Problem.

5-Romans

.The Purple Sapphire (1924), The Gold Tooth (1927),.....

Jacques Touchard (1885 − 1968) est un mathématicien français. En 1953, il prouva que tout nombre parfait impair est de la forme 12k + 1 ou 36k + 9. Il a introduit les polynômes de Touchard (en), qui interviennent en combinatoire et en théorie des probabilités. Il est aussi connu pour avoir résolu le problème des ménages.

Don Bernhard Zagier, est un mathématicien américain **né en 1951**, spécialisé en théorie des nombres, en théorie des formes modulaires et leurs liens avec la topologie. Il est titulaire de la chaire de théorie des nombres au Collège de France à Paris1, et professeur à l'institut Max-Planck de mathématiques à Bonn.

Samuel Standfield Wagstaff, Jr. est un American mathematicien américain **né en 1945**, chercheur en informatique dont les intérêts de recherche sont dans les domaines de la cryptographie, calcul parallèle , et l'analyse d'algorithmes , en particulier les algorithmes de la théorie des nombres . Il est actuellement professeur de sciences informatiques et mathématiques à l'université de Purdue (USA).

Zhi Wei Sun est un mathématicien chinois **né en 1965**, chercheur en théorie des nombres, en combinatoire, et en théorie des groupes, professeur à l'université de Nankin.

Bibliographie

[1] M. Abramowitz and I.A. Stegun. Handbook of Mathematical Functions : with Formulas, Graphs and Mathematical tables, Dover Publications, 1972

[2] T.Apostol, Introduction to analytic number theory.vol.1.springer, (1976).

[3] D. Barsky, & B. Benzaghou, Nombres de Bell et somme de factorielles. Journal de théorie des nombres de Bordeaux, 16(1), (2004), 1-17.

[4] D. Barsky, & B. Benzaghou, Erratum à l'article Nombres de Bell et somme de factorielles. Journal de Théorie des Nombres de Bordeaux, 23(2), (2011), 527-527.

[5] Z.I. Borevitch, & I R. Chafarevitch, Théorie des Nombres, Gauthier-Villars, Paris. Zbl0145, vol. 4901. (1967).

[6] G. Bisson, & D. Zagier, Autour des nombres et des polynomes de Bernoulli. (*http ://www.normalesup.org/˜bisson/tea/bernoulli.pdf).*

[7] E.Berrebi, Devillebichot, G, Berrebi (Edmond)-Mathématique, exercices corrigés. T. II (Année préparatoire, licence ès sciences économiques, 2e année, étudiants des grandes écoles). Préface de Maurice Girault. Revue économique, 18(1), (1967) 134-134.

[8] A. Chambert-Loir, A, Algebre Commutative.*Polycopié de maîtrise de l'université Pa,* (2000).

[9] L. Comtet, Analyse combinatoire, tome premier, Collection Sup. Le mathématicien, Presses universitaires de France.L, (1970).

[10] L. Comtet, Analyse combinatoire avancée. Techniques de l'ingénieur. Sciences fondamentales, (AF201), AF201-1, AF202-5 (2001).

[11] M. Demazure, Cours d'algèbre : primalité, divisibilité, codes (Vol. 1). Paris : Cassini. (1997).

[12] G. Dobinski, "Summirung der Reihe \textstyle\sum\frac{n^m}{n!} für m = 1, 2, 3, 4, 5, ... ", Grunert's Archiv, volume 61, 1877, pages 333–336.

[13] G.Eguether, AI-Problemes de denombrement, BF-nombres de Stirling et nombres de Bell,CK-formule de Dibruno, (http ://iecl.univ-lorraine.fr/˜Gerard.Eguether/zarticle/BF.pdf), et à (http ://iecl.univ-lorraine.fr/˜Gerard.Eguether/zarticle/CK.pdf).

[14] A. Gertsch, & Robert, A. M, Some congruences concerning the Bell numbers. Bulletin of the Belgian Mathematical Society Simon Stevin, 3(4), (1996), 467-476.A.

[15] X.Gourdon, Les maths en tête :mathématiques pour M'.Ellipses, (1994).

[16] A. Girannd, Nombres de Bell 2012, (*http ://perso.univ-rennes1.fr/arnaud.girand/pdf/dvp_ agreg/bell.pdf).*

[17] G. Hurst, G., & A. Schultz, An elementary (number theory) proof of Touchard's congruence. arXiv preprint arXiv :0906.0696. (2009)

[18] Rota, G.-C. "The Number of Partitions of a Set." Amer. Math. Monthly 71, (1964), 498-504.

[19] Sloane, N. J, The on-line encyclopedia of integer sequences. (https ://oeis.org/)

[20] P.Sun, A note on the number of dérangements.Applied mathématics E-notes, vol 5, (2005), 176-178

[21] Samuel S. Wagstaff, Jr. The period of the Bell exponential integers modulo a prime. In Mathematics of Computation 1943-1993 : a half-century of computational mathematics (Vancouver, BC, 1993), volume 48 of Proc. Sympos. Appl. Math, pages 595-598. Amer. Math. Soc, Providence, RI, 1994.

[22] L. Tao Kai, Bell numbers and Bell numbers modulo a prime number,Mathematical Medley vol 55 (1997)

[23] J. Touchard, 'Propriétés arithmétiques de certains nombres recurrents', Ann. Soc. Sci. Bruxelles 53A (1933), 21–31.

[24] Zhi-Wei Sun, On arithmetic properties of Bell numbers, Delannoy numbers and Schroder numbers, (2011), (http ://math.nju.edu.cn/~zwsun/BellDelannoy.pdf).

[25] Zhi-Wei Sun and Don Zagier, On a curious property of Bell numbers, Bull. Aust. Math. Soc. 84 (2011), 153–158.