N d'ORDRE : **34/2012-M/MT**

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

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

MEMOIRE

Présenté pour l'obtention du diplôme de MAGISTER
EN: MATHÉMATIQUES
Spécialité : Algèbre et Théorie des Nombres

Par : Nora MAHLOUL

CONGRUENCES DES NOMBRES DE STIRLING ET DES SUITES REMARQUABLES

Soutenu publiquement le 08 Mai 2012 à 10h devant le jury composé de :

M Abdelkader	KELLADI	Professeur	USTHB	Président
M Benali	BENZAGHOU	Professeur	USTHB	Directeur de Mémoire
M Hacene	BELBACHIR	Maitre de Conferences /A	USTHB	Examinateur
M Abderrahmane	TADJINE	Maitre Assistant /A	USTHB	Invité
Mme Schérazade	ZERROUKHAT	Maitre Assistant /A	USTHB	Invitée

CONGRUENCES DES NOMBRES DE STIRLING ET DES SUITES REMARQUABLES

Mémoire présenté pour l'obtention du diplôme de Magistère

en Mathématiques, Spécialité Algèbre et Théorie des Nombres

par

Nora MAHLOUL

Mai 2012

Table des matières

A mes amis.

" Aux amis de toute ma vie, délicieux et terrifiants, les nombres "

François le Lyonnais *Les nombres remarquables*

Remerciements

Avant tout je remercie Allah, sans ma foi en lui, je n'aurai jamais eu ni le courage ni la volonté d'entreprendre ce voyage surtout après une longue coupure .

Après Dieu, je dois me remercier car la reprise n'a pas été evidente et il m'a fallu beaucoup de courage et de patience pour mener à terme ce fatiguant mais très agréable voyage .

On dit que celui qui est ingrat et ne remercie pas les gens est aussi ingrat envers Dieu. Ces gens que l'on trouve sur nos chemins pour nous guider et nous orienter ne sont là que par la volonté de Dieu.

Commençons les remerciements :

J'aimerais tout d'abord remercier Monsieur le Professeur Benali Benzaghou qui m'a proposé l'intéressant et captivant sujet qui constitue le mémoire de ce Magister. Je lui suis reconnaissante pour tous ses conseils et ses encouragements qui m'ont permis de mener à bien ce travail.

J'aimerais aussi remercier les Professeurs Hacène Belbachir et Abdelkader Khelladi d'avoir accepté de faire partie du jury. jJe les remercie aussi pour leurs encouragements et leurs critiques avant ,pendant et après la soutenance .

Je remercie également Monsieur Abderrahmane Tadjine et Madame Schérazade Zerroukhat pour leur conseils et suggestions.

Si j'ai pu remercier et exprimer ma gratitude envers certaines personnes qui m'ont aidés, je me trouve par contre dans l'incapacité de remercier à leur juste valeur d'autres personnes et plus précisement **deux personnes** envers lesquelles je ne pourrai jamais m'acquitter totalement de ma dette ,et je laisse ça à Dieu, lui seul pourra mesurer l'immensité de ce qu'elles ont fait pour moi et les récompenser à leur juste valeur. Je vise particulièrement les très braves et sincères **Leila Benferhat Cherchem** et .**Yamina Rouani Oudni** .

Je termine par remercier ma très chère et tendre famille de m'avoir toujours aimé et soutenu.

Introduction

"Le goût des sciences abstraites en général et plus particulièrement pour les mystères des nombres est fort rare ; on ne s'en étonne pas. Les charmes enchanteurs de cette science sublime ne se révèlent dans toute leur beauté qu'à ceux qui ont le courage de l'explorer en profondeur"

Lettre du **30** *avril* **1807** *de C. F. GAUSS* $(\mathbf{1777-1855})$ *à Mlle Sophie GERMAIN* $(\mathbf{1776-1831})$.

Ce mémoire est consacré à une étude des congruences, quand Monsieur le Professeur Benali Benzaghou m'a proposé cette étude en me suggérant de commencer par recenser dans un premier temps les congruences classiques connues sur les coefficients binomiaux et sur les nombres de Stirling de première et seconde espèce, j' étais loin de me douter de ce que mes recherches allaient me faire découvrir :

- De nombreux théorèmes dont certains sont devenus de grands classiques ; chacun d'eux avec son histoire plus ou moins ancienne, plus ou moins connue et dans laquelle souvent, s'entremêlent les noms d'illustres mathématiciens.

- Une avalanche continuelle de résultats qui s'accumulent jusqu'à aujourd'hui, mais aussi un immense chantier où de nombreuses questions restent posées, où de nombreuses conjectures restent sans réponse.

Enfin, pour être bref, il s'agissait d'un monde à explorer, une véritable et immense planète à découvrir. J' ai entrevu la difficulté de cette recherche. J' ai aussi pris goût à cette entreprise fascinante.

Je dois avouer qu'avant de débuter, j'ignorais beaucoup pour ne pas dire tout du sujet, j'avais une certaine idée des congruences sans doute pas très précise, un peu plus que celle qu'on a généralement quand on termine ses études de graduation, en explorant le sujet essentiellement par de très nombreuses recherches par Internet, je découvrais une histoire fantastique, passionnante et captivante. Je restais des heures à télécharger des "Giga-octets" de documents scientifiques : livres rares, articles anciens et nouveaux. Grace à de bons moteurs de recherche, je me rendais compte que je pouvais avoir accès à un nombre considérable d'in-

formations. C'est ainsi que je suis restée littéralement scotchée durant de nombreuses heures devant mon ordinateur.

J'apprenais que l'origine de la notion de congruence remonte en fait à l'aube de l'humanité. Le fameux théorème des restes chinois daterait de plus de 2000 ans. Au cours des siècles, la connaissance sur les congruences s'est transmise, parfois perdue mais souvent retrouvée ou redécouverte par des mathématiciens illustres. Tous les grands mathématiciens de ce monde se sont intéressés aux congruences. Sans pouvoir, ni vouloir dresser une liste exhaustive de ces nombreux et souvent illustres mathématiciens qui ont apporté leur contribution à l'étude des congruences, on peut commencer par citer Sun Zi connu pour le théorème chinois des restes. Dans le livre de Sun Zi, le *Sunzi suanjing* datant du IIIe siècle, on touve le problème suivant :

« *Combien l'armée de Han Xing comporte-t-elle de soldats si, rangés par 3 colonnes, il reste deux soldats, rangés par 5 colonnes, il reste trois soldats et, rangés par 7 colonnes, il reste deux soldats ?* »

La réponse proposée par Sun Zi est la suivante :

‹‹Multipliez le reste de la division par 3,c'est à dire 2 par 70 ,ajoutez lui le reste de la division par 5 c'est à dire 3 par 21 ,ensuite rajoutez aussi le reste de la division par 7 c'est à dire 2 par 15,tant que le nombre est superieur à 105 ,retirez 105 ››.

Le concept de congruence est aussi présent dans l'oeuvre de **Brahmagupta** (**598 − 668**), dans son *Bhrama-Sphuta-Siddhanta*, traité d'astronomie et de mathématiques. La forme originale du théorème des restes chinois, apparait dans un livre du mathématicien chinois **Qin Jiushao** publié en **1247**.

On arrive enfin aux mathématiciens les plus cités aujourd'hui : **Pierre de Fermat** (**1601 − 1665**), **Leonhard Euler** (**1707 − 1783**), **John Wilson** (**1741 − 1793**), **Adrien-Marie Legendre** (**1752 − 1833**), **Carl Friedrich Gauss** (**1777 − 1855**), **Carl Gustave Jacobi** (**1804 − 1851**), **Ferdinand Gotthold Max Eisenstein** (**1823 − 1852**), **Augustin Louis Cauchy** (1789 − 1857), **Sophie Germain** (**1776 − 1857**), **Edouard Lucas** (**1842 − 1891**),**Derrick Norman Lehmer** (**1867 − 1938**) **Leonard Carlitz** (**1907 − 1999**), **Derrick Henry Lehmer** (**1905 − 1991**), **Emma Trotskaia Lehmer** (**1906 − 2007**) sans oublier le fameux **Srivasa Ramanujan** (**1887 − 1920**) pour ses congruences sur la fonction $p(n)$ qui donne le nombre de partitions d'un entier n. Rappelons que $p(n)$ désigne le nombre de manières d'écrire l'entier n comme une somme d'entiers décroissants. Même le géomètre mathématicien bien connu pour son célèbre théorème sur les trisectrices d'un triangle **Frank Morley** (**1860 − 1937**) s'est illustré en énonçant et prouvant une congruence vérifiée par certains coefficients binomiaux qu'il obtient d'une manière particulièrement subtile, une congruence que C. Aebi et G. Cairns [3] n'ont pas hésité à qualifier de congruence "miraculeuse". Son travail faisait suite à des travaux de **Joseph Wolstenholme** (**1829 − 1891**) lesquelles encore généralisaient un résultat de **Charles Babbage** (**1791 − 1871**),mathématicien connu surtout comme étant un précursseur de l'informatique.

La tâche de faire "un état des lieux", tache qui m'avait semblé au premier abord assez simple s'est tout d'un coup transformée en une entreprise de longue haleine certes, mais aussi et surtout en une entreprise captivante. Ce mémoire est un peu le fruit de ces nombreuses longues et passionnantes recherches sur cette fabuleuse théorie des congruences. Est-il utile de rappeler que nos jours, la cryptographie a entrainé un regain considérable d'intérêt pour l'étude des congruences du fait même des applications de la théorie des congruences aux problèmes de codage ?

Si l'on fait souvent référence à **Pierre de Fermat** $(\mathbf{1601-1665})$ pour voir apparaitre les premiers énoncés profonds (souvent donnés sans démonstration) relatifs à la divisibilité de certaines familles d'entiers, il faudra attendre **Gauss** $(\mathbf{1777-1855})$ pour voir naître la notation actuelle des congruences et surtout les premières preuves de certains énoncés dans son célèbre ouvrage "Disquisitiones Arithmeticae" paru en 1801, alors qu'il avait à peine 24 ans. Gauss a donné un éclairage nouveau sur cette notion. Son apport et ses contributions à l'arithmétique sont d'autant plus remarquables qu'il avait affirmé peu avant la parution de ce célèbre ouvrage qu'il n'avait pu prendre connaissance des travaux de ses prédécesseurs qu'après l'avoir achevé. Dans cet "immortel " ouvrage, considéré par un grand nombre de mathématiciens comme une bible de l'arithmétique moderne, Gauss a éclairé, guidé et motivé la recherche en arithmétique pour les générations de mathématiciens des deux siècles qui ont suivi.

Ce mémoire est constitué de cinq chapitres dont nous allons donner une brève description.

Le premier chapitre porte sur des généralités concernant les congruences. On y précise la terminologie, les conventions. On y rappelle la définition de l'anneau $\mathbb{Z}_p$ des entiers p-adiques et du corps $\mathbb{Q}_p$ des nombres p-adiques. On montre aussi l'utilité des congruences dans la résolution de certains problèmes. Nous rappelons dans ce chapitre la définition des nombres de Bernoulli, l'énoncé du théorème de Von staudt et clausen, la définition des polynômes de Gauss (qui est le fruit d'efforts personnels) et quelques précisions l'algèbre de Hurwitz construite sur un corps $\mathbb{C}$ de caractéristique zéro,cette théorie permet d'entrevoir comment on pourrait agréablement récupérer des relations sur les nombres de Stirling de première et seconde espèce. Nous avons fait que détailler certains résultats obtenus par Messieurs les Professeurs Benzaghou et Barsky.

Le deuxième chapitre est sans doute le plus important. Il est consacré à l'étude de certaines congruences vérifiées par les coefficients binomiaux. Nous n'avons pas hésité à retourner aux sources et à écrire en termes modernes les démonstrations de certains théorèmes parfois quelque peu oubliées. Nous avons repris les démonstrations originelles et les avons comparé avec les démonstrations actuelles. Nous avons fait un peu revivre ces démonstrations qu'on ne retrouve plus souvent que dans les écrits originaux, mais qui souvent recèlent d'idées et d'astuces originales. On trouvera dans ce chapitre les preuves détaillées,modernisées et quelque peu simplifiées des théorèmes de Babbage, de Wolstenholme. Nous détaillerons plus

particulièrement un theorème du à Morley . Ces théorèmes font encore l'objet aujourd'hui de démonstrations simplifiées ou de généralisations. Nous en examinons aussi quelques unes trés récentes.

Le troisième chapitre porte sur certaines super congruences, c'est à dire sur des congruences modulo une puissance d'un nombre premier. Nous donnerons dans ce chapitre une preuve originale et courte de la congruence de Morley .Nous nous intérresserons aux nombreuses extensions du théorème de **Babbage-Wolstehholme** et nous en donnerons un survey de cette congruence $(\mathbf{1819-2012})$.

Le quatrième chapitre commence par donner un petit apercu historique des nombres de Stirling ,on apprends que ces nombres étaient déjà connu au seizième siècle par le mathématicien anglais **Thomas Harriot** $(\mathbf{1560-1621})$,aussi on apprendra que ces nombres n'ont jamais été standartisés et on les connaitra sous plusieurs notations dans ce chapitre on décrira aussi l'analogie des propriétés arithmétiques entre les nombres de Stirling de première et seconde espèce et les coefficients binomiaux qui sont des entiers . On y précise certaines congruences vérifiées par ces deux classes d'entiers. Ces nombres entiers sont liés aussi avec les nombres de Bernoulli (qui se trouvent être des nombres rationnels). C'est en particulier, la relation existante entre les nombres de Bernoulli et les nombres de Stirling de deuxième espèce qui a permis à **EdouardLucas**$(\mathbf{1842-1891})$ de donner une démonstration particulièrement élégante du fameux théorème de **Karl Von Staudt** $(\mathbf{1798-1867})$ et **Thomas Clausen** $(1801-1885)$**.** La preuve de ce théorème fait appel aux propriétés de congruences vérifiées par les nombres de Stirling de deuxième espèce. Nous détaillons cette preuve dans ce chapitre. Ces deux auteurs avaient découvert ce théorème indépendamment l'un de l'autre en **1840**. Ce même théorème fut redécouvert plus tard par Ramanujan qui en ignorait alors l'existence.

Nous avons pu constater aussi que la littérature scientifique était bien plus généreuse en résultats sur les congruences des nombres de Stirling de seconde espèce que pour les congruences pour les nombres de Stirling de première espèce. C'est là une remarque que Monsieur le Professeur Benali BENZAGHOU nous avait signalé.

Le chapitre cinq est consacré à l'énoncé de quelques conjectures. L'expérimentation (avec les ordinateurs d'aujourd'hui) demeure une source d'inspiration et de recherches pour l'étude des congruences pour les suites remarquables d'entiers (ou de nombres rationnels) qui ne se laissent pas apprivoiser facilement. Plusieurs résultats énoncés par Gauss furent d'ailleurs obtenus expérimentalement. C'est d'abord par de nombreux essais numériques que **Wilson** $(\mathbf{1741-1793})$ a été amené à énoncer un théorème qui porte son nom, qui ne sera prouvé en toute rigueur que bien après lui, un résultat qui en fait était déjà connu par le mathématicien arabe **Alhazen** $(\mathbf{965-1039})$). Babbage et Wolstentholme ont aussi expérimenté avant d'énoncer et de prouver leur résultat.

On peut citer les nombreuses conjectures énoncées par Wei Sun, et qu'on peut retrouver sur la page web du Professeur Wei Sun. Un grand nombre des conjectures que nous énonçons dans

ce chapitre proviennent de cette page web. On arrive péniblement à en prouver quelques unes. Il s'agit dénoncés faciles à formuler, dont on peut tester la véracité pour de très nombreuses valeurs des paramètres, mais que souvent, on n'arrive pas à prouver.

Nous ne pouvons qu'être en accord avec le Professeur W. S. CASSELS quand il affirme :

" Number theory is an experimental science."

. **W. S. Cassels** (**1922**) Professor Emeritus of Mathematics, The University of Cambridge.

Notations

$\mathbb{N}$ ensemble des entiers naturels

$\mathbb{N}^*$ ensemble des entiers naturels non nuls

$\mathbb{Z}$ ensemble des entiers relatifs

$\mathbb{Q}$ ensemble des rationnels

$\mathbb{R}$ ensemble des réels

$\mathbb{C}$ ensemble des complexes

$[P]$ symbole d'Iverson avec la signification suivante

$[P] == \begin{cases} 1 \text{ si l'énoncé } P \text{ est vrai} \\ 0 \text{ sinon.} \end{cases}$

$|x|$ valeur absolue du nombre réel x

$v_p(x)$ valuation $p-$adique de x : pour x

$|x|_p$ valeur absolue p-adique du nombre rationnel x : $|x|_p = \frac{1}{p^{v_p(x)}}$, pour $x \neq 0$ et $|0|_p = 0$.

$\mathbb{Z}_p$ anneau des entiers p-adiques

$\mathbb{Z}_p^*$ groupe des unités de l'anneau $\mathbb{Z}_p$

$\mathbb{Z}_{(p)}$ anneau constitué par les nombres rationnels de valuation p-adique positive :$\mathbb{Z}_{(p)} = \mathbb{Z}_p \cap \mathbb{Q}$

$\mathbb{Q}_p$ corps des nombres p-adiques

$\lfloor x \rfloor$ partie entière (inférieure) du nombre réel x

$H_n = 1 + \frac{1}{2} + \frac{1}{3} + ... + \frac{1}{n}$ le $n - ième$ nombre harmonique

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

$x^{\bar{n}} = x\,(x+1)\cdots(x+n-1)$ factorielle ascendante de x

$x^{\underline{n}} = x\,(x-1)\cdots(x-n+1)$ factorielle descendante de x

$a \equiv b \bmod n$

$\ln(x)$ logarithme népérien de x

$q_p(a)$ quotient de Fermat $q_p(a) = \frac{a^{p-1}-1}{p}$

(a, b) couple (a, b) ou $\text{pgcd}(a, b)$ selon le contexte

φ fonction indicatrice d'Euler.

$s_q(n)$ somme des chiffres de n écrit en base q (pour $q \geq 2$)

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

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

$\begin{bmatrix} n \\ k \end{bmatrix}$ nombre de Stirling de première espèce non signé : $\begin{bmatrix} n \\ k \end{bmatrix} = |s(n, k)|$

$S(n, k) = \begin{Bmatrix} n \\ k \end{Bmatrix}$ nombre de Stirling de deuxième espèce

$\binom{n}{k}_q$ polynôme de Gauss

$B_{n,k}$ polynôme exponentielpartiel de Bell

Y_n polynôme exponentiel complet de Bell

P_n *n-ième* nombre de Bell

$P_n(x)$ *n-ième* polynôme de Bell

B_n *n-ième* nombre de Bernoulli

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

C corps commutatif de caractéristique zéro

$C\left[[x]\right]$ anneau des séries formelles à coefficient dans C

$C^{\mathbb{Z}}$ ensemble des suites $u : \mathbb{Z} \longrightarrow C$

$\text{supp}(u)$ support d'une suite $u \in C^{\mathbb{Z}} : \text{supp}(u) = \{n \in \mathbb{Z} : \ u(n) \neq 0\}$

$\text{ord}(u)$ ordre d'une suite $u \in C^{\mathbb{Z}} : \text{ord}(u) = \inf \text{supp}(u)$. Pour $u \neq 0$, $\text{ord}(u) \in \mathbb{Z} \cup \{-\infty\}$.

$s(C) = \left\{u \in C^{\mathbb{Z}} : \text{ord}(u) > -\infty\right\}$

$s_0(C) = \left\{u \in C^{\mathbb{Z}} : \text{ord}(u) \geq 0\right\}$

Ψ Notation du produit de Hurwitz de deux suites de $s_0(C)$

$\mathcal{A} = s_0(C)$ algèbre de Hurwitz définie sur $s_0(C)$.

$\gamma(n)$ factorielle de Roman : extension de la factorielle de n

$\gamma(n) = n!$ pour $n \geq 0$, $\gamma(n) = \frac{(-1)^{n+1}}{(-n-1)!}$ pour $n < 0$.

Chapitre 1

Généralités

"Mathematicians do not study objects ; but relations among objects ; they are indifferent to the replacement of objects by others as long as relations do not change. Matter is not important, only form interests them."

Henri POINCARE (1854 − 1912).

1.1 Introduction

La théorie des congruences est l'étude de la divisibilité centrée sur la notion du reste. L'idée de base étant de travailler non pas sur les entiers, mais sur les restes de leur division par un autre entier. Bien que les origines de la notion de congruence remontent à l'antiquité et bien que cette notion avait été déjà utilisé par Euler (1707 − 1783), Lagrange (1736 − 1813) et Legendre (1752 − 1833) et par d'autres mathématiciens, les historiens des mathématiques s'accordent pour associer la naissance de la théorie des congruences avec l'année 1801, date de la publication du livre *Disquisitiones Arithmeticae* de Carl Friedrich Gauss (1777 − 1855). Gauss n'avait que 24 ans en 1801 ! Il est vrai que dans cet ouvrage, Gauss simplifie la démonstration d'importants résultats tels que le théorème de Wilson en page 56 de *[32]*, ou encore le petit théorème de Fermat en page 50 de *[32]*. Gauss élucide aussi la célèbre conjecture à son époque de la loi de réciprocité quadratique en page 96 de [32]. L'ouvrage de Gauss a été traduit en 1807 en français [32] et a été depuis, de nombreuses fois réimprimé. Il faut dire que malgré que plus de deux siècles se soient écoulés depuis sa parution, cette œuvre n'a pas pris une seule ride et demeure encore de nos jours un ouvrage de références dans le développement de la théorie des congruences. C'est à Gauss que l'on est redevable de la notation et de la définition suivante (données par Gauss dans Disquisitiones Arithmeticae), encore adoptées de nos jours.

" Si un nombre a divise la différence des nombres b et c, b et c sont dits congrus suivant a,

sinon incongrus ; a s'appellera le module ; chacun des nombres b et c, résidu de l'autre dans le premier cas et non résidu dans le second."

$$b \equiv c \pmod{a}.$$

Les congruences ont donné naissance aux nombres p-adiques. Les historiens des sciences situent la découverte des nombres p-adiques au début du XX-ième siècle, avec les travaux de Kurt HENSEL $(1861 - 1941)$.

Nous préciserons les points essentiels de la construction de l'anneau des entiers p-adiques et du corps des nombres p-adiques dans le pararaphe suivant. Nous examinerons aussi le point de vue topologique où l'on voit $\mathbb{Q}_p$ comme le complété de $\mathbb{Q}$ reltivement à une valeur absolue. Il s'agit là d'un point essentiel comme l'a si bien signalé le Professeur Charles PISOT en début de son article intitulé "L'analyse en Théorie des Nombres" en affirmant :

« La théorie des nombres a fait de grands progrés quand on y a introduit l'analyse,... »

Signalons que de nombreux auteurs ont écrit des ouvrages d'initiation et de recherche. En plus du cours du Professeur BENZAGHOU de Post Graduation d'Algèbre et de Théorie des nombres, signalons sur les ouvrages qui nous ont été utiles pour notre recherche dans le cadre de ce mémoire. Nous avons consulté tout d'abord le cours du Professeur D. BARSKY. Il s'agit d'un document polycopié de 80 pages intitulé " Fonction p-adique et applications" regroupant les cours donnés par le Professeur D. BARSKY à l'USTHB du 9 au 14 décembre 2005 [8], les ouvrages classiques d' Y. AMICE [5], BOREVITCH CHAFAREVITCH [13], N. KOBLITZ [56], NEUKIRCH [74], A.ROBERT[85],SILVERMAN[**?**], GOEVEAN[39], W. H. SCHIKHOF [92].

1.2 Ecriture d'un entier en base q

1.2.1 Division euclidienne dans $\mathbb{Z}$ et propriétés élémentaires des congruences dans $\mathbb{Z}$

Rappelons que $\mathbb{Z}$ est un anneau euclidien. Pour tous entiers a et $b \neq 0$, il existe un unique couple d'entiers(q, r) tels que

$$a = bq + r \quad \text{avec } 0 \leqslant r < |b| . \tag{1.1}$$

Si $b > 0$, alors en désignant par $\lfloor x \rfloor$ la partie entière du nombre réel x, on a :

$$a = bq + r \quad \text{avec } 0 \leqslant r < b \Longleftrightarrow \quad q = \left\lfloor \frac{a}{b} \right\rfloor \quad \text{et } r = a - b \left\lfloor \frac{a}{b} \right\rfloor . \tag{1.2}$$

La définition communément adoptée de deux nombres a et b congrus modulo m est alors la suivante :

Définition 1 *Soient a et b deux entiers et $m \in \mathbb{Z} - \{0\}$, a et b sont dits congrus modulo m, lorsque m divise $a - b$, autrement dit lorsque $a - b \in m\mathbb{Z}$. Pour exprimer cette relation, on se sert de la notation de Gauss,on écrit*

$$a \equiv b \pmod{m}. \tag{1.3}$$

On dit alors que a et b sont résidus l'un de l'autre modulo m. Dans le cas contraire, on dit que a est non congru à b modulo m

$$a \neq b \pmod{m}.$$

m est appelé module de le congruence.

La notation de Gauss permet de mettre en évidence l'analogie qui existe entre les égalités et les congruences, sans introduire de confusion. La relation de congruence modulo m définit une relation d'équivalence sur $\mathbb{Z}$. Cette relation d'équivalence est de plus compatible avec l'addition et la mutiplication définis sur $\mathbb{Z}$.La notation suivante est aussi couramment utilisée au lieu de (1.3) :

$$a \equiv_m b.$$

Etant donnés a et b deux entiers et $m \in \mathbb{Z} - \{0\}$, si l'on désigne par r_a et r_b les restes respectivement de a et b dans la division euclidienne de a et b par m, on peut constater que :

$$a - b \in m\mathbb{Z} \Leftrightarrow r_a = r_b$$

Autrement dit, deux entiers sont congrus modulo m si et seulement si ils ont même reste dans leur division euclidienne par m.

1.2.2 Développement en base q

La division euclidienne dans $\mathbb{Z}$ permet de prouver que q étant un entier $\geqslant 2$, tout entier naturel admet une unique décomposition en base q.

Proposition 2 *Pour tout entier $n \in \mathbb{N}$, il existe une unique suite d'entiers $(n_k)_{k\geq 0}$ telle que*

$$n = \sum_{k=0}^{\infty} n_k q^k \quad \textit{avec } 0 \leqslant n_k \leqslant q-1, \textit{ pour tout } k \geqslant 0. \tag{1.4}$$

La somme figurant au second membre de (1.4) définit bien un entier car on montre que les termes de cette somme sont nuls pour k assez grand.

Preuve. On constate facilement que l'écriture (1.4) implique

$$n_k = \left[\frac{n}{q^k}\right] - q\left[\frac{n}{q^{k+1}}\right]. \tag{1.5}$$

Ce qui prouve l'unicité de l'écriture de n sous la forme (1.4). On établit alors l'existence de cette écriture en vérifiant (1.4) pour ces valeurs n_k et en s'assurant que l'on a bien $0 \leqslant n_k \leqslant q-1$, pour tout $k \geqslant 0$ et $n_k = 0$, pour $k \geq \left\lfloor \frac{\ln(n)}{\ln(q)} \right\rfloor + 1$. □

1.3 L'anneau $\mathbb{Z}_q$ des entiers q-adiques

Nous suivons dans ce pararaphe la démarche de W. H. Schikhof [92], qui dans son ouvrage intitulé "Ultrametric Calculus An introduction to p-adic analysis, version 2006, dans son introduction à l'étude des nombres p-adiques. W. H. Schikhof. L'anneau des entiers p-adiques se présente comme une généralisation des développements en base p des entiers naturels, $\mathbb{Z}_p$ se présente comme un anneau de séries formelles contenant $\mathbb{Z}$ comme sous anneau. La nécessité de choisir un nombre premier pour obtenir un anneau intègre est souligné dans le texte de Schikhof.

Définition 3 *Pour tout entier $q \in \{2,3,4,...\}$, on désigne par $\mathbb{Z}_q$ l'ensemble défini par*

$$\mathbb{Z}_q = \left\{ \sum_{k=0}^{\infty} a_k q^k : 0 \leqslant a_k \leqslant q-1, \text{ pour tout } k \geqslant 0 \right\},$$

où $\sum_{k=0}^{\infty} a_k q^k$ est une série formelle qu'on identifie à l'entier $x = \sum_{k=0}^{m} a_k q^k$ de $\mathbb{N}$ quand on a $a_k = 0$, pour tout $k \geqslant m$. Les éléments de $\mathbb{Z}_q$ sont appelés entiers q-adiques.

Pour l'entier q spécifié, on convient par souci de simplification d'écrire $x = ...a_m a_{m-1}...a_1 a_0$ au lieu de $x = \sum_{k=0}^{\infty} a_k q^k$. Quand $a \in \mathbb{N}$, les entiers a_k non nuls sont en nombre fini.

Nous allons maintenant définir une addition et une multiplication sur l'ensemble $\mathbb{Z}_q$.

Définition 4 *Pour $x = \sum_{k=0}^{\infty} a_k q^k$ et $y = \sum_{k=0}^{\infty} b_k q^k$ deux éléments de $\mathbb{Z}_q$. On définit la somme $x+y$ et le produit xy comme étant les éléments de $\mathbb{Z}_q$ définis par*

$$x + y = \sum_{k=0}^{\infty} c_k q^k \qquad et \qquad xy = \sum_{k=0}^{\infty} d_k q^k$$

où $0 \leqslant c_k \leqslant q-1$ et $0 \leqslant d_k \leqslant q-1$, pour tout $k \geqslant 0$, sont déterminés de manière unique par les égalités

$$\sum_{k=0}^{m} c_k q^k = \sum_{k=0}^{m} (a_k + b_k) q^k \pmod{q^{m+1}} \tag{1.6}$$

et

$$\sum_{k=0}^{m} d_k q^k = (\sum_{k=0}^{m} a_k q^k\ )(\sum_{k=0}^{m} b_k q^k\ )\ (\mathrm{mod}\, q^{m+1}). \tag{1.7}$$

Remarquons tout de suite que si x et y sont dans $\mathbb{N}$, la somme $x+y$ et le produit xy ainsi définis dans $\mathbb{Z}_q$ coincident avec la somme et le produit de x et y sont dans $\mathbb{N}$. Nous n'avons fait qu'ecrire dans ce cas l'addition et le produit de x et y en base q. Il n'est pas difficile de constater qu'avec ces deux opérations, $\mathbb{Z}_q$ est un anneau commutatif contenant $\mathbb{N}$ et par suite contenant $\mathbb{Z}$.

Dans $\mathbb{Z}_q$, on a

$$\begin{aligned} -1 &= ...a_m a_{m-1}...a_1 a_0 \quad \text{avec } a_k = q-1, \text{ pour tout } k \geqslant 0. \\ -2 &= ...b_m b_{m-1}...b_1 b_0 \quad \text{avec } b_0 = q-2 \text{ et } b_k = q-1, \text{ pour tout } k \geqslant 1. \end{aligned}$$

On a aussi

$$q^m = \sum_{k=0}^{\infty} c_k q^k \text{ avec } c_k = \begin{cases} 0 & \text{pour } k \neq m \\ 1 & \text{pour } k = m \end{cases}$$

et

$$-q^m = \sum_{k=0}^{\infty} c_k q^k \text{ avec } c_k = \begin{cases} 0 & \text{pour } k < m \\ q-1 & \text{pour } k \geqslant m \end{cases}.$$

Soit $x \in \mathbb{Z}_q$, tel que

$$x = \sum_{k=0}^{\infty} a_k q^k.$$

Alors on a [92]

$$x \in \mathbb{Z} \text{ et } x \geqslant 0 \Longleftrightarrow \exists k_0 \in \mathbb{N},\ \forall k \geqslant k_0, a_k = 0$$

et

$$x \in \mathbb{Z} \text{ et } x < 0 \Longleftrightarrow \exists k_0 \in \mathbb{N},\ \forall k \geqslant k_0, a_k = q-1.$$

L'anneau $\mathbb{Z}_{10}$ n'est pas un anneau intègre. On peut en effet trouver des diviseurs de zéro dans cet anneau. En suivant l'exemple donnée par Schikhof en page 6 de [92], on peut définir deux éléments a et b de $\mathbb{Z}_{10}$ tels que $a \neq 0$, $b \neq 0$ et $ab = 0$ avec $a = ...1101010010112$, $b = ...3724365234375$. On a alors $ab = ...0000000000000$. Par contre si $q = p$ est un nombre premier, la situation est meilleur et on montre (cf [92], p.7) que si p est un nombre premier, alors $\mathbb{Z}_p$ est un anneau intègre. Un élément $...a_m a_{m-1}...a_1 a_0$ de $\mathbb{Z}_p$ admet un inverse dans $\mathbb{Z}_p$ si et seumement si $a_0 \neq 0$.

1.3.1 Définition d'une valuation sur $\mathbb{Z}_p$

Rappelons la définition d'une valuation sur un corps ou sur un anneau intègre K.

Définition 5 *Soit K un corps commutatif Une valeur absolue sur K est une application $|.| : K \longrightarrow \mathbb{R}$ satisfaisant les conditions*

1. $|x| \geqslant 0$ *et* $|x| = 0$ *si et seulement si* $x = 0$.
2. $|x + y| \leqslant |x| + |y|$,
3. $|xy| = |x|\,|y|$.

Un corps muni d'une valeur absolue est un corps valué. Un corps valué est immédiatement muni d'une métrique (ou distance) $d : K \times K \longrightarrow \mathbb{R}$ définie par

$$d(x, y) = |x - y|.$$

Il est en effet facile de vérifier que l'application d vérifie bien les axiomes définissant une distance sur un ensemble.

Définition 6 *Soit p un nombre premier et soit $...a_m a_{m-1}...a_1 a_0$ un élément de $\mathbb{Z}_p$. On définit l'ordre de $...a_m a_{m-1}...a_1 a_0$ qu'on note $\mathrm{ord}_p(...a_m a_{m-1}...a_1 a_0)$ par*

$$\mathrm{ord}_p(...a_m a_{m-1}...a_1 a_0) = \begin{cases} \infty & \text{si pour } i \geqslant 0, \text{ on a } a_i = 0 \\ \min\{s : a_s \neq 0\} & \text{sinon} \end{cases}$$

De plus, on pose

$$|...a_m a_{m-1}...a_1 a_0|_p = \begin{cases} 0 & \text{si pour } i \geqslant 0, \text{ on a } a_i = 0 \\ p^{-\mathrm{ord}_p(...a_m a_{m-1}...a_1 a_0)} & \text{sinon} \end{cases}.$$

La fonction $||_p$ est une valeur absolue p-adic définie sur $\mathbb{Z}_p$.

Proposition 7 *Soit p un nombre premier et $x, y \in \mathbb{Z}_p$.Alors*

1. $|x|_p \geqslant 0$ *et* $|x|_p = 0$ *si et seulement si* $x = 0$.
2. $|x + y|_p \leqslant \max\left\{|x|_p, |y|_p\right\}$
3. $|xy|_p = |x|_p\,|y|_p$.

Preuve. La preuve est facile. On observera que l'ensemble des valeurs de $|.|_p$ est $\{0, 1, p^{-1}, p^{-2}, ...\}$. □

On alors la caractérisation suivante des éléments inversibles de $\mathbb{Z}_p$

Proposition 8 *Soit p un nombre premier, alors on a*

1. *Un élément x de $\mathbb{Z}_p$ est inversible dans $\mathbb{Z}_p$ si et seulement si $|x|_p = 1$.*
2. *Si x est un élément non nul de $\mathbb{Z}_p$, alors on peut écrire*
$$x = p^{\mathrm{ord}_p(x)} y \text{ avec } y \in \mathbb{Z}_p \text{ et } |y|_p = 1.$$
3. *Soit*
$$p\mathbb{Z}_p := \{py : \ y \in \mathbb{Z}_p\}.$$
Alors $p\mathbb{Z}_p$ est un idéal maximal de $\mathbb{Z}_p$ et $\mathbb{Z}_p/p\mathbb{Z}_p$ est le corps à p éléments.

Désinons par $\mathbb{Z}_p^*$ le groupe des unités de $\mathbb{Z}_p$, on a :
$$\mathbb{Z}_p^* = \left\{ \ x \in \mathbb{Z}_p : |x|_p = 1 \ \right\}.$$

1.4 Le corps $\mathbb{Q}_p$ des nombres p-adiques

$\mathbb{Z}_p$ étant un anneau intègre, il admet un corps de fractions (défini à isomorphisme près) qu'on appelle $\mathbb{Q}_p$. Tout élément x de $\mathbb{Q}_p$ s'écrit $x = \frac{a}{b} = ab^{-1}$, avec $a \in \mathbb{Z}_p$ et $b \in \mathbb{Z}_p$, $b \neq 0$. L'addition et la multiplication de $\mathbb{Z}_p$ se prolongeant naturellement à $\mathbb{Q}_p$. Or, on a vu que à la 36 que tout élément b non nul de $\mathbb{Z}_p$ pouvait s'écrire $b = p^{\mathrm{ord}_p(b)}c$ avec $c \in \mathbb{Z}_p$ et $|c|_p = 1$, et du fait que $|c|_p = 1$, c est inversible dans $\mathbb{Z}_p$ et $\frac{a}{c} = ac^{-1}$ est un élément de $\mathbb{Z}_p$. Il en résulte tout élément x de $\mathbb{Q}_p$ s'écrit $x = p^m y$ avec $y \in \mathbb{Z}_p$ et $m \in \mathbb{Z}$. De plus comme y s'écrit $y = \sum_{i=0}^{\infty} y_i p^i$, on peut écrire $x = p^m \sum_{i=0}^{\infty} y_i p^i = \sum_{i=0}^{\infty} y_i p^{i+m} = \sum_{k=m}^{\infty} y_{k-m} p^k = \sum_{k=m}^{\infty} x_k p^k$, avec $x_k = y_{k-m}$, pour tout $k \geqslant 0$. Finalement on peut écrire
$$\mathbb{Q}_p = \left\{ \sum_{k=m}^{\infty} a_k p^k : m \in \mathbb{Z} \ \text{ et } \ 0 \leqslant a_k \leqslant p-1, \ \text{pour tout } k \geqslant 0 \right\}.$$
Les éléments de $\mathbb{Q}_p$ sont les nombres p-adiques.

Les nombres p-adiques pour lesquelles on a $a_{-1} = a_{-2} = ... = a_{-m} = 0$, sont identifiés (ou confondus) avec les entiers p-adiques.

On a
$$\mathbb{Z} \subset \mathbb{Z}_p \subset \mathbb{Q}_p.$$
Comme $\mathbb{Q}_p$ est un corps contenant $\mathbb{Z}$, $\mathbb{Q}_p$ est un corps de caractéristique nulle et on a aussi.
$$\mathbb{Q} \subset \mathbb{Q}_p.$$
On peut caractériser les éléments de $\mathbb{Q} \cap \mathbb{Z}_p$, autrement dit les entiers p-adiques qui sont des nombres rationnels. On pose
$$\mathbb{Z}_{(p)} = \mathbb{Q} \cap \mathbb{Z}_p.$$

Tout nombre rationnel non nul x s'écrit de manière unique $x = \frac{u}{v}$ avec $(u, v) \in \mathbb{N} \times \mathbb{Z}^*$ et $(u, v) = 1$; u est appelé numérateur de x et v est appelé denominateur de x.Nous noterons :

$$u = \text{num}(x) \text{ et } v = \text{denom}(x)$$

On a alors la carctérisation suivante des entiers p-adiques rationnels :

Proposition 9 *Pour tout nombre premier p, on a*

$$\mathbb{Z}_{(p)} = \mathbb{Q} \cap \mathbb{Z}_p = \{x \in \mathbb{Q} : \text{denom}(x) \notin p\mathbb{Z}\}.$$

Autrement dit, les entiers p-adiques rationnels sont les rationnels dont le numérateur n'est pas divisible par p. Remarquons que $\mathbb{Z}_{(p)}$ est un sous annneau de $\mathbb{Q}$. Les éléments de $\mathbb{Z}_{(p)}$ sont appelés des p-entiers.

Remarque 10 *Avec Maple12*

$$> \quad with(padic) : \tag{1.8}$$

$$> \quad Digitsp := 15 : \tag{1.9}$$

$$> \quad evalp(-2011/624, 5) : \tag{1.10}$$

$$1 + 2.5 + 1.5^3 + 4.5^4 + 2.5^5 + 1.5^7 + 4.5^8 + 2.5^9 + 1.5^{11} + 4.5^{12} + 2.5^{13} + O(5^{14}) \tag{1.11}$$

*L'instruction (1.8) "charge" la librairie padic. L'instruction (1.9) fixe le nombre de chiffres désiré dans les développements p-adiques. L'instruction (1.9) commande de donner les "chiffres" du développement 5-adique du nombre rationnel $-2011/624$. Ainsi, avec Maple*12*, on a*

$$-\frac{2011}{624} = \sum_{k=0}^{\infty} a_k 5^k$$

avec

$$\begin{aligned} a_0 &= 1, \\ a_1 &= 2, \\ a_2 &= a_6 = a_{10} = 0, \\ a_3 &= a_7 = a_{11} = 1, \\ a_4 &= a_8 = a_{12} = 4, \\ a_5 &= a_9 = a_{13} = 2. \end{aligned}$$

On peut vérifier qu'on a en fait pour tout entier $k \geqslant 0$:

$$a_{2+4k} = 0, \quad a_{3+4k} = 1, \quad a_{4+4k} = 4, \ a_{5+4k} = 2.$$

Il suffit de remarquer que pour tout nombre premier p, on a dans $\mathbb{Z}_p$

$$\frac{1}{1-p} = \sum_{k=0}^{\infty} p^k$$

Et de constater que l'on a

$$-\frac{2011}{624} = \frac{1+2.5+5^3+3.5^4}{1-5^4} = \frac{1}{1-5^4} + \frac{2.5}{1-5^4} + \frac{5^3}{1-5^4} + \frac{3.5^4}{1-5^4}.$$

1.4.1 Définition d'une valeur absolue sur $\mathbb{Q}_p$

On définit sur $\mathbb{Q}_p$ une valeur absolue qui prolonge celle déjà définie sur $\mathbb{Z}_p$.

Définition 11 *Soit p un nombre premier et soit $x = ...a_m a_{m-1}...a_1 a_0, a_{-1}a_{-2}...$un élément de $\mathbb{Q}_p$. On définit l'ordre de x qu'on note $\mathrm{ord}_p(x)$ par*

$$\mathrm{ord}_p(x) = \begin{cases} \infty & \text{si pour } i, \text{ on a } a_i = 0 \\ \min\{s : a_s \neq 0\} & \text{sinon} \end{cases}$$

De plus, on pose

$$|x|_p = \begin{cases} 0 & \text{si pour } i, \text{ on a } a_i = 0 \\ p^{-\mathrm{ord}_p(x)} & \text{sinon} \end{cases}.$$

La fonction $||_p$ est une valeur absolue définie sur $\mathbb{Q}_p$.

Remarque 12

1. *Tout nombre p-adique non nul x peut s'écrire de manière unique*

$$x = p^m u$$

où $m \in \mathbb{Z}$ et u une unité de $\mathbb{Z}_p$. De plus, on a $m = \mathrm{ord}_p(x)$.

2. *si x est un nombre rationnel x non nul, il existe un unique entier $m \in \mathbb{Z}$ tel que*

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

avec a et b des entiers tels que p ne divise pas ab. On pose $m = v_p(x)$. m est appelé valaution p-adique de m. On a alors $\frac{a}{b} \in \mathbb{Z}_p^*$ et $m = \mathrm{ord}_p(x) = v_p(x)$.

1.5 Congruences dans $\mathbb{Z}$

Edouard Lucas ($1842-1891$) est un mathématicien et plus précisément un arithméticien français bien connu pour l'étude de la suite de Fibonacci ainsi que de la suite associée appelée de nos jours suite de Lucas en son honneur. Il a aussi inventé un test de primalité qui est couramment utilisé encore aujourd'hui. Il utilisa ce test pour prouver que le nombre $2^{127}-1$ de 39 chiffres est un nombre premier. Avant Lucas, Euler avait démontré que le nombre de seulement 10 chiffres $2^{31}-1$ est un nombre premier.

$$\begin{aligned} 2^{31}-1 &= 2\ 147\ 483\ 647. \\ 2^{127}-1 &= 170\ 141\ 183\ 460\ 469\ 231\ 731\ 687\ 303\ 715\ 884\ 105\ 727 \end{aligned}$$

Lucas avait avait commencé par tester la primalité de ce nombre (à la main) en 1857 alors qu'il n'avait que 15 ans. Il n'acheva ses calculs et finit par prouver que ce nombre était effectivement premier qu'en 1876, soit 19 années plus tard ! Aujourd'hui encore, le nombre $2^{127}-1$ reste le plus grand nombre premier découvert sans l'aide d'un ordinateur.

Lucas est aussi connu pour être l'inventeur du problème des tours de Hanoï qu'il publia sous le nom de Claus de Siam, professeur au collège de Li-Sou-Tsiam, anagramme de Lucas d'Amiens, professeur à Saint-Louis.Lucas.Il publia plusieurs livres sur les mathématiques. On peut citer les quatre fameux tomes des récréations mathématiques, dont les deux derniers furent publiés à titre posthume ($1882-1894$). Il avait envisagé d'écrire une « grande Théorie des nombres » qui devait comporter quatre volumes. Sa mort tragique à l'âge de 49 ans l'en empêcha. Seul paru le premier tome [62] l'année même de son décès. Dans la préface de ce livre « Théorie des Nombres », Lucas commence par parler du premier traité d'Arithmétique supérieur de Legendre [59], qu'il qualifie d'excellent ouvrage. Il parle ensuite du livre de Gauss en ne tarissant pas d'éloges pour son auteur. Voici ce qu'il écrit à propos de cet ouvrage

« *Ce livre, monument impérissable, dévoile l'immense étendue, l'étonnante profondeur de la pensée humaine. Son auteur excella dans toutes les parties des sciences mathématiques ; dans l'analyse algébrique ; dans la Théorie des fonctions, dans le Calcul des probabilités, dans la Géométrie des surfaces, dans l'Astronomie physique et pratique, dans la Mécanique céleste, dans l'Optique, dans le Magnétisme, dans la Théorie des attractions, etc. ; ses compatriotes l'ont avec raison, surnommé Princeps mathematicorum. Mais ce que ce savant illustre, que l'on doit placer à côté des plus grands génies scientifiques de l'humanité, préférait par dessus tout ; c'était sa chère Arithmétique, ainsi qu'il le répétait continuellement dans sa correspondance ; nous n'y contredirons point.* »

En page 51 de son livre, Lucas donne les exemples suivants pour illustrer la notion de congruence

Exemple 13 *On démontre que*

$$2^{32}+1 \text{ } \textit{est divisible par } 641$$

$$\begin{aligned} 2^{2^6}+1 \text{ } &\textit{est divisible par } 274\ 177 \\ 2^{2^{12}}+1 \text{ } &\textit{est divisible par } 114\ 689, \\ 2^{2^{23}}+1 \text{ } &\textit{est divisible par } 162\ 772\ 161, \\ 2^{2^{36}}+1 \text{ } &\textit{est divisible par } 2\ 748\ 779\ 069\ 441. \end{aligned} \tag{1.12}$$

Lucas poursuit en écrivant

«*Ce dernier exemple prouve que le calcul par congruences est parfois indispensable, attendu qu'il est impossible d'écrire le nombre* $2^{2^{36}}+1$, *qui a plus de* 20 *milliards de chiffres ; la bande de papier qui le contiendrait ferait le tour de la terre. D'ailleurs, on ne connaît pas d'autre démonstration de ce curieux résultat, dû à M. Seelhooff, de Brême.*»

Signalons que nous avons rectifié l'énoncé de (1.12) qui comportait une erreur typographique sans doute. L'énoncé initiale affirmait que $2^{2^{25}}+1$ (au lieu de $2^{2^{23}}+1$) était divisible par 162 772 161, ce qui n'est pas vérifié. Avec Maple on vérifie en effet que $2^{2^{23}}+1$ est divisible par 167 772 161 et que de plus

$$2^{2^{25}}+1 \equiv 2 (\mathrm{mod}\, 167\ 772\ 161) \text{ et donc } 2^{2^{25}}-1 \text{ est divisible par } 167\ 772\ 161.$$

Posons

$$F_n = 2^{2^n}+1$$

et

$$M_p = 2^p - 1.$$

Les nombres entiers F_n sont appelés nombres de Fermat. Au chapitre 2, nous constaterons que les diviseurs premiers de F_n sont de la forme $k2^{n+1}+1$. Les nombres M_p sont appelés nombres de Mersenne. Il est facile de constater que le nombre 2^p-1 ne peut être premier que si p est premier. Le logiciel de calcul formel Maple 12, permet de verifier aisément de nombreux résultats mais bien sûr, devant l'énormité de certains calculs, il ya lieu d'adopter une stratégie adéquate pour limiter les calculs et obtenir une réponse de Maple 12.

Avec

$$> \quad F := n -> 2^{2^n}+1 : \tag{1.13}$$

$$> \quad \text{ifactor}(F(6)); \tag{1.14}$$

$$(67280421310721)(274177) \tag{1.15}$$

L'instruction (1.13) définit les nombres de Fermat ($F(n) = F_n$). L'instruction (1.14commande la factorisation de F_6). En (1.15), on obtient la factorisation de F_6.

$$F_6 = 2^{2^6}+1 = (67280421310721)(274177).$$

A l'aide de Maple12, nous pouvons aussi tester la primalité des nombres $M_p = 2^p - 1$.

$$> \quad M := p- > 2^p - 1 : \tag{1.16}$$
$$> \quad \text{isprime}(M(31)); \tag{1.17}$$
$$\quad true \tag{1.18}$$
$$> \quad \text{isprime}(M(127)); \tag{1.19}$$
$$\quad true \tag{1.20}$$

L'instruction (1.16) définit les nombres $M_p = 2^p - 1$.Les instructions (1.17) et (1.19) commandent le test de primalité pour respectivement M_{31} et M_{127}. En (1.18) et (1.20), on obtient la reponse "$true$" dans chacun des deux cas. Ce qui signifie (si l'on fait confiance à Maple12) que les nombres de Mersenne M_{31} et M_{127} sont premiers.

1.5.1 Applications des congruences à la résolution de quelques problèmes

Les congruences permettent souvent de répondre facilement à la non existence de solutions entières pour certaines équations diophantiennes.

Exemple 14 *Voici des exemples extraits du livre Theorie des Nombres de Z. I. Borevitch et I.R. chafarévitch [13](exercices* $1, 2,$ *et* 3 *page* 3*)*

1. *L'équation* $15x^2 - 7y^2 = 9$ *n'a pas de solution en nombres entiers.*
2. *L'équation* $5x^3 + 11y^3 + 13y^3 = 0$ *n'a pas d'autre solution en nombres entiers que la solution triviale* $x = 0$, $y = 0$, $z = 0$.
3. *Les nombres entiers de la forme* $8n + 7$ *ne peuvent pas s'écrire comme somme de trois carrés de nombres entiers.*

Voici un autre exemple plus surprenant d'application des congruences

Exemple 15 *On a*

$$\frac{1}{\pi}\arctan(\frac{4}{3}) \notin \mathbb{Q}.$$

En annexe, on trouvera une preuve de ces affirmations.

1.6 Systèmes de résidus modulo m

1.6.1 La fonction indicatrice φ d'Euler

Rappelons qu'on désigne par φ la fonction arithmétique définie sur $\mathbb{N}^*$ par

$$\varphi(n) := \{k \in \{1, 2, ..., n\} : \quad \text{pgcd}(n, k) = 1\}.$$

Autrement dit, pour $n \geqslant 1$, $\varphi(n)$ est le nombre d'entiers compris entre 1 et n et qui sont premiers avec n.

En désignant par $U(\mathbb{Z}/n\mathbb{Z})$ le groupe des unités de l'anneau $\mathbb{Z}/n\mathbb{Z}$, on a

$$\text{card}(U(\mathbb{Z}/n\mathbb{Z})) = \varphi(n).$$

En effet, on a

$$U(\mathbb{Z}/n\mathbb{Z}) = \{k + n\mathbb{Z} : k \in \{1, 2, ..., n\} \text{ et } \text{pgcd}(n, k) = 1\}.$$

On sait que φ est une fonction multiplicative, c'est à dire que pour tous entiers non nuls m et n, on a

$$(m, n) = 1 \Longrightarrow \varphi(mn) = \varphi(m)\varphi(n).$$

La propriété de mutiplicativité de la fonction d'Euler est une conséquence du fait que pour m et n premiers entre eux, l'application de $f : \mathbb{Z}/mn\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ définie par $f(a+mn\mathbb{Z}) = (a + m\mathbb{Z}, a + n\mathbb{Z})$ est bien définie et esst un isomorphisme d'anneau. Il en résulte alors que $\varphi(mn) = \text{card}(U(\mathbb{Z}/mn\mathbb{Z})) = \text{card}(U(\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z})) = \text{card}(U(\mathbb{Z}/m\mathbb{Z})).\,\text{card}(U(\mathbb{Z}/n\mathbb{Z})) = \varphi(m)\varphi(n)$.

Plus généralement le théorème chinois des restes qui suit est une conséquence de l'isomorphisme des anneaux $\mathbb{Z}/m_1m_2...m_r\mathbb{Z}$ et $(\mathbb{Z}/m_1\mathbb{Z}) \times (\mathbb{Z}/m_2\mathbb{Z}) \times \cdots \times (\mathbb{Z}/m_r\mathbb{Z})$ qui a lieu quand on a $(m_i, m_j) = 1$, pour tout $i, j \in \{1, 2...m\}$, tels que $i \neq j$.

Théorème 16 *Soit m_1,m_2, ..., m_r des entiers naturels premiers entre eux deux à deux. Soit a_1,a_2, ..., a_r des entiers quelconques. Alors le système de congruences*

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ . \\ . \\ . \\ x \equiv a_r \pmod{m_r} \end{cases}$$

possède une unique solution modulo $m_1m_2...m_r$.

Comme il est facile de constater que pour tout entier $k \geqslant 1$, on a

$$\varphi(p^k) = p^k - p^{k-1},$$

on en déduit que

$$\varphi(n) = n \prod_{p \text{ divise } n} (1 - \frac{1}{p}), \tag{1.21}$$

le produit (1.21) portant sur tous les nombres premiers p divisant n.

Pour p premier, $\mathbb{Z}/p\mathbb{Z}$ est un corps.

Théorème 17 *Le groupe multiplicatif $(\mathbb{Z}/p\mathbb{Z})^*$ est cyclique.*

Preuve. Plus généralement, on sait que si K est un corps commutatif, tout sous-groupe fini du groupe multiplicatif K^* est cyclique et est formé de racines de l'unité ([86], Théorème 1, page 28). □

1.6.2 Systèmes complet et systèmes réduits de résidus modulo m

Définition 18 – *Un ensemble d'entiers $\{x_1, x_2, ..., x_m\}$ est appelé un système complet de résidus modulo m si pour chaque entier y, il existe un et un seul x_i tel que $y \equiv x_i \pmod m$.*

– *Un ensemble d'entiers $\{x_1, x_2, ..., x_s\}$ où $s = \varphi(n)$ est appelé un système réduit de résidus modulo m si pour chaque entier y premier avec m, il existe un et un seul x_i tel que $y \equiv x_i \pmod m$.*

1.7 Congruences dans $\mathbb{Z}_p$

Etant donné un anneau commutatif A, on appelle plus généralement congruence définie sur A toute relation d'équivalence définie sur A, compatible avec l'addition et la mutiplication de A. Il est facile de constater que si $\mathcal{R}$ est une congruence définie sur A, l'ensemble $I := \{x \in A : \ x\mathcal{R}0\}$ est un idéal de A et que l'on a alors

$$x\mathcal{R}y \iff x - y \in I. \tag{1.22}$$

De plus, réciproquement, si on se donne un idéal I de A, la relation $\mathcal{R}$ definie par la relation (1.22) est une congruence définie sur A. On convient d'écrire $x \equiv y \pmod I$, pour $x\mathcal{R}y$.

Les seuls idéaux d'un corps K commutatif sont $\{0\}$ et K. Les congruences définies par ces idéaux ne présentent pas d'intérêt. On ne peut donc pas défnir de véritables congruences intéressantes sur $\mathbb{Q}$. Cependant, on va contourner cette difficulté en adoptant la convention suivante

Convention 19 *Soient x et y deux nombres rationnels, nous utiliserons la notation*

$$x \equiv y \pmod m,$$

pour exprimer que $x - y$ est un nombre rationnel dont le numérateur est divisible par m. Autrement dit

$$x \equiv y \pmod m \Leftrightarrow \mathrm{num}(x-y) \in m\mathbb{Z}.$$

Dans la suite, nous allons considérer des congruences du type

$$\mathrm{num}(x) \equiv 0 \pmod{np^r},$$

où $x \in \mathbb{Q}$, p est un nombre premier, n et r des entiers naturels. Cette congruence peut s'interpréter et s'écrire différemment. On a

$$\mathrm{num}(x) \equiv 0 \pmod{np^r} \;\Leftrightarrow\; x = np^r \frac{u}{v} \text{ avec } u \in \mathbb{Z},\ v \in \mathbb{N}^* \text{ et } p \text{ ne divise pas } v \qquad (1.23)$$

Le rationnel $\frac{u}{v}$ figurant au second membre de (1.23) est un rationnel dont le numérateur n'est pas divisible par p, c'est donc un élément de $\mathbb{Z}_p$ et plus précisément, c'est un élément de $\mathbb{Z}_p \cap \mathbb{Q}$. On peut donc écrire

$$\mathrm{num}(x) \equiv 0 \pmod{np^r} \;\Leftrightarrow\; x \in np^r\mathbb{Z}_p \Longleftrightarrow x \equiv 0 \pmod{np^r\mathbb{Z}_p}$$

Soient x et y deux nombres rationnels, nous utiliserons le notation

$$x \equiv y \pmod{np^r\mathbb{Z}_p}$$

pour exprimer que

$$x - y \equiv 0 \pmod{np^r\mathbb{Z}_p},$$

1.8 Valuation p-adique de $n!$

Pour un nombre entier n,la valuation p-adique de n est donnée par

$$v_p(n) = \sup\left\{a \in \mathbb{N} :\ n \equiv 0 \pmod{p^a}\right\}.$$

1.8.1 Formule de Legendre

Théorème 20 *Pour tout entier $n \geqslant 1$ et pour tout nombre premier p, on a*

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

Preuve. Soit p un nombre premier. Remarquons tout d'abord que pour tout entier $m \geq 1$, on a

$$v_p(m) = \sum_{j=1}^{\infty} \left[p^j \text{ divise } m\right]. \tag{1.24}$$

Dans la relation (1.24), nous avons utilisé le symbole d'Iverson avec la signification suivante

$$\left[p^j \text{ divise } m\right] = \begin{cases} 1 \text{ si } p^j \text{ divise } m, \\ 0 \text{ sinon.} \end{cases}$$

En effet si $v_p(m) = r$, alors $m = p^r q$ avec q premier avec p. Si $r = 0$, alors $[p^j \text{ divise } k] = 0$, pour tout entier $j \geq 1$, car p ne divise pas m et (1.24) est bien vérifiée. Si $r \geq 1$, alors $[p^j \text{ divise } m] = 1$ seulement pour $j \in \{1, 2, ..., r\}$, soit pour r valeurs de j et (1.24) est encore vérifiée. Cela nous permet d'écrire :

$$\begin{aligned} v_p(n!) &= v_p(1.2..., n) \\ &= \sum_{m=1}^{n} v_p(m) \\ &= \sum_{m=1}^{n} \sum_{j=1}^{\infty} \left[p^j \text{ divise } m\right] \\ &= \sum_{j=1}^{\infty} \sum_{m=1}^{n} \left[p^j \text{ divise } m\right] \end{aligned} \tag{1.25}$$

En remarquant alors que si la division euclidienne de n par p^j s'écrit

$$n = q_j p^j + r \text{ avec } 0 \leq r \leq p^j - 1 \text{ et } q_j = \left\lfloor \frac{n}{p^j} \right\rfloor,$$

alors il y a exactement q entiers $m \in \{1, 2, ..., n\}$ divisibles par p^j. Ce sont $p^j, 2p^j, ..., qp^j$. Par conséquent on a

$$\sum_{m=1}^{n} \left[p^j \text{ divise } m\right] = q_j = \left\lfloor \frac{n}{p^j} \right\rfloor \tag{1.26}$$

De (1.25) et (1.26) découle la relation$v_p(n!) = \sum_{j=1}^{\infty} \left\lfloor \frac{n}{p^j} \right\rfloor$ □

Théorème 21 *Soit p un nombre premier et n et k des entiers $\geqslant 1$. Alors on a*

$$v_p(n!) = \frac{n - s_p(n)}{p - 1}$$

Preuve. En effet, considérons la décomposition de n en base p :

$$n = a_0 + a_1 p + a_2 p^2 + \cdots + a_d p^d.$$

On a d'après la formule de Legendre (20)

$$\begin{aligned} v_p(n!) &= \sum_{k=1}^{\infty} \left\lfloor \frac{n}{p^k} \right\rfloor = \sum_{k=1}^{d} a_k + a_{k-1} p + \cdots + a_d p^{d-k} \\ &= \sum_{k=1}^{d} a_k (p^{k-1} + p^{k-2} + \cdots + p + 1) \\ &= \sum_{k=1}^{d} a_k \frac{p^k - 1}{p-1} = \frac{n - s_p(n)}{p-1}. \end{aligned}$$

□

1.9 Nombres de Bernoulli

Définition des nombres de Bernoulli

La suite des nombres de Bernoulli $(B_n)_{n \geqslant 0}$ est définie par sa série génératrice exponentielle

$$\sum_{n=0}^{\infty} B_n \frac{z^n}{n!} = \frac{z}{e^z - 1}. \tag{1.27}$$

Cette relation peut s'écrire

$$(\sum_{n=0}^{\infty} B_n \frac{z^n}{n!})(e^z - 1) = z, \tag{1.28}$$

En identifiant les coefficients de z dans chacun des deux membres de (1.28), on trouve

$$B_0 = 1. \tag{1.29}$$

Pour $n \geqslant 1$, en identifiant les coefficients de z^{n+1} dans chacun des deux membres de (1.28), on trouve

$$\frac{B_0}{0!(n+1)!} + \frac{B_1}{1!n!} + \frac{B_2}{2!(n-1)!} + \cdots + \frac{B_n}{n!1!} = 0 \tag{1.30}$$

En multipliant les deux membres de la relation (1.30) par $(n+1)!$, on trouve

$$\binom{n+1}{0} B_0 + \binom{n+1}{1} B_1 + \binom{n+1}{2} B_2 + \cdots + \binom{n+1}{n} B_n = 0. \tag{1.31}$$

On déduit de (1.31) une expression de B_n en fonction de B_0, B_1, B_2, ...et B_{n-1} :

$$B_n = -\frac{1}{n+1}\sum_{k=0}^{n-1}\binom{n+1}{k}B_k \quad \text{pour tout } n \geqslant 1. \tag{1.32}$$

La suite des nombres de Bernoulli $(B_n)_{n\geq 0}$ est aussi bien définie par sa série génératrice exponentielle que par les relations de récurrence suivantes obtenues à partir de (1.29) et (1.32)

$$\begin{cases} B_0 = 1 \\ B_n = -\frac{1}{n+1}\sum_{k=0}^{n-1}\binom{n+1}{k}B_k \quad \text{pour tout } n \geqslant 1. \end{cases} \tag{1.33}$$

La relation (1.33) nous permet de déterminer facilement les premières valeurs des nombres de Bernoulli, on trouve

$$(B_0, B_1, B_2, ...) = (1, -\frac{1}{2}, \frac{1}{6}...)$$

En fait, tous les nombres de Bernoulli d'indices impairs strictement plus grand que 1 sont nuls. On a

Proposition 22 *Pour tout entier $n \geqslant 1$, on a*

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

Preuve. il suffit de remarquer que la serie $S(z) = \frac{z}{2} + \sum_{n=0}^{\infty} B_n \frac{z^n}{n!}$ est une série paire du fait que l'on a $S(z) = \frac{z}{2} + \frac{z}{e^z - 1} = \frac{z}{2}(\frac{e^{\frac{z}{2}} + e^{-\frac{z}{2}}}{e^{\frac{z}{2}} - e^{-\frac{z}{2}}})$. □

Théorème de Staudt et Clausen

En 1840 Karl Von Staudt $(1798 - 1867)$ et Thomas Clausen $(1801 - 1842)$ ont independamment l'un de l'autre découvert le théorème suivant nommé en leur honneur Théorème de Von Staudt-Clausen.

Théorème 23 *Pour tout entier $n \geqslant 1$, on a la relation suivante*

$$B_{2n} + \sum_{p-1 \ divise \ 2n} \frac{1}{p} \in \mathbb{Z}. \tag{1.34}$$

La sommation étant étendue à tous les nombres premiers p divisant l'entier $2n$.

Eude de la suite des entiers $I_{2n} = B_{2n} + \sum_{p-1 \text{ divise } 2n} \frac{1}{p}$ Définissons I_{2n} par l'égalité

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

Par de simples calculs, on a

n	1	2	3	4	5	6	7	8	9	10	11	12
B_{2n}	$\frac{1}{6}$	$-\frac{1}{30}$	$\frac{1}{42}$	$-\frac{1}{30}$	$\frac{5}{66}$	$-\frac{691}{2730}$	$\frac{7}{6}$	$-\frac{3617}{510}$	$\frac{43867}{798}$	$-\frac{174611}{330}$	$\frac{854513}{138}$	$-\frac{236364091}{2730}$
I_{2n}	1	1	1	1	1	1	2	-6	56	-528	6193.	-86579

La suite $(I_{2n})_{n\geq 1}$ est repertoriée dans l'encyclopédie des suites d'entiers Sloane [93], sous la référence $A000146$.

1.10 Théorème p- adique des accroissements finis

Le théorème des accroissements finis suivant est du à A. Robert [85] :

Théorème 24 *On considère un espace de Banach ultramétrique $(E, |.|)$ sur un corps complet K, un polynôme $f(t) \in E[t]$ à cefficients dans E et deux éléments h, $a \in E$, avec $|a| \leqslant 1$. On munit $E[t]$ de la norme de Gauss $\left\|\sum a_k t^k\right\|_{E[t]} = \max\{|a_k| : k \geqslant 0\}$.*

1. *Si $|h| \leqslant |p|^{1/(p-1)}$, alors $|f(a+h) - f(a)| \leqslant |h| . \|f'\|_{E[t]}$,*
2. *Si p est impair et $|h| \leqslant |p|^{1/(p-2)}$, alors $|f(a+h) - f(a) - hf'(a)| \leqslant \left|\frac{h^2}{2}\right| . \|f''\|_{E[t]}$, la même conclusion étant valable dans le cas $p = 2$ dès que $|h| \leqslant |h|^{1/2}$.*

1.10.1 La fonction Gamma $p-$adique de Morita

Y. Morita,[72], a defini en 1975 un analogue p-adique, Γ_p, de la fonction Gamma en posant pour $n \in \mathbb{N}$

$$\Gamma_p = (-1)^n \prod_{\substack{1\leq j\leq 1n-1 \\ (j,p)=1}} j \ .$$

Il a montré que cette application est prolongeable par uniforme continuité en une fonction continue sur $\mathbb{Z}_p$, l'anneau des entiers p-adiques, définissant ainsi un prolongement à $\mathbb{Z}_p$ que l'on note encore Γ_p . Cette fonction amma p-adique possède des propriétés fonctionnelles proches de celle de la fonction Gamma d'Euler

$$\begin{cases} \Gamma_p(0) = 0, \\ \Gamma_p(x+1) = \begin{cases} -x\Gamma_p(x) & \text{si } x \in \mathbb{Z}_p^* \\ -\Gamma_p(x) & \text{si } x \in p\mathbb{Z}_p \end{cases} \\ \Gamma_p(x)\Gamma_p(1-x) = (-1)^{R(p)} \end{cases}$$

où $R(p) \in \{1, 2, ..., p\}$ et $R(p) \equiv x \bmod p\mathbb{Z}_p$.

1.10.2 Applications

Comme l'a si bien fait remarquer Junod [52] dans sa thèse, la version p-adique des accoissements finis permet d'améliorer aisément plusieurs résultats connus sur les nombres de Bernoulli. Ainsi, Junod prouve le résultat suivant

Théorème 25 *Junod (2003) Pour $n \geq 1$, on a*

$$pB_n \equiv \sum_{k=1}^{p-1} k^n \equiv \begin{cases} 0 & \text{si } (p-1) \text{ ne divise pas } n \\ p-1 & \text{si } (p-1) \text{ divise } n \end{cases} \pmod{\frac{np}{2}\mathbb{Z}_p}$$

Preuve. cf [52], P. 9 □

De ce théorème découlent les résultats de Kummer et de Von staudt et Clausen

- Si $p-1$ ne divise pas n, alors $B_n \in n\mathbb{Z}_p$ et plus précisément $B_n(a) \in n\mathbb{Z}_p$ pour tout $a \in \mathbb{Z}_p$. On a aussi $pB_n \equiv -1 \pmod{p\mathbb{Z}_p}$ lorsque $p-1$ divise n pair ≥ 2.
- $B_{2n} + \sum_{p-1 \text{ divise } 2n} \frac{1}{p}$ est un nombre entier pour tout $n \geq 1$.

De plus le résultat de Kummer qui affirme que

$$\frac{B_{m+p-1}}{m+p-1} \equiv \frac{B_m}{m} \pmod{p\mathbb{Z}_p}$$

peut -être amélioré comme suit, la preuve de ce résultat se trouvant dans la thèse de Junod [52].

Théorème 26 *Junod (2003) Si $m \geq 1$ et $p-1$ ne divise pas $m+n$, alors on a la congruence*

$$\frac{B_{m+np}(a)}{m+np} \equiv \frac{B_{m+n}(a)}{m+n} \pmod{np\mathbb{Z}_p}$$

pour tout entier p-adique $a \in \mathbb{Z}_p$.

1.11 Polynômes de Gauss

Ces notes sur les polynômes de Gauss ne sont dans aucun ouvrage ,ce sont le fruit d'efforts personnels .

Soit A unanneau commutatif et $(a_n)_n$ une suite d'éléments de A. considérons la suite de polynômes $(P_n(x))_n$ associé à cette suite et défini de la manière suivante

$$P_n(x) = \prod_{j=1}^{n}(1 + a_j x), \text{ pour tout } n \geq 0.$$

On a $P_0(x) = 1$, en adoptant la convention classique qu'un produit vide vaut 1. On a aussi

$$\begin{aligned} P_1(x) &= 1 + a_1 x \\ P_2(x) &= 1 + (a_1 + a_2)x + a_1 a_2 x^2 \\ P_3(x) &= 1 + (a_1 + a_2 + a_3)x + (a_1 a_2 + a_1 a_3 + a_2 a_3)x^3. \end{aligned}$$

Plus généralement, avec $\sigma_0 = 1$ et

$$\sigma_j = \sum_{1 \leq i_1 < i_2 < \cdots < i_j \leq n} a_{i_1} a_{i_2} ... a_{i_j}, \text{ pour } 1 \leq j \leq n,$$

on a

$$P_n(x) = \sum_{k=0}^{n} \sigma_k x^k.$$

Considérons maintenant le cas particulier où $A = \mathbb{Z}[q]$, q étant une indéterminée et où la suite $(a_n)_n$ est définie par $a_n = q^n$. dans ce cas, on a

$$\sigma_k = \sum_{1 \leq i_1 < i_2 < \cdots < i_k \leq n} q^{i_1 + i_2 + \cdots + i_k}, \text{ pour } 1 \leq k \leq n. \tag{1.35}$$

Dans ce cas, la relation (1.35) montre que pour tout $k \in \{0, 1...n\}$, σ_k qui est dans ce cas un polynôme de $\mathbb{Z}[q]$ est divisible par $q^{\frac{k(k+1)}{2}}$. En effet cela est triviale pour $k = 0$. Pour $k \geq 1$, on a dans la sommation (1.35), les indices $i_1, i_2, \cdots, i_k$ étant tels que $1 \leq i_1 < i_2 < \cdots < i_k \leq n$ vérifient nécéssairement les relations $i_j \geq j$ pour tout $j \in \{1...k\}$. (On a en effet $i_1 \geq 1$ et si $i_{r-1} \geq r - 1$ avec $r - 1 < n$, alors $i_r > i_{r-1} \geq r - 1$ et donc $i_r > r$). Par suite $i_1 + i_2 + \cdots + i_k \geq 1 + 2 + \cdots + k = \frac{k(k+1)}{2}$ et Il résulte de la relation (1.35) que le polynôme σ_k de $\mathbb{Z}[q]$ est divisilble par $q^{\frac{k(k+1)}{2}}$. Il existe donc pour tout $k \in \{0...n\}$ un polynôme de $\mathbb{Z}[q]$ que nous noterons $\binom{n}{k}_q$ vérifiant

$$\sigma_k = q^{\frac{k(k+1)}{2}} \binom{n}{k}_q.$$

Il n'est pas difficile de constater que le dégré du polynôme $\binom{n}{k}_q$ est égale à $k(n-k)$ et que la coefficient dominant de ce polynôme vaut 1. En effet dans la sommation (1.35), le terme de plus haut degré en q est unique et est obtenue pour $i_k = n$, $i_k = n-1, ..., i_k = n-(k-1)$. Ce qui correspond à un esposant $i_1 + i_2 + \cdots + i_k = n + (n-1) + \cdots + n - (k-1) = kn - \frac{k(k-1)}{2}$ pour le terme de plus haut dégré de σ_k. Il en résulte que le monome de plus haut degré de $\binom{n}{k}_q$ est $kn - \frac{k(k-1)}{2} - \frac{k(k+1)}{2} = k(n-k)$ et que de plus le coefficient de ce monome est égale à 1. Ainsi, on a

$$\prod_{j=1}^{n} (1 + q^j x) = \sum_{k=0}^{n} q^{\frac{k(k+1)}{2}} \binom{n}{k}_q x^k. \tag{1.36}$$

La relation (**??**) de la proposition **??** est ainsi justifiée. Prouvons maintenant que l'on a

$$\binom{n}{k}_q = \prod_{j=1}^{n} \frac{1 - q^{n+1-j}}{1 - q^j}.$$

Remarquons pour cela qu'en remplaçant x par qx dans (1.36), on obtient en remarquant que $k+\frac{k(k+1}{2}=\frac{k(k+3)}{2}$

$$\prod_{j=1}^{n}(1+q^{j+1}x)=\sum_{k=0}^{n}q^{\frac{k(k+3)}{2}}\binom{n}{k}_q x^k. \tag{1.37}$$

En multipliant les deux membres de le relation 1.37 par $1+qx$, on obtient

$$(1+qx)\prod_{j=1}^{n}(1+q^{j+1}x)=(1+qx)(\sum_{k=0}^{n}q^{\frac{k(k+3)}{2}}\binom{n}{k}_q x^k). \tag{1.38}$$

Remarquons alors que le premier membre de (1.38) peut s'écrire

$$\begin{aligned}(1+qx)\prod_{j=1}^{n}(1+q^{j+1}x) &= \prod_{j=1}^{n+1}(1+q^{j}x)\\ &= (1+q^{n+1}x)\prod_{j=1}^{n}(1+q^{j}x)\\ &= (1+q^{n+1}x)(\sum_{k=0}^{n}q^{\frac{k(k+1)}{2}}\binom{n}{k}_q x^k). \end{aligned}\tag{1.39}$$

De (1.38) et (1.39), on déduit la relation

$$(1+q^{n+1}x)(\sum_{k=0}^{n}q^{\frac{k(k+1)}{2}}\binom{n}{k}_q x^k)=(1+qx)(\sum_{k=0}^{n}q^{\frac{k(k+3)}{2}}\binom{n}{k}_q x^k). \tag{1.40}$$

En identifiant les coefficients de x^k dans chacun des deux membres de la relation 1.40, on obtient

$$q^{\frac{k(k+1)}{2}}\binom{n}{k}_q+q^{n+1}q^{\frac{k(k-1)}{2}}\binom{n}{k-1}_q=q^{\frac{k(k+3)}{2}}\binom{n}{k}_q+q^{1+\frac{(k-1)(k+2)}{2}}\binom{n}{k-1}_q. \tag{1.41}$$

En divisant les deux membres de (1.41) par $q^{\frac{k(k+1)}{2}}$, on obtient

$$\binom{n}{k}_q+q^{n+1-k}\binom{n}{k-1}_q=q^k\binom{n}{k}_q+\binom{n}{k-1}_q. \tag{1.42}$$

On en déduit de (1.42) que

$$(1-q^k)\binom{n}{k}_q=(1-q^{n+1-k})\binom{n}{k-1}_q,$$

soit

$$\binom{n}{k}_q=\frac{1-q^{n+1-k}}{1-q^k}\binom{n}{k-1}_q.$$

On en déduit que

$$\prod_{j=1}^{k}\binom{n}{j}_q = \prod_{j=1}^{k}\frac{1-q^{n+1-j}}{1-q^j}\binom{n}{j-1}_q$$

soit

$$\binom{n}{k}_q\prod_{j=1}^{k-1}\binom{n}{j}_q = (\prod_{j=1}^{k}\frac{1-q^{n+1-j}}{1-q^j})(\prod_{j=0}^{k-1}\binom{n}{j}_q)$$

En remarquant que $\binom{n}{0}_q = 1$, on obtient en simplifiant par $\prod_{j=1}^{k-1}\binom{n}{j}_q$:

$$\binom{n}{k}_q = \prod_{j=1}^{k}\frac{1-q^{n+1-j}}{1-q^j}. \tag{1.43}$$

Autrement dit

$$\binom{n}{k}_q = \frac{(1-q^{n+1})(1-q^n)...(1-q^{n+1-k})}{(1-q)(1-q^2)...(1-q^k)}.$$

Remarquant qu'en posant

$$\begin{aligned}[n]_q &= 1+q+q^2+\cdots+q^{n-1},\\ [n]_q! &= [n]_q\,[n-1]_q\cdots[1]_q\,.\end{aligned}$$

On peut écrire

$$\begin{aligned}(1-q^m) &= (1-q)(1+q+q^2+\cdots+q^{m-1})\\ &= (1-q)\,[m]_q\,.\end{aligned}$$

La relation (1.43) peut aussi s'écrire

$$\begin{aligned}\binom{n}{k}_q &= \prod_{j=1}^{k}\frac{1-q^{n+1-j}}{1-q^j}\\ &= \prod_{j=1}^{k}\frac{(1-q)\,[n+1-j]_q}{(1-q)\,[j]_q}\\ &= \prod_{j=1}^{k}\frac{[n+1-j]_q}{[j]_q}.\end{aligned}$$

Ainsi

$$\begin{aligned}\binom{n}{k}_q &= \frac{[n]_q\,[n-1]_q\,...\,[n+1-k]_q}{[1]_q\,[2]_q\,...\,[k]_q}\\ &= \frac{([n]_q\,[n-1]_q\,...\,[n+1-k]_q)([n-k]_q\,[n-k-1]_q\,...\,[1]_q)}{([1]_q\,[2]_q\,...\,[k]_q)([n-k]_q\,[n-k-1]_q\,...\,[1]_q)}\\ &= \frac{[n]_q!}{[k]_q!\,[n-k]_q!}.\end{aligned}$$

1.12 Algèbre de Hurwitz

Cette partie sur l'Algèbre de Hurwitz s'inspire largement des articles de Monsieur le Professeur Benzaghou [9] et [10] .

Soit C un corps commutatif de caractéristique zéro. Pour un suite $u : \mathbb{Z} \to C$, nous définissons le support de u que nous notons $\text{supp}(u)$ et l'ordre de u que nous notons $\text{ord}(u)$ par

$$\text{supp}(u) = \{n \in \mathbb{Z};\ u(n) \neq 0\} \quad \text{et} \quad \text{ord}(u) = \inf(\text{supp}(u)).$$

On a : $\inf(\text{supp}(u)) \in \mathbb{Z} \cup \{-\infty\}$, pour $u \neq 0$.

Nous désignons par $s(C)$ l'ensemble des suites (éléments de $C^{\mathbb{Z}}$) d'ordre fini et par $s_0(C)$ l'ensemble des suites (éléments de $C^{\mathbb{Z}}$) d'ordre un entier narturel

$$s(C) = \left\{u \in C^{\mathbb{Z}};\ \text{ord}(u) > -\infty\right\} \text{ et } s_0(C) = \left\{u \in C^{\mathbb{Z}};\ \text{ord}(u) \geq 0\right\}.$$

Autrement dit un suite $u : \mathbb{Z} \to C$, est élément de $s(C)$ si et seulement s'il existe un entier $n_0 \in \mathbb{Z}$ tel que $u(n) = 0$ pour $n \leq n_0$ et si de plus $n_0 \in \mathbb{N}$, alors $u \in s_0(C)$. Pour tout entier $k \in \mathbb{Z}$, nous définissons la suite $e_k : \mathbb{Z} \to C$, en posant

$$e_k(n) = \delta_{n,k}$$

L' application $g : s_0(C) \to C[[X]]$ qui à $u \in s_0(C)$ associe $g_u(X) \in C[[X]]$ défini par

$$g_u(X) = \sum_{n=0}^{\infty} u(n)\frac{X^n}{n!}. \tag{1.44}$$

est naturellement bijective. Nous convenons d'appeler $g_u(x)$ serie exponentielle de Hurwitz associé à u.

Pour $u \in s_0(C)$ et $v \in s_0(C)$, nous définissons le produit de Hurwitz des deux suites u et v que nous noterons $u\Psi v$, comme étant le produit obtenue en transportant par l'application réciproque g_u^{-1} le produit des series formelles. Autrement dit nous défissons $u\Psi v$ par l'égalité

$$g_{u\Psi v}(X) = g_u(X)g_v(X).$$

Comme on a

$$\begin{aligned}(\sum_{n=0}^{\infty} u(n)\frac{X^n}{n!})(\sum_{n=0}^{\infty} v(n)\frac{X^n}{n!}) &= \sum_{n=0}^{\infty\prime}(\sum_{i+j=n,i,j\in\mathbb{N}} \frac{u(j)}{j!}\frac{v(i)}{i!})X^n \\ &= \sum_{n=0}^{\infty\prime}(\sum_{i+j=n,i,j\in\mathbb{N}} n!\frac{u(j)}{j!}\frac{v(i)}{i!})\frac{X^n}{n!}\end{aligned}$$

On en déduit que $u\omega v$ est définie par l'égalité

$$(u\Psi v)(n) = \sum_{j=0}^{n} \binom{n}{j} u(j)v(n-j). \tag{1.45}$$

La somme de deux suites $u \in s_0(C)$ et $v \in s_0(C)$ est définie classiquement par

$$(u+v)(n) = u(n) + v(n).$$

On a aussi

$$g_{u+v}(X) = g_u(X) + g_v(X).$$

Définition 27 *L' opérateur d'avance (ou opérateur "shift") noté T est l'application T :*

$s(C) \longrightarrow s(C)$ qui à $u \in s(C)$ associe l'application $Tu \in s(C)$ définie par

$$(Tu)(n) = u(n+1), \text{ pour tout } n \in \mathbb{Z}.$$

L'opérateur q est l'application q :

$s(C) \longrightarrow s(C)$ qui à $u \in s(C)$ associe l'application $qu \in s(C)$ définie par

$$(qu)(n) = n.u(n), \text{ pour tout } n \in \mathbb{Z}.$$

Désignons par $\frac{d}{dX} : C[[x]] \longrightarrow C[[x]]$ l'opérateur de dérivation formelle définie sur $C[[x]]$ par

$$\frac{d}{dX}(\sum_{n=0}^{\infty} a_n \frac{X^n}{n!}) = \sum_{n=1}^{\infty} n a_n \frac{X^{n-1}}{n!}.$$

On a

$$\begin{aligned} \frac{d}{dX}(\sum_{n=0}^{\infty} a_n \frac{X^n}{n!}) &= \sum_{n=1}^{\infty} a_n \frac{X^{n-1}}{(n-1)!} \\ &= \sum_{n=1}^{\infty} a_{n+1} \frac{X^n}{n!}. \end{aligned} \tag{1.46}$$

Le résultat suivant est alors immédiat :

Proposition 28 *Pour tout $u \in \mathcal{A} = s_0(C)$, on a*

$$g_{Tu}(X) = \frac{d}{dX} g_u(X) \tag{1.47}$$

et

$$g_{qu}(X) = X \frac{d}{dX} g_u(X). \tag{1.48}$$

Preuve. En effet, soit $u \in \mathcal{A} = s_0(C)$, alors

$$g_u(X) = \sum_{n=0}^{\infty} u(n)\frac{X^n}{n!}.$$

On a alors

$$\begin{aligned} g_{Tu}(X) &= \sum_{n=0}^{\infty}(Tu)(n)\frac{X^n}{n!} \\ &= \sum_{n=0}^{\infty} u(n+1)\frac{X^n}{n!}. \end{aligned} \tag{1.49}$$

D'après la propriété (1.46), on peut écrire

$$\begin{aligned} g_{Tu}(X) &= \frac{d}{dX}(\sum_{n=0}^{\infty} u(n)\frac{X^n}{n!}) \\ &= \frac{d}{dX}(g_u(X)). \end{aligned} \tag{1.50}$$

Ce qui établit (1.47).

De même, on a

$$\begin{aligned} g_{qu}(X) &= \sum_{n=0}^{\infty}(qu)(n)\frac{X^n}{n!} \\ &= \sum_{n=0}^{\infty} nu(n)\frac{X^n}{n!} \\ &= \sum_{n=1}^{\infty} u(n)\frac{X^n}{(n-1)!} \\ &= \sum_{n=0}^{\infty} u(n+1)\frac{X^{n+1}}{n!} \\ &= X(\sum_{n=0}^{\infty} u(n+1)\frac{X^n}{n!}). \end{aligned}$$

D'après (1.49) et (1.50), on a alors

$$g_{qu}(X) = X\frac{d}{dX}g_u(X).$$

Ce qui établit (1.48). □

Extension de la définition de la factorielle à $\mathbb{Z}$: la factorielle de Roman

La factorielle de n est définie par

$$n! = 1.2...n, \text{ pour } n \geq 1.$$

Elle vérifie la relation

$$(n+1)! = (n+1).n!, \text{ pour tout entier } n \in \mathbb{Z}. \tag{1.51}$$

Si on veut que cette relation soit vérifiée pour $n = 0$, on constate qu'il suffit de poser $0! = 1$, et c'est ce qu'on fait. Par contre, il est impossible de prolonger la relation (1.51) pour qu'elle soit valable à tout $\mathbb{Z}$ pour la simple raison que pour $n = -1$, cette relation ne peut pas être vérifiée ($0! = 1 \neq 0$). On contourne cette difficulté en définissent un prolongement γ de la factorielle de n à $\mathbb{Z}$ de la manière suivante :

$$\begin{cases} \gamma(n) = n! \text{ pour tout } n \in \mathbb{N} \\ \gamma(-1) = 1 \\ \gamma(n+1) = (n+1)\gamma(n) \text{ pour tout entier } n \in \mathbb{Z}, \text{ tel que } n \neq -1. \end{cases} \tag{1.52}$$

On peut remarquer que la condition

$$\gamma(n+1) = (n+1)\gamma(n) \text{ pour tout entier } n \in \mathbb{Z}, \text{ tel que } n \neq -1$$

est équivalente à dire qu'on définit un prolongement γ de la factorielle de n à $\mathbb{Z}$ de manière à ce que si l'on prolonge la définition de l' application $g : s_0(C) \to C[[X]]$ définie par (1.44) en une application qu'on notera encore par abus de notation $g : s(C) \to C[[X]]$ en posant pour tout suite $u \in s(C)$,

$$g_u(X) = \sum_{n \in \mathbb{Z}} u(n) \frac{X^n}{\gamma(n)},$$

la relation

$$g_{Tu}(X) = \frac{d}{dX} g_u(X) \tag{1.53}$$

se trouve encore vérifiée pour toute suite $u \in s(C)$ telle que $u(0) = 0$, ($\frac{d}{dX}$ étant l'opérateur de dérivation naturellement prolongé).

En effet, la relation (1.53) se traduit par

$$\sum_{n \in \mathbb{Z}} u(n+1) \frac{X^n}{\gamma(n)} = \sum_{n \in \mathbb{Z}} nu(n) \frac{X^{n-1}}{\gamma(n)}. \tag{1.54}$$

Comme $nu(n) = 0$, pour $n = 0$, on peut réécrire la relation (1.54) après un changement d'indices

$$\sum_{n \in \mathbb{Z}} u(n+1) \frac{X^n}{\gamma(n)} = \sum_{n \in \mathbb{Z},\ n \neq -1} (n+1)u(n+1) \frac{X^n}{\gamma(n+1)}. \tag{1.55}$$

La relation (1.55) se traduit alors bien par

$$\gamma(n+1) = (n+1)\gamma(n) \text{ pour tout } n \in \mathbb{Z},\ n \neq -1. \tag{1.56}$$

On établit aisémént que l'unique fonction γ vérifiant (1.52) est donnée par

$$\gamma(n) = \begin{cases} n! & \text{pour tout } n \geq 0, \\ \frac{(-1)^{-n-1}}{(-n-1)!} & \text{pour tout } n < 0. \end{cases} \tag{1.57}$$

En effet, pour $n < 0$, on a pour $n = -1$

$$\gamma(-1) = 1,$$

ce qui est conforme avec la définition (1.57). Pour $n = -2$, l'application de relation(1.56) donne

$$\gamma(-2) = \frac{\gamma(-1)}{(-1)} = \frac{1}{(-1)}.$$

Pour $n = -3$, l'application de nouveau de la relation(1.56) donne

$$\gamma(-3) = \frac{\gamma(-2)}{(-2)} = \frac{1}{(-2)(-1)}.$$

On établit ainsi par un raisonnement par récurrence sur m que pour $m > 0$, on a

$$\begin{aligned} \gamma(-m) &= \frac{1}{(-(m-1))...(-2)(-1)} \\ &= \frac{(-1)^{m-1}}{(m-1)!}. \end{aligned}$$

Avec $m = -n$, on obtient ainsi

$$\gamma(n) = \frac{(-1)^{-n-1}}{(-n-1)!},\ \text{pour tout } n < 0.$$

On établit ainsi l'unicité de la fonctionγ. On vérifie alors qu'avec la définition (1.57), les relations (1.52) sont bien réalisées.

Prolongement du produit de Hurwitz définie sur $s_0(C)$ à $s(C)$

Soit $C((X)) = \left\{ \sum_{n\in\mathbb{Z}} a_n X^n :\ a_n \in C \text{ et il existe } r \in \mathbb{Z} \text{ tel que } a_n = 0 \text{ pour tout } n \leq r \right\}$

Définition 29 *Définissons l'application $g : s(C) \to C((X))$ qui à $u \in s_0(C)$ associe $g_u(X) \in C[[X]]$ défini par*

$$g_u(X) = \sum_{n\in\mathbb{Z}} u(n)\frac{X^n}{\gamma(n)}. \tag{1.58}$$

L'application g ainsi définie prolonge celle définie en (1.44). On est amené à prolonger la definition du produit de Hurwitz définie sur $s_0(C)$ à un produit de Hurwitz définie sur $s(C)$ en posant :

Définition 30 *Soient u et v deux éléménts de $s(C)$, on définit le produit de Hurwitz de u et v qu'on note $u\Psi v$ par l'égalité*

$$g_{u\Psi v}(X) = g_u(X)g_v(X).$$

Soient u et v deux éléménts de $s(C)$, alors $\mathrm{ord}(u) > -\infty$ et $\mathrm{ord}(v) > -\infty$. Il existe donc deux entiers r et s tels que

$$u(n) = 0 \text{ pour } n < r \text{ et } v(n) = 0 \text{ pour } n < s\ .$$

On a alors

$$g_u(X) = \sum_{n\in\mathbb{Z}} u(n)\frac{X^n}{\gamma(n)} = \sum_{n\geq r} u(n)\frac{X^n}{\gamma(n)}$$

et

$$g_v(X) = \sum_{n\in\mathbb{Z}} v(n)\frac{X^n}{\gamma(n)} = \sum_{n\geq s} v(n)\frac{X^n}{\gamma(n)}.$$

Par suite, on a

$$\begin{aligned} g_u(X).g_v(X) &= (\sum_{k\geq r} u(k)\frac{X^k}{\gamma(k)}).(\sum_{l\geq s} v(l)\frac{X^l}{\gamma(l)}) \\ &= \sum_{n\geq r+s}(\sum_{k+l=n} \gamma(n)\frac{u(k)}{\gamma(k)}.\frac{v(l)}{\gamma(l)})\frac{X^n}{\gamma(n)} \\ &= \sum_{n\in\mathbb{Z}}(u\Psi v)(n)\frac{X^n}{\gamma(n)}. \end{aligned} \tag{1.59}$$

Avec

$$(u\Psi v)(n) = \sum_{k+l=n} \gamma(n)\frac{u(k)}{\gamma(k)}.\frac{v(l)}{\gamma(l)}.$$

La sommation dans (1.59) porte sur $\mathbb{Z}$. Cela a un sens car $(u\Psi v)(n) = 0$ pour $n < r + s$, du fait que si $k + l = n$ avec $n < r + s$, alors $k < r$ ou $l < s$ (car sinon $k + l \geq r + s$) et donc $u(k)v(l) = 0$ et $(u\Psi v)(n) = 0$. De plus, en définissant le coefficient $\binom{n}{k}^*$ par

$$\binom{n}{k}^* = \frac{\gamma(n)}{\gamma(k)\gamma(n-k)}, \text{ pour } n \in \mathbb{Z} \text{ et } k \in \mathbb{Z},$$

on a

$$(u\Psi v)(n) = \sum_{\substack{k+l=n \\ k\in\mathbb{Z} \text{ et } l\in\mathbb{Z}}} \binom{n}{k}^* u(k).v(l). \tag{1.60}$$

La relation (1.60) généralise la relation (1.45). De plus $\binom{n}{k}^*$ est le coefficient de Roman [84]. $s(C)$ muni de l'addition et du produit de Hurwitz est alors un corps. C'est le corps des fractions de l'anneau intègre $s_0(C)$.

Polynômes de Bell

On distingue deus types de polynômes exponentiels de Bell : les polynômes exponentiels partiels de Bell et le polynômes exponentiels complets de Bell. La définition classique de ces polynômes de Bell est donné par L. Comtet ([19] page 144).

Définition 31 *Les polynômes* $B_{n,k} = B_{n,k}(x_1, x_2, ..., x_{n-k+1})$ *définis par le développement en série*

$$\frac{1}{k!}(\sum_{m\geq 1} x_m \frac{t^m}{m!})^k = \sum_{n\geq k} B_{n,k}\frac{t^n}{n!}, \quad k = 0, 1, 2...$$

sont appelés polynômes de Bell (exponentiels) partiels. Les polynômes de Bell (exponentiels) complets sont les polynômes $Y_n = Y_n(x_1, x_2, ..., x_n)$ *définis par le développement en série*

$$\exp(\sum_{m\geq 1} x_m \frac{t^m}{m!}) = 1 + \sum_{n\geq 1} Y_n(x_1, x_2, ..., x_n)\frac{t^n}{n!}.$$

Autrement dit

$$Y_n(x_1, x_2, ..., x_n) = \sum_{k=1}^{n} B_{n,k}(x_1, x_2, ..., x_{n-k+1}).$$

Les premiers polynômes de Bell sont facilement calculables avec Maple12. Les instructions suivantes

$> \quad B := (n, k) \longrightarrow \text{simplify}(n!coeff(\frac{1}{k!}(add(x(m).\frac{t^m}{m!}, m = 1..n - k + 1))^k, t, n)) :$

$> \quad Y := n \longrightarrow add(B(n, k), k = 1..n) :$

permettent d'obtenir les pour n et k donnés $B_{n,k}$ et Y_n. On obtient ainsi par exemple les résultats suivants :

$$\begin{aligned}
B_{0,0} &= 1 \text{ et } B_{n,0} = 0 \text{ pour } n \geq 1\\
B_{n,1} &= x_n \text{ pour } n \geq 1\\
B_{2,2} &= x_1^2\\
B_{3,2} &= 3x_1x_2\\
B_{4,2} &= 4x_1x_3 + 3x_2^2\\
B_{5,2} &= 5x_1x_4 + 10x_2x_3\\
B_{3,3} &= x_1^3\\
B_{4,3} &= 6x_1^2x_2\\
B_{6,3} &= 15x_1^2x_4 + 60x_1x_2x_3 + 15x_2^3
\end{aligned}$$

Les premiers polynômes complets de Bell sont :

$$\begin{aligned}
Y_1 &= x_1 \\
Y_2 &= x_1^2 + x_2 \\
Y_3 &= x_1^3 + 3x_1x_2 + x_3 \\
Y_4 &= x_1^4 + 6x_1^2x_2 + 4x_1x_3 + 3x_2^2 + x_4 \\
Y_5 &= x_1^5 + 10x_1^3x_2 + 15x_1x_2^2 + 10x_1^2x_3 + 10x_2x_3 + 5x_1x_4 + x_5
\end{aligned}$$

Définition de la Composition

Soit $g_u(X) = \sum_{n=0}^{\infty} u(n)\frac{X^n}{n!})$ tel que $\mathrm{ord}(u) \geq 1$. Alors

$$g_u(X) = \sum_{n=1}^{\infty} u(n)\frac{X^n}{n!}$$

Pour $v \in s_0(C)$, on a

$$g_v(X) = \sum_{n=0}^{\infty} v(n)\frac{X^n}{n!}.$$

On peut définir la composée $(g_v \circ g_u)(X)$ en posant

$$\begin{aligned}
(g_v \circ g_u)(X) &= g_v(g_u(X)) \\
&= \sum_{n=0}^{\infty} v(n)\frac{1}{n!}(\sum_{m=1}^{\infty} u(m)\frac{X^m}{m!})^n \\
&= \sum_{k=0}^{\infty} v(k)\frac{1}{k!}(\sum_{m=1}^{\infty} u(m)\frac{X^m}{m!})^k \\
&= \sum_{k=0}^{\infty} v(k)(\sum_{n\geq k} B_{n,k}(u_1,u_2,\ldots u_{n-k+1})\frac{X^n}{n!}) \\
&= \sum_{n=0}^{\infty}(\sum_{0\leq k\leq n} B_{n,k}(u_1,u_2,\ldots u_{n-k+1})v(k))\frac{X^n}{n!} \qquad (1.61)
\end{aligned}$$

Définition 32 *Soient $u \in s_0(C)$ et $v \in s_0(C)$ tel que* $\mathrm{ord}(u) \geq 1$. *On définit $v \circ u \in s_0(C)$ par la realtion*

$$(g_v \circ g_u)(X) = g_{v\circ u}(X).$$

Proposition 33 *Soient $u \in s_0(C)$ et $v \in s_0(C)$. On a*

$$(v \circ u)(n) = \sum_{0\leq k\leq n} B_{n,k}(u_1,u_2,\ldots u_{n-k+1})v(k). \qquad (1.62)$$

Preuve. En effet, on a d'après la relation (1.61)

$$(g_v \circ g_u)(X) = \sum_{n=0}^{\infty}\Big(\sum_{0\leq k\leq n} B_{n,k}(u_1,u_2,\ldots u_{n-k+1})v(k)\Big)\frac{X^n}{n!} \tag{1.63}$$

$$= \sum_{n=0}^{\infty}(v\circ u)(n)\frac{X^n}{n!}. \tag{1.64}$$

En identifiant les coefficients de X^n dans (1.63) et (1.64), on obtient la relation(1.62). □

Groupe des suites de $s_0(C)$ d'ordre un et expressions des nombres de Stirling à l'aide des polynômes de Bell

Proposition 34 *L'ensemble Ω constitué par les suites de $s_0(C)$ d'ordre un est un groupe pour la composition des suites. Dans Ω, l'inverse $\overline{u}$ de u correspond à la série $g_{\overline{u}}(X)$ réciproque de la série $g_u(X)$.*

Proposition 35 *Soient a et $\overline{a}$ les suites définies par les relations*

$$g_a(X) = e^X - 1$$

et

$$g_{\overline{a}}(X) = \log(1+X).$$

Alors on a

$$B_{n,k}(a) = S(n,k)$$

et

$$B_{n,k}(\overline{a}) = s(n,k).$$

$S(n,k)$ et $s(n,k)$ étant les nombres de Stirling de deuxième et première espèce.

Chapitre 2

Congruences vérifiées par les coefficients binomiaux

"La mathématique est la reine des Sciences, mais la théorie des nombres est la reine des sciences mathématiques"

GAUSS (1777 – 1855).

2.1 Introduction

La notion de congruence ainsi que sa notation ont été introduites par Gauss $(1777 - 1855)$ dans son célèbre ouvrage "Disquisitiones Arithmeticae" paru en 1801, alors qu'il avait à peine 24 ans. Cet ouvrage fait date dans l'histoire des Mathématiques et dans l'histoire de la théorie des nombres en particulier. Il a constitué une source de motivation et d'inspiration pour les générations de mathématiciens, qui succédèrent à Gauss. On peut citer parmi ces célèbres mathématiciens, ceux qui furent élèves de Gauss : Dirichlet $(1805 - 1859)$, Eisenstein $(1823 - 1852)$, Riemann $(1826 - 1866)$ et Richard Dedekind $(1831 - 1916)$. Dans cet ouvrage, qui lui a valu d'être "couronné" Prince des mathématiciens, Gauss énonce et surtout démontre de nombreux théorèmes d'arithmétique. Ce n'est qu'après avoir finalisé l'écriture de l'ouvrage qu'il s'aperçut que plusieurs des résultats qu'il avait découvert étaient en fait déjà connus mais le plus souvent non prouvés !

2.1.1 Définition du coefficient binomial

Soient $n \geq 0$ et $k \geq 0$ des entiers, on définit le coefficient binomial

$$\binom{n}{k} = \frac{\prod_{j=1}^{k}(n-j+1)}{k!}.$$

On a

$$\begin{aligned}
\binom{n}{0} &= 1, \qquad \text{pour } n \geqslant 0, \\
\binom{n}{k} &= 0 \qquad \text{pour } k > n, \\
\binom{n}{k} &= \frac{n(n-1)...(n-k+1)}{k!} \text{ pour } k \geq 1, \\
\binom{n}{k} &= \frac{n!}{k!(n-k)!} \text{ pour } 0 \leq k \leq n.
\end{aligned}$$

La coefficient binomial $\binom{n}{k}$ vérifie les propriétés bien connues

$$\binom{n}{k} \in \mathbb{N}, \text{ pour } \ n \geq 0 \, et \, k \geq 0.$$

$$\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1} \text{ pour } \ n \geq 1 \text{et } \ k \geq 1.$$

On généralise la définition du coefficient binomial en posant

$$\binom{x}{k} = \frac{\prod_{j=1}^{k}(x-j+1)}{k!},$$

x pouvant être un nombre complexe ou une indéterminée et k un entier naturel.

2.1.2 Interprétation combinatoire et formule du binôme

L' entier $\binom{n}{k}$ est égal au nombre de parties de $\{1, 2, ..., n\}$ ayant k éléments. La formule du binome, valable pour a et b éléments d'un anneau commutatif, s'ecrit

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

2.1.3 Les principales identités sur les coefficients binomiaux

$$\begin{aligned}
\binom{n}{k} &= \frac{n!}{k!(n-k)!}, n \geqslant k \geqslant 0, (n,k) \text{ entiers} \\
\binom{n}{k} &= \binom{n}{n-k}, n \geqslant 0, k \text{ entier} \\
\binom{r}{k} &= \frac{r}{k}\binom{r-1}{k-1}, k \neq 0, k \text{ entier} \\
\binom{r}{k} &= \binom{r-1}{k} + \binom{r-1}{k-1} \; k \text{ entier} \\
\binom{r}{k} &= (-1)^k\binom{k-r-1}{k} k \text{ entier} \\
\binom{r}{m}\binom{m}{k} &= \binom{r}{k}\binom{r-k}{m-k} \; m,k \text{ entiers} \\
\sum_{k\leqslant n}\binom{r+k}{k} &= \binom{r+n+1}{n} \; n \text{ entier} \\
\sum_{0\leqslant k\leqslant n}\binom{k}{m} &= \binom{n+1}{m+1} m,n \geqslant 0, \text{entiers} \\
\sum_{k}\binom{r}{k}\binom{s}{n-k} &= \binom{r+s}{n}, n \text{ entier}
\end{aligned}$$

2.1.4 Valuation p-adique du coefficient binomial

$s_p(n)$ désignant la somme des chiffres en base p de l'entier naturel n, on a

Proposition 36 *Pour tout nombre premier p et pour tous entiers n et k tels que $0 \leqslant k \leqslant n$, on a*

$$v_p(\binom{n}{k}) = \frac{s_p(k) + s_p(n-k) - s_p(n)}{p-1}.$$

Preuve. En appliquant le théorème 21, on a

$$\begin{aligned}
v_p(\binom{n}{k}) &= v_p(\frac{n!}{(n-k)!k!}) \\
&= v_p(n!) - v_p((n-k)!) - v_p(k!) \\
&= \frac{n - s_p(n)}{p-1} - \frac{(n-k) - s_p(n-k)}{p-1} - \frac{k - s_p(k)}{p-1} \\
&\quad \frac{s_p(k) + s_p(n-k) - s_p(n)}{p-1}.
\end{aligned}$$

□

2.2 Une propriété des coefficients binomiaux

La propriété suivante est bien connue .

Théorème 37 *Pour tout entier p premier, on a*

$$\binom{p}{k} \equiv 0 \bmod p, \text{ pour tout } k \in \{1, 2, ..p-1\} .$$

Preuve. A partir de la relation $k\binom{p}{k} = p\binom{p-1}{k-1}$, le théorème de Gauss permet d'affirmer que p divise $\binom{p}{k}$ pour tout $k \in \{1, 2, ..p-1\}$, puisque p est alors premier avec k. □

Le théorème 37 admet une réciproque

Théorème 38 *Pour tout entier $n \geq 2$, on a*

$$\text{si } \binom{n}{k} \equiv 0 \bmod n, \text{ pour tout } k \in \{1, 2, ..n-1\}, \text{ alors } n \text{ est un nombre premier.} \quad (2.1)$$

Preuve. Il suffit de prouver la contraposée de l'implication (2.1). Soit n un nombre composé, alors n admet un diviseur premier p et n s'écrit :

$$n = mp \text{ avec } m \geq 2.$$

On alors pour $k = p$, $k \in \{1, 2, ..n-1\}$ et

$$\binom{n}{k} = \binom{mp}{p} = m\frac{(mp-1)(mp-2)...(mp-(p-1))}{1.2...(p-1)} \equiv (-1)^{p-1}m \pmod n,$$

et donc

$$\binom{n}{k} \neq 0 \pmod n.$$

□

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

Théorème 39 *Pour tout entier p premier et m un entier ≥ 1, alors on a*

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

Preuve. Soit $k \in \{1, 2, ..p^m - 1\}$. D'après le théorème (20), on a

$$\begin{aligned} v_p(\binom{p^m}{k}) &= v_p(\frac{p^m!}{k!(p^m-k)!}) \\ &= v_p(p^m!) - (v_p(k!) + v_p((p^m-k)!) \\ &= \sum_{j=1}^{\infty} \left\lfloor \frac{p^m}{p^j} \right\rfloor - (\sum_{j=1}^{\infty} \left\lfloor \frac{k}{p^j} \right\rfloor + \sum_{j=1}^{\infty} \left\lfloor \frac{p^m-k}{p^j} \right\rfloor) \\ &= \sum_{j=1}^{m} \left\lfloor \frac{p^m}{p^j} \right\rfloor - \sum_{j=1}^{m} (\left\lfloor \frac{k}{p^j} \right\rfloor + \left\lfloor \frac{p^m-k}{p^j} \right\rfloor) \\ &= S_1 + S_2, \end{aligned} \tag{2.2}$$

avec

$$S_1 = \sum_{j=1}^{m} \left\lfloor \frac{p^m}{p^j} \right\rfloor$$

et

$$S_2 = \sum_{j=1}^{m} (\left\lfloor \frac{k}{p^j} \right\rfloor + \left\lfloor \frac{p^m-k}{p^j} \right\rfloor.$$

On a alors d'une part

$$\begin{aligned} S_1 &= \sum_{j=1}^{m} \left\lfloor \frac{p^m}{p^j} \right\rfloor = \sum_{j=1}^{m} p^{m-j} \\ &= \sum_{j=0}^{m-1} p^j. \end{aligned} \tag{2.3}$$

D'autre part, pour $1 \leq j \leq m$, si la division euclidienne de k par p^j s'écrit

$$k = q_j p^j + r_j, \text{ avec } 0 \leq r \leq p^j - 1,$$

alors la division euclidienne de $p^m - k$ par p^j s'écrit

$$p^m - k = q'_j p^j + r'_j, \text{ avec } q'_j = p^{m-j} - q_j - 1 \quad \text{et } r'_j = p^j - r \text{ si } 1 \leq r_j \leq p^j - 1,$$

et

$$p^m - k = q'_j p^j + r'_j, \text{ avec } q'_j = p^{m-j} - q_j \text{ et } r'_j = 0 \text{ si } r_j = 0.$$

On en déduit que

$$\left\lfloor \frac{k}{p^j} \right\rfloor + \left\lfloor \frac{p^m-k}{p^j} \right\rfloor = q_j + q'_j = \begin{cases} p^{m-j} - 1 \text{ si } 1 \leq r_j \leq p^j - 1, \\ p^{m-j} \qquad \text{si } r_j = 0. \end{cases}$$

Ainsi

$$\left\lfloor \frac{k}{p^j} \right\rfloor + \left\lfloor \frac{p^m-k}{p^j} \right\rfloor = p^{m-j} - 1 + \left[p^j \text{ divise } k\right] \tag{2.4}$$

Dans l'écriture (2.4), nous avons utilisé le symbole d'Iverson préconisé par Graham, Knuth, Patashnik [40] avec la signification suivante :

$$\left[p^j \text{ divise } k\right] = \begin{cases} 1 & \text{si } p^j \text{ divise } k \\ 0 & \text{sinon} \end{cases}$$

Il en résulte que

$$\begin{aligned} S_2 \quad : \quad &= \sum_{j=1}^{m} \left(\left\lfloor \frac{k}{p^j} \right\rfloor + \left\lfloor \frac{p^m - k}{p^j} \right\rfloor = \sum_{j=1}^{m} (p^{m-j} - 1 + \left[p^j \text{ divise } k\right]) \right. \\ &= \sum_{j=0}^{m-1} p^j - m + \sum_{j=0}^{m-1} \left[p^j \text{ divise } k\right] \\ &= \sum_{j=0}^{m-1} p^j - m + v_p(k). \end{aligned} \tag{2.5}$$

A l'aide de (2.2),(2.3) et (2.5), on obtient alors :

$$\begin{aligned} v_p(\binom{p^m}{k}) &= S_1 + S_2 \\ &= \sum_{j=0}^{m-1} p^j + (\sum_{j=0}^{m-1} p^j - m + v_p(k)) \\ &= m - v_p(k). \end{aligned}$$

□

Le Théorème 39 a pour corollaire la généralisation suivante du théorème 37.

Corollaire 40 *Pour tout entier p premier et m un entier ≥ 1, alors on a*

$$\binom{p^m}{k} \equiv 0 \bmod p, \text{ pour tout } k \in \{1, 2, ..p^m - 1\} \ .$$

Preuve. En effet, pour $k \in \{1, 2, ..p^m - 1\}$, on a $v_p(k) \leq m - 1$, (car sinon on aurait $v_p(k) \geq m$, p^m diviserait k et on aurait $k \geq p^m$, contrairement à ce qu'on a supposé). Par le théorème 39, on a alors

$$v_p(\binom{p^m}{k}) = m - v_p(k) \geq 1.$$

On en déduit que p divise $\binom{p^m}{k}$ pour tout $k \in \{1, 2, ..p^m - 1\}$. □

2.3 Petit théorème de Fermat (1640)

Pierre de Fermat ($1601 - 1665$) est un juriste et mathématicien français, surnommé « le prince des amateurs ». Il a laissé à la communauté mathématiques un grand nombre de "théorèmes" intéressants, malheureusement presque tous sans démonstration.

Le théorème qui suit est connu sous le nom de petit Théorème de Fermat. Selon Michel Demazure [25] ce théorème a été enoncé par Fermat en 1640 et demontré par Euler en 1736.

Théorème 41 *soit p un nombre premier. On a alors*

$$a^p \equiv a \bmod p, \text{ pour tout entier } a \tag{2.6}$$

et

$$a^{p-1} \equiv 1 \bmod p, \text{ pour tout entier } a \text{ premier à } p. \tag{2.7}$$

Preuve. Pour tout entier a, on a par la formule du binôme et par le théorème 37

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

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 on a $a^p - a = -(|a|^p - |a|) \equiv 0 \bmod p$, la relation (2.6) est ainsi établie. On a alors $a(a^{p-1} - 1) \equiv 0 \bmod p$, si a est premier à p, on en déduit qu'on a $a^{p-1} - 1 \equiv 0 \bmod p$, ce sui prouve (2.7). □

2.3.1 Une application de théorème de Fermat à l'étude des divieurs des nombres de Fermat

Nombres de Fermat et nombres de Mersenne

La proposition qui suit, facile à établir, motive la définition des nombres de Fermat et des nombres de Mersenne.

Proposition 42 *Soient $a \geq 2$ et $m \geq 2$ des entiers.*

1. *Si le nombre $2^m + 1$ est premier, alors m est une puissance de 2 et il existe un entier $n \geq 1$ tel que $m = 2^n$. Dans ce cas $2^m + 1 = 2^{2^n} + 1$.*
2. *Si le nombre $a^m - 1$ est premier, alors $a = 2$ et m est un nombre premier. Dans ce cas $a^m + 1 = 2^p + 1$, avec p premier.*

Preuve.

1. Si m n'était pas une puissance de $2, m$ serait divisible par un nombre impair, on aurait $m = (2n+1)q$ avec $q \geq 1$, entier et $2^m + 1$ serait divisible par $2^q + 1$ du fait qu'on aurait :

$$2^m + 1 = (2^q)^{2m+1} + 1 = (2^q + 1)((2^q)^{2m} - (2^q)^{2m-1} + \cdots - 2^q + 1).$$

   $2^m + 1$ ne serait pas premier.

2. Pour tout entier $a \geq 2$, on a

$$a^m - 1 = (a-1)(a^{m-1} + a^{m-2} + \cdots a + 1),$$

   et donc $a - 1$ divise $a^m - 1$ et $a^m - 1$ n'est pas premier pour $a \neq 2$. Supposons que $a = 2$, alors $a^m - 1 = 2^m - 1$. Si m n'était pas un nombre premier, m s'écrirait $m = rs$ avec $r \geq 2$ et $s \geq 2$ et $2^m - 1$ serait divisible par $2^r - 1$ du fait qu'on aurait

$$2^m - 1 = (2^r)^s - 1 = (2^r - 1)((2^r)^{s-1} + (2^r)^{s-2} + \cdots + 2^r + 1).$$

   $2^m - 1$ ne serait pas premier.

□

Définition 43 *1. On appelle nombre de Fermat tout entier F_n s'écrivant*

$$F_n = 2^{2^n} + 1$$

avec $n \geqslant 1$.

2. On appelle nombre de Mersenne tout entier M_p s'écrivant

$$M_p = 2^p - 1$$

Les premières valeurs des nombres de Fermat sont

$$\begin{aligned} F_0 &= 3, \\ F_1 &= 5, \\ F_2 &= 17, \\ F_3 &= 257, \\ F_4 &= 65537. \end{aligned}$$

Tous ces nombres $(F_0, F_{1,}F_{2,}F_3, F_4)$ sont des nombres premiers. Fermat émit en 1640 la conjecture que tous les nombres F_n étaient premiers. Cette conjecture se révéla fausse, et Fermat ne le sût jamais. En effet Fermat mourut en 1665 et il faudra encore attendre de nombreuses années avant qu'Euler $(1707 - 1783)$ ne prouve en 1732, soit prés d'un siècle après l'énoncé

de cette conjecture que $F_5 = 4\ 294\ 967\ 297$, en fait n'est pas premier. Euler prouva que 641 divise F_5.

Marin Mersenne $(1588-1648)$ est un religieux français érudit, mathématicien et philosophe. Il affirma sans preuve que les seuls nombres premier ≤ 257 pour lesquelles M_p était premier étaient $p = 2, 3, 5, 7, 13, 17, 19, 31, 67, 127, 257$. La liste de Mersenne s'avéra inexacte. Il fallut plus de 300 ans pour constater en 1947 que finalement Mersenne avait commis cinq erreurs dans cette liste. Plus précisément M_{67} et M_{257} sont composés et doivent être donc supprimés de cette liste alors que M_{61}, M_{89}, et M_{107} sont premiers et doivent donc être rajoutés à cette liste.

La liste de Mersenne

La liste exacte des nombres premiers $p \leq 257$ pour lesquels M_p est premier s'établit ainsi $2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107, 127$. Remarquons qu'il y a exactement 55 nombres premiers $p \leq 257$. Ce sont $2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89,$

$97, 101, 103, 107, 109, 113, 127, 131, 137, 139, 149, 151, 157, 163, 167, 173, 179, 181, 191, 193, 197,$

$199, 211, 223, 227, 229, 233, 239, 241, 251, 257.$

Etude des diviseurs premiers des nombres de Fermat

Euler prouva que 641 divise F_5. Comment Euler parvint-il à ce résultat ? Essayons de comprendre la démarche qu'a pû avoir cet illustre mathématicien. Tout d'abord, on peut penser que Fermat ait été découragé pour tenter de trouver un diviseur premier de F_5 par la méthode des diviseurs successives. Il aurait fallu tester la divisibilité du nombre F_5 par à priori tous les nombres premiers inférieurs à sa racine, soit par tous les nombres premiers inférieurs ou égaux à 65521,soit 6542 essais à faire (car il y a 6542 nombres premiers inférieurs ou égaux à 65521), ce qui était quasiment inenvisageable ! A postériri, on pourrait penser qu'Euler ait eu le courage d'éssayer et qu'il soit tombé par hasard sur le diviseur premier 641 de F_5.comme 641 est le $116ième$ nombre premier, la méthode des essais nécéssite de tester la divisibilité par chacun des 116 nombres premiers nombres premiers, ce qui est encore loin d'être une bonne méthode et en tout cas nécessiterait un temps considérable. Nous allons maintenant montrer comment le petit thérème de Fermat permet de prouver que les divieurs premiers de F_5 sont de le forme $64k+1$ et permet donc de limiter le nombre d'essais. En effet, les premiers nombres premiers de cette forme sont $193,\ 257, 449, 577, 641, 769, ...$Il suffit alors d'effectuer seulement 4 tests trés simples pour découvrir au bout du quatrième essai que 641 divise F_5.

Diviseurs premiers des nombres de Fermat

Théorème 44 *Soit p un nombre premier. Si p divise F_n, alors il existe un entier $k \geqslant 1$ tel que $p = k2^{n+1} + 1$.*

Autrement dit, les diviseurs premiers de F_n sont de la forme $k2^{n+1} + 1$ avec $k \geqslant 1$.

Preuve. Soit p un diviseur premier de $F_n = 2^{2^n} + 1$. Comme F_n est un nombre impair, tous ses diviseurs sont impairs et en particulier p est impair. On a

$$F_n \equiv 0 \pmod{p},$$

ce qui peut s'écrire

$$2^{2^n} \equiv -1 \pmod{p}. \tag{2.8}$$

Pour tout entier m tel que $1 \leqslant m \leqslant n$, on a alors

$$(2^{2^m})^{2^{n-m}} = 2^{2^n} \equiv -1 \pmod{p}$$

Il résulte de cette dernière congruence que l'on a

$$2^{2^m} \neq 1 \pmod{p}, \text{ pour } 1 \leqslant m \leqslant n$$

On a alors, en élevant au carré de (2.8)

$$2^{2^{n+1}} \equiv 1 \pmod{p}. \tag{2.9}$$

la relation (2.9) signifie que dans le groupe cyclique multiplicatif $(\mathbb{Z}/p\mathbb{Z})^*$, 2 est d'ordre un diviseur de 2^{n+1}. Comme les divieurs de 2^{n+1} sont de la forme 2^m avec $0 \leqslant m \leqslant n+1$ et que l'on a $2^{2^m} \neq 1 \pmod{p}$, pour $1 \leqslant m \leqslant n$ et $2^{2^0} = 2 \neq 1 \pmod{p}$, il en résulte que l'ordre de 2 dans $(\mathbb{Z}/p\mathbb{Z})^*$ est nécessairement egal à $2^{2^{n+1}}$.

D'autre part, on sait d'aprés le petit théorème de Fermat, p étant impair et donc premier avec 2, on a

$$2^{p-1} \equiv 1 \pmod{p}.$$

Il en résulte que $p-1$ est un multiple de l'ordre de 2 dans $(\mathbb{Z}/p\mathbb{Z})^*$. Par conséquent, il existe un entier $k \geqslant 1$ tel que

$$p - 1 = k2^{n+1}$$

Soit

$$p = k2^{n+1} + 1.$$

□

Appliquons le théorème 44 à la détermination d'un diviseur premier du nombre de Fermat F_5. Rappelons que

$$F_5 = 2^{2^5} + 1 = 4294967297.$$

D'après le théorème 44, tout divieur premier de F_5 est de la forme $k2^6+1$ avec $k \geqslant 1$, c'est à dire de la forme $64k+1$ avec $k \geqslant 1$. Les premières valeurs de la suite $(64k+1)_{k\geqslant 1}$ sont

$$(64k+1)_{k\geq 1} = (65, 129, 193, 257, 321, 385, 449, 513, 577, 641, 705, ...)$$

Si on ne retient de cette liste que les nombres premiers, on obtient la liste restreinte suivante des premiers nombres premiers de la forme $64k+1$:

$$(193, 257, 449, 577, 641, ...).$$

On peut alors tester la divisibilité de F_5 par chacun de ces nombres premiers, à la main bien comme l'a sans doute fait Euler et comme aurait pu le faire Fermat :

n	193	257	449	577	641
$2^8 \bmod n$	63	256	256	256	256
$2^{16} \bmod n$	109	1	431	335	154
$2^{32} \bmod n$	108	1	324	287	640
$F_5 \bmod n$	109	2	325	288	0

On constate ainsi que

$$F_5 \equiv 0 \bmod 641.$$

On a d'ailleurs

$$F_5 = 4\ 294\ 967\ 297 = (641).(6\ 700\ 417).$$

Remarquons que

$$6\ 700\ 417 = 52347.2^7 + 1$$

Il est facile de vérifier à la main que 6 700 417 est un nombre premier. En effet tout diviseur premier de 6 700 17 est un diviseur premier de F_5 donc un nombre premier de la forme $64k+1$, avec $k \geqslant 10$. (On sait en effet qu'aucun nombre premier de la forme $64k+1$, avec $1 \leqslant k \leqslant 9$ ne divise F_5,et par conséquent aucun de ces nombres ne peut diviser 6 700 417 qui est un diviseur de F_5. De plus, on sait que si un nombre n n'est pas premier, il admet un diviseur premier $\leqslant \sqrt{n}$. Comme $\sqrt{6\ 700\ 417} = 2588,52...$et que la plus petite valeur de k tel que $64k+1 > \sqrt{6\ 700\ 417}$ est égale à 41. Pour prouver la primalité du nombre 6 700 417, il suffit de prouver que ce nombre n'est divisible par aucun nombre premier de la forme $64k+1$ avec k, tel que $10 \leqslant k \leqslant 40$. Or les seuls nombres premiers p de cette forme sont 769, 1153, 1217, 1409, 1601 et 2113 et il est facile de vérifier à la main que

$$\begin{aligned} 6\ 700\ 417 &\equiv 120 \pmod{769} \\ &\equiv 334 \pmod{1153} \\ &\equiv 832 \pmod{1217} \\ &\equiv 232 \pmod{1601} \\ &\equiv 94 \pmod{2113}. \end{aligned}$$

La méthode nous a permis aussi de prouver par un calcul à la main que 6 700 417 est un nombre premier. La méthode classique de tester la divisibilité du nombre par tous les nombres premiers inférieurs ou égaux à la racine de ce nombre est pratiquement infaisable dans ce cas car elle nécessiterait un temps considérable alors que la méthode de calcul précédente, par congruences, bien que quelque peu laborieuse, permet d'obtenir le résultat en un temps très raisonnable.

2.3.2 Une autre application du theorème de Fermat : le test de primalité de Proth (1878)

François Proth (1852-1879) est un mathématicien qui découvrit un théorème constituant un test de primalité pour les entiers de la forme $k2^n + 1$ avec $k < 2^n$ et k impair. Les entiers de la forme $k2^n + 1$ avec $k < 2^n$ et k impair sont appelés nombres de Proth. Les nombres de Proth sont repertoriés dans l'encyclopédie en ligne des entiers sous la référence $A080075$. Les premiers entiers de Proth sont $(3, 5, 9, 13, 17, 25, 33, ...)$

Théorème 45 *Proth (1878)Soit n nombre entier de la forme $n = k2^m + 1$ avec k entier naturel impair tel que $k < 2^m$. S'il existe un entier a tel que*

$$a^{(n-1)/2} \equiv -1 (\mathrm{mod}\, n),$$

alors n est premier.

Remarque 46 *Le theorème de Proth ne permet pas de prouver que le quotient de F_5 par 641,c'est à dire 6 700 417, est un nombre premier. On a $6700417 = 52347.2^7 + 1$, et 6700417 n'est pas un nombre de Proth car $52347 > 2^7$.*

2.3.3 Application du théorème de Fermat à l'étude des sommes $\sum_{k=1}^{p-1} \frac{1}{k^n}$ et $\sum_{k=1}^{(p-1)/2} \frac{1}{k^n}$ modulo p

Le petit théorème de Fermat permet de prouver aisément le théorème suivant

Théorème 47 *Soit p un nombre premier impair et n un entier, alors*

$$\sum_{k=1}^{p-1} k^n \equiv \begin{cases} -1 \ (\mathrm{mod}\, p) & \textit{si } p-1 \textit{ divise } n \\ 0 \quad (\mathrm{mod}\, p) & \textit{sinon} \end{cases}$$

Preuve. Soit p un nombre premier impair . Posons

$$S = \sum_{k=1}^{p-1} k^n.$$

Soit g un générateur du groupe cyclique multiplicatif $\mathbb{Z}/p\mathbb{Z}$. Posons pour $m \in \mathbb{Z}$

$$\overline{m} = m + p\mathbb{Z}.$$

Alors, on a pour $n \in \mathbb{N}$

$$\begin{aligned} \overline{S} &= \sum_{k=1}^{p-1} \overline{k}^n \\ &= \sum_{j=0}^{p-2} g^{jn} \\ &= \sum_{j=0}^{p-2} (g^n)^k. \end{aligned}$$

Soit

$$\overline{S} = \sum_{j=0}^{p-2} (g^n)^k \tag{2.10}$$

Deux cas présentent

1. $p-1$ divise n. Dans ce cas, on a $g^n = \overline{1}$. Par suite

$$\overline{S} = \sum_{j=0}^{p-2} \overline{1} = \overline{p-1} = \overline{-1.}$$

   Dans ce cas $S \equiv -1 \pmod{p}$

2. $p-1$ ne divise pas n. Dans ce cas, on sait que $g^n \neq \overline{1}$. En multipliant les deux membres de la relation (2.10) par $g^n - 1$, on obtient

$$\begin{aligned} (g^n - \overline{1})\overline{S} &= (g^n - \overline{1})(\sum_{j=0}^{p-2} (g^n)^k) \\ &= (g^n)^{p-1} - \overline{1} \\ &= (g^{p-1})^n - \overline{1} \\ &= \overline{0} \end{aligned}$$

   Dans ce cas, on obtient que sinon $(g^n - 1)\overline{S} = \overline{0}$. Comme on a de plus $g^n - 1 \neq 0$. Il en résulte que $\overline{S} = 0$, c'est à dire $S \equiv 0 \pmod{p}$.

□

Preuve. Dans le cas où $n < 0$, il suffit de remarquer que les sommes $\sum_{k=1}^{p-1} \overline{k}^n$ et $\sum_{k=1}^{p-1} \overline{k^{-1}}^n$ sont égales pour arriver à la même conclusion. □

Corollaire 48 *Soit p un nombre premier impair et $n \geqslant 0$ un entier, alors*

$$\sum_{k=1}^{(p-1)/2} \frac{1}{k^{2n}} \equiv \begin{cases} \frac{1}{2}(p-1) \pmod p & \textit{si } \frac{p-1}{2} \textit{ divise } n \\ 0 \pmod p & \textit{sinon} \end{cases}$$

Corollaire 49 *Pour tout nombre premier $p \geq 5$, on a*

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

2.4 Théorème de Wilson (1770)

2.4.1 Historique

Selon son histoire rapportée par Roshdi Rashed ,il devrait s'appeller Théorème d'Al Haitham-Leibniz-Wilson-Waring–Lagrange-Euler-Gauss,mais on le connait sous le nom du Théorème de Wilson .

le théorème de Wilson a été découvert à la fin du dixième siècle par le mathématicien arabe Ibn al-Haytham qu'on nomme aussi Alhazen $(965-1039)$ démontrant une remarquable avance sur les sciences occidentales .

On retrouve la trace de ce théorème vers 1682 chez Gottfried Wilhelm von Leibniz $(1646-1716)$ qui fait réfèrence à ce résultat mais n'a pas publié sa preuve selon Roshdi Rashed pour des considérations historiques ,Leonard Euler prouve le théorème (opuscula annale tome 1 page 329)et l'utilise pour sa démonstration du théorème des deux carrés de Fermat .

Le résultat ressurgit, sans démonstration, à la fin du dix-huitième siècle dans les écrits de Edward Waring$(1736-1798)$ qui l'attribue en 1770 à son élève John Wilson $(1741-1793)$ qui pensait avoir decouvert ce qu'il croyait être une conjecture et en a partagé la découverte avec son professeur Edward Waring qui publia ce résultat en 1770 dans Méditationes Cambridge J.Archeacon ,ni Waring ni son étudiant Wilson ne semblaient connaitre la preuve du théorème,et d'aprés Lagrange **??**il parait même insinuer que personne ne l'a encore trouvée ,du moins il semble qu'il la regarde comme extremement difficile ,car après avoir rapporté ce théorème avec quelques d'autres qui en dépendent il (Eduard Waring)ajoute "Démonstrationes vero hujusmodi propositionum eo magis difficiles erunt ,quod nulla finge potest notatio,que primum numerum exprimat".Et c'est cette raison présentée presque un comme défi jointe à

l'élégance et à l'utilité du théorème qui a poussé Lagrange [60] à en chercher une démonstration (mais il en présenta même deux) et celle qu'il présenta mérita l'attention des géomètres tant par elle même que parce qu'elle fait connaitre en même temps d'autres propriètes des nombres premiers ,qui n'avaient pas encore été remarquées .

L'année suivante soit 1771 la première démonstration officielle donnée est présentée et elle était du à Lagrange$(1736-1813)$,il en donne même deux demonstrations du théorème .

Nombreux historiens pensent que Al Hazen avait la démonstration de ce théorème ,il avait déjà publié un court ‹‹Opuscule›› dans lequel il énonçait le résultat et il apparait clairement qu'il en possédait la justification ,probablement basée sur une forme de l'identité de Bezout ,mais malheureusement beaucoup de ses écrits n'ayant pas été retrouvés ,ses connaissances exactes n'ont pas pu être reconstituées .

Selon Roshdi Rashed [82] Ibn Al Haithem $(965-1039$) avait démontré le théorème suivant "si p est un nombre premier alors $(p-1)+1$est un multiple de p ",il dit aussi que ce type de problème est connu de Léonard de Pise $(1170-1240$)en Italie au début du XIII ^{e}siècle .

L'Opuscule d'Al Haitham commence par l'énoncé du problème suivant :

"Trouver un nombre tel que si l'on le divise par deux il en reste un ,

si l'on le divise par trois il en reste un ,

si l'on le divise par trois il en reste un ,

si l'on le divise par quatre il en reste un ,

si l'on le divise par cinq il en reste un ,

si l'on le divise par six il en reste un ,

si l'on le divise par sept il en reste rien .

Ibn Al Haithem donne deux methodes

la première qu'il qualifie de ‹‹canonique›› consiste à exhiber le nombre $6!+1=721$ qui répond à la question,la seconde permet de trouver toutes les solutions du problème ,qui en a une infinité .On pourrait penser que Ibn Al Haitham n'a résolu qu'un problème particulier ,une devinette arithmétique en quelque sorte .Mais voiçi comment il poursuit son exposé ,après la description des deux methodes dans le cas particulier $n=7$.Ceci étant posé ,nous disons que cette propriété est nécessaire pour tout nombre premier c'est à dire que pour tout nombre premier (qui est un nombre qui n'est multiple que de l'unité)si on multiple les nombres qui le precedent les uns par les autres selon la manière que nous avons introduite ,et si on ajoute un au produit ,alors si on divise la somme par chacun des nombres qui précèdent le nombre premier ,il en reste un ,et si on la divise par le nombre premier p il n'en reste rien .

Le cas $n=7$ n'est qu'un artifice pédagogique .Ibn Al haitham savait que son exposé est

tout à fait cair ,beaucoup plus clair que ceux de ses successeurs qui reprendront le même problème à partir de ses écrits .Enfin il n'y que Ibn Al Haitham qui poura en conclure ,lui qui ne semblait pas juger que son résultat méritait une aussi longue postérité .

Parmi les imminents chercheurs qui ont démontré ce théorème ,on citera ,Lagrange(1773) ,Euler (1783),Gauss (1801) ,Dirichlet (1828) Moritz Abraham Stern (1860),(on rappelle que Monsieur Stern était étudiant Monsieur Gauss et lui succeda le 30 juillet 1859 à la chaire universitaire de Mathématiques de l'université de Gottingen).

Aussi on trouve sur le site numérisé Numdam divers articles qui présentent des démonstrations et même des généralisations sur ce fameux théorème [80],[81],[95].

2.4.2 Démonstrations données par Lagrange (1773)

Première démonstration donnée par Lagrange

Etant donné le produit continuel

$$(x+1)(x+2)(x+3).....(x+p-2)(x+p-1$$

On se propose de le développer suivant les puissances de x.

Il est visible que l'on aura

$$\begin{aligned} & (x+1)(x+2)(x+3)(x+4)..... + (x+p-1) \\ = \;& x^{p-1} + A_1 x^{p-2} + A_2 x^{p-3} + A_3 x^{p-4}.....A_{p-1} \end{aligned} \tag{2.11}$$

Remplacant x par $x+1$ et multipliant la relation (2.11)par x+1 on obtient

$$\begin{aligned} & (x+1)(x+2)(x+3).....(x+p) \\ = \;& (x+1)^p + A_1(x+1)^{p-1} + A_2(x+1)^{p-2} + ...A_{p-1}(x+1) \end{aligned} \tag{2.12}$$

Multipliant la relation (2.11) par $(x+p)$,on voit d'aprés les relations (2.11) et (2.12)

que

$$\begin{aligned} & (x+p)\left[x^{p-1} + A_1 x^{p-2} + A_2 x^{p-3} + A_3 x^{p-4}..... + A_{p-1}\right] \\ = \;& (x+p)^p + A_1(x+1)^{p-1} + A_2(x+1)^{p-2}..... + A_{p-1}(x+1) \end{aligned} \tag{2.13}$$

Aprés expansion de la relation (2.13) et regroupement des termes on trouve

$$\begin{aligned} A_1 &= \binom{p}{2} \\ 2A_2 &= \binom{p}{3} + A_1\binom{p-1}{2} \\ 3A_3 &= \binom{p}{4} + A_1\binom{p-1}{3} + A_2\binom{p-2}{2} \end{aligned} \tag{2.14}$$

(2.15)

$$\begin{aligned} (p-2)A_{p-2} &= p + (p-1)A_1 + (p-2)A_2.....3A_{p-3} \\ (p-1)A_{p-1} &= A_{p-2} + A_{p-3}..... + A_3 + A_2 + A_1 + 1 \end{aligned}$$

D'une manière génèrale pour pour tout k, $1 \leq k \leq p-1$ on a

$$\begin{aligned} kA_k &= \binom{p}{k+1} + A_1\binom{p-1}{k} + A_2\binom{p-2}{k-1} + ... \\ &\quad +.....A_{k-2}\binom{p-k+2}{3} + A_{k-1}\binom{p-k+1}{2} \end{aligned} \tag{2.16}$$

soit p un nombre premier ,alors $0 < k < p$ alors p divise $\binom{p}{k}$,de la on déduit que p divise $A_1, 2A_2, 3A_3, , , , , , , , , , , , , , , (p-2)A_{p-2}$

Aussi si $k = p-1$ la relation (2.16) devient alors

$$\begin{aligned} (p-1)A_{p-1} &= \binom{p}{p} + \binom{p-1}{p-1}A_1 + \binom{p-2}{p-2}A_2 + ...\binom{3}{3}A_{p-3} + \binom{2}{2}A_{p-2} \quad (2.17) \\ (p-1)A_{p-1} &= 1 + A_1 + A_2..... + A_{p-3} + A_{p-2} \end{aligned}$$

Ainsi il s'ensuit que

$$\begin{aligned} (p-1)A_{p-1} &\equiv 1 (\mathrm{mod}\, p) \\ (-1)A_{p-1} &\equiv 1 (\mathrm{mod}\, p) \\ A_{p-1} + 1 &\equiv 0 (\mathrm{mod}\, p) \end{aligned} \tag{2.18}$$

La relation (2.18) montre que p divise $\mathrm{A}_{p-1} + 1$

Reprenons la relation (2.11) ,on voit que d'après cette relation

$$A_{p-1} + 1 \equiv 0(\mathrm{mod}\, p)$$

c'est à dire que

$$(p-1)! + 1 \equiv 0(\mathrm{mod}\, p) \tag{2.19}$$

qui est bien le théorème de Wilson .

Il est important de signaler que les nombres A_k sont connus aujourd'hui comme étant les nombres de Stirling de première éspèce ,une moderne notation pour $A_k = s(p, p-k)$ pour $k = 1, 2, ...p$.

Lagrange fut le premier à prouver que $s(p,k) \equiv 0(\mathrm{mod}\, p)$ pour k telque $2 \leqslant k \leqslant p-1$,voir ([20]) p 218 − 219,([77]) $p27$.

Deuxième démonstration donnée par Lagrange

Lagrange en donna une deuxième démonstration qui est basée sur une célébre formule donnée par Euler :

Pour tout $a \geq n$ on a

$$n! = a^n - n(a-1)^n + \binom{n}{2}(a-2)^n - \binom{n}{3}(a-3)^n .....(-1)^n \binom{n}{n}(a-n)^n \tag{2.20}$$

En prenant $n = p-1$ et $a = p$,la relation (2.20) devient alors

$$\begin{aligned}(p-1)! &= p^{p-1} - (p-1)(p-1)^{p-1} + \binom{p-1}{2}(p-2)^{p-1} \\ &\quad - \binom{p-1}{3}(p-3)^{p-1} + ... + (-1)^{p-1}\binom{p-1}{p-1}\end{aligned} \tag{2.21}$$

en utilisant le petit théorème de Fermat par rapport à p

$$\begin{aligned}(p-1)! &\equiv 0 - \binom{p-1}{1} + \binom{p-1}{2} - \binom{p-1}{3} + ... \\ &\quad ..... - \binom{p-1}{p-2} + (-1)^{p-1}\binom{p-1}{p-1}(\mathrm{mod}\, p)\end{aligned} \tag{2.22}$$

comme on sait que

$$\begin{aligned}(1+(-1))^{p-1} &= \binom{p-1}{0}1^{p-1}+(-1)^1\binom{p-1}{1}1^{p-2}+(-1)^2\binom{p-1}{2}1^{p-3} \\ &\quad +(-1)^3\binom{p-1}{3}1^{p-4}.....(-1)^{p-1}\binom{p-1}{p-1} \end{aligned} \tag{2.23}$$

d'après les relations (2.22) et (2.22)

$$0=(1-1)^{p-1}\equiv 1+(p-1)!(\mathrm{mod}\, p) \tag{2.24}$$

la relation (2.24) est bien le théorème de Wilson

2.4.3 Démonstration donnée par Euler (1783)

L'idée d'Euler consiste à utiliser le fait que le groupe F_p^*.est cyclique c'est à dire engendré par une classe a particulière qui est une racine primitive .

Soit a^2 une racine primitive de p avec $pgcd(a,p)=1$,$ordre(a)=\Phi(p)=p-1$

et $a^{p-1}\equiv 1(\mathrm{mod}\, p)$.

On considère les deux ensembles I et J tels que :

$$I=\left\{1,a,a^2,a^3,.....a^{p-2}\right\} \tag{2.25}$$

et

$$J=\{1,2,3,4.....p-1\} \tag{2.26}$$

le produit des élèments de l'ensemble I est congruent au produit des élèments de l'ensemble J

$$1.a.a^2.a^3.....a^{p-2}=1.2.3.4.....p-1(\mathrm{mod}\, p) \tag{2.27}$$

comme

$$1.a.a^2.a^3.....a^{p-2}=a^{\frac{(p-1)(p-2)}{2}}$$

et

$$1.2.3.....p-1=(p-1)!$$

la relation (2.27) devient alors

$$a^{\frac{(p-1)(p-2)}{2}} \equiv (p-1)!(\mathrm{mod}\, p) \tag{2.28}$$

On suppose que $p > 2$ et $p = 2n + 1$ pour n entier donc

$$a^n = a^{\frac{p-1}{2}}$$

puisque d'une part on

$$a^{p-1} - 1 = (a^{\frac{p-1}{2}} - 1)(a^{\frac{p-1}{2}} + 1) \tag{2.29}$$

et d"autre part on d'après le théorème de Fermat

$$a^{p-1} \equiv 1(\mathrm{mod}\, p) \tag{2.30}$$

or d'après le petit théorème de Fermat on a

$$p/(a^{p-1} - 1)$$

c'est à dire que

$$p/(a^{\frac{p-1}{2}} - 1) ou p/(a^{\frac{p-1}{2}} + 1)$$

Puisque a est une racine primitive c'est à dire que

$$p \nmid a^{\frac{p-1}{2}} - 1$$

donc

$$p/a^{\frac{p-1}{2}} + 1 \tag{2.31}$$

c'est à dire que

$$a^{\frac{p-1}{2}} + 1 \equiv 0(\mathrm{mod}\, p) \tag{2.32}$$

comme $p = 2n + 1$ alors n=$\frac{p-1}{2}$.$alors$.

$$a^{\frac{(p-1)(p-2)}{2}} = a^{\frac{2n(2n-1)}{2}} = a^{n(2n-1)} = (a^n)^{2n-1} \tag{2.33}$$

et pour p premier avec $p = 2n + 1$ c'est

$$a^n = a^{\frac{p-1}{2}} \equiv -1(\mathrm{mod}\, p)$$

donc

$$(a^n)^{2n-1} \equiv (-1)^{2n-1}(\mathrm{mod}\, p) \tag{2.34}$$

ce qui implique avec les relations 2.28 et 2.34 que

$$(p-1)! + 1 \equiv 0(\mathrm{mod}\, p) \tag{2.35}$$

la relation 2.35 est bien le théorème de Wilson

2.4.4 Démonstration donnée par Gauss(1801)

Utilisant les notations de l'arithmétique modulaire qu'il introduite dans son célébre ouvrage [31],Gauss reformula les démonstrations données par Lagrange et on donna une troisième ou plutôt une quatrième (puisque Lagrange avait présenté deux démonstrations).

Voiçi ce que dit Gauss sur le théorème de Wilson dans son ouvrage [31]

" Ce théorème élégant qu'on énonce ordinairement de cette manière : le produit de tous les nombres plus petits qu'un nombre ,étant augmenté de l'unité ,est divisible par ce nombre premier , a été publié par Waring qui l'attribue à Wilson (Méditationes Algeb,Ed 5p580) ; mais aucun des deux n'a pu le démontrer ,et Waring avoue que la démonstration lui en semble d'autant plus difficile qu'il n'y a point de notation par laquelle on puisse exprimer un nombre premier ,pour nous ,nous pensons que la démonstration de cette sorte de vérité doit être puisée dans les principes plutôt que dans la notation .Lagrange en a depuis donné une démonstration (Nouv Mém de l'Ac de Berlin 1771),dans laquelle il s'appuie sur la considération des coefficients que l'on trouve en développant le produit

$$(x+1)(x+2)(x+3).....(x+p-1)$$

et il fait voir qu'en supposant ce produit

$$= x^{p-1} + Ax^{p-2} + Bx^{p-3}.....Mx + N$$

Les coefficients A, B, C.....et M sont divisibles par p .

Le terme constant $N = 1.2.3.4...p-1$

si $x = 1$ le produit sera divisible par p ,mais alors il sera $\equiv 1 + N(\mathrm{mod}\, p)$

donc $N + 1 \equiv 0(\mathrm{mod}\, p)$.

Enfin Euler (Opuscula ,analy Tome $1p - 329$)en a donné une démonstration

qui rentre dans celle que nous venons exposer ,ainsi puisque de tels hommes n'ont pas cru ce sujet indigne de leurs méditations ,nous éspèrons qu'on ne nous désapprouvera pas d'offrir encore une autre manière de démontrer ce théorème .

Nous dirons que deux nombres sont associés ,comme l'a fait Euler ,lorsque leur produit sera congru à l'unité ,tout nombre premier moindre que p aura toujours un nombre ,associé moindre que p et il n'en aura qu'un ,or il est facile de prouver que parmi les nombres $1, 2, 3, ...p-1$,il n'y a que 1 et $p-1$ qui soient eux même leurs associés ;car ceux qui jouiront de cette propriété seront donnés par la congruence $x^2 \equiv 1$ qui ne peut avoir que deux racines 1 et $p-1$.Supprimant donc ces deux nombres , les autres $2, 3, 4, ...p-2$,seront associés deux à deux, donc leurs produits sera $\equiv 1$,enfin multipliant par $p-1$,le produit de tous $1.2.3...p-1 \equiv p-1 \equiv -1(modp)$

Exemple : pour $n = 13$, les nombres 2,3,4,5,6,7,8,9,10,11s'associent de la manière suivante :2 avec 7 ;3 avec 9 ; 4 avec 10 ; 5 avec 8 ; 6 avec 11 et

$$1.2.3.4.....10.11.12 \equiv 12 \equiv -1(\mathrm{mod}\, 13)$$

2.4.5 Généralisation du théorème de Wilson

Selon L.E.Dickson [28] il semblerait que Gauss fut le premier à avoir généralisé le théorème de Wilson.

Simple généralisation du théorème de Wilson

$\forall\, n \in \mathbb{N}.$:

$$(n-1)! \equiv \begin{cases} -1(\mathrm{mod}\, n)...\text{si.}n \text{ est premier} \\ 2(\mathrm{mod}\, n)...\text{si } n = 4. \\ 0(\mathrm{mod}\, n)... \sin on \end{cases}$$

Généralisation de Gauss

Pour tout p premier ,et α.un entier positif

$$\prod_{k=1,(k,n)=1}^{n-1} k \equiv \begin{cases} 0(\mathrm{mod}\, n)..\mathrm{si}.....n = 1..... \\ -1(\mathrm{mod}\, n)..\mathrm{si}....n = 4, p^{\alpha}, p^{2\alpha} \\ 1(\mathrm{mod}\, n).... \sin on..... \end{cases}$$

2.4.6 Nombre de Wilson

Un nombre premier p est appelé nombre premier de Wilson si p est tel que p^2 divise $(p-1)!+1$, c'est à dire que pour tout p premier

$$(p-1)! + 1 \equiv 0(\mathrm{mod}\, p^2)$$

les seuls nombres de Wilson connus sont $5, 13, 563$,(Encyclopédie éléctronique des suites entières) $IdA007540$ .si d'autres existent ils doivent être plus grands que 5.10^8.

Il a été conjecturé qu'il existe une infinité de nombres premier de Wilson et que le nombre de nombres de Wilson dans un intervalle $[x, y]$ est environ $\frac{\log\log y}{\log x}$

2.5 Théorème d'Euler (1736)

Théorème 50 *Soit a et n deux entiers premiers entre eux, alors*

$$a^{\varphi(n)} \equiv 1 \ (\mathrm{mod}\, n)$$

Preuve. Soit $\{r_1, r_2, ..., r_{\varphi(n)}\}$ un système réduit de résidus modulo n. Alors $\{ar_1, ar_2, ..., ar_{\varphi(n)}\}$ est aussi un système réduit de résidus modulo n. On peut donc écrire

$$\prod_{i=1}^{\varphi(n)} ar_i \equiv \prod_{i=1}^{\varphi(n)} r_i \ (\mathrm{mod}\, n).$$

On a donc

$$a^{\varphi(n)} \prod_{i=1}^{\varphi(n)} r_i \equiv \prod_{i=1}^{\varphi(n)} r_i \ (\mathrm{mod}\, n).$$

Puisque $(m, \prod_{i=1}^{\varphi(n)} r_i) = 1$, on peut conclure que

$$a^{\varphi(n)} \equiv 1 \ (\mathrm{mod}\, n),$$

d'où la conclusion. □

2.6 Congruences vérifiées par les quotients de Fermat : Théorèmes d'Eisenstein (1850) de Glaisher (1900), Granville (2004), Dichler et Skula (2006)

Soit p un nombre premier et $a \in \mathbb{Z} - p\mathbb{Z}$, alors on sait d'après le petit théorème de Fermat que $a^{p-1} - 1 \equiv 0 \pmod p$. Il en résulte que $\frac{a^{p-1}-1}{p} \in \mathbb{Z}$. On est amené à la définition suivante

Définition 51 *Pour tout nombre premier p et pour tout entier $a \in \mathbb{Z} - p\mathbb{Z}$, le nombre entier $q_p(a)$ défini par*

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

est appelé quotient de Fermat de p en base a.

Dans [43], A. Granville a souligné le rôle important que jouent les quotients de Fermat dans l'étude des corps cyclomotiques et dans l'étude du grand théorème de Fermat. Les congruences vérifiées par les quotients de Fermat de 2 en base p, où p est un nombre premier impair, c'est à dire les $q_p(2)$, ont fait l'objet de nombreuses études.

Selon G. H. Hardy et E. M. Wright [45], le théorème suivant est du à Eisenstein. Il montre que le quotient de Fermat $q_p(2)$ est congru modulo p à la somme des inverses des entiers impairs $\leqslant p - 1$.

Théorème 52 *(Eisenstein 1850) Si p est un nombre premier impair, alors*

$$q_p(2) = \frac{2^{p-1} - 1}{p} \equiv 1 + \frac{1}{3} + \frac{1}{5} + \cdots + \frac{1}{p-2} \pmod p. \tag{2.36}$$

Corollaire 53 *Si p est un nombre premier impair, alors*

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

Corollaire 54 *Si p est un nombre premier impair, alors*

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

Le lemme qui suit montre que modulo p, l'étude de la somme $1 + \frac{1}{3} + \frac{1}{5} + \cdots + \frac{1}{p-2}$ se ramène à l'étude de la somme alternée $1 - \frac{1}{2} + \frac{1}{3} + \cdots - \frac{1}{p-1}$.

Lemme 55 *Si p est un nombre premier impair, alors*

$$H_{p-1} = 1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{p-1} \equiv 0 \pmod{p}. \tag{2.37}$$

et

$$1 - \frac{1}{2} + \frac{1}{3} + \cdots - \frac{1}{p-1} \equiv 2(1 + \frac{1}{3} + \frac{1}{5} + \cdots + \frac{1}{p-2}) \pmod{p}. \tag{2.38}$$

Preuve. En effet, il suffit de remarquer que l'on a

$$\begin{aligned} 1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{p-1} &= \sum_{k=1}^{(p-1)/2} \frac{1}{k} + \sum_{k=(p+1)/2}^{p-1} \frac{1}{k} \\ &= \sum_{k=1}^{(p-1)/2} \frac{1}{k} + \sum_{k=1}^{(p-1)/2} \frac{1}{p-k} \\ &= \sum_{k=1}^{(p-1)/2} \frac{p}{k(p-k)} \\ &\equiv 0 \ (\mathrm{mod}\, p). \end{aligned}$$

La relation (2.37) est établie. On obtient alors la relation (2.38) en observant que l'on a alors

$$1 - \frac{1}{2} + \frac{1}{3} + \cdots - \frac{1}{p-1} = 2(1 + \frac{1}{3} + \frac{1}{5} + \cdots + \frac{1}{p-2}) - (1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{p-1}).$$

□

Preuve. Nous sommes en mesure de prouver maintenant le théorème 52 les corollaires (53) et (54). On sait, daprès le théorème 37 que

$$\binom{p}{k} \equiv 0 \pmod{p} \text{ pour } 1 \leq k \leq p-1.$$

Il existe donc des entiers x_1, $x_{2,}...,x_{p-1}$ tels que

$$\binom{p}{k} = px_k \text{ pour } 1 \leq k \leq p-1.$$

On a

$$\begin{aligned} k!x_k &= (p-1)(p-2)...(p-k+1) \\ &\equiv (-1)^{k-1}\ (k-1)! \pmod{p}, \end{aligned}$$

ou encore

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

D'où

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

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

Il en résulte que

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

ou encore

$$2\frac{2^{p-1}-1}{p} \equiv \sum_{k=1}^{p-1}(-1)^{k-1}\frac{1}{k} \pmod p. \tag{2.39}$$

D'après la relation (2.38) du 55, on a

$$\sum_{k=1}^{p-1}(-1)^{k-1}\frac{1}{k} \equiv 2(1+\frac{1}{3}+\frac{1}{5}+\cdots+\frac{1}{p-2}) \pmod p. \tag{2.40}$$

On déduit ainsi de (2.39) et (2.40) que

$$2\frac{2^{p-1}-1}{p} \equiv 2(1+\frac{1}{3}+\frac{1}{5}+\cdots+\frac{1}{p-2}) \pmod p \tag{2.41}$$

Comme p est impair, on peut diviser par 2 les deux membres de (2.41). On obtient ainsi la relation (2.36) du théorème 52. Le corollaire 53 a aussi éte prouvé ; c'est la relation (2.39). Remarquons que l'on

$$1-\frac{1}{2}+\frac{1}{3}+\cdots-\frac{1}{p-1} = H_{p-1} - H_{(p-1)/2}. \tag{2.42}$$

En effet, on a

$$\begin{aligned} 1-\frac{1}{2}+\frac{1}{3}+\cdots-\frac{1}{p-1} &= (1+\frac{1}{2}+\frac{1}{3}+\cdots+\frac{1}{p-1}) - 2(\frac{1}{2}+\frac{1}{4}+\cdots+\frac{1}{p-1}) \\ &= (1+\frac{1}{2}+\frac{1}{3}+\cdots+\frac{1}{p-1}) - (1+\frac{1}{2}+\frac{1}{3}+\cdots+\frac{1}{(p-1)/2}). \end{aligned}$$

Comme d'après la relation 2.37, on a $H_{p-1} \equiv 0 \pmod p$ et que d'après le corollaire 53 $1-\frac{1}{2}+\frac{1}{3}+\cdots-\frac{1}{p-1} \equiv 2q_p(2) \pmod p$, on déduit de (2.42) que l'on a

$$H_{(p-1)/2} \equiv -2q_p(2) (\mathrm{mod}\, p).$$

Signalons que cette relation sera ameliorée par E. Lehmer qui prouva que pour tout nombre premier impair p, on a

$$H_{(p-1)/2} \equiv -2q_p(2) + pq_p(2)^2 \pmod{p^2}. \tag{2.43}$$

□

En 1900, J. W. L. Glaisher établit le résultat suivant qui comme le théorème d'Eisenstein concerne une congruence modulo p pour $q_p(2)$

Théorème 56 *(J. W. L. Glaisher,* 1900) *Pour tout nombre premier p impair, on a*

$$q_p(2) = \frac{2^{p-1}-1}{p} \equiv -\frac{1}{2}(\frac{2^1}{1} + \frac{2^2}{2} + \cdots + \frac{2^{p-1}}{p-1}) \pmod{p}. \tag{2.44}$$

Nous donnerons aussi une preuve détaillée de ce théorème, après l'énoncé des théorèmes 56 et 57 qui suivent.

En 2004, répondant à une conjecture de Skula, A. Granville [43], prouve le résultat suivant

Théorème 57 *Pour tout nombre premier p, on a*

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

En 2006, K. Dichler et L. Skula prouvent (cf l'article de A. Granville [43]) que

Théorème 58 *Pour tout nombre premier $p \geqslant 5$, on a*

$$(q_p(2))^3 = (\frac{2^{p-1}-1}{p})^3 \equiv -3(\frac{2^1}{1^3} + \frac{2^2}{2^3} + \cdots + \frac{2^{p-1}}{(p-1)^3}) + \frac{7}{4}\sum_{j=1}^{p-1}\frac{(-1)^j}{j^3} \pmod{p}.$$

ou de manière équivalente

$$(q_p(2))^3 = (\frac{2^{p-1}-1}{p})^3 \equiv -3(\frac{2^1}{1^3} + \frac{2^2}{2^3} + \cdots + \frac{2^{p-1}}{(p-1)^3}) + \frac{7}{16}\sum_{j=1}^{(p-1)/2}\frac{1}{j^3} \pmod{p}.$$

Dans ce qui suit, nous allons donner une démonstration du théorème de Glaisher. Celle ci repose sur le lemme suivant

Lemme 59 *Pour tout nombre réel x, et pour tout entier $n \geqslant 1$, on a*

$$\frac{x}{1} + \frac{x^2}{2} + \cdots + \frac{x^{n-1}}{n-1} = \sum_{k=1}^{n-1}\binom{n-1}{k}\frac{(x-1)^k - (-1)^k}{k} \tag{2.45}$$

Nous prouvons le lemme 59 en fin de démonstration du théorème 56. Soit p un nombre premier impair. Pour $n = p$ et $x = 2$, le lemme 60 fournit la relation

$$\frac{2^1}{1} + \frac{2^2}{2} + \cdots + \frac{2^{p-1}}{p-1} = \sum_{k=1}^{p-1}\binom{p-1}{k}\frac{1-(-1)^k}{k}. \tag{2.46}$$

Il est alors facile de constater que l'on a pour $1 \leqslant k \leqslant p-1$:

$$\binom{p-1}{k} = \frac{(p-1)(p-2)...(p-k)}{k!} \equiv \frac{(-1)^k k!}{k!} \equiv (-1)^k \pmod{p}. \tag{2.47}$$

Compte tenu de (2.47), la relation (2.46) devient

$$\frac{2^1}{1}+\frac{2^2}{2}+\cdots+\frac{2^{p-1}}{p-1}\equiv\sum_{k=1}^{p-1}(-1)^k\frac{1-(-1)^k}{k}\equiv\sum_{k=1}^{p-1}\frac{(-1)^k}{k}-\sum_{k=1}^{p-1}\frac{1}{k}\ (\mathrm{mod}\,p). \tag{2.48}$$

Compte tenu de la relation (2.37) du lemme 55 et du corollaire 53, on déduit de (2.48) que :

$$\frac{2^1}{1}+\frac{2^2}{2}+\cdots+\frac{2^{p-1}}{p-1}\equiv -2q_p(2)\ (\mathrm{mod}\,p). \tag{2.49}$$

la relation 2.44 en résulte.Le théorème de Glaisher est prouvé. Pour que cette preuve soit complète, il nous reste à prouver le lemme 59.

Preuve du lemme 59 : Soit G la fonction réelle d'une variable réelle définie pour tout x réel par :

$$G(x):=\frac{x}{1}+\frac{x^2}{2}+\cdots+\frac{x^{n-1}}{n-1}. \tag{2.50}$$

On a pour x réel, la dérivée de G s'écrit

$$G'(x):=1+x+x^2+\cdots+x^{n-2}. \tag{2.51}$$

Pour $x\neq 1$, on a

$$\begin{aligned} G'(x) &= \frac{x^{n-1}-1}{x-1} \\ &= \frac{1}{x-1}((1+(x-1))^{n-1}-1) \\ &= \frac{1}{x-1}(\sum_{k=1}^{n-1}\binom{n-1}{k}(x-1)^k) \\ &= \sum_{k=1}^{n-1}\binom{n-1}{k}(x-1)^{k-1}. \end{aligned} \tag{2.52}$$

Ainsi, on a obtenu pour $x\neq 1$,

$$G'(x)=\sum_{k=1}^{n-1}\binom{n-1}{k}(x-1)^{k-1}. \tag{2.53}$$

La relation (2.53) est encore vérifiée pour $x=1$, car d'une part on a d'après (2.51) :

$$G'(1)=n-1.$$

D'autre part, le second membre de (2.53) vaut

$$\sum_{k=1}^{n-1}\binom{n-1}{k}(1-1)^{k-1}=\binom{n-1}{1}=n-1.$$

La realtion (2.53) étant vérifiée pour tout x réel on obtient par intégration

$$G(x) = \sum_{k=1}^{n-1} \binom{n-1}{k} \frac{(x-1)^k}{k} + C, \tag{2.54}$$

où C est une constante. Comme d'après (2.50), on a $G(x) = 0$, on en déduit que

$$C = -\sum_{k=1}^{n-1} \binom{n-1}{k} \frac{(-1)^k}{k}. \tag{2.55}$$

De (2.54) et (2.55), découle la relation

$$G(x) = \sum_{k=1}^{n-1} \binom{n-1}{k} \frac{(x-1)^k - (-1)^k}{k}$$

Soit

$$\frac{x}{1} + \frac{x^2}{2} + \cdots + \frac{x^{n-1}}{n-1} = \sum_{k=1}^{n-1} \binom{n-1}{k} \frac{(x-1)^k - (-1)^k}{k}$$

la preuve du lemme 59 est ainsi établie. La preuve du théorème de Glaisher est complète.

2.7 Théorème de Charles Babbage (1819)

En 1819, soit à peine 18 ans après la parution du fameux livre de Gauss "Diquisiones Arithmeticae", Charles Babbage enonce et démontre le théorème suivant

Théorème 60 *Pour tout nombre premier $p \geq 3$*

$$\binom{2p-1}{p-1} \equiv 1 \pmod{p^2}$$

Preuve. Dans la preuve qu'il donne dans [11], voici ce que Charles Babbage affirme au tout début de son article

"The singular theorem of Wilson respecting Prime Numbers, which was first published by Waring in his Mediationes Analyticoe, and to which neither himself nor its autor could supply the demonstration, excited the attention of the most celebrated analysts of the continent, and the labours of Lagrange and Euler we are indebted for several modes of proof ; and more recently it has been considerably extended by the profound investigations contained in the Disquisitiones Arithmeticae.

It is well know that, in the theorem in question, a certain expression is aserted to be divisible by n, whenever that number is a prime, but it is not divisible if n is not prime. In attempting

to discover some analogous expression which should be divisible by n^2, Whenever n is a prime, but not divisible if n is a composite number, I met with those properties of primes which form the subject of the present paper.

The theorem of Wilson asserts that

$$1.2.3...(n-1)+1$$

is always divible by n when n is a prime number, otherwise it is not. The theorem which I have arrived at is as follows,

$$\frac{(n+1).(n+2).(n+3)...(2n-1)}{1.2.3...(n-1)}-1$$

is always divible by n^2 when n is a prime number, otherwise it is not."

Ce qu'on pourrait traduire comme suit :

"Le théorème de Wilson relatif aux nombres premiers, qui a d'abord été publiée par Waring dans son ouvrage "Mediationes Analyticoe", et pour lequel ni lui ni son auteur n'avait pu fournir de démonstration, a excité l'attention des analystes les plus célèbres du continent. Plusieures preuves de ce théorème sont maintenant dues à Lagrange et Euler, et plus récemment, des extensions considérables ce théorème ont été obtenues dans *Arithmeticae Disquisitiones*.

Il est bien connu que, dans le théorème en question, il est affirmé qu'une certaine expression est divisible par n, chaque fois que ce nombre est un nombre premier mais n'est pas divisible par n si n n'est pas premier. En essayant de découvrir une expression analogue qui doit être divisible par n^2, chaque fois que n est un nombre premier, mais pas divisible par n^2 si n est un nombre composé, j'ai rencontré les propriétés des nombres premiers qui font l'objet du présent document. □

Le théorème de Wilson affirme que

$$1.2.3...(n-1)+1$$

est toujours divisible par n où n est un nombre premier, sinon il n'est pas. Le théorème auquel je suis parvenu s'énonce comme suit

$$\frac{(n+1).(n+2).(n+3)...(2n-1)}{1.2.3...(n-1)}-1$$

est toujours divisible par n^2 où n est un nombre premier, sinon il n'est pas. "

Charles Babbage commence par énoncer un résultat bien connu

Lemme 61 *Pour tout entier naturel n, on a*

$$\sum_{k=0}^{n}\binom{n}{k}^2=\binom{2n}{n}$$

Preuve. *Ce lemme est en fait un cas particulier d'un produit de convolution de Chu-Van der Monde ; il est facile de constater que*

$$\sum_{i+j=p} \binom{n}{i}\binom{m}{j} = \binom{n+m}{p}.$$

C'est un résultat qu'on obtient aisément en égalant les coefficients de x^p dans $(1+x)^n(1+x)^m$ et $(1+x)^{n+m}$. Le lemme s'en déduit en considérant le cas particulier où $m = p = n$ et en remarquant que $\binom{n}{i} = \binom{n}{j}$ pour $i + j = n$. □

Démonstration du théorème de Babbage

Soit un nombre premier $p \geq 3$, on a d'après le lemme 61 :

$$\binom{2p-1}{p-1} \equiv 1 \pmod{p^2}$$

$$\begin{aligned}\binom{2p}{p} &= \sum_{k=0}^{p} \binom{p}{k}^2 \\ &= 2 + \sum_{k=1}^{p-1} \binom{p}{k}^2. \end{aligned} \tag{2.56}$$

Or on sait d'après le théorème 37 que

$$\binom{p}{k} \equiv 0 \bmod p, \text{ pour tout } k \in \{1, 2, ..p-1\} \ .$$

On en déduit que

$$\binom{p}{k}^2 \equiv 0 \bmod p^2, \text{ pour tout } k \in \{1, 2, ..p-1\} \ .$$

Par conséquent, on a avec (2.56)

$$2\binom{2p-1}{p-1} \equiv 2 \mod p^2. \tag{2.57}$$

Comme $p \geq 3$, p est impair et on déduit de (2.57) que

$$\binom{2p-1}{p-1} \equiv 1 \mod p^2.$$

Ce qui termine la démonstration du théorème de Babbage.

2.8 Congruences de Kummer (1851) et de Zhi-Hong Sun (2000) pour les nombres de Bernoulli

En 1851, Kummer prouve les célèbres congruences suivantes (cf page 541 de [87])

Théorème 62 *Soit $n \geqslant 1$ un entier et $p > 3$ un nombre premier tel que $p-1$ ne divise pas $2n$, alors on a*

$$\frac{B_{2n+p-1}}{2n+p-1} \equiv \frac{B_{2n}}{2n} = 0 \pmod p$$

De ce theorème résulte le corollaire immédiat suivant

Corollaire 63 *Soit $n \geqslant 1$ un entier et $p > 3$ un nombre premier tel que $p-1$ ne divise pas $2n$, alors on a*

$$\frac{B_{2n+k(p-1)}}{2n+k(p-1)} \equiv \frac{B_{2n}}{2n} \pmod p \quad \textit{pour} \quad k = 0, 1, 2, ...$$

En 2000, Zhi-Hong Sun [102] a généralisé les congruences de Kummer

Théorème 64 *Soit $n \geqslant 1$ un entier et $p > 3$ un nombre premier tel que $p-1$ ne divise pas $2n$, alors on a*

$$\frac{B_{2n+k(p-1)}}{2n+k(p-1)} \equiv k\frac{B_{2n+p-1}}{2n+p-1} - (k-1)(1-p^{2n-1})\frac{B_{2n}}{2n} \pmod{p^2} \quad \textit{pour} \quad k = 0, 1, 2, ...$$

et

$$\begin{aligned} \frac{B_{2n+k(p-1)}}{2n+k(p-1)} &\equiv \binom{k}{2} k\frac{B_{2n+2(p-1)}}{2n+2(p-1)} - k(k-2)\frac{B_{2n+p-1}}{2n+p-1} + \binom{k-1}{2}(1-p^{2n-1})\frac{B_{2n}}{2n} \pmod{p^3} \\ \textit{pour} \quad k &= 0, 1, 2, ... \end{aligned}$$

Ces résultats lui permettent d'obtenir

Théorème 65 *Soit $p > 3$ un nombre premier. Alors pour $k = 1, 2, ...; p-4$, on a*

$$\sum_{x=1}^{p-1} \frac{1}{x^k} \equiv \begin{cases} \binom{k+1}{2}\frac{B_{p-2-k}}{p-2-k}p^2 \pmod{p^3} & \textit{si } k \textit{ est impair,} \\ k(\frac{B_{2p-2-k}}{2p-2-k} - 2\frac{B_{p-1-k}}{p-1-k})p \pmod{p^3} \textit{pour tout } n \geqslant 1 & \textit{si } k \textit{ est pair.} \end{cases}$$

En choisisant $k = 1$, on trouve

Corollaire 66

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

Remarque 67 *Ce dernier résultat, comme le souligne Zhi-Hong Sun implique le théorème de Wolstenholme.*

En choisissant $k = 3$, on trouve

Corollaire 68 *Pour tout nombre premier $p > 5$, on a*

$$1 + \frac{1}{2^3} + \frac{1}{3^3} + \cdots + \frac{1}{(p-1)^3} \equiv -\frac{6}{5}p^2 B_{p-5} \pmod{p^3}$$

Remarque 69 *Les résultats précédents vont amener Zhi Wei Sun à formuler la conjecture A30 chapitre consacrée à certaines conjectures de ce mèmoire*

2.9 Théorème de Kummer (1852)

Avant d'énoncer et de prouver ce célèbre et classique théorème de Kummer datant de 1852, qui est relatif à la valuation p-adique du coefficient binomial $\binom{n}{m}$, précisons ce que l'on entend quand on parle de "retenues" dans l'addition de deux entiers écrits en base p.

Soient a , b et c trois entiers naturels tels que $c = a + b$ et dont les décomposition en base p, où $p \geqslant 2$ est supposé être un entier qui pour le moment n'est pas nécessairemet un nombre premier, s'écrivent

$$\begin{aligned} a &= a_0 + a_1 p + a_2 p^2 + a_3 p^3 + ... \\ b &= b_0 + b_1 p + b_2 p^2 + b_3 p^3 + ... \\ c &= c_0 + c_1 p + c_2 p^2 + c_3 p^3 + ... \end{aligned}$$

où a_i ,b_i , $c_i \in \{0, 1, ...p-1\}$ pour tout $i \geqslant 0$. c étant la somme de a et b,on a les relations suivantes

$$a_0 + b_0 = c_0 + \varepsilon_0 p,$$

où

$$\varepsilon_0 := \begin{cases} 0 & \text{si } a_0 + b_0 \leqslant p-1 \\ 1 & \text{sinon} \end{cases} .$$

On a ensuite

$$\varepsilon_0 + a_1 + b_1 = c_1 + \varepsilon_1 p,$$

avec

$$\varepsilon_1 := \begin{cases} 0 & \text{si } \varepsilon_0 + a_1 + b_1 \leqslant p-1 \\ 1 & \text{sinon} \end{cases} .$$

De manière générale, en posant

$$\varepsilon_{-1} := 0,$$

on définit $.\varepsilon_i$ pour $i \geq 1$ par la relation

$$\varepsilon_{i-1} + a_i + b_i = c_1 + \varepsilon_i p \tag{2.58}$$

avec

$$\varepsilon_i := \begin{cases} 0 & \text{si } \varepsilon_{i-1} + a_i + b_i \leqslant p-1 \\ 1 & \text{sinon} \end{cases}.$$

Alors le nombre de retenues dans l'addition de a et b est par définition le nombre d'entiers ε_i non nuls, c'est donc $\sum_{i\geq 0} \varepsilon_i$.

Soient maintenant p un nombre premier et n et m des entiers naturels tels que $n \geq m$ Posons

$$a = m, \quad b = n - m, \quad c = n.$$

On a $a + b = c$. Avec les notations et définitions donnés plus haut on a le théorème suivant donnée par Kummer en 1852.

Théorème 70 *Kummer (1852) Soit p un nombre premier et n et m des entiers naturels tels que $n \geq m$. Alors l'exposant de la plus grande puissance de p qui divise le coefficient binomial $\binom{n}{m}$ est égal au nombre de retenues dans l'addition de m et $n-m$ en base p.*

$$v_p(\binom{n}{m}) = \sum_{i\geq 0} \varepsilon_i \tag{2.59}$$

Preuve. Par application de la propostion 36, on a

$$\begin{aligned} v_p(\binom{n}{m}) &= \frac{s_p(m) + s_p(n-m) - s_p(n)}{p-1} \\ &= \frac{1}{p-1}(\sum_{i\geq 0} a_i + \sum_{i\geq 0} b_i - \sum_{i\geq 0} c_i) \\ &= \frac{1}{p-1} \sum_{i\geq 0} (a_i + b_i - c_i) \end{aligned}$$

A l'aide de la relation (2.58) on a alors

$$\begin{aligned} v_p(\binom{n}{m}) &= \frac{1}{p-1} \sum_{i\geq 0} (\varepsilon_i p - \varepsilon_{i-1}) \\ &= \frac{1}{p-1}(\sum_{i\geq 0} \varepsilon_i)p - (\sum_{i\geq 0} \varepsilon_{i-1})) \\ &= \sum_{i\geq 0} \varepsilon_i. \end{aligned}$$

La relation (2.59) est prouvée. La preuve du théorème de Kummer est complète. □

Exemple 71 *Calculons* $v_3(\binom{1702}{14})$ *de deux manières différentes*

1. *En appliquant la formule de Legendre*
2. *En appliquant le theorème de Kummer*

Solution 72 *On a*

1. *En appliquant la formule de Legendre*

$$\begin{aligned} v_3(\binom{1702}{14}) &= v_3(\frac{1702!}{14!1688!}) \\ &= v_3(1702!) - v_3(14!) - v_3(1688!). \end{aligned}$$

Le calcul de $v_3(1702!)$, $v_3(14!)$ *et* $v_3(1688!)$ *s'effectuent à l'aide de la formule de Legendre*

$$\begin{aligned} v_3(1702!) &= \sum_{k=1}^{\infty} \left\lfloor \frac{1702}{3^k} \right\rfloor \\ &= \sum_{k=1}^{6} \left\lfloor \frac{1702}{3^k} \right\rfloor \\ &= 849. \end{aligned}$$

$$\begin{aligned} v_3(14!) &= \sum_{k=1}^{\infty} \left\lfloor \frac{14}{3^k} \right\rfloor \\ &= \sum_{k=1}^{2} \left\lfloor \frac{14}{3^k} \right\rfloor \\ &= 5. \end{aligned}$$

$$\begin{aligned} v_3(1688!) &= \sum_{k=1}^{\infty} \left\lfloor \frac{1688}{3^k} \right\rfloor \\ &= \sum_{k=1}^{6} \left\lfloor \frac{1688}{3^k} \right\rfloor \\ &= 839. \end{aligned}$$

Ainsi

$$\begin{aligned} v_3(\binom{1702}{14}) &= v_3(1702!) - v_3(14!) - v_3(1688!) \\ &= 849 - 5 - 839 \end{aligned}$$

Soit

$$v_3(\binom{1702}{14}) = 5.$$

2. En appliquant le théorème de Kummer, on retrouve bien le même résultat. on a

$$\begin{aligned} 14 &= 2+1.3+1.3^2 \\ 1688 &= 2+1.3+1.3^2++\,2.3^3+2.3^4+2.3^6 \\ 1702 &= 1+1.3^5+2.3^6 \end{aligned}$$

et

$$\begin{array}{rcccccccc} \textit{reports}\ \varepsilon_i & : & & 1 & 1 & 1 & 1 & 1 & \\ m\ =14 & : & 2 & +1\times 3 & +1\times 3^2 & +0\times 3^3 & +0\times 3^4 & +0\times 3^5 & +0\times 3^6 \\ n-m=1688: & & 2 & +1\times 3 & +1\times 3^2 & +2\times 3^3 & +2\times 3^4 & +0\times 3^5 & +2\times 3^6 \\ n=1702: & & 1 & +0\times 3 & +0\times 3^2 & +0\times 3^3 & +0\times 3^4 & +1\times 3^5 & +2\times 3^6 \end{array}$$

On a

$$\varepsilon_1 = \ \varepsilon_2=1\ \ \varepsilon_3=1\ \ \varepsilon_4=1\ \ \varepsilon_5=1\ \ \varepsilon_6=\ \ \varepsilon_7=\ \ 0,\ \ \varepsilon_i=0 \textit{ pour } i\geq 7$$

et

$$v_3(\binom{1702}{14})=\sum_{i\geq 0}\varepsilon_i=5.$$

2.10 Théorème de Wolstenholme (1862)

En 1862, Wostenholme énonce un théorème qu'il obtient par des investigations numériques

Théorème 73 *Pour tout nomnbre premier $p\geq 5$, on a*

1. Le numérateur de

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

est divisible par p^2. Autrement dit

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

2. Le numérateur de

$$1+\frac{1}{2^2}+\frac{1}{3^2}+\cdots+\frac{1}{(p-1)^2}$$

est divisible par p. Autrement dit

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

3. On a

$$\binom{2p-1}{p-1}\equiv 1\ (\mathrm{mod}\, p^3). \tag{2.60}$$

2.10.1 La preuve de Wolstenholme revisitée

Dans un récent article [16], 2009, M. Chamberland et K. Dichler précisent que de la congruence (2.60) présente un intérêt particulier du fait qu'aucun nombre composé vérifiant cette congruence n'est connu et que de plus la réciproque du théorème de Wolstenholme semble être un problème difficile.

Pour prouver ce thèorème, nous allons donner un nouvel éclairage de la démonstration de wolstenholme donnée en 1862. Nous suivrons la démarche de Wolstenholme mais en simplifiant certains passages de sa démonstration. Ce dernier commence par énoncer et prouver un lemme "bien connu"

Lemme 74 *Pour tout entier $n \geq 1$, on a*

$$1+\frac{1}{2}+\frac{1}{3}+\cdots+\frac{1}{n}=\sum_{k=1}^{n}\frac{(-1)^{k-1}}{k}\binom{n}{k}$$

Preuve. Posons pour tout entier $n \geq 1$

$$f(n)=\sum_{k=1}^{n}\frac{(-1)^{k-1}}{k}\binom{n}{k}.$$

On a alors pour $n \geq 2$,

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

Il en résulte que

$$\begin{aligned} f(n) &= f(1) + \sum_{k=2}^{n} (f(k) - f(k-1)) \\ &= 1 + \sum_{k=2}^{n} \frac{1}{k} \\ &= 1 + \frac{1}{2} + \frac{1}{3} + ... + \frac{1}{n}. \end{aligned}$$

Autrement dit

$$f(n) = H_n$$

ce qui établit le résultat du lemme.

1. Wolstenholme exploite le lemme comme suit. Soit p un nombre premier ≥ 5, alors on a d'après le lemme précédent

$$\begin{aligned} H_{p-1} &= \sum_{k=1}^{p-1} \frac{(-1)^{k-1}}{k} \binom{p-1}{k} \\ &= \sum_{k=1}^{p-1} (-1)^{k-1} \frac{(p-1)!}{k!(p-k)!} \frac{p-k}{k} \end{aligned} \tag{2.61}$$

En changeant l'indice de sommation k en $p-k$ dans (2.61), on obtient

$$\begin{aligned} H_{p-1} &= \sum_{k=1}^{p-1} (-1)^{p-k-1} \frac{(p-1)!}{k!(p-k)!} \frac{k}{p-k}, \\ &= -\sum_{k=1}^{p-1} (-1)^{p-k} \frac{(p-1)!}{k!(p-k)!} \frac{k}{p-k}. \end{aligned} \tag{2.62}$$

Il en résulte qu'en sommant membre à membre (2.61) et (2.62), on trouve

$$\begin{aligned} 2H_{p-1} &= \sum_{k=1}^{p-1} (-1)^{k-1} \frac{(p-1)!}{k!(p-k)!} \left\{ \frac{p-k}{k} - \frac{k}{p-k} \right\}, \\ &= \sum_{k=1}^{p-1} (-1)^{k-1} \frac{(p-1)!}{k!(p-k)!} \frac{(p^2-2kp)}{k(p-k)} \\ &= \sum_{k=1}^{p-1} \frac{(-1)^{k-1}(p-1)(p-2)...(p-k+1)(p^2-2kp)}{k!k(p-k)}. \end{aligned}$$

Il est alors facile de constater que pour $k \in \{1, 2, ...p-1\}$, on a d'une part

$$\begin{aligned} (-1)^{k-1}(p-1)(p-2)...(p-k+1)(p^2-2kp) &\equiv -2(1-p)(2-p)...(k-1-p)kp \pmod{p^2} \\ &\equiv -2k!p \pmod{p^2}, \end{aligned}$$

et d'autre part,

$$(k!k(p-k), p) = 1.$$

Il en résulte que

$$\begin{aligned} 2H_{p-1} &= \sum_{k=1}^{p-1} \frac{(-1)^{k-1}(p-1)(p-2)...(p-k+1)(p^2-2kp)}{k!k(p-k)} \\ &\equiv \sum_{k=1}^{p-1} \frac{-2k!p}{k!k(p-k)} \pmod{p^2} \\ &\equiv -2\sum_{k=1}^{p-1} \frac{p}{k(p-k)} \pmod{p^2}. \end{aligned} \tag{2.63}$$

En remarquant que l'on a

$$\begin{aligned} \sum_{k=1}^{p-1} \frac{p}{k(p-k)} &= \sum_{k=1}^{p-1} \frac{k+(p-k)}{k(p-k)} \\ &= \sum_{k=1}^{p-1} \frac{1}{p-k} + \frac{1}{k} \\ &= \sum_{k=1}^{p-1} \frac{1}{p-k} + \sum_{k=1}^{p-1} \frac{1}{k} \\ &= 2H_{p-1}, \end{aligned} \tag{2.64}$$

on déduit de (2.63) et (2.64)

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

soit

$$6H_{p-1} \equiv 0 \pmod{p^2}. \tag{2.65}$$

Si on suppose $p \geqslant 5$, on a alors

$$(6, p^2) = 1,$$

ce qui avec la relation(2.65) permet de conclure

$$H_{p-1} \equiv 0 \pmod{p^2}.$$

2. La demonstration repose sur les deux lemmes suivants

Lemme 75 *Soient $x_{1,}x_{2,}x_{3,}..., x_n$ des nombres complexes, alors, on a*

$$\sum_{k=1}^{n} x_k^2. = (\sum_{k=1}^{n} x_k)^2 - \sum_{r=1}^{n}(x_r((\sum_{\substack{k=1 \\ k\neq r}}^{n} x_k))).$$

□

Preuve. Il suffit de remarquer que

$$\begin{aligned}\sum_{r=1}^{n}(x_r((\sum_{\substack{k=1\\k\neq r}}^{n}x_k))) &= \sum_{r=1}^{n}(x_r((\sum_{k=1}^{n}x_k)-x_r))\\ &= (\sum_{r=1}^{n}x_r)(\sum_{k=1}^{n}x_k)-\sum_{r=1}^{n}x_r^2\\ &= (\sum_{k=1}^{n}x_k)^2-\sum_{r=1}^{n}x_r^2.\end{aligned}$$

□

Lemme 76 *Pour tout nombre impair n, on a*

$$H_{n-1}=\sum_{k=1}^{(n-1)/2}\frac{n}{k(n-k)}$$

Preuve. On a

$$\begin{aligned}H_{n-1} &= \sum_{k=1}^{n-1}\frac{1}{k}\\ &= \sum_{k=1}^{(n-1)/2}\frac{1}{k}+\sum_{k=(n+1)/2}^{n-1}\frac{1}{k}\\ &= \sum_{k=1}^{(n-1)/2}\frac{1}{k}+\sum_{k=1}^{(n-1)/2}\frac{1}{p-k}\\ &= \sum_{k=1}^{(n-1)/2}(\frac{1}{k}+\frac{1}{p-k})\\ &= \sum_{k=1}^{(n-1)/2}\frac{n}{k(n-k)}.\end{aligned}$$

□

En appliquant le lemme, avec $x_i=\frac{1}{i}$, on obtient

$$\begin{aligned}1+\frac{1}{2^2}+\frac{1}{3^2}+...+\frac{1}{(p-1)^2} &= (\sum_{k=1}^{p-1}\frac{1}{k})^2-\sum_{r=1}^{p-1}(\frac{1}{r}((\sum_{\substack{k=1\\k\neq r}}^{p-1}\frac{1}{k})))\\ &= H_{p-1}^2-\sum_{r=1}^{p-1}(\frac{1}{r}(H_{p-1}-\frac{1}{r}))\end{aligned}$$

Or, on a

$$H_{p-1} \equiv 0 \ (\mathrm{mod}\, p^2).$$

et

$$\begin{aligned} H_{p-1} - \frac{1}{r} &= \frac{1}{p-r} + \sum_{k=1}^{(p-1)/2} \frac{p}{k(n-k)} - (\frac{1}{r} + \frac{1}{p-r}) \\ &= \frac{1}{p-r} + \sum_{k=1}^{(p-1)/2} \frac{p}{k(n-k)} - \frac{p}{r(p-r)} \\ &= \frac{1}{p-r} + \sum_{\substack{k=1 \\ k\neq r}}^{(p-1)/2} \frac{p}{k(n-k)}. \end{aligned}$$

On en déduit que

$$H_{p-1} - \frac{1}{r} \equiv \frac{1}{p-r} \ (\mathrm{mod}\, p).$$

Par conséquent, on a

$$\begin{aligned} 1 + \frac{1}{2^2} + \frac{1}{3^2} + ... + \frac{1}{(p-1)^2} &= H_{p-1}^2 - \sum_{r=1}^{p-1} (\frac{1}{r}(H_{p-1} - \frac{1}{r})) \\ &\equiv -\sum_{r=1}^{p-1} \frac{1}{r(p-r)} \ (\mathrm{mod}\, p). \end{aligned} \tag{2.66}$$

Or

$$\begin{aligned} p\sum_{r=1}^{p-1} \frac{1}{r(p-r)} &= \sum_{r=1}^{p-1} \frac{r + (p-r)}{r(p-r)} \\ &= \sum_{r=1}^{p-1} \frac{1}{r} + \frac{1}{p-r} \\ &= 2H_{p-1} \\ &\equiv 0 \ (\mathrm{mod}\, p^2). \end{aligned}$$

On a donc

$$\sum_{r=1}^{p-1} \frac{1}{r(p-r)} \equiv 0 \ (\mathrm{mod}\, p) \tag{2.67}$$

Les relations (2.66) et (2.67) permettent de conclure

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

3. La preuve repose sur le résultat suivant :

Considérons le polynôme $P(x)$ de $\mathbb{Z}[x]$ défini par

$$P(x) = (x+1)(x+2)...(x+p-1),$$

en développant ce polynôme, on trouve

$$P(x) = x^{p-1} + a_{p-2}x^{p-2} + \cdots + a_2x^2 + a_1x + a_0,$$

avec

$$\begin{aligned} a_0 &= (p-1)!, \\ a_1 &= \sum_{i=1}^{p-1} \frac{(p-1)!}{i} \\ &= (p-1)!H_{p-1}, \end{aligned}$$

et

$$\begin{aligned} a_3 &= \sum_{1\leqslant<j\leqslant p-1} \frac{(p-1)!}{ij} \\ &= \frac{1}{2} \sum_{\substack{1\leqslant i\leqslant p-1 \\ 1\leqslant j\leqslant p-1 \\ i\neq j}} \frac{(p-1)!}{ij} \\ &= \frac{1}{2} \sum_{r=1}^{p-1} \frac{1}{r}(H_r - \frac{1}{r}). \end{aligned}$$

On a les relations de congruences suivantes

$$\begin{aligned} a_0 &\equiv (p-1)! \pmod{p^3} \\ a_1p &\equiv 0 \pmod{p^3} \\ a_2p^2 &\equiv 0 \pmod{p^3}. \end{aligned}$$

Il en résulte d'abord que

$$\begin{aligned} P(p) &\equiv a_2p^2 + a_1p + a_0 \pmod{p^3} \\ &\equiv (p-1)! \pmod{p^3} \\ \binom{2p-1}{p-1} &= \frac{(2p-1)(2p-2)...(p+1)}{(p-1)!} \\ &= \frac{(p+1)(p+2)...(p+(p-1))}{(p-1)!} \\ &= \frac{P(p)}{(p-1)!} \\ &\equiv \frac{(p-1)!}{(p-1)!} \pmod{p^3} \\ &\equiv 1 \pmod{p^3}. \end{aligned}$$

Ce qui achève la preuve du théorème de Wolstenholme.

Que peut-on dire concernant la réciproque du théorème de Wolstenholme ?

D'imminents chercheurs se sont posé la question sur la réciproque du théorème de Wolstenholme on citera R.J. MCIntosh[64] et Vilmar Trevisan .Kenneth Weber [96].

Signalons aussi que divers auteurs ont étudié la reciproque du théorème de Wolstenholme ,citons par exemple l'ouvrage de R.K.Guy [44] ;page84 et l'ouvrage de P.Ribenboim[83] ;page21

Voiçi ce que disent Vilmar Trevisan et Kenneth Weber dans un article intitulé "Testing the controverse of Wolsthholme's theorem" [96]

Afin de préserver l'autenthicité et l'originalité du texte ,nous avons préfère l'exposer dans sa langue d'origine sans traduction .

"(Wolstenholme,1862) if p is a prime number ,$p \geq 5$ then

$$\binom{2p-1}{P-1} \equiv 1(\mathrm{mod}\, p^3) \tag{2.68}$$

Apparently ,it was James .P.Jones [44] who first conjectured that the converse of this theorem is true ,namely that a naturel number p satisfying the congruence of property 2.68 is necessarily prime .The controverse of Wolstenholme's theorem is regarded as a very difficult problem.

In [64] R.J.McIntosh obtains restrictives conditions on n for solutions of

$$\binom{2n-1}{n-1} \equiv 1(\mathrm{mod}\, p^3)$$

and concludes that Wolstenholme's controverse is probably true .

For exemple ,he shows that if p is a prime number and $n = p^2$

satisfies la relation 2.68 (which would be a counterexample to the controverse) ,then p satisfies

$$\binom{2p-1}{p-1} \equiv 1(\mathrm{mod}\, p^6)$$

which is unlikely ;McIntosh also reports that the controverse is known to be true for all composite numbers $< 10^9$

No proof however has been obtained for the controverse of Wolstenholme's property.In section 3 we partially fill this gap ,by proving that property 2.68 does not hold for positive even numbers .This resultat is probably known to other authors who work on the subject ,but we are unaware of a published proof .

Moreover ,the proof we present uses only elementary mathématics .

For a given composite number n,to show that

$$\binom{2n-1}{n-1} \ncong 1(\mathrm{mod}\, n^3)$$

it suffices to show that

$$\binom{2n-1}{n-1} \ncong 1(\mathrm{mod}\, R)$$

where $R > 1$,R is any factor of n .

Using this idea ,we study the controverse of wolstenholme's theorem for powers of primes p,by determining the value of the binomial coefficient modulo $p^3, p^4$and p^5.

In section 4 we prove that if n is a power of 3,than it does not satisfy property 2.68,

providing that the controverse is true for $n = 3^{\,l}$.

Aditionally,we prove that if p is a prime number and $n = p^l$,$l \geq 2$ then

$$\binom{2n-1}{n-1} \equiv \binom{2p-1}{p-1}(\mathrm{mod}\, p^4) \tag{2.69}$$

which reduces the size of the computational task for testing the controverse .

Finally ,we claim that the controverse of Wolstenholme's theorem is true for all powers $p < \ 2.5 \times 10^8(\mathrm{sec}\, tion5)$, by using the criteria given by equation 2.69

2.10.2 Une généralisation du théorème de Wolstenholme

Nous allons prouver dans ce qui suit la généralisation suivante du théorème de Wolstenholme

Théorème 77 *Pour tout entier $r \geq 1$ et pour tout nombre premier $p \geq 5$,on a*

$$\binom{rp-1}{p-1} \equiv 1 \ (\mathrm{mod}\, p^3).$$

Pour $r = 2$, on retrouve le théorème de Wolsthenholme.

Preuve. Considérons l'application f de $\mathbb{Z}[x]$ dans $\mathbb{Z}/p\mathbb{Z}[x]$ définie qui à $P(x) = \sum a_n x^n$ associe $\overline{P}(x) = \sum \overline{a_n} x^n$ où $\overline{a_n} = a_n + p\mathbb{Z}$. Il est(facile de constater que f est un morphisme d'anneaux. Considérons alors le polynôme $x^p - x$ à coefficients dans le corps $\mathbb{Z}/p\mathbb{Z}$. D'après

le petit théorème de Fermat, le polynôme unitaire $x^p - x$ de degré p admet les $p-1$ élémemts de $\mathbb{Z}/p\mathbb{Z} - \left\{\overline{0}\right\}$ comme racines. Il en résulte que l'on a la factorisation suivante dans $\mathbb{Z}/p\mathbb{Z}\,[x]$

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

Posons

$$A_p(x)=(x-1)(x-2)..(x-(p-1)).$$

On a

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

où $s(n,k)$ sont entiers et sont des nombres de Stirling de première espèce. L'application f étant un morphisme d"anneaux, on en déduit que

$$\begin{aligned}\sum_{k=1}^{p} \overline{s(p,k)}x^{k-1} &= (x-\overline{1})(x-\overline{2})..(x-\overline{p-1}) \\ &= x^{p-1} - \overline{1}.\end{aligned}$$

Par identification des coefficients, on obtient les congruences

$$s(p,1) \equiv -1 \pmod{p} \tag{2.70}$$

et

$$s(p,k) \equiv 0 \pmod{p} \quad \text{pour } 2 \leq k \leq p-1.$$

On peut alors prouver une congruence plus forte pour $s(p,2)$. On a

$$s(p,2) \equiv 0 \pmod{p^2}. \tag{2.71}$$

En effet, on a

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

ce qui s'écrit

$$(p-1)! = s(p,1) + s(p,2)p^2 + \cdots + s(p,p)p^{p-1}. \tag{2.72}$$

Or

$$s(p,1) = (-1)^{p-1}(p-1)! = (p-1)!,$$

En simplifiant (2.72), on obtient

$$s(p,2) + s(p,3)p + \cdots + s(p,p)p^{p-2} = 0$$

Comme on a (pour $p \geq 5$)

$$s(p,3) \equiv 0 \pmod{p},$$

il en résulte la relation (2.71).

Pour tout entier $r \geq 1$, on a alors pour $p \geq 5$

$$\begin{aligned} A_p(rp) &= (rp-1)(rp-2)..(rp-(p-1)) = \sum_{k=1}^{p} s(p,k) r^{k-1} p^{k-1} \\ &\equiv s(p,1) + s(p,2)rp \pmod{p^3}. \end{aligned}$$

Comme on a

$$s(p,1) \equiv (p-1)! \text{ et } s(p,2) \equiv 0 \pmod{p^2} \tag{2.73}$$

et

$$((p-1)!, p^2) = 1,$$

on en déduit que

$$\frac{(rp-1)(rp-2)..(rp-(p-1))}{(p-1)!} \equiv 1 \pmod{p^3}$$

c'ést à dire

$$\binom{rp-1}{p-1} \equiv 1 \pmod{p^3}.$$

Remarquons que l'on a prouvé au passage les théorèmes de Wilson et de Wolstenholme. En effet la relation (2.70) et (2.73) impliquent la relation $(p-1)! \equiv -1 \pmod{p}$, ce qui est le théorème de Wilson. En remarquant que

$$s(p,2) = (p-1)!H_{p-1},$$

La relation (2.71) se traduit par

$$(p-1)!H_{p-1} \equiv 0 \pmod{p^2}.$$

En remarquant alors que $((p-1)!, p^2) = 1$, on en déduit que

$$\text{denom}(H_{p-1}) \equiv 0 \pmod{p^2},$$

ce qui est le théorème de Wolstenholme. □

Le corollaire suivant est une conséquence immédiate du théorème 77.

Corollaire 78 *Pour tout entier $r \geq 1$ et pour tout nombre premier $p \geq 5$,on a*

$$\binom{rp}{p} \equiv r \pmod{p^3}.$$

2.10.3 Une généralisation du théorème de Wolstenholme par Bayat (1997) et par Gessel (1998)

En 1997, Bayat 79 énonce le résultat suivant.

Théorème 79 *Soit p un nombre premier, n et k des entiers naturels tel que $k < p-2$. Alors le numérateur de la fraction*

$$\sum_{\substack{1\leq i\leq p^n\\(i,p)=1}} \frac{1}{i^k}$$

est divisible par p^n si k est pair et par p^{n+1} si k est impair.Autrement dit

Nous suivrons la preuve que Gessel a donné dans une généralisation de ce théorème [33]. Pour tous entiers $m \geq 2$ et $k \geq 1$, posons

$$\sigma(m,k) = \sum_{i\in R_m} \frac{1}{i^k},$$

où R_m est l'ensemble des nombres entiers compris entre 1 et $m-1$ et premiers avec m. R_m est un système réduit de résidus modolo m.La preuve du théorème 79 repose sur les deux lemmes suivants

Lemme 80 *Pour tout entiers $m \geq 2$, $k \geq 1$ et a tels que a soit premier avec m, on a*

$$(a^k-1)\sum_{i\in R_m} \frac{1}{i^k} \equiv 0 \pmod m \tag{2.74}$$

Preuve. En effet $\{ai;\ i \in R_m\}$ est un système réduit de résidus modulo m. Il en résulte que l'on a

$$\sigma(m,k) = \sum_{i\in R_m} \frac{1}{i^k} \equiv \sum_{i\in R_m} \frac{1}{(ai)^k} = \frac{1}{a^k}\sum_{i\in R_m} \frac{1}{i^k} = \frac{1}{a^k}\sigma(m,k) \pmod m.$$

Par conséquent, on a

$$\frac{(a^k-1)}{a^k}\sigma(m,k) \equiv 0 \pmod m.$$

La relation (2.74) en résulte. □

Lemme 81 *Pour tout entiers $m \geq 2$, $k \geq 1$ tels que k soit impair, on a*

$$2\sigma(m,k) \equiv -mk\sigma(m,k+1) \pmod{m^2} \tag{2.75}$$

Preuve. En effet, si k est impair, la formule du binôme nous permet d'écrire pour tout entier i

$$\begin{aligned} i^k + (m-i)^k &= i^k - (i-m)^k \\ &= i^k - (i^k + \binom{k}{1} i^{k-1}(-m) + \sum_{j=2}^{k} \binom{k}{j} i^{k-j}(-m)^j \\ &\equiv mki^{k-1} \pmod{m^2}. \end{aligned}$$

On a donc en remarquant que $\{m-i;\ i \in R_m\}$ est aussi un système réduit de résidus modulo m :

$$\begin{aligned} 2\sigma(m,k) &\equiv \sum_{i \in R_m} \frac{1}{i^k} + \frac{1}{(m-i)^k} \\ &= \sum_{i \in R_m} \frac{i^k + (m-i)^k}{i^k(m-i)^k} \\ &\equiv \sum_{i \in R_m} \frac{mki^{k-1}}{i^k(m-i)^k} \pmod{m^2} \\ &\equiv \sum_{i \in R_m} \frac{mk}{i(m-i)^k} \pmod{m^2} \end{aligned}$$

Remarquons que l'on a

$$\frac{1}{(m-i)^k} \equiv \frac{1}{(-i)^k} \pmod{m},$$

et donc

$$\frac{mk}{i(m-i)^k} \equiv \frac{mk}{i(-i)^k} \pmod{m}.$$

Ainsi

$$\begin{aligned} 2\sigma(m,k) &\equiv -mk \sum_{i \in R_m} \frac{1}{i^{k+1}} \\ &\equiv -mk\sigma(m,k+1) \pmod{m^2}. \end{aligned}$$

□

Preuve du théorème 79

Soit p un nombre premier, n et k des entiers naturels tel que $k < p-2$. On peut remarquer que l'on a

$$\sum_{\substack{1 \le i \le p^n \\ (i,p)=1}} \frac{1}{i^k} = \sigma(p^n, k)$$

Il est possible de trouver un entier a tel que $a^k - 1$ ne soit pas divisible par p. Il suffit de choisir a tel que $g = a + p\mathbb{Z}$ soit un générateur du groupe cyclique $\mathbb{Z}/p\mathbb{Z}$. Pour un tel entier a, on sait l'on a pour tout entier natrurel $a^n - 1 \equiv 0 \pmod p$ si et seulement si $p-1$ divise n. Comme par hypothèse on a $1 \leq k \leq p-2$, $p-1$ ne divise pas k et donc $a^k - 1 \neq 0 \pmod p$. L'application du lemme **??** nous founit la relation

$$(a^k - 1) \sum_{i \in R_{p^n}} \frac{1}{i^k} \equiv 0 \pmod{p^n}.$$

Comme p et premier avec $a^k - 1$, p^n est aussi premier avec $a^k - 1$. On en conclut que nécessairement p^n divise $\sum_{i \in R_{p^n}} \frac{1}{i^k}$. Autrement dit

$$\sum_{\substack{1 \leq i \leq p^n \\ (i,p)=1}} \frac{1}{i^k}.$$

Si k est impair. dans ce cas $2 \leq k+1 < p-1$. On a encore d'après ce qui précède

$$\sigma(p^n, k+1) = \sum_{\substack{1 \leq i \leq p^n \\ (i,p)=1}} \frac{1}{i^{k+1}} \equiv 0 \pmod{p^n}.$$

L'application du lemme 81 nous fournit la relation

$$\begin{aligned} 2\sigma(p^n, k) &\equiv -p^n k \sigma(p^n, k+1) \pmod{p^{2n}} \\ &\equiv 0 \pmod{p^{2n}} \end{aligned}$$

En 1998, Gessel **??** rectifie la preuve donnée par Bayat du théorème 79, et le généralise en prouvant le théorème suivant :

Théorème 82 *Soient m et k deux entiers naturels et*

$$\sigma(m, k) = \sum_{i \in R_m} \frac{1}{i^k}$$

où R_m est l'ensemble des nombres entiers compris entre 1 et $m-1$ et premiers avec m.

1. Si k n'est pas un multiple de $p-1$ pour tout nombre premier p divisant m, alors on
$$\sigma(m, k) \equiv 0 \pmod m.$$
2. Si k est impair et de plus $k+1$ n'est pas un multiple de $p-1$ pour tout nombre premier p divisant m, alors on
$$\sigma(m, k) \equiv 0 \pmod{m^2}.$$

2.11 Théorème de Hermite (1876) et de Glaisher (1899)

Dans, [41], Granville signale les deux théorèmes suivants

Théorème 83 *Hermite* (1876). *Soit p un nombre premier et n un nombre entier naturel impair. Alors ; on a*

$$\sum_{\substack{m\equiv 0 \pmod{(p-1)}\\ 0\leq m\leq n}} \binom{n}{m} \equiv 0 \pmod{p}$$

En 1899, Glaisher a généralisé le théorème d' Hermite 83, en prouvant le

Théorème 84 *Glaisher (1899). Pour tout nombre premier p et pour tous entiers j et k tels que $1 \leq j \leq p-1$ et $1 \leq k \leq p-1$, on a pour tout entier n tel que $n \equiv k \pmod{(p-1)}$*

$$\sum_{\substack{m\equiv j \pmod{(p-1)}\\ 1\leq m\leq n}} \binom{n}{m} \equiv \binom{k}{j} \pmod{p}$$

2.12 Théorème d'Edouard Lucas (1878)

C'est dans son ouvrage paru en 1878 (réimprimé en 1961 par la librairie Blanchard) qu'Edouard Lucas ènonce un théorème permettant de trouver aisement le reste

Théorème 85 *Soit p un nombre premier et soit*

$$\begin{aligned} a &= a_0 + a_1 p + a_2 p^2 + \cdots + a_m p^m \quad \textit{avec} \quad 0 \leq a_i < p, \\ b &= b_0 + b_1 p + b_2 p^2 + \cdots + b_m p^m \quad \textit{avec} \quad 0 \leq b_j < p. \end{aligned}$$

Alors

$$\binom{a}{b} \equiv \binom{a_0}{b_0}\binom{a_1}{b_1}..\binom{a_m}{b_m} \pmod{p}$$

Cette formule a été généralisée par plusieurs auteurs ([57], 1989), ([49], 1994), ([14], 2001).

Preuve. Nous avons

$$\begin{aligned} (1+x)^a &= (1+x)^{a_0}(1+x)^{pa_1}(1+x)^{p^2a_2}...(1+x)^{p^m a_m} \\ &\equiv (1+x)^{a_0}(1+x^p)^{a_1}(1+x^{p^2})^{a_2}...(1+x^{p^m})^{a_m} \pmod{p} \end{aligned}$$

Soit

$$\sum_{k\geq 0}\binom{a}{k}x^k \equiv (\sum_{0\leq k_0\leq a_0}\binom{a_0}{k_0}x^{k_0})(\sum_{0\leq k_1\leq a_1}\binom{a_1}{k_1}(x^p)^{k_1})...(\sum_{0\leq k_m\leq a_m}\binom{a_m}{k_m}(x^{p^m})^{k_m}) \pmod{p}$$

En identifiant les coefficients de x^b dans chacun des deux membres, on, obtient

$$\binom{a}{b} \equiv \sum_{\substack{(k_0,k_1...k_m)\in\mathbb{N}^m \text{ et } 0\leq k_i\leq a_i \text{ pour } 1\leq i\leq m \\ k_0+k_1p+...+k_mp^m=b}} \binom{a_0}{k_0}\binom{a_1}{k_1}...\binom{a_m}{k_m} \pmod p \tag{2.76}$$

Or on sait qu'il y a unicité de l'écriture de k en base p. On a donc pour$(k_0, k_1...k_m) \in \mathbb{N}^m$, avec $0 \leq k_i \leq a_i < p$ pour $1 \leq i \leq m$

$$\begin{aligned} k_0 + k_1p + ... + k_mp^m &= b \Leftrightarrow k_0 + k_1p + \cdots + k_mp^m = b_0 + b_1p + b_2p^2 + ... + b_kp^m \\ &\Leftrightarrow (k_0, k_1...k_m) = (b_0, b_1...b_m). \end{aligned}$$

Il en résulte que dans la sommation figurant au second membre de (2.76), il n'y a qu'un seul terme , celui correspondant au cas où $(k_0, k_1...k_m) = (b_0, b_1...b_m)$. Ainsi on a

$$\binom{a}{b} \equiv \binom{a_0}{b_0}\binom{a_1}{b_1}...\binom{a_0}{b_m} \pmod p$$

□

On déduit du théorème de Lucas un intéressant corollaire

Corollaire 86 *Pour tout nombre premier p, et pour tout entier $n \geqslant 1$, on a*

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

pour $1 \leqslant k \leqslant p^n - 1$.

Preuve. En effet, il suffit de remarquer du fait que $1 \leqslant k < p^n$, les écritures de p^n et k en base en p s'écrivent comme suit

$$\begin{aligned} p^n &= 0 + 0p + 0p^2 + \cdots 0p^{n-1} + 1p^n \\ k &= k_0 + k_1p + k_2p^2 + \cdots k_{n-1}p^{n-1} + 0p^n \quad \text{avec} \quad 0 \leq k_j < p, \end{aligned}$$

En appliquant le théorème de Lucas, on obtient

$$\binom{p^n}{k} \equiv \binom{0}{k_0}\binom{0}{k_1}..\binom{0}{k_{n-1}}\binom{1}{0} \equiv 0 \pmod p.$$

□

2.13 Théorème de Anton (1869), Stickelberger (1890), Hensel (1902).

Le résultat suivant, rapporté par A. Granville à été découvert par Anton (1869) et redécouvert par Stickelberer (1890), Hensel (1902) et par plusieurs autres auteurs depuis !

Théorème 87 *Soient p un nombre premier, a, b, r des entiers tels que $a \geqslant b$, et $r = a - b$.Si les décompositions des entiers a, b, r en base p s'écrivent*

$$\begin{aligned} a &= a_0 + a_1 p + a_2 p^2 + \cdots + a_m p^m \quad avec \;\; 0 \leq a_i \leq p, \\ b &= b_0 + b_1 p + b_2 p^2 + \cdots + b_m p^m \quad avec \;\; 0 \leq b_j \leq p, \\ r &= r_0 + r_1 p + r_2 p^2 + \cdots + r_m p^m \quad avec \;\; 0 \leq r_j \leq p, \end{aligned}$$

alors, on a

$$\frac{(-1)^k}{p^k}\binom{a}{b} \equiv \frac{a_0!}{b_0! r_0!}\,\frac{a_1!}{b_1! r_1!} \cdots \frac{a_m!}{b_m! r_m!} \pmod p.$$

Pour $k = 0$ on retrouve le théorème de Lucas **??**

2.14 Théorèmes de Morley (1895), de Granville (1997) et de Xu et Pan (2007)

2.14.1 Théorème de Morley

Frank Morley ($1860 - 1937$) est mathématicien géomètre bien connu pour son théorème de géométrie élémentaire qui affirme que les trois points d'intersection des trisectrices d'un triangle adjacentes aux côtés d'un triangle forment un triangle équilatéral. En 1895, il donna une ingénieuse preuve basée sur une forme explicite d'un théorème de De Moivre pour prouver le résultat suivant

Théorème 88 *(F. Morley,* 1895*) Pour tout nombre premier $p \geqslant 5$, on a*

$$(-1)^{(p-1)/2}\binom{p-1}{(p-1)/2} \equiv 4^{p-1} \pmod{p^3}$$

Remarque 89 *Quand deux nombres entiers a et b sont premiers avec un entier n, il est facile de vérifier que l'on a l'équivalence*

$$a \equiv b \pmod n \iff \frac{a}{b} \equiv 1 \pmod n \iff \frac{b}{a} \equiv 1 \pmod n.$$

Cette remarque s'applique ici avec

$$a = (-1)^{(p-1)/2}\binom{p-1}{(p-1)/2}, \quad b = 4^{p-1} \ \text{ et } \ n = p^3.$$

Le théorème de Morley revient donc à prouver que

$$\frac{4^{p-1}}{(-1)^{(p-1)/2}\binom{p-1}{(p-1)/2}} \equiv 1 \ (\bmod p^3). \tag{2.77}$$

C'est effectivement cette dernière relation que l'on va prouver en exploitant 'une identité remarquable énoncé et prouvé astucieusement par Morley.

La démonstration de Morley repose en effet sur l'indentité suivante qu'il établit

Proposition 90 *Pour tout entier $n \geq 1$, on a*

$$4^n \prod_{k=1}^{n} \frac{2k}{2k+1} = \sum_{k=0}^{n} \frac{(-1)^{n-k}}{2n+1-2k}\binom{2n+1}{k}. \tag{2.78}$$

Preuve. Posons

$$z := \cos x + i \sin x.$$

Alors on

$$2\cos x = (z + z^{-1}).$$

Par suite, on a

$$\begin{aligned} 2^{2n+1}\cos^{2n+1} x &= (z+z^{-1})^{2n+1} \\ &= \sum_{k=0}^{2n+1}\binom{2n+1}{k} z^{2n+1-2k} \\ &= \sum_{k=0}^{n}\binom{2n+1}{k} z^{2n+1-2k} + \sum_{k=n+1}^{2n+1}\binom{2n+1}{k} z^{2n+1-2k}. \end{aligned} \tag{2.79}$$

En changeant l'indice de sommation k en $2n+1-k$ dans la deuxième sommation de (2.79), on obtient

$$\begin{aligned} 2^{2n+1}\cos^{2n+1} x &= \sum_{k=0}^{n}\binom{2n+1}{k} z^{2n+1-2k} + \sum_{k=0}^{n}\binom{2n+1}{k} z^{-(2n+1-2k)} \\ &= \sum_{k=0}^{n}\binom{2n+1}{k} (z^{2n+1-2k} + z^{-(2n+1-2k)}) \\ &= 2\sum_{k=0}^{n}\binom{2n+1}{k} \cos((2n+1-2k)x). \end{aligned} \tag{2.80}$$

Ainsi, on obtient, après avoir diviser les deux membres de (2.80) par 2 :

$$2^{2n}\cos^{2n+1}x=\sum_{k=0}^{n}\binom{2n+1}{k}\cos((2n+1-2k)x).$$

En intégrant, entre 0 et $\frac{\pi}{2}$, on obtient

$$\begin{aligned}
2^{2n}\int_0^{\frac{\pi}{2}}\cos^{2n+1}x dx &= \sum_{k=0}^{n}\binom{2n+1}{k}\int_0^{\frac{\pi}{2}}\cos((2n+1-2k)x)dx\\
&= \sum_{k=0}^{n}\binom{2n+1}{k}\frac{\sin((2n+1-2k)\frac{\pi}{2})}{2n+1-2k}\\
&= \sum_{k=0}^{n}\binom{2n+1}{k}\frac{\sin(\frac{\pi}{2}+(n-k)\pi)}{2n+1-2k}\\
&= \sum_{k=0}^{n}\frac{(-1)^{n-k}}{2n+1-2k}\binom{2n+1}{k}. \qquad (2.81)
\end{aligned}$$

Il est bien connu et facile de prouver que

$$\int_0^{\frac{\pi}{2}}\cos^{2n+1}x dx=\prod_{k=1}^{n}\frac{2k}{2k+1}. \qquad (2.82)$$

On déduit alors des relations (2.81) et (2.82)

$$4^n\prod_{k=1}^{n}\frac{2k}{2k+1}=\sum_{k=0}^{n}\frac{(-1)^{n-k}}{2n+1-2k}\binom{2n+1}{k}.$$

On a ainsi établit la relation (2.81). Pour compléter, il reste à prouver le résultat classique(2.82).Celui ci se prouve en établissant une relation de récurrence grace à une intégration par parties. En effet, en posant

$$I_n:=\int_0^{\frac{\pi}{2}}\cos^{2n+1}x dx,$$

on a pour $n\geqslant 1$

$$\begin{aligned}
I_n &= \int_0^{\frac{\pi}{2}}\cos^{2n}x d(\sin x)\\
&= \left[\cos^{2n}x.\sin x\right]_0^{\frac{\pi}{2}}-\int_0^{\frac{\pi}{2}}\sin x d(\cos^{2n}x)\\
&= 0-2n\int_0^{\frac{\pi}{2}}\cos^{2n-1}x(-\sin^2 x)dx\\
&= 2n\int_0^{\frac{\pi}{2}}\cos^{2n-1}x(1-\cos^2 x)dx\\
&= 2n\int_0^{\frac{\pi}{2}}\cos^{2n-1}x dx-2n\int_0^{\frac{\pi}{2}}\cos^{2n+1}x dx\\
&= 2nI_{n-1}-2nI_n. \qquad (2.83)
\end{aligned}$$

On déduit de (2.83) la relation de récurrence suivante

$$(2n+1)I_n = 2nI_{n-1}, \text{ pour } n \geqslant 1.$$

Il est immédiat de constater

$$\begin{aligned} I_0 &= \int_0^{\frac{\pi}{2}} \cos x dx \\ &= [\sin x]_0^{\frac{\pi}{2}} \\ &= 1. \end{aligned}$$

Par conséquent

$$\begin{aligned} I_n &= \frac{2n}{(2n+1)} I_{n-1} \\ &= \frac{2n}{(2n+1)} \frac{2n-2}{(2n-1)} I_{n-2} \\ &= \frac{(2n)(2n-2) \quad ...2}{(2n+1)(2n-1)..3.} I_0 \\ &= \prod_{k=1}^{n} \frac{2k}{2k+1} \end{aligned}$$

□

Voyons maintenant comment on peut exploiter la proposition pour établir le théorème de Morley. Tout d'abord, il faut remarquer qu'on a une relation entre $\prod_{k=1}^{n} \frac{2k}{2k+1}$, qui est la valeur de I_n et $(-1)^n \binom{2n}{n}$. En effet, on a

$$\begin{aligned} \binom{2n}{n}^{-1} &= \frac{n!n!}{(2n)!} \\ &= \frac{n!n!}{1.2.3...(2n)} \\ &= \frac{n!n!}{(2.4.6...(2n))(1.3.5...(2n-1))} \\ &= \frac{n!n!}{2^n n!(1.3.5...(2n-1))} \\ &= \frac{1.2.3...n}{2^n(1.3.5...(2n-1))} \\ &= \frac{2.4.6...(2n)}{2^n 2^n(1.3.5...(2n-1))} \\ &= \frac{2n+1}{4^n} \prod_{k=1}^{n} \frac{2k}{2k+1}. \end{aligned} \tag{2.84}$$

La relation (2.78) peu alors s'écrire, compte tenu du résultat (5) de la proposition

$$\frac{4^{2n}}{(-1)^n\binom{2n}{n}} = \sum_{k=0}^{n}(-1)^k\frac{(2n+1)}{2n+1-2k}\binom{2n+1}{k}, \text{ pour tout entier } n \geqslant 1. \tag{2.85}$$

Soit alors $p \geqslant 5$, un nombre premier, posons

$$n = \frac{p-1}{2}.$$

Autrement dit $p = 2n+1$. La relation (2.85) s'ecrit *

$$\frac{4^{p-1}}{(-1)^{(p-1)/2}\binom{p-1}{(p-1)/2}} = \sum_{k=0}^{n}(-1)^k\frac{p}{p-2k}\binom{p}{k}, \text{ pour tout entier } n \geqslant 1. \tag{2.86}$$

On a vu que en remarque que l'on avait l'équivalence

$$(-1)^{(p-1)/2}\binom{p-1}{(p-1)/2} \equiv 4^{p-1} \pmod{p^3}. \Longleftrightarrow \frac{4^{p-1}}{(-1)^{(p-1)/2}\binom{p-1}{(p-1)/2}} \equiv 1 \pmod{p^3}. \tag{2.87}$$

En tenant compte de la relation qu'on a établit (2.86), on peut affirmer que l'on a

$$(-1)^{(p-1)/2}\binom{p-1}{(p-1)/2} \equiv 4^{p-1} \pmod{p^3}. \Longleftrightarrow \sum_{k=0}^{(p-1)/2}(-1)^k\frac{p}{p-2k}\binom{p}{k} \equiv 1 \pmod{p^3}. \tag{2.88}$$

Ainsi prouver le thérème de Morley est équivalent à prouver la relation $\sum_{k=0}^{(p-1)/2}(-1)^k\frac{p}{p-2k}\binom{p}{k} \equiv 1 \pmod{p^3}$.Nous allons constater que ce problème est beaucoup plus simple. La preuve de cette relation repose sur le lemme suivant

On a tout d'abord en exploitant d'abord la relation (2.89) et le corollaire 49

Remarquons que l'on a pour tout entier $k \in \{1, 2, ...p-1\}$,

$$\binom{p-1}{k-1} = \prod_{k=1}^{k-1}\frac{p-k}{k} \equiv (-1)^{k-1} \pmod{p}. \tag{2.89}$$

On en déduit que

$$\begin{aligned}
\sum_{k=1}^{\frac{p-1}{2}}(-1)^k\frac{1}{(p-2k)k}\binom{p-1}{k-1} &\equiv \sum_{k=1}^{\frac{p-1}{2}}(-1)^k\frac{1}{(p-2k)k}(-1)^{k-1} \pmod{p}. \\
&\equiv -\sum_{k=1}^{\frac{p-1}{2}}\frac{1}{(p-2k)k} \pmod{p} \\
&\equiv \frac{1}{2}\sum_{k=1}^{\frac{p-1}{2}}\frac{1}{k^2} \pmod{p} \\
&\equiv 0 \pmod{p}.
\end{aligned}$$

Ainsi, on a

$$\sum_{k=0}^{n}(-1)^k\frac{1}{(p-2k)k}\binom{p-1}{k-1}\equiv 0\ (\bmod p). \tag{2.90}$$

En multipliant les deux membres de (2.90) par p^2, on obtient une congruence modulo p^3

$$\sum_{k=1}^{\frac{p-1}{2}}(-1)^k\frac{P}{(p-2k)}\frac{p}{k}\binom{p-1}{k-1}\equiv 0\ (\bmod p^3),$$

soit

$$\sum_{k=1}^{\frac{p-1}{2}}(-1)^k\frac{p}{(p-2k)}\binom{p}{k}\equiv 0\ (\bmod p^3). \tag{2.91}$$

Oo en deduit en rajoutant un terme correspondant à $k=0$

$$\sum_{k=0}^{\frac{p-1}{2}}(-1)^k\frac{p}{(p-2k)}\binom{p}{k}\equiv 1\ (\bmod p^3). \tag{2.92}$$

ce qui est bien la relation qu'on voulait prouver.

2.14.2 La démonstration de Morley

Morley commence par prouver le lemme suivant

Lemme 91 *Pour tout nombre premier $p>3$, on a*

$$1+\frac{1}{3^2}+\frac{1}{5^2}+\cdots+\frac{1}{(p-2)^2}\equiv 0\ (\bmod p).$$

La démonstration que donne Morley de son théorème repose alors sur la formule trigonométrique suivante qui exprime $\cos px$ comme une polynôme en $\cos x$, p étant un nombre impair

$$(-1)^{\frac{p-1}{2}}\cos(px)=p\cos(x)-\frac{p(p^2-1^2)}{3!}\cos^3 x+\frac{p(p^2-1^2)(p^2-3^2)}{5!}\cos^5 x-\cdots+(-1)^{\frac{p-1}{2}}2^{p-1}\cos^p x$$

En multipliant par dx et en intégrant de 0 à $\frac{\pi}{2}$, ontrouve en utilisant (2.82)

$$\frac{1}{p}=p-\frac{p(p^2-1^2)}{3!}\frac{2}{3}+\frac{p(p^2-1^2)(p^2-3^2)}{5!}\frac{2.4}{3.5}+\cdots+(-1)^{\frac{p-1}{2}}2^{p-1}\frac{2.4...(p-1)}{3.4...p}.$$

On a donc

$$\frac{1}{p}-(-1)^{\frac{p-1}{2}}2^{p-1}\frac{2.4...(p-1)}{3.4...p}\equiv p(1+\frac{1}{3^2}+\frac{1}{5^2}+\cdots+\frac{1}{(p-2)^2})\ (\bmod p^3)$$

Avec le lemme 91, on en déduit que

$$\frac{1}{p} - (-1)^{\frac{p-1}{2}} 2^{p-1} \frac{2.4...(p-1)}{3.4...p} \equiv 0 \ (\mathrm{mod}\, p^2).$$

Par suite, on a

$$1 - (-1)^{\frac{p-1}{2}} 2^{p-1} \frac{2.4...(p-1)}{3.4...(p-2)} \equiv 0 \ (\mathrm{mod}\, p^3)$$

On en déduit que

$$2^{4n} - (-1)^n \frac{(2n)!}{(n!)^2} \equiv 0 \ (\mathrm{mod}\, p^3)$$

où $2n+1 = p$ est un nombre premier strictement plus grand que 3.

2.14.3 Théorème de Granville (1997)

Un peu plus d'un siècle après l'enoncé de ce théorème, plus précisément en 1997, Granville [40] prouve l'extension suivante du Théorème de Morley

Théorème 92 *(Granville,* 1997*) Pour tout nombre premier $p \geqslant 3$, et pour tout entier $m \geqslant 2$, on a*

$$(-1)^{\frac{(p-1)(m-1)}{2}} \prod_{k=1}^{m-1} \binom{p-1}{\lfloor pk/m \rfloor} \equiv m^p \ - m + 1 \ (\mathrm{mod}\, p^2)$$

2.14.4 Théorème de Xu et Pan (2007)

En 2007, Ping Xu et Hao Pan [100] généralisent le théorème de Granville 92 en prouvant

Théorème 93 *Ping Xu et Hao Pan* (2007) *Pour tous entiers n, $m \geq 2$ tels que $(n; 2m) = 1$, on a*

$$(-1)^{\frac{\varphi(n)(m-1)}{2}} \prod_{k=1}^{m-1} \prod_{d \ divise \ n} \binom{d-1}{\lfloor dk/m \rfloor}^{\mu(n/d)} \equiv m(m^{\varphi(n)} \ - 1) + 1 \ (\mathrm{mod}\, n^2)$$

Dans ce théorème φ est la fonction d"Euler et μ la fonction de Möbius définie par $\mu(1) = 1$, $\mu(n) = (-1)^k$ si l'entier n est un produit de k nombres premiers distincts et $\mu(n) = 0$ sinon.

2.15 Théorème de Fleck (1913)

En 1913, A. Fleck (cf. [28], *p.*274) démontre le résultat suivant :

Théorème 94 *Pour tout nombre premier p et pour tous entiers j et n tels que $1 \leqslant r \leqslant p-1 < n$, on a*

$$\sum_{\substack{k\equiv r \pmod p \\ 1\leq k\leq n}} (-1)^k \binom{n}{k} \equiv 0 \pmod{p^{\left\lfloor \frac{n-1}{p-1} \right\rfloor}},$$

Preuve. Soit

$$\xi = e^{\frac{2i\pi}{p}}.$$

Posons

$$f_j = \sum_{\substack{m\equiv j \pmod p \\ 1\leq m\leq n}} (-1)^m \binom{n}{m}.$$

et

$$g_i = \sum_{0\leq j\leq p-1} f_j \xi^{i.j}$$

On a alors

$$\begin{aligned} g_i &= \sum_{0\leq j\leq p-1} f_j \xi^{i.j} = \sum_{0\leq j\leq p-1} \sum_{\substack{m\equiv j \pmod p \\ 1\leqslant m\leqslant n}} (-1)^m \binom{n}{m} \xi^{i.m} \\ &= \sum_{0\leq m\leq n} (-1)^m \binom{n}{m} \xi^{i.m} \\ &= (1-\xi^i)^n. \end{aligned}$$

On en déduit que

$$g_i \in (1-\xi)^n \mathbb{Z}\left[\xi\right].$$

On montre alors que

$$pf_j = \sum_{0\leq i\leq p-1} g_i \xi^{-i.j} \in \mathbb{Z} \cap \left((1-\xi)^{n+1}\mathbb{Z}\left[\xi\right]\right) = p^{r+1}\mathbb{Z}.$$

Par suite

$$f_j \in p^r \mathbb{Z}.$$

□

2.15.1 Généralisation du théorème de Fleck par C. S. Weisman (1977)

En 1977, C.S. Weisman généralise le théorème de Fleck en établissant le théorème suivant

Théorème 95 *Pour tout nombre premier p et pour tous entiers α, j et n tels que $1 \leqslant j \leqslant p^\alpha - 1 < n$, on a*

$$\sum_{\substack{m \equiv j \pmod{p^\alpha} \\ 1 \leq m \leq n}} (-1)^m \binom{n}{m} \equiv 0 \pmod{p^{\left\lfloor \frac{n-p^\alpha}{p^{\alpha-1}(p-1)} \right\rfloor}},$$

2.15.2 Généralisation du théorème de Fleck par D. Wan (2005)

En 2005, D. Wan obtient la généralisation suivante du théorème de Fleck

Théorème 96 *Pour tout nombre premier p et pour tous entiers l, j et n tels que $1 \leqslant j \leqslant p - 1 < n$, et $n > lp$, on a*

$$\sum_{\substack{m \equiv j \pmod{p} \\ 1 \leq m \leq n}} (-1)^m \binom{n}{m} \binom{(m-j)/p}{l} \equiv 0 \pmod{p^{\left\lfloor \frac{n-lp-1}{p-1} \right\rfloor}},$$

2.16 Théorèmes d' Emma Lehmer (1938) et de Zhi-Hong Sun (2000)

Emma Trotskaia Lehmer $(1906 - 2007)$ est une mathématicienne américaine d'origine russe, née à Samara sur le grand fleuve de la Volga, comme elle aimait le dire. Son mari Derrick Henry Lehmer $(1905 - 1991)$ et son beau père Derrick Norman Lehmer $(1867 - 1938)$ étaient aussi mathématiciens, et théoriciens des nombres. Ils collaborèrent ensemble sur des sujets tels que l'étude des nombres de Bernoulli, l'étude des congruences, les calculs sur ordinateur : factorisation d'entiers et tests de primalité (c'est à D. H. Lehmer qu'on est redevable d'une amélioration du test de primalité des nombres de Mersenne de Lucas appelée test de Lucas-Lehmer). Les contributions importantes de ces trois éminents mathématiciens ont été soulignées en 2000 lors d'une rencontre entre mathématiciens organisée à Berkeley, spécialement consacrée à leurs travaux. Emma Lehmer fut l'invitée d'honneur.

En 1938, dans un article intitulé «On congruences involving Bernoulli numbers and the quotients of Fermat and Wilson », E. Lehmer retrouve et généralise (entre autres résultats), de nombreux résultats dus à Glaisher, Vandiver, Friedmann, Tamarkin, Mirimanoff, Lerf, Nielsen et Mordell.

En conclusion de cette article, elle applique au problème de trouver les résidus modulo p et p^2 de certains coefficients binomiaux. Elle retrouve en particulier le résultat de Morley :

$$\binom{p-1}{(p-1)/2} \equiv (-1)^{(p-1)/2} 4^{p-1} \pmod{p^3}, \text{ pour } p > 3$$

qui peut aussi s'écrire

$$\binom{p-1}{\lfloor \frac{p}{2} \rfloor} \equiv (-1)^{(p-1)/2} 4^{p-1} \pmod{p^3}, \text{ pour } p > 3$$

ainsi que d'autres résultats similaires

$$\binom{p-1}{\lfloor \frac{p}{3} \rfloor} \equiv (-1)^{\lfloor \frac{p}{3} \rfloor} \frac{3^p - 1}{2} \pmod{p^2}, \text{ pour } p > 3$$

$$\binom{p-1}{\lfloor \frac{p}{4} \rfloor} \equiv (-1)^{\lfloor \frac{p}{4} \rfloor} (3.2^{p-1} - 2) \pmod{p^2}, \text{ pour } p > 3$$

et

$$\binom{p-1}{\lfloor \frac{p}{6} \rfloor} \equiv (-1)^{\lfloor \frac{p}{6} \rfloor} \frac{2^{p+1} + 3^p - 5}{2} \pmod{p^2}, \text{ pour } p > 5$$

Soit p un nombre premier impair. On sait grace au petit théorème de Fermat que $2^P - 1 \equiv 1 \pmod{p}$, il en résulte que $\frac{2^P - 1}{p} \in \mathbb{N}$. Ce qui justifie la définition suivante

Définition 97 *Pour tout nombre premier p, et pour tout entier naturel a premier à p, on appelle quotient de Fermat le nombre $q_p(a)$ défini par*

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

Théorème 98 *(E. Lehmer). Pour tout nombre premier impair p, on a*

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

La démonstation que nous donnerons se base sur un récent article de Monsieur Roméo Mestrovic intitulé "An Extension Of A Congruence By Kohnen" [66]

Mr Roméo Mestrovic démontre le théorème d'Emma Lehmer en utilisant ces quatres lemmes :

Lemme 99 *Si p est un entier premier alors*

$$\binom{p-1}{k} \equiv (-1)^k - (-1)^k p H_k + (-1)^k p^2 \sum_{1 \leq i < j < k} \frac{1}{ij} \pmod{p^3} \tag{2.93}$$

pour tout $k = 1, 2, ...p-1$

Preuve. voir [67] □

Lemme 100 *Pour tout n entier positif alors*

$$\sum_{k=1}^{2n}(-1)^k H_k = \frac{1}{2}H_n \tag{2.94}$$

Preuve. *voir [67]* □

Lemme 101 *Pour tout n entier positif alors*

$$\sum_{k=2}^{2n}\sum_{1\leq i<j\leq k}\frac{(-1)^k}{ij} = \sum_{1\leq i<j\leq 2n}\frac{1}{ij} \tag{2.95}$$

Preuve. *voir [67]* □

Lemme 102 *Soit p un entier premier ,$p \geq 5$*

$$\sum_{k=1}^{p-1}\frac{(-1)^k H_{k-1}}{k} \equiv 2\sum_{1\leq i<j\leq p-1}\frac{1}{ij} \equiv q_p^2(2) \tag{2.96}$$

Preuve. voir [67] □

On a

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

$$2^{p-1} - 1 = \sum_{k=1}^{p-1}\binom{p-1}{k}$$

En utilisant la relation 2.93 et en la sommant de $k = 1$ jusqu'à $k = p-1$

on obtient alors cette nouvelle congruence

$$2^{p-1} - 1 = \sum_{k=1}^{p-1}\binom{p-1}{k} \equiv \sum_{k=1}^{p-1}(-1)^k - p\sum_{k=1}^{p-1}(-1)^k H_k + p^2\sum_{k=1}^{p-1}\sum_{1\leq i<j\leq k}\frac{(-1)^k}{ij}(\mathrm{mod}\, p^3) \tag{2.97}$$

comme pour tout p impair, $p-1$ serait pair alors

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

et d'aprés le lemme 101 et pour $2n = p-1$

$$\sum_{k=1}^{p-1}(-1)^k H_k = \frac{1}{2}H_{\frac{p-1}{2}}$$

et d'aprés le lemme 102

$$\sum_{k=2}^{2n}\sum_{1\leq i<j\leq k}\frac{(-1)^k}{ij} = \sum_{1\leq i<j\leq p-1}\frac{1}{ij}$$

Alors la relation 2.97 deviendrait

$$2^{p-1}-1 \equiv -\frac{p}{2}H_{\frac{p-1}{2}} + p^2\sum_{1\leq i<j\leq p-1}\frac{1}{ij}(\mathrm{mod}\, p^3) \tag{2.98}$$

En divisant les deux membres de la relation 2.98 par p on obtient

$$\frac{2^{p-1}-1}{p} \equiv -\frac{1}{2}H_{\frac{p-1}{2}} + p\sum_{1\leq i<j\leq p-1}\frac{1}{ij}(\mathrm{mod}\, p^2) \tag{2.99}$$

$$H_{\frac{p-1}{2}} \equiv -2q_p(2) + 2p\sum_{1\leq i<j\leq p-1}\frac{1}{ij}(\mathrm{mod}\, p^2) \tag{2.100}$$

en utilisant la relation 2.96 la relation 2.100 deviendrait alors

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

Ce qui est bien la congruence d'Emma Lehmer

Extensions et généralisations par Zhi-Hong Sun (2000)

En 2000, Zhi Hong Sun a généralisé ce résultat en prouvant (théorème $5-2, p$ 208 de [102])

Théorème 103 *Zhi Hong Sun,* (2000)*. Soit $p > 3$ un nombre premier.*

1. *Si $k \in \{2, 4, ..., p-5\}$, alors*

$$\sum_{x=1}^{(p-1)/2}\frac{1}{x^k} \equiv \frac{k(2^{k+1}-1)}{2}\left(\frac{B_{2p-2-k}}{2p-2-k} - 2\frac{B_{p-1-k}}{p-1-k}\right)p \ (\mathrm{mod}\, p^3)$$

2. Si $k \in \{3, 5, ..., p-4\}$ *, alors*

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

3. Avec $q_p(2) = (2^{p-1} - 2)/p$*, on a*

$$\sum_{x=1}^{(p-1)/2} \frac{1}{x} \equiv -2q_p(2) + pq_p^2(2) - \frac{2}{3}p^2q_p^3(2) - \frac{7}{12}p^2B_{p-3} \pmod{p^3}$$

La derniere comgruence de ce théorème est une amélioration du théorème de Lehmer qui donnait seulement une congruence modulo p^2 pour $H_{\frac{p-1}{2}}$.

2.17 Théorème de Ljunggren (1952) et Jacobsthal

En 1952, Ljunggren a généralisé le theorème de Wolstenholme en prouvant le résultat suivant :

Théorème 104 *Pour tout nombre premier* $p \geqslant 5$*, on a*

$$\binom{np}{mp} \equiv \binom{n}{m} \pmod{p^3} \tag{2.101}$$

Remarquons que ce théorème généralise le théorème (78) qui est correspond aux notations près au cas où $m = 1$.

Preuve. Observons tout d'abord que la relation (2.101) est trivialement vérifié pour $m > n$. Supposons donc que $m \leq n$. On a alors

$$\begin{aligned}
\binom{np}{mp} &= \prod_{k=0}^{mp-1} \frac{np-k}{mp-k} \\
&= \prod_{j=0}^{m-1}\prod_{i=0}^{p-1} \frac{np-pj-i}{mp-pj-i} \\
&= (\prod_{j=0}^{m-1} \frac{n-j}{m-j})(\prod_{j=0}^{m-1}\prod_{i=1}^{p-1} \frac{(n-j)p-i}{(m-j)p-i}) \\
&= \binom{n}{m}(\prod_{j=0}^{m-1} \binom{(n-j)p-1}{p-1}(\prod_{j=0}^{m-1} \binom{(m-j)p-1}{p-1}^{-1}).
\end{aligned} \tag{2.102}$$

En remarquant que le théorème 77 implique

$$\prod_{j=0}^{m-1} \binom{(n-j)p-1}{p-1} \equiv 1 \pmod{p^3}$$

et

$$\prod_{j=0}^{m-1} \binom{(m-j)p-1}{p-1} \equiv 1 \pmod{p^3},$$

la relation (2.101) découle alors de (2.102). □

Jacobsthal obtient la généralisation suivante

Théorème 105 *Pour tout nombre premier $p \geqslant 5$, on a*

$$\frac{\binom{np}{mp}}{\binom{n}{m}} \equiv 1 \pmod{p^q}$$

où $q := v_p(p^3nm(n-m))$

2.18 Théorème de Carlitz (1953)

Théorème 106 *Pour tout nombre premier $p \geqslant 3$, et pour tout entier $q \geqslant 1$, si p^{q-1} divises n, alors on a*

$$p + (p-1) \sum_{\substack{1 \leq m \leq n-1 \\ m \equiv 0 \pmod{(p-1)}}} \binom{n}{m} \equiv 0 \pmod{p^q},$$

2.19 Théorème de Bhaskaran (1965)

En 1965, Bhaskaran (cf. [42]), prouve le résultat suivant :

Théorème 107 *Pour tout nombre premier p impair, on a*

$$p+1 \text{ divise } n \Longleftrightarrow \forall j \in \{1,3,5,...,p-2\}, \sum_{1 \leq m \leq n \text{ et } m \equiv j \pmod{(p-1)}} (-1)^{\frac{m-j}{p-1}} \binom{n}{m} \equiv 0 \pmod{p}.$$

Dans [42], Granville a donné une preuve particulièrement astucieuse de ce théorème que nous allons détailler, en utilisant comme il l'affirme "A little algebraic number theory". La démonstration est basée sur le lemme suivant :.

Lemme 108 *Pour tous entiers a , $b \neq 0$ et $d \neq 0$, les suites $(u_n)_{n\geq 0}$ et $(v_n)_{n\geq 0}$ définies par*

$$u_n = \frac{1}{2b\sqrt{d}}((a+b\sqrt{d})^n - (a-b\sqrt{d})^n)$$

et

$$v_n = ((a+b\sqrt{d})^n + (a-b\sqrt{d})^n)$$

sont à valeurs entières. De plus

- *Pour tous entiers q et n,*

$$u_q \text{ divise } u_n \text{ si } q \text{ divise } n. \tag{2.103}$$

- *Pour tout nombre premier p, on a*

$$u_{p+1} \equiv a(1 + b^{p-1}d^{\frac{p-1}{2}}) \pmod p \tag{2.104}$$

Preuve. On vérifie facilement que l'on a

$$u_n = \sum_{1\leq m\leq n \text{ et } m \text{ impair}} \binom{n}{m} a^{n-m}b^{m-1}d^{\frac{m-1}{2}} \tag{2.105}$$

et

$$v_n = \sum_{1\leq m\leq n \text{ et } m \text{ pair}} 2\binom{n}{m} a^{n-m}b^{m}d^{\frac{m}{2}}. \tag{2.106}$$

Les expressions de u_n et v_n données par (2.105) et (2.106) prouvent que $u_n \in \mathbb{Z}$ et $v_n \in \mathbb{Z}$.

On verifie aussi que pour tout entier naturel m, on a l'identité

$$x^m - y^n = (x-y)(\sum_{k=0}^{\lfloor \frac{m-1}{2} \rfloor} (xy)^k(x^{m-2k-1} + y^{m-2k-1}) - (\frac{1-(-1)^m}{2})(xy)^{\lfloor \frac{m-1}{2} \rfloor}).$$

En choisissant $x = (a+b\sqrt{d})^q$ et $y = (a-b\sqrt{d})^q$, on en déduit que l'on a

$$u_{qm} = Au_q$$

avec

$$A = \sum_{k=0}^{\lfloor \frac{m-1}{2} \rfloor} (a^2-db^2)^k v_{m-2k-1} - (\frac{1-(-1)^m}{2})(a^2-db^2)^{\lfloor \frac{m-1}{2} \rfloor}$$

Comme $A \in \mathbb{Z}$, on en déduit que u_q divise u_{qm} et donc que si n est divisible par q, alors u_n est divisible par u_q. La propriété (2.103) est établie.

Maintenant si p est un nombre premier, on a d'après le théorème 37

$$\binom{p+1}{m} = \binom{p}{m} + \binom{p}{m-1} \equiv 0 \pmod p, \text{ pour } m \in \{2, ..., p-1\}.$$

On a donc

$$\begin{aligned} u_{p+1} &= \sum_{1\leq m\leq n \text{ et } m \text{ impair}} \binom{p+1}{m} a^{p+1-m} b^{m-1} d^{\frac{m-1}{2}} \\ &\equiv \binom{p+1}{1} a^p + \binom{p+1}{p} a b^{p-1} d^{\frac{p-1}{2}} \ (\mathrm{mod}\, p) \\ &\equiv a + a b^{p-1} d^{\frac{p-1}{2}} \equiv a(1 + b^{p-1} d^{\frac{p-1}{2}}) \ (\mathrm{mod}\, p), \end{aligned}$$

ce qui prouve (2.104). □

Preuve du théorème 107 Soit p un nombre premier impair. Posons pour $j \in \{1, 3, ..., p-2\}$:

$$\nu_j = \sum_{1\leq m\leq n \text{ et } m\equiv j \ (\mathrm{mod}(p-1))} (-1)^{\frac{m-j}{p-1}} \binom{n}{m} \equiv 0 \ (\mathrm{mod}\, p).$$

Soient $d_1, d_1, ..., d_m$ des représentants des $m = \frac{p-1}{2}$ non résidus quadratiques modulo p. Soient a et b deux entiers premiers avec p et $d \in \{d_1, d_1, ..., d_m\}$. Soit $(u_n)_{n\geq 0}$ la suite d'éléments d'entiers définie par

$$u_n = \frac{(a + b\sqrt{d})^n - (a - b\sqrt{d})^n}{2b\sqrt{d}}. \tag{2.107}$$

On a alors

$$u_{p+1} \equiv 0 \ (\mathrm{mod}\, p). \tag{2.108}$$

En effet, on a $b^{p-1} \equiv 1 \ (\mathrm{mod}\, p)$, $d^{\frac{p-1}{2}} \equiv -1 \ (\mathrm{mod}\, p)$ et d'après le lemme 108

$$u_{p+1} \equiv a(1 + b^{p-1} d^{\frac{p-1}{2}}) \equiv a(1 + 1(-1)) \equiv 0 \ (\mathrm{mod}\, p).$$

Posons

$$E_n = \{m \in \{1, 2, .., n\} ; \ m \equiv 1 \ (\mathrm{mod}\, 2)\}.$$

La division euclidienne d'un entier $n \in E_n$ par $p-1$ donne un reste impair (car $p-1$ est pair). On peut donc écrire E_n comme une réunion disjointe d'ensembles $E_{n,j}$ comme suit :

$$\begin{aligned} E_n &= \cup_{j\in\{1,3,...,p-2\}} E_{n,j} \\ &= \cup_{1\leq j\leq p-1 \text{ et } j\equiv 1 \ (\mathrm{mod}\, 2)} E_{n,j}, \end{aligned}$$

où

$$E_{n,j} = \{m \in \{1, 2, .., n\} ; \ m \equiv j \ (\mathrm{mod}\, p-1)\}.$$

Il en résulte que d'après (2.105), on a

$$\begin{aligned} u_n &= \sum_{m\in E_n} \binom{n}{m} a^{n-m} b^{m-1} d^{\frac{m-1}{2}} \\ &= \sum_{1\le j\le p-1} \left\{ \sum_{m\in E_{n,j}} \binom{n}{m} a^{n-m} b^{m-1} d^{\frac{m-1}{2}} \right\} \\ &= \sum_{1\le j\le p-1} \left\{ \sum_{m\equiv j \ (\mathrm{mod}\, p-1)} \binom{n}{m} a^{n-m} b^{m-1} d^{\frac{m-1}{2}} \right\} \end{aligned}$$

En observant que a et b étant premiers avec p , on a d'après le petit théorème de Fermat $a^{p-1} \equiv 1 \ (\mathrm{mod}\, p)$, $b^{p-1} \equiv 1 \ (\mathrm{mod}\, p)$. Par suite avec $m \equiv j \ (\mathrm{mod}\, p-1)$, on a :

$$a^{n-m} \equiv a^{n-j} \ (\mathrm{mod}\, p), \quad b^{m-1} \equiv b^{j-1} \ (\mathrm{mod}\, p). \ \text{ et } d^{\frac{j-1}{2}}$$

Pour $m \equiv j \ (\mathrm{mod}\, p-1)$, on peut écrire

$$m = (\frac{m-j}{p-1})(p-1) + j,$$

avec $\frac{m-j}{p-1} \in \mathbb{N}$. On alors

$$\frac{m-1}{2} = (\frac{m-j}{p-1})(\frac{p-1}{2}) + \frac{j-1}{2}.$$

Comme par hypothèse d est un non résidu quadratique modulo p, on a

$$d^{\frac{p-1}{2}} \equiv -1 \ (\mathrm{mod}\, p)$$

et

$$d^{\frac{m-1}{2}} \equiv (d^{\frac{p-1}{2}})^{\frac{m-j}{p-1}} \ d^{\frac{j-1}{2}} \equiv (-1)^{\frac{m-j}{p-1}} \ d^{\frac{j-1}{2}} \ (\mathrm{mod}\, p)$$

Par suite

$$u_n \equiv \sum_{1\le j\le p-1 \text{ et } j\equiv 1 \ (\mathrm{mod}\, 2)} \left\{ \sum_{m\equiv j \ (\mathrm{mod}\, p-1)} (-1)^{\frac{m-j}{p-1}} \binom{n}{j} a^{n-j} b^{j-1} d^{\frac{j-1}{2}} \right\} \ (\mathrm{mod}\, p)$$

Ainsi

$$u_n \equiv \sum_{0\le j\le p-1 \text{ et } j \text{ impair}} \nu_j a^{n-j} b^{j-1} d^{\frac{j-1}{2}} \ (\mathrm{mod}\, p). \tag{2.109}$$

– Prouvons l'implication : $p+1$ divise $n \Longrightarrow \forall j \in \{1,3,5,...,p-2\}, \nu_j \equiv 0 \ (\mathrm{mod}\, p)$.

Supposons donc que $p+1$ divise n, alors on sait d'après le lemme 108 que u_{p+1} divise u_n. Or d'après (2.108), p divise u_{p+1} ; il en résulte que p divise u_n. On a donc

$$\sum_{0\leq j\leq p-1 \text{ et } j \text{ impair}} \nu_j a^{n-j} b^{j-1} d^{\frac{j-1}{2}} \equiv 0 \ (\mathrm{mod}\, p). \tag{2.110}$$

Choisissons $a=b=1$ dans (2.109) et $d=d_i$ dans (2.110), on obtient

$$\sum_{j\in\{1,3,5,\ldots,p-2\}} \nu_j d_i^{\frac{j-1}{2}} \equiv 0 \ (\mathrm{mod}\, p), \quad \text{pour } i=1,2,\ldots,\frac{p-1}{2}. \tag{2.111}$$

Le système (2.111) peut-être interprété comme un système de $m=\frac{p-1}{2}$ équations linéaires à m inconnues $\nu_1,\nu_3,\ldots,\nu_{p-2}$ (dans $\mathbb{Z}/p\mathbb{Z}$ en confandant les éléments de $\mathbb{Z}$ avec leur classes) et dont le déterminant Δ est un déterminant de Vondermonde :

$$\Delta = \det(d_i^{j-1})_{\substack{1\leq i\leq m\\ 1\leq j\leq m}} = \prod_{1\leq i<j\leq m} (d_j - d_i).$$

On a $\Delta\neq 0$. Par conséquent le système considéré est un système de Cramer homogène (sans second membre). Il admet comme unique solution la solution triviale dans $\mathbb{Z}/p\mathbb{Z}$: $\nu_j=0$ pour$j\in\{1,3,5,\ldots,p-2\}$. Autrment dit, on a bien : $\forall j\in\{1,3,5,\ldots,p-2\}, \nu_j\equiv 0\ (\mathrm{mod}\, p)$.

– Prouvons l'implication : $\forall j\in\{1,3,5,\ldots,p-2\}, \nu_j\equiv 0\ (\mathrm{mod}\, p) \Longrightarrow p+1$ divise n.

Dans ce cas on a d'après (2.109)

$$u_n \equiv 0\ (\mathrm{mod}\, p), \tag{2.112}$$

pour tous choix de a et b premiers avec p.

Commençons par constater que l'anneau $\mathbb{Z}\left[\sqrt{d}\right]/p\mathbb{Z}\left[\sqrt{d}\right]$ est un corps. Posons $A=\mathbb{Z}\left[\sqrt{d}\right]$. On sait que $\mathbb{Z}\left[\sqrt{d}\right]\backsimeq\mathbb{Z}[X]/(X^2-d)$. On a donc $A/pA\backsimeq\mathbb{Z}[X]/(p,X^2-d)\backsimeq IF_p[X]/(X^2-\overline{d})$. Comme d est un non résidu quadratique modulo p, $\overline{d}$ n'est pas un carré dans $IF_p[X]$ et le polynôme $X^2-\overline{d}$ est irréductible dans $IF_p[X]$. Par suite $F_p[X]/(X^2-\overline{d})$ est un corps. Il en résulte que est aussi A/pA un corps. Comme le dégré de $X^2-\overline{d}$ est égale à 2, le corps A/pA possède p^2 éléments. On sait aussi que le groupe multiplicatif de de corps, c'est à dire $G:=A/pA-\{0\}$ est un groupe cyclique à p^2-1 éléments. Soit $\overline{g}=\overline{a+b\sqrt{d}}$ un générateur de ce groupe avec a, $b\in\{1,2..p-1\}$. Ce choix de $\overline{g}$ definit ainsi des entiers a et b premiers avec p.

Remarquons que pour un tel choix de a et b, on a

$$(a+b\sqrt{d})^p \equiv a-b\sqrt{d}\ (\mathrm{mod}\, p). \tag{2.113}$$

En effet, comme $\binom{p}{k} \equiv 0 \pmod p$ pour $1 \leq k \leq p-1$, on a

$$\begin{aligned}(a+b\sqrt{d})^p &= \sum_{k=0}^{p} \binom{p}{k} a^{p-k}(b\sqrt{d})^k \\ &\equiv a^p + b^p(d^{\frac{p-1}{2}})\sqrt{d} \pmod p \\ &\equiv a - b\sqrt{d} \pmod p.\end{aligned}$$

Il résulte de (2.113) que

$$(a+b\sqrt{d})^{p-1} \equiv \frac{a-b\sqrt{d}}{a+b\sqrt{d}} \pmod p. \tag{2.114}$$

De (2.112) et (2.107) on déduit que

$$(\frac{a-b\sqrt{d}}{a+b\sqrt{d}})^n \equiv 1 \pmod p. \tag{2.115}$$

De (2.114) et (2.115), on déduit que

$$(a+b\sqrt{d})^{n(p-1)} \equiv 1 \pmod p$$

Mais comme $\overline{g} = \overline{a+b\sqrt{d}}$ a pour ordre p^2-1 dans G, $n(p-1)$ divise nécessairement p^2-1, ce qui imlplique que $p-1$ divise $n+1$.

2.20 théorèmes liés à la répresentation d'un nombre premier p par une forme quadratique

2.20.1 Théorème de Gauss (1828)

Soit p un nombre premier tel que $p = 4n+1$, avec n entier, alors il existe un unique couple d'entiers naturels (a,b) telle que $p = a^2+b^2$ avec $a \equiv 1 \pmod p$.En 1828, Gauss 109, a prouvé que l'on a alors

Théorème 109

$$\binom{(p-1)/2}{(p-1)/4} \equiv 2a \pmod p$$

2.20.2 Théorème de Jacobi (1846)

Théorème 110 *Pour tout nombre premier $p \equiv 1 \pmod 3$. Alors en écrivant $4p = a^2+27b^2$, où le signe de a est choisit tel que $a \equiv 1 \pmod 3$, on a*

$$\binom{2(p-1)/3}{(p-1)/3} \equiv -a \pmod p$$

2.21 Théorème de Chowla ; Dwork et Evans (1986)

Avec la même définition de a que dans le théorème 109

Théorème 111 *Pour tout nombre premier $p \equiv 1 \pmod 4$, on a*

$$\binom{(p-1)/2}{(p-1)/4} \equiv (1 + \frac{2^{p-1}-1}{2})(2a - \frac{p}{2a}) \pmod{p^2}$$

2.22 Généralistions : q-analogues de certains théorèmes classiques

2.22.1 Définition des polynômes de Gauss

C'est à Gauss qu'on doit la généralisation des coefficients binomiaux qu'on 'a déja défini dans le premier chapitre de ce mémoire.

De nombreux auteurs ([18],1995), ([7],1999), ([91],2007) ([78],2007), ([24],2008), ([29],2008) ont déterminé des q-analogues pour des congruences classiques (congruences de Babbage, Wolstenholme, Glaisher,Wilson, Lehmer...).

Ainsi en 1995, Clark [18] obtint comme q-analogue pour la congruence de Babbage la congruence suivante

Théorème 112 *(Clark, 1995)*

$$\binom{ap}{bp}_q \equiv \binom{a}{b}_{q^{p^2}} \pmod{[p]_q^2}$$

En 2011, A. Straub ([94]) établit un $q-$analogue de la congruence classique de Ljunggren qui rappelons le affirme que pour tous entiers naturels a et b, on a :

$$\binom{ap}{bp} \equiv \binom{a}{b} \pmod{p^3}, \text{ pour tout nombre premier } p \geqslant 5. \tag{2.116}$$

Théorème 113 *Pour tout nombre premier $p \geqslant 5$, et pour tous entiers naturels a et b, on a*

$$\binom{ap}{bp}_q \equiv \binom{a}{b}_{q^{p^2}} - \binom{a}{b+1}\binom{b+1}{2}\frac{p^2-1}{12}(q^p-1)^2 \pmod{[p]_q^3} \tag{2.117}$$

La congruence (2.117) signifiant que l'on a

$$\binom{ap}{bp}_q - \left\{ \binom{a}{b}_{q^{p^2}} - \binom{a}{b+1}\binom{b+1}{2}\frac{p^2-1}{12}(q^p-1)^2 \right\} \in [p]_q^3 \mathbb{Z}[q]$$

La congruence 2.117 est bien un q-anologue de la congruence (2.116). On retrouve (2.116) quand on fait tendre q vers 1 dans 2.117.

Dans la preuve du théorème 113, Staub exploite le théorème suivant du à Shi and Pan [**?**]

Théorème 114 *Shi and Pan (2007). Pour tout nombre premier $p \geq 5$, on a*

$$\sum_{i=1}^{p-1} \frac{1}{[i]_q} = -\frac{p-1}{2}(q-1) + \frac{p^2-1}{24}(q-1)^2 [p]_q \pmod{[p]_q^2} \tag{2.118}$$

et

$$\sum_{i=1}^{p-1} \frac{1}{[i]_q^2} = -\frac{(p-1)(p-5)}{12}(q-1)^2 \pmod{[p]_q} \tag{2.119}$$

Les congruences (2.118) et (2.119) sont respectivement des q-analogues aux congruences cassiques

$$\sum_{i=1}^{p-1} \frac{1}{i} = 0 \pmod{p^2}$$

et

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

Chapitre 3

Super Congruences

"Mathematicians do not study objects ; but relations among objects ; they are indifferent to the replacement of objects by others as long as relations do not change. Matter is not important, only form interests them."

Henri POINCARE (1854 − 1912).

3.1 Introduction

Les congruences modulo une puissance d'un nombre premier sont appelées super congruences. L'une des plus anciennes super congruences est la congruence de Babbage obtenue en 1819 (Théorème 60 de ce mémoire) qu'on peut reformuler comme suit

$$\binom{2p}{p} \equiv \binom{2}{1} \pmod{p^2}, \text{ pour tout nombre premier } p \geqslant 3.$$

Une autre célèbre super congruence est la congruence de Morley obtenue en 1895 qui affirme que pour tout nombre premier $p \geqslant 5$, on a

$$(-1)^{(p-1)/2}\binom{p-1}{(p-1)/2} \equiv 4^{p-1} \pmod{p^3}.$$

Ces deux congruences on fait l'objet de généralistions et extensions les années qui suivirent l'année de leur pubication et cela jusqu'à nos jours.

Dans ce chapitre nous allons tout d'abord exposer une démonstration originale du théorème de Morley. Nous nous intéresserons ensuite aux nombreuses extensions du théorème de Babbage.

3.2 Preuve originale du théorème de Morley

Dans un récent papier (Prepint), intitulé "Morley's other miracle", C. Aebi et G. Cairns [3] parlent du théorème de Morley publié dans Annals of Mathematics en 1894/95 en ces termes

"*To appreciate the "miraculous" nature of this congruence, one first needs to compare it with other congruences know at the time. Some famous ones for primes* p include :

- *Fermat's little theorem :* $2^{p-1} \equiv 1 \pmod{p}$.
- *Wilson's theorem :* $(p-1)! \equiv -1 \pmod{p}$.
- *Lucas's theorem : If* $0 \leq n,\ j < p$, *then* $\binom{pm+n}{pi+j} \equiv \binom{m}{i}\binom{n}{i} \pmod{p}$.

Notice that they are all modulo p, *while Morley's congruence is modulo* p^3. *The difference between* $\bmod p^3$ *and* $\bmod p$ *is analogous to having a result to three significant figures, rather than just one sugnificant figure.*

The other striking aspect of Morley's congruence was the nature ofr his original proof, which made an ingenious use of integrationof trigonometric sums....".

Dans le même papier [3], C. Aebi et G. Cairns recensent les preuves données du théorème du théorème de Morley jusqu'à aujourd'hui en ces termes !

"*Subsequently two alternate proofs were given that used the properties of Bernoulli numbers : the* 1913 *Royal Danish Academy of Sciences paper by Nielsen ([?], p* 353*) and the* 1938 *Annals of Mathematics paper by Emma Lehmer ([61], p* 360*). More recently, we remark that Morley's congruence can be quickly deduced from Granville's elegant proof of Skula's conjecture [43].*

The main aim of this note is to establish Morley's congruence by entirey elementary number theory arguments... "

La preuve du théorème de Morley est obtenu alors par C. Aebi et G. Cairns au bout de deux pages de calculs sans doute élémentaires mais pour le moins basée sur des affirmations qui ne nous ont pas semblées évidentes. Leur preuve repose essentiellement sur le résultat suivant "$If\ p\ is\ prime\ and\ p > 3, then\ \sum_{0<i<j<p,\ i\ odd,\ j\ even} \frac{1}{ij} \equiv 0 \pmod{p}$", dont la preuve est loin d'être simple.

Dans ce qui suit nous allons exposer notre preuve du théorème de Morley de manière trés complète [63].

Notre preuve repose sur les trois lemmes suivants :

Lemme 115 *Pour tout nombre premier $p = 2n+1 \geq 5$, on a*

$$\sum_{k=1}^{2n} \frac{1}{k^2} \equiv 0 \ (\mathrm{mod}\, p). \tag{3.1}$$

$$\sum_{k=1}^{n} \frac{1}{k^2} \equiv 0 \ (\mathrm{mod}\, p) \tag{3.2}$$

$$\sum_{k=1}^{n} \frac{1}{(2k-1)^2} \equiv 0 \ (\mathrm{mod}\, p). \tag{3.3}$$

Lemme 116 *Pour tout entier $n \geq 1$, on a*

$$2^{2n}(2n)! = \prod_{k=1}^{n}((2n+1)^2 - (2k-1)^2) \tag{3.4}$$

Lemme 117 *Pour tout enier $n \geq 1$ et pour tous entiers non nuls $a_1, a_2, ..., a_n$, on a*

$$\prod_{k=1}^{n}(x^2 + a_k) \equiv \prod_{k=1}^{n} a_k + (\prod_{k=1}^{n} a_k)(\sum_{k=1}^{n} \frac{1}{a_k})x^2 \ (\mathrm{mod}\, x^4\mathbb{Z}[x]). \tag{3.5}$$

Les preuves de ces lemmes sont trés simples. Elles sont données en fin de démonstration.

Soit $p \geq 5$ un nombre premier, alors p peut s'écrire $p = 2n+1$ où $n = \frac{p-1}{2}$ est un entier ≥ 1. Lapplication de lemme 116 fournit la relation

$$2^{2n}(2n)! = \prod_{k=1}^{n}(p^2 - (2k-1)^2) \tag{3.6}$$

L'application du lemme 117 avec $a_k = -(2k-1)^2$ et pour $x = p$ nous fournit la relation

$$\prod_{k=1}^{n}(p^2 - (2k-1)^2) \equiv (-1)^n 1^2 3^2 ... (p-2)^2 - (-1)^n 1^2 3^2 ... (p-2)^2)(\sum_{k=1}^{n} \frac{1}{(2k-1)^2})p^2 \ (\mathrm{mod}\, p^4). \tag{3.7}$$

Or d'après le lemme 115, on a

$$(\sum_{k=1}^{n} \frac{1}{(2k-1)^2})p^2 \equiv 0 \ (\mathrm{mod}\, p^3) \ . \tag{3.8}$$

On déduit de (3.7) et (3.8) la congruence modulo p^3 suivante

$$\prod_{k=1}^{n}(p^2 - (2k-1)^2) \equiv (-1)^n 1^2 3^2 ... (p-2)^2 \ (\mathrm{mod}\, p^3). \tag{3.9}$$

Il résulte de (3.6),(3.9)

$$2^{2n}(2n)! \equiv (-1)^n 1^2 3^2 ... (p-2)^2 \pmod{p^3}. \tag{3.10}$$

Remarquons alors que l'on a

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

Soit

$$1^2 3^2 ... (p-2)^2 = \frac{((2n)!)^2}{2^{2n} n! n!}. \tag{3.11}$$

A la lumière de (3.11), la congruence (3.10) s'écrit

$$2^{2n}(2n)! \equiv (-1)^n \frac{((2n)!)^2}{2^{2n} n! n!} \pmod{p^3}. \tag{3.12}$$

comme $(2n)! = (p-1)!$ est un entier premier avec p et donc premier avec p^3, on déduit de (3.12) après simplification par $(2n)!$ et multiplication par 2^{2n} :

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

Ce qu'on peut encore écrire

$$(-1)^n \binom{2n}{n} \equiv 4^{2n} \pmod{p^3}. \tag{3.13}$$

Comme $n = \frac{p-1}{2}$, la relation (3.13) s'écrit

$$(-1)^{(p-1)/2} \binom{p-1}{(p-1)/2} \equiv 4^{p-1} (\bmod p^3)$$

Ce qui est bien la congruence de Morley.

Pour être que cette démonstrationsoit complète, il nous rest à prouver les lemmes 115, 116, 117.

Preuve du lemme 115 Bien que la relation (3.1) est un cas particulier du théorème On sait que $R_p = \{1, 2, ..p-1\}$ est u n système réduit de résidus modulo p. Comme $p \geq 5$, p est impair $\mathcal{R}_p = \{2k\,;\ k \in R_p\}$ est aussi un système de résidus modulo p. Il en résulte que

$$\sum_{k=1}^{2n} \frac{1}{k^2} = \sum_{k \in R_p} \frac{1}{k^2} \equiv \sum_{k \in \mathcal{R}_p} \frac{1}{k^2} = \sum_{k=1}^{2n} \frac{1}{(2k)^2} = \frac{1}{4}(\sum_{k=1}^{2n} \frac{1}{k^2}) \pmod{p}.$$

On en déduit que

$$\frac{3}{4} \sum_{k=1}^{2n} \frac{1}{k^2} \equiv 0 \pmod{p}, \qquad \text{pour } p \geq 5.$$

Il en résulte que pour

$$\sum_{k=1}^{2n} \frac{1}{k^2} \equiv 0 \ (\mathrm{mod}\, p).$$

La relation est prouvée.

Pour prouver la relation , remarquons que l

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

Il en résulte que

$$2\sum_{k=1}^{n} \frac{1}{k^2} \equiv (\sum_{k=1}^{n} \frac{1}{k^2} + \sum_{k=1}^{n} \frac{1}{(p-k)^2}) = \sum_{k=1}^{p-1} \frac{1}{k^2} \equiv 0 \ (\mathrm{mod}\, p)$$

On en déduit la relation (3.2).

Remarquons alors qu'on alors en vertu des relations (3.1) et (3.2)

$$\begin{aligned} \sum_{k=1}^{n} \frac{1}{(2k-1)^2} &= (\sum_{k=1}^{n} \frac{1}{(2k-1)^2} + \sum_{k=1}^{n} \frac{1}{(2k)^2}) - \sum_{k=1}^{n} \frac{1}{(2k)^2} \\ &= \sum_{k=1}^{2n} \frac{1}{k^2} - \frac{1}{4}\sum_{k=1}^{n} \frac{1}{k^2} \equiv 0 \ (\mathrm{mod}\, p). \end{aligned}$$

Preuve du lemme 116 *Pour tout entier $n \geq 1$, on a :*

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

Preuve du lemme 117 Soit un entier $n \geq 1$ et $a_1, a_2, ..., a_n$ des entiers non nuls. Posons pour $k \in \{1, 2, ..., n\}$:

$$\sigma_k = \sum_{1 \leq i_2 < i_2 < \cdots < i_k \leq n} a_{i_1} a_{i_2} ... a_{i_k}.$$

Pour $n = 1$, la relation (3.5) se vérifie directement. On peut donc supposer $n \geq 2$. On a alors

$$\prod_{k=1}^{n}(x + a_k) = \sigma_n + \sigma_{n-1}x + \sigma_{n-2}x^2 + \cdots + \sigma_1 x^{n-1} + x^n \tag{3.14}$$

$$\equiv \sigma_n + \sigma_{n-1}x \ (\mathrm{mod}\, x^2\mathbb{Z}[x]). \tag{3.15}$$

On en déduit la relation (3.5) en remplaçant x par x^2 dans (3.15) et en remarquant que

$$\sigma_n = \prod_{k=1}^{n} a_k \ \text{ et } \ \sigma_{n-1} = (\prod_{k=1}^{n} a_k)(\sum_{k=1}^{n} \frac{1}{a_k}).$$

Ce qui serait une amélioration de la congruence de Morley

3.3 Congruences de Babbage

Rappelons que Babbage affirme dans son article que c'est en cherchant une congruence analogue à la congruence de Wilson qui affirme que $(p-1)! + 1 \equiv 0 \ (\mathrm{mod}\, p)$ qu'il a été amené à découvrir cette congruence.

Signalons que le théorème de Lucas de 1878 (Théorème 85 de ce mémoire) permet d'obtenir seulement

$$\binom{2p}{p} \equiv \binom{2}{1} \ (\mathrm{mod}\, p)$$

Comme nous l'avons vu, au chapitre 2, la congruence de Babbage a été améliorée par Wolstenholme en 1862 (Théorème 73 de ce mémoire) en un résultat qu'on peut reformuler comme suit

$$\binom{2p}{p} \equiv \binom{2}{1} \ (\mathrm{mod}\, p^3). \text{ pour } p \geqslant 5.$$

Signalons que c'est après de nombreuses investigations numériques que Wolstenholme a été conduit à formuler et prouver ce dernier résultat.

En 1900, Glaisher (Théorème de ce mémoire) généralise le théorème de Wolstenholme en prouvant que pour tout entier naturel n, on a

$$\binom{np}{p} \equiv \binom{n}{1} \ (\mathrm{mod}\, p^3). \text{ pour } p \geqslant 5.$$

Il faut alors attendre l'année 1952 pour voir le congruence de Glaisher améliorée par Ljunggren (Théorème **??** de ce mémoire) et par Jacobsthal (Théorème 105 de ce mémoire).Glaisher prouve que l'on a pour tous entiers naturels n et m :

$$\binom{np}{mp} \equiv \binom{n}{m} \ (\mathrm{mod}\, p^3). \text{ pour } p \geqslant 5,$$

alors que Jacobsthal obtient la généralisation suivante du théorème deLjunggren

$$\binom{np}{mp}/\binom{n}{m} \in 1 + p^3nm(n-m)\mathbb{Z}_p \text{ pour } p \geqslant 5,$$

où $\mathbb{Z}_p$ est l'anneau des entiers p-adiques.

Remarquons encore que le théorème de Lucas de 1878 (Théorème 85 de ce mémoire) permettait déjà d'obtenir :

$$\binom{np}{mp} \equiv \binom{n}{m} \pmod{p}.$$

Signalons qu'en 1990, D. F. Bailey retrouve la congruence de Ljunggren de manière combinatoire ainsi qu'une extension du théorème de Lucas, en prouvant que

$$\binom{Np^3+n}{Mp^3+m} \equiv \binom{N}{M}\binom{n}{m} \pmod{p^3}. \text{ pour } p \geqslant 5.$$

En 1960, G. S. Kazandzidis étudie les congruences de Jacobsthal et des congruences similaires et obtient de remarquables résultats que nous allons exposer au paragraphe suivant.

Signalons qu'en 1990 J.W.L.Glaisher avait amélioré la congruence de Wolstenholme en prouvant que pour tout entier p premier ≥ 5 on a

$$\binom{2p-1}{p-1} \equiv 1 - 2p\sum_{k=1}^{p-1}\frac{1}{k} \pmod{p^4} \tag{3.16}$$

En utilisant le nombres de Bernoulli B_{p-3} la relation de Glaisher 3.16 devient alors pour tout nombre premier $p \geq 7$

$$\binom{2p-1}{p-1} \equiv 1 - \frac{2}{3}p^3B_{p-3} \pmod{p^4} \tag{3.17}$$

Mieux encore J.L.W.Glaisher prouva en 1900 dans ses articles que pour tout entier n positif $n \geq 1$ et pour tout nombre premier $p \geq 5$ alors on

$$\binom{np-1}{p-1} \equiv 1 - \frac{1}{3}n(n-1)p^3B_{p-3} \pmod{p^4} \tag{3.18}$$

En prenant $n = 2$ dans la relation 3.18 on retrouvera la relation 3.17

En 1995 R.J.McIntosh avait établi une généralisation de la congruence de Glaisher

en prouvant que pour tout p premier ≥ 7 on a

$$\binom{2p-1}{p-1} \equiv 1 - p^2\sum_{k=1}^{p-1}\frac{1}{k^2} \pmod{p^5} \tag{3.19}$$

En utilisant le nombre de Bernoulli $B_{p^3-p^2-2}$ dans la relation 3.19

$$\binom{2p-1}{p-1} \equiv 1 - p^3 B_{p^3-p^2-1} (\mathrm{mod}\, p^5) \tag{3.20}$$

aussi en 2007 J Zhao prouva que pour tout entier premier $p \geq 7$ on a

$$\binom{2p-1}{p-1} \equiv 1 + 2p \sum_{k=1}^{p-1} \frac{1}{k} (\mathrm{mod}\, p^5) \tag{3.21}$$

En 2008 C.Helou et G.Terjanian [46]ont établi plusieurs types de congruence de Wolstenholme modulo p^k pour p premier et k entier $\in \mathbb{N}$et $k \leq 6$

$$\binom{2p-1}{p-1} \equiv 1 - p^3 B_{p^3-p^2-1} + p^5 (\frac{1}{3} B_{p-3} - \frac{6}{5} B_{p-5}) (\mathrm{mod}\, p^6) \tag{3.22}$$

En 2010 R Tauraso prouva que pour tout p premier ≥ 7 on a

$$\binom{2p-1}{p-1} \equiv 1 + 2p \sum_{k=1}^{p-1} \frac{1}{k} + \frac{2p^3}{3} \sum_{k=1}^{p-1} \frac{1}{k^3} (\mathrm{mod}\, p^6) \tag{3.23}$$

cette dernière congruence peut être écrite aussi comme suit 2.94

$$\binom{2p-1}{p-1} \equiv 1 - 2p \sum_{k=1}^{p-1} \frac{1}{k} - 2p^2 \sum_{k=1}^{p-1} \frac{1}{k^2} (\mathrm{mod}\, p^6) \tag{3.24}$$

ces deux congruences modulo p^6peuvent être considerées comme généralisation de la congruence de Wolstenholme .

Récemment en Aout 2011 R Méstrovic 2.93prouva que

$$\binom{2p-1}{p-1} \equiv 1 - 2p \sum_{k=1}^{p-1} \frac{1}{k} + 4p^2 \sum_{1 \leq i < j \leq p-1} \frac{1}{ij} (\mathrm{mod}\, p^7) \tag{3.25}$$

sachant que

$$2 \sum_{1 \leq i < j \leq p-1} \frac{1}{ij} = (\sum_{k=1}^{p-1} \frac{1}{k})^2 - \sum_{k=1}^{p-1} \frac{1}{k^2}$$

la relation 3.25 devient alors

$$\binom{2p-1}{p-1} \equiv 1 - 2p\sum_{k=1}^{p-1}\frac{1}{k} + 2p^2((\sum_{k=1}^{p-1}\frac{1}{k})^2 - \sum_{k=1}^{p-1}\frac{1}{k^2})(\mathrm{mod}\, p^7) \tag{3.26}$$

En 2011 R.Mestrovic appliqua à la relation 3.25 la technique de C.Helou et G.Terjanian et il obtint la relation suivante

$$\begin{aligned}\binom{2p-1}{p-1} &\equiv 1 - p^3 B_{p^4-p^3-2} + p^5(B_{p^2-p-4} - 2B_{p^4-p^3-4} \\ &\quad + p^6(\frac{2}{9}B_{p-3}^2 - \frac{1}{3}B_{p-3} - \frac{1}{10}B_{p-5})(\mathrm{mod}\, p^7)\end{aligned}$$

Très récèmment après Aout 2011 date de parution de l'article [65] R Tauraso dans une correspondance privée à R Méstrovic l'informa qu'en appliquant à la relation 3.26une formule similaire à celle appliquée pour trouver la congruence modulo 7 la relation 3.26 deviendra alors comme suit

$$\begin{aligned}\binom{2p-1}{p-1} &\equiv 1 + 2p\sum_{k=1}^{p-1}\frac{1}{k} + \frac{2}{3}p^3\sum_{k=1}^{p-1}\frac{1}{k^3} + 2p^2(\sum_{k=1}^{p-1}\frac{1}{k})^2 + \\ &\quad + \frac{2}{5}p^5\sum_{k=1}^{p-1}\frac{1}{k^5} + \frac{4}{3}p^5(\sum_{k=1}^{p-1}\frac{1}{k})(\sum_{k=1}^{p-1}\frac{1}{k^3})(\mathrm{mod}\, p^9)\end{aligned}$$

Ce qui est une amélioration de la congruence de Wolstenholme modulo p^9

et en transformant le terme $\sum_{k=1}^{p-1}\frac{1}{k^5}$

$$\begin{aligned}\binom{2p-1}{p-1} &\equiv 1 + p\sum_{k=1}^{p-1}\frac{1}{k} - \frac{p^2}{2}(5(\sum_{k=1}^{p-1}\frac{1}{k})^2 + \sum_{k=1}^{p-1}\frac{1}{k^2}) \\ &\quad - \frac{p^3}{3}(15(\sum_{k=1}^{p-1}\frac{1}{k})(\sum_{k=1}^{p-1}\frac{1}{k^2}) - 2\sum_{k=1}^{p-1}\frac{1}{k^3}) \\ &\quad + \frac{p^4}{40}(35(\sum_{k=1}^{p-1}\frac{1}{k^2})^2 - 26\sum_{k=1}^{p-1}\frac{1}{k^4})(\mathrm{mod}\, p^9)\end{aligned}$$

3.4 Congruences de Kazandzidis

Kazandzidis ([53] et [54]) définit un coefficient qu'on notera dans ce mémoire $\binom{n}{k}^*$ ayant des propriétés similaires au coefficient binomial.

Définition 118 *Pour des entiers n et $k \geqslant 0$, on définit*

$$\begin{aligned}\binom{n}{0}^* &= 1\\ \binom{n}{k}^* &= \frac{n(n+1)\cdots(n+k-1)}{k!},\ \textit{pour } k \geqslant 1.\end{aligned}$$

Pour tous entiers n et $k \geqslant 0$, $\binom{n}{k}^*$ est un entier. On a d'ailleurs

$$\binom{n}{k}^* = \binom{n+k-1}{k}.$$

Kazandzidis obtient le résultat suivant

Théorème 119 *Soit n un entier, m un entier naturel et $p \geqslant 3$ un nombre premier. Alors*

$$\binom{np}{mp}^* / \binom{n}{m}^* \equiv \begin{cases} 1 - p^2nm(n+m) \pmod{p^3} & \textit{si } p = 3 \\ 1 \pmod{p^3} & \textit{si } p > 3 \end{cases},$$

et

$$\binom{np}{mp} / \binom{n}{m} \equiv \begin{cases} 1 - p^2nm(n-m) \pmod{p^3} & \textit{si } p = 3 \\ 1 \pmod{p^3} & \textit{si } p > 3 \end{cases},$$

Théorème 120 *(de Lucas) Soit p un nombre premier et n un entier naturel, alors on a*

$$\binom{np}{nm} \equiv \binom{p}{m} \pmod{pn\mathbb{Z}_p}$$

Théorème 121 *Pour tout nombre premier $p \geq 5$, on a*

$$\binom{np}{mp} \equiv \binom{n}{m} \pmod{p^3nm(n-m)\binom{n}{m}\mathbb{Z}_p}$$

$$\binom{3n}{3k} \equiv \binom{n}{m} \pmod{3^2nm(n-m)\binom{n}{m}\mathbb{Z}_3}$$

Preuve. cf [85], p. 380. □

3.4.1 Congruences de Jacobsthal-Kazandzidis

Théorème 122 *Soient m et n deux entiers tels que $0 \leqslant m \leqslant n$ et soit p un nombre premier. Alors on a*

$$\binom{np}{mp} \equiv K_p(n,m)\binom{n}{m} \pmod{p^4 nm(n-m)\binom{n}{m}\mathbb{Z}_p}$$

où

$$K_p(n,m) = \begin{cases} 1-(B_{p-3}/3)p^3 mn(m-n) & si\ p \geqslant 5 \\ 1+45nm(n-m) & si\ p=3 \\ (-1)^{m(n-m)}P(n,m) & si\ p=2, \end{cases}$$

avec

$$P(n,m) = 1+6nm(n-m)-4nm(n-m)(n^2-nm+m^2)+2(nm(n-m))^2$$

3.5 Théorème de Zhao (2006)

En 2006, J. Zhao [101] prouve le résultat suivant

Théorème 123 *Zhao (2006) Pour tout nombre premier $p \geq 7$, on a*

$$\binom{np}{mp}/\binom{n}{m} \equiv 1-\frac{1}{3}p^2 nm(n-m)B_{p-3} \pmod{p^5} .$$

J. Zhao établit ce résultat grace à une étude des propriétés des sommes

$$H(s_1,s_2,...,s_d\ ;n) := \sum_{1\leq k_1<\cdots<k_d\leq n} k_1^{-s_1}...k_d^{-s_d},$$

comme la propriété suivante :

$$H(s\ ;n)H(t\ ;n) = H(t,s\ ;n)+H(t+s\ ;n)+H(s,t\ ;n).$$

Preuve. voir **??** □

Chapitre 4

Congruences vérifiées par les nombres de Stirling

"As with everything else, so with a mathematical theory : beauty can be perceived, but not explained

Arthur CAYLEY (1821 − 1895).

4.1 Introduction

Selon le mathématicien écossais Charles Tweedy (1868 − 1925), [97] et [98], c'est à Niels Nielsen (1865 − 1931) qu'on doit la dénomination "nombres de Stirling", en l'honneur de James Stirling (1692 − 1770) pour deux familles d'entiers qui s' avèreront particulièrement importantes en mathématiques.

Ces nombres entiers apparaissent pour la première fois en 1730 dans l'ouvrage de James Stirling [89]. Ils ont été étudiés depuis par de nombreux auteurs parmi lesquelles on peut citer Niels Nielsen (1865 − 1965) et Charles Jordan(1871 − 1959),Louis Comtet (1928) ,H.W.Gould (1938).

Il semblerait même que les nombres de stirling de première éspèce étaient déjà connus par le mathématicien anglais Thomas Herriot (1560 − 1621) ,au musée de British on trouve un de ses manuscrits [47] qui traite du développement des polynomes $\binom{n}{k}$ pour $k \leqslant 7$.

Niels Nielsen a publié en 1923 un "traité élémentaire des nombres de Bernoulli" de près de 400 pages [76] qui ne fut réédité que seulement en 2005 et aussi un ouvrage [77] intitulé "Recherches sur les polynômes de Stirling" en 1920 (108 pages) . Dans l'introduction de ce dernier ouvrage il écrit

"*Les nombres de Stirling étant intimement liés aux nombres de Bernoulli, j'étudie depuis*

plus de trente ans, ces nombres compliqués, sur lesquels j'ai publié plusieurs notes, savoir :..."

L'importance de l'étude des nombres de Stirling a été aussi souligné par Charles Jordan en ces termes dans son ouvrage [51] intitulé "Calculus of Finite Difference". Ce dernier ouvrage de près de 700 pages a plusieurs fois été réédité.

"*Stirling's Numbers are of the greatest utility in Mathematical Calculus. This however has not been fully recognised ; the numbers have been neglected, and are seldom used. This is especially due to the fact that different authors have reintroduced them under different names and notations, not mentioning that they dealt with the same numbers. Stirling's numbers are as important or even more so than Bernoulli's numbers ; they should occupy a central position in the Calculus of Finite Differences.*"

Après **James Stirling** nombreux sont les mathématiciens qui se sont interressés et ont étudié les nombres de Stirling, on peut citer :

- Niels Nielsen (1865 – 1931)
- Charles Tweedie (1868 – 1925)
- Charles Jordan (1871 – 1959)
- Leonard.Carlitz (1907 – 1999)
- D.S.Mitrinovic (1908 – 1995) et R.S.mitrinovic (1909 – 1993)
- Louis Comtet (1928 – 2008)
- Henry wadsworth Gould (1928)
- Donald.Ervin.Knuth (1938)

Ce chapitre comporte quatre paragraphes. Nous rappelons dans le second paragraphe la définition, les notations utilisées par divers mathématiciens ,on en citera Nielsen ,Comtet et Knuth et on donnera certaines propriétés basiques des nombres de Stirling. Dans le troisieme paragraphe, nous nous intéresserons à différentes congruences vérifiées par les nombres de Stirling. Nous terminerons ce chapitre par un quatrième paragraphe consacré à la démonstration qu'a donné Edouard Lucas du théorème de Von staudt et Clausen.

4.2 Définitions et notations des nombres de Stirling.

Il n'y a pas de notations standards pour les nombres de Stirling

Donald.E.Knuth dans son article intitulé "two notes on notation" qualifie de presque scandaleux cette absence de standartisation des nombres de Stirling .

K.Goldberg ,**M.Newman** ,**E.Haynsworth** ,débutent leur chapitre "Combinatorial Analysis " dans le NBS handbook en remarquant que les nombres de Stirling n'ont jamais été standartisés.

Charles Jordan dans son ouvrage "Calculus of finite differences " édité en 1947 souligne

l'importance des nombres de Stirling en Mathématiques qui n'ont pas encore été totalement reconnus et explique la raison de leur rare utilisation au fait qu'ils ont souvent été réintroduits par des auteurs sous d'autres formes et notations méconnues sans pour autant signaler qu'il s'agissait des mêmes nombres.

Tableau des notations des nombres de Stirling de première espèce

Notation	*Auteur*	*Source*
$s(n,k)$	J.Riordan	Combinatorial Identities (1968)
$S_1(n,k)$	L.Carlitz	Numeros papers (1971)
$(-1)^{n-k}S_1(n-1,n-k)$	H.W.Gould	Divers papiers (1956)
$(-1)^{n-k}\begin{bmatrix}n\\k\end{bmatrix}$	D.E.Knuth	The art of computer programming (1968)
$(-1)^{n-k}\mathbf{S}_k^n$	G.Polya	Notes on combinatorics (1978)
$(-1)^{n-k}\left[C_{n-k}(n-1)\right]$	J.G.Hagen	Combinationen ohne Wiederholungen (1891)
$(-1)^{n-k}C_n^{n-k}$	N Nielsen	1906
S_n^k	C Jordan	1939
$S_n^{(k)}$	K Goldberg	1959
$s(n,k)$	L Comtet	1970

Tableau des notations des nombres de Stirling de deuxième espèce

Notation	*Auteur*	*Source*
$S(n,k)$	J.Riordan	Combinatorial Identities (1968)
$S(n,k)$	L.Carlitz	Numeros papers (1971)
$S_2(k,n-k)$	H.W.Gould	Divers papiers (1956
$\begin{Bmatrix}n\\k\end{Bmatrix}$	D.E.Knuth	The art of Computer Programming (1968)
S_k^n	G.Polya	Notes on combinatorics (1978)
$\left[C_{n-k}^{\omega}(k)\right]$	J.G.Hagen	Combinationen mit Wiederholungen(1891)
$\check{C}_{k+1}^{n-k}$	N Nielsen	1906
C_n^k	C Jordan	1939
$\mathbb{S}_n^{(k)}$	K Goldberg	1959
$S(n,k)$	L Comtet	1970

Nous préçiserons et exposerons les notations utilisées par quelques mathématiciens exemple **Niels Nielsen**,**Louis Comtet** et **Donald E Knuth** ,préçisons donc ces notations :

Notations de Nielsen Niels Nielsen à écrit divers ouvrages sur les nombres de Stirling ,on citera "Recherches sur les polynômes de Stirling "qui a été édité en 1920 et aussi "Traité élémentaire des nombres de Bernoulli "

Voici ce que dit Niels Nielsen dans son ouvrage "Recherches sur les polynômes de Stirling "

"Jacobus Stirling dans son traité "Methodus Differentialis" interressant mais peu connu a étudié les deux classes de nombres positifs entiers que nous désignerons dans ce qui suit par

C_{n+1}^{p} et $\check{C}_{n+1}^{p}$,et l'étude de Stirling est si profonde qu'il a calculé des petites tables et des C_{n+1}^{p} et des $\check{C}_{n+1}^{p}$,c'est pourquoi nous désignons comme nombres de Stirling de première espèce et seconde espèce les C_{n+1}^{p} respectivement les $\check{C}_{n+1}^{p}$.

Les deux classes de positifs entiers introduits par Stirling jouant un rôle assez fondamental et dans l'Analyse et dans la théorie des Nombres ,ils ont été étudiés par beaucoup de géomètres ,nous nous bornerons à citer ici EULER,LAPLACE,HERSCHEL,GRUNERT,et SCHLOMILCH.

Nielsen définit d'abord les factorielles ω_n et ω_{-n} respectivement d'ordre positif et négatif

Pour $n \geqslant 0$ les factorielles d'ordres $+n$ et $-n$ sont définies comme suit

$$\begin{aligned} \omega_n(x) &= x(x+1)(x+2).....(x+n-1) \\ \omega_{-n}(x) &= \frac{1}{x(x+1)(x+2).....(x+n-1)} \\ \omega_0(x) &= 1 \end{aligned}$$

Alors

$$\omega_{n+1}(x) = \sum_{p=0}^{n+1} C_{n+1}^{p} x^{n+1-p}$$

$$\omega_{n+1}(x) = C_{n+1}^{0} x^{n+1} + C_{n+1}^{1} x^{n} + ...C_{n+1}^{p} x^{n+1-p}..... + C_{n+1}^{n} x$$

Les entiers positifs C_{n+1}^{p} sont désignés comme les coefficients de factorielle positive ou les nombres de Stirling de première espèce de l'ordre $n+1$ et on a

$$\begin{aligned} C_{n}^{0} &= 1 \quad n \geqslant 0 \\ C_{n+1}^{n} &= n! \end{aligned}$$

et les entiers positifs $\check{C}_{n+1}^{p}$ sont désignés comme les coefficients de la factorielle négative ou les nombres de Stirling de seconde espèce de l'ordre $-n-1$ et on a

$$\begin{aligned} \omega_{-(n+1)}(x) &= \sum_{s=0}^{\infty} \frac{(-1)^s \check{C}_{n+1}^{s}}{x^{n+s+1}} \quad \text{pour} \quad |x| > n \\ \check{C}_{n+1}^{r} &= \frac{1}{n!} \sum_{s=0}^{s=n} (-1)^s \binom{n}{s} (n-s)^{n+r} \\ \check{C}_{n}^{0} &= 1 \quad n \geqslant 0 \end{aligned}$$

Nielsen souligne que les nombres de Stirling de première espèce ne sont définis que de façon combinatoire alors que les nombres de Stirling de deuxième espèce dont donnés par des expressions explicites.

Notations de Comtet Pour $n \in \mathbb{N}$, $(x)_n$ et $\langle x \rangle_n$ sont les polynômes de $\mathbb{Z}[x]$ définis par

$$(x)_n = \prod_{k=0}^{n-1}(x-k) \qquad \text{et} \qquad \langle x \rangle_n = \prod_{k=0}^{n-1}(x+k).$$

Les polynômes $(x)_n$ et $\langle x \rangle_n$ sont appelés respectivement poynômes factorielles descendantes et polynômes factorielles montantes. On a $(x)_0 = 1$, $(x)_n = x(x-1)...(x-n+1)$ pour $n \geq 1$, $\langle x \rangle_0 = 1$ et $\langle x \rangle_n = x(x+1)...(x+n-1)$ pour $n \geq 1$. Pour tout $n \geq 0$, on a $\deg(x)_n = \deg \langle x \rangle_n = n$. Il en résulte que $((x)_n)_{n\geq 0}$ et $(\langle x \rangle_n)_{n\geq 0}$ constituent des bases du $\mathbb{Q}$ espace vectoriel $\mathbb{Q}[x]$. Les nombres de Stirling de première espèce $s(n,k)$ et de seconde espèce $S(n,k)$ sont définis par les relations

$$(x)_n = \sum_{k\geq 0} s(n,k)x^k \qquad \text{et} \qquad x^n = \sum_{k\geq 0} S(n,k)(x)_k.$$

Notations de Knuth Pour $n \in \mathbb{N}$, $x^{\underline{n}}$ et $x^{\bar{n}}$ sont les polynômes de $\mathbb{Z}[x]$ définis par

$$x^{\underline{n}} = \prod_{k=0}^{n-1}(x-k) \qquad \text{et} \qquad x^{\bar{n}} = \prod_{k=0}^{n-1}(x+k). \tag{4.1}$$

Les nombres de Stirling de première espèce non signés $\begin{bmatrix} n \\ k \end{bmatrix}$ et de seconde espèce $\begin{Bmatrix} n \\ k \end{Bmatrix}$sont définis par les relations

$$x^{\bar{n}} = \sum_{k\geq 0} \begin{bmatrix} n \\ k \end{bmatrix} x^k \quad \text{et} \quad x^n = \sum_{k\geq 0} \begin{Bmatrix} n \\ k \end{Bmatrix} x^{\underline{k}} \tag{4.2}$$

On a les relations suivantes

$$\begin{aligned} (x)_n &= x^{\underline{n}}, \quad \langle x \rangle_n = x^{\bar{n}} \\ s(n,k) &= (-1)^{n-k} \begin{bmatrix} n \\ k \end{bmatrix} \\ S(n,k) &= \begin{Bmatrix} n \\ k \end{Bmatrix} \end{aligned}$$

Dans ce mémoire, nous utiliserons indifféremment aussi bien les notations de Comtet que les notations de Jovan Karamata préconisées par Graham, Knuth et Patashnik [40]

Analogie de propriétés vérifiées par les nombres de Stirling et les coefficients binomiaux Proches de la notation $\binom{n}{k}$ des coefficients binomiaux (pour $(n,k) \in \mathbb{N}^2$), les notations de Knuth se justifient par les nombreuses propriétés des nombres de Stirling analogues a celles des coefficients binomiaux. Ainsi les nombres de Stirling vérifient des propriétés analogues aux propriétés suivantes vérifiées par les coefficients binomiaux :

$$\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1} \text{ pour } n \geq 1 \text{ et } k \geq 1$$

et

$$\binom{n}{0} = 1 \text{ et } \binom{0}{k} = \delta_{0,k} \text{ pour } n \geq 0 \quad \text{et } \ k \geq 0.$$

Pour les notations de Nielsen

$$\begin{aligned} C_{n+1}^r &= C_n^r + nC_n^{r-1} \quad 1 \leqslant r \leqslant n-1 \\ C_{n+1}^n &= nC_n^{n-1} = n! \\ C_{n+1}^0 &= C_n^0 = 1 \quad n > 0, C_1^r = 0 \ r \geqslant 1 \end{aligned}$$

$$\begin{aligned} \check{C}_n^r &= \check{C}_{n+1}^r - n\check{C}_{n+1}^{r-1} \ \ r \geqslant 1 \\ \check{C}_{n+1}^0 &= \check{C}_n^0 = 1 \quad n \geqslant 0 \\ \check{C}_1^r &= 0 \quad r \geqslant 1 \end{aligned}$$

On a en effet les deux théorèmes suivants :

Théorème 124 *On a*

$$\begin{bmatrix} n \\ k \end{bmatrix} = (n-1)\begin{bmatrix} n-1 \\ k \end{bmatrix} + \begin{bmatrix} n-1 \\ k-1 \end{bmatrix} \ \ \textit{pour } n \geq 1 \ \ \textit{et } \ k \geq 1 \tag{4.3}$$

et

$$\begin{bmatrix} n \\ 0 \end{bmatrix} = \delta_{n,0} \ \textit{et} \ \begin{bmatrix} 0 \\ k \end{bmatrix} = \delta_{0,k} \ \textit{pour } n \geq 0 \ \ \textit{et } \ k \geq 0$$

Preuve. Il suffit de remarquer que l'on a pour $n \geq 1$

$$x^{\bar{n}} = \prod_{k=0}^{n-1}(x+k) = \ x^{\overline{n-1}}(x+n-1)$$

Ce qui se traduit par la relation

$$\sum_{k\geq 0} \begin{bmatrix} n \\ k \end{bmatrix} x^k \ = (x+n-1)\sum_{k\geq 0} \begin{bmatrix} n-1 \\ k \end{bmatrix} x^k. \tag{4.4}$$

En identifiant le coefficient de x^k dans le premier membre de (4.4) avec le coefficient de x^k dans le second membre de (4.4), on trouve

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

Les relations

$$\begin{bmatrix} n \\ 0 \end{bmatrix} = \delta_{n,0} \text{ et } \begin{bmatrix} 0 \\ k \end{bmatrix} = \delta_{0,k} \text{ pour } n \geq 0 \text{ et } k \geq 0$$

sont immédiates avec la définition (4.2). □

Avec les notations de Comtet, la première relation de (4.3) s'écrit

$$s(n,k) = s(n-1,k-1) - (n-1)s(n-1,k) \text{ pour } n \geq 1 \text{ et } k \geq 1. \tag{4.5}$$

Avec les notations de Nielsen la première relation de 4.3 s'écrit

$$C_{n+1}^{r} = C_{n}^{r} + nC_{n}^{r-1} \quad 1 \leqslant r \leqslant n-1$$

On a aussi pour les nombres de Stirling de deuxième espèce des relations analogues

Théorème 125

$$\begin{Bmatrix} n \\ k \end{Bmatrix} = k\begin{Bmatrix} n-1 \\ k \end{Bmatrix} + \begin{Bmatrix} n-1 \\ k-1 \end{Bmatrix} \textit{ pour } n \geq 1 \textit{ et } k \geq 1 \tag{4.6}$$

et

$$\begin{Bmatrix} n \\ 0 \end{Bmatrix} = \delta_{n,0} \textit{ et } \begin{Bmatrix} 0 \\ k \end{Bmatrix} = \delta_{0,k} \textit{ pour } n \geq 0 \textit{ et } k \geq 0.$$

Observons que l'on a

$$\begin{aligned} x(x)_k &= (x-k)(x)_k + k(x)_k \\ &= (x)_{k+1} + k(x)_k. \end{aligned}$$

Il en résulte que l'on a

$$\begin{aligned} x^n &= \sum_{k\geq 0} S(n,k)(x)_k \\ &= x(\sum_{k\geq 0} S(n-1,k)(x)_k \\ &= \sum_{k\geq 0} S(n-1,k)((x)_{k+1} + k(x)_k) \end{aligned}$$

Ainsi on a

$$x^n = \sum_{k\geq 0} S(n,k)(x)_k = \sum_{k\geq 0} S(n-1,k)((x)_{k+1} + k(x)_k) \tag{4.7}$$

La relation (4.7) représente deux décompositions du vecteur x^n sur la base $((x)_k)_{k\geq 0}$. En identifiant la composante de x^n sur $(x)_k$ qui vaut $S(n,k)$ dans le premier membre de (4.7) avec la composante de $(x)_k$ dans le second membre de (4.7), on obtient

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

C'est à dire avec les notations de Knuth

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

Les relations $\left\{ {n \atop 0} \right\} = \delta_{n,0}$ et $\left\{ {0 \atop k} \right\} = \delta_{0,k}$ pour $n \geq 0$ et $k \geq 0$, sont immédiates sur la définition (4.2).

Et avec les notations de Nielsen

$$\check{C}_n^r = \check{C}_{n+1}^r - n\check{C}_{n+1}^{r-1} \quad r \geqslant 1$$

Les relations (4.3) et (4.6) permettent de construire les triangles de Stirling de manière analogue à la construction du triangle de Pascal pour les coefficients binomiaux.

Triangle de stirling pour les nombres de Stirling de première espèce $\left[{n \atop k} \right]$

n	$\left[{n \atop 0} \right]$	$\left[{n \atop 1} \right]$	$\left[{n \atop 2} \right]$	$\left[{n \atop 3} \right]$	$\left[{n \atop 4} \right]$	$\left[{n \atop 5} \right]$	$\left[{n \atop 6} \right]$	$n!$
0	1							1
1	0	1						1
2	0	1	1					2
3	0	2	3	1				6
4	0	6	11	6	1			24
5	0	24	50	35	10	1		120
6	0	120	274	225	85	15	1	720

On a

$$\sum_{k=0}^{n} \left[{n \atop k} \right] = 2^n$$

Triangle de Stirling pour les nombres de Stirling de seconde espèce $\left\{ {n \atop k} \right\}$

n	$\left\{ {n \atop 0} \right\}$	$\left\{ {n \atop 1} \right\}$	$\left\{ {n \atop 2} \right\}$	$\left\{ {n \atop 3} \right\}$	$\left\{ {n \atop 4} \right\}$	$\left\{ {n \atop 5} \right\}$	$\left\{ {n \atop 6} \right\}$	P_n
0	1							1
1	0	1						1
2	0	1	1					2
3	0	1	3	1				5
4	0	1	7	6	1			15
5	0	1	15	25	10	1		52
6	0	1	31	90	65	15	1	203

Définition 126 *Le n-ième de Bell P_n est définie par*

$$P_n = \sum_{k=0}^{n} \left\{ {n \atop k} \right\}.$$

P_n est le nombre de partitions d'un ensemble à n éléments, on a

$$P_0 = 1, \quad P_1 = 1, \quad P_2 = 2, \quad P_3 = 5, \quad P_4 = 15, \quad P_5 = 52, \quad P_6 = 203.$$

interprétation combinatoire Les nombres de Stirling $\left[{n \atop k} \right]$ et $\left\{ {n \atop k} \right\}$ ont une interprétation combinatoire analogue à celle du coefficient binomial $\binom{n}{k}$. On a :

$\binom{n}{k} =$ nombre de parties de $\{1, 2, ..., n\}$ à k éléments.

$\left[{n \atop k} \right]$ = nombre de permutations de $\{1, 2, ..., n\}$ à k orbites.

$\left\{ {n \atop k} \right\}$ = nombre de partitions de $\{1, 2, ..., n\}$ à k éléments.

Séries génératrices Signalées déja parTweedie en 1918 ([97], *p.*10) et retrouvées en 2008 par Janjic [58], les propriétés des nombres de Stirling données dans le lemme suivant permettent de retrouver (ou de découvrir) aisément des relations vérifiées par les nombres de Stirling. Dans ce lemme, $D = \frac{d}{dx}$ désigne l'opérateur de dérivation.

Lemme 127 *Pour tous polynômes f et g de $\mathbb{C}[x]$, on a*

$$D^n(f(\ln(1+x)) = \frac{1}{(1+x)^n} \sum_{k=1}^{n} s(n,k) f^{(k)}(\ln(1+x)) \text{ pour } n \geq 0$$

et

$$D^n(g(e^x)) = \sum_{k=1}^{n} S(n,k) e^{kx} \; g^{(k)}(e^x)$$

Ce lemme se prouve aisément à l'aide d'un raisonnement par récurrence et en exploitant les relations des théorèmes (124) et (125).

En appliquant ce lemme à f et g définies par

$$f(x) = \frac{x^k}{k!} \quad \text{et} \quad g(x) = \frac{(x-1)^k}{k!}$$

On trouve que

$$D^n(\frac{(\log(1+x))^k}{k!})_{x=0} = s(n,k) \;\; \text{et} \;\; D^n(\frac{(\exp(x)-1)^k}{k!})_{x=0} = S(n,k).$$

Il en résulte que l'on a les séries génératrices suivantes (bien connues [19] et [20]) :

$$\frac{(\log(1+x))^k}{k!} = \sum_{n\geq 0} s(n,k)\frac{x^n}{n!}$$
$$\frac{(\exp(x)-1)^k}{k!} = \sum_{n\geq 0} S(n,k)\frac{x^n}{n!}$$

Expressions de $s(n,k)$ et $S(n,k)$ à l'aide des coefficients binomiaux. Une des formules explicites connues parmi les plus simples exprimant $s(n,k)$ à l'aide de coefficients binomiaux est celle donnée dans le théorème suivant :

Théorème 128 *Pour tous entiers $n \geq 0$ et $k \geq 0$, on a*

$$s(n,k) = \sum_{0\leq j\leq h\leq n-k} (-1)^{j+h}\binom{h}{j}\binom{n-1+h}{n-k+h}\binom{2n-k}{n-k-h}\frac{(h-j)^{n-k+h}}{h!}.$$

Cette formule exacte des nombres de Stirling de première espèce a été découverte par Schlomilch en 1852 (voir [38], [20])

Preuve. voir [23],page 14 ,[19] tome 2 page 51,[20] page 216 . □

On peut cependant obtenir des formules simples dans des cas particuliers. Ainsi il est facile de constater que :

$$s(n,1) = (-1)^{n-1}(n-1)! \tag{4.8}$$
$$s(n,2) = (-1)^n(n-1)!H_{n-1} \tag{4.9}$$

$$s(n,n-1) = -\binom{n}{2}$$
$$s(n,n) = 1$$

Dans des articles [69],[70],[71],les mathématiciens D.S.Mitrinovitch et R.S.Mitrinovic ont établi des tableaux relatifs aux nombres de stirling de 1 ere espèce,on citera quelques exemples

.

$$s(n,n-9) = \frac{1}{768}\binom{n}{10}n(n-1)P_9(n)$$
$$s(n,n-8) = \frac{1}{3840}\binom{n}{9}P_8(n)$$
$$s(n,n-7) = \frac{1}{144}\binom{n}{8}n(n-1)P_7(n)$$

$$s(n,n-6)=\frac{1}{576}\binom{n}{7}P_6(n)$$

$$s(n,n-5)=\frac{1}{16}\binom{n}{6}n(n-1)P_5(n)$$

$$s(n,n-4)=\frac{1}{48}\binom{n}{5}P_4(n)$$

$$s(n,n-3)=\frac{1}{2}\binom{n}{4}n(n-1)P_3(n)$$

$$s\left(n,n-2\right)=\frac{1}{4}\binom{n}{3}(3n-1)P_2(n)$$

ou $P_k(n)$ $(k=2,3,4,5,6,7,8,9)$ sont des polynomes de Stirling et ont les formes suivantes

$P_2(n)=3n-1,$

$P_3(n)=-1,$

$P_4(n)=15n^3-30n^2+5n+2$

$P_5(n)=-3n^2+7n+2$

$P_6(n)=63n^5-315n^4+315n^3+91n^2-42n-16$

$P_7(n)=-9n^4+54n^3-51n^2-58n-16$

$P_8(n)=135n^7-1260n^6+310n^5-840n^4-2345n^3-540n^2+404n+144$

$P_9(n)=-15n^6+165n^5-465n^4-17n^3+648n^2+548n+144$

Théorème 129 *Pour tous entiers $n\geq 0$ et $k\geq 0$, on a*

$$S(n,k)=\frac{1}{k!}\sum_{j=0}^{n}(-1)^{k-j}\binom{k}{j}j^n. \tag{4.10}$$

Preuve. Dans [23], *p.*2, Comtet donne une preuve combinatoire de la formule (4.10). La preuve qui suit se base sur des propriétés des opérateurs linéaires I, E et Δ définies sur $\mathbb{C}\left[x\right]$ de la manière suivante.

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

On vérifie facilement que

$$\Delta(x^{\underline{n}})=nx^{\underline{n-1}}$$

et plus généralement

$$\Delta^k(x^{\underline{n}}) = n(n-1)...(n-k+1)x^{\underline{n-k}}, \text{pour } 0 \leq k \leq n.$$

On établit alors la formule de Grégory valable pour tout polynôme $P(x)$ de $\mathbb{C}[x]$

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

On a en particulier pour $P(x) = x^n$

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

On sait d'après 4.2 que $x^n = \sum_{k\geq 0} \left\{ {n \atop k} \right\} x^{\underline{k}}$, on en déduit que

$$\left\{ {n \atop k} \right\} = \frac{1}{k!}(\Delta^k P)(0). \tag{4.11}$$

Il est facile de constater que l'on a

$$\Delta = E - I$$

et que de plus les opérateurs E et I commutent. On a donc

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

Par application cette dernière formule, on a alors

$$\Delta^k(x^n) = \sum_{j=0}^{k} (-1)^{k-j} \binom{k}{j} (x+j)^n. \tag{4.12}$$

On déduit de (4.11) et (4.12) :

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

□

Relation entre les nombres de Stirling de 1 er espèce et de 2 eme espèce .

$$s(n,k) = \sum_{0\leq h\leq n-k} (-1)^h \binom{n-1+h}{n-k+h} \binom{2n-k}{n-k-h} S(n-k+h,h) \tag{4.13}$$

$$s(n,k) = \sum_{0\leq j\leq h\leq n-k} (-1)^{j+h} \binom{h}{j} \binom{n-1+h}{n-k+h} \binom{2n-k}{n-k+h} \frac{(h-j)^{n-k+h}}{h!}$$

Selon Louis Comtet [20] et H.W.Gould [38] ,que c'est au mathématicien allemand Oskar Xaver Schlomilch $(1823-1901)$ que nous devons la formule qui donnait la relation exacte entre les nombres de Stirling de 1 er espèce et 2 eme espèce,formule trouvée en 1852 .

Selon H.W.Gould [38] le mathématicien Berne (suisse) Ludwing Schlafli $(1814-1895)$ avait trouve en 1867 une autre formule donnant une relation très simple entre les nombres de Stirling de $1ere$ espèce et $2eme$ espèce .

$$s(n-1,k)=\sum_{j=0}^{k}\binom{k+n}{k-j}\binom{k-n}{k+j}S(j,k) \tag{4.14}$$

les relations 4.13 et 4.14 sont equivalentes .

Formules d'inversion

La propriété suivante vérifiée par les coefficients binomiaux

$$\sum_{k\geq 0}(-1)^{n-k}\binom{n}{k}\binom{k}{m}=\delta_{n,m}$$

a pour analogue la propriété suivante vérifiée par les nombres de Stirling

$$\sum_{k\geq 0}(-1)^{n-k}\begin{bmatrix}n\\k\end{bmatrix}\begin{Bmatrix}k\\m\end{Bmatrix}=\delta_{n,m}.$$

Ces deux propriétés impliquent qu'on a les relations suivantes entre matrices d'ordre $n+1$ à coefficients dans $\mathbb{Z}$:

$$\left(\binom{i}{j}\right)^{-1}_{0\leq i,j\leq n}=\left((-1)^{i-j}\binom{i}{j}\right)_{0\leq i,j\leq n}$$

et

$$\left(\begin{bmatrix}i\\j\end{bmatrix}\right)^{-1}_{0\leq i,j\leq n}=\left((-1)^{i-j}\begin{Bmatrix}i\\j\end{Bmatrix}\right)_{0\leq i,j\leq n}.$$

Il en résulte les formules d'inversion suivantes dans lesquelles $(u_n)_{n\geq 0}$, et $(v_n)_{n\geq 0}$ sont deux suites d'éléments de nombres complexes :

On a la formule d'inversion de Pascal

$$(\forall n\in\mathbb{N};v_n=\sum_{k\geq 0}\binom{n}{k}u_k)\Longleftrightarrow(\forall n\in\mathbb{N};u_n=\sum_{k\geq 0}(-1)^{n-k}\binom{n}{k}v_k$$

et une formule d'inversion analogue pour les nombres de Stirling

$$(\forall n\in\mathbb{N};v_n=\sum_{k\geq 0}\begin{bmatrix}n\\k\end{bmatrix}v_k)\Longleftrightarrow(\forall n\in\mathbb{N};v_n=\sum_{k\geq 0}(-1)^{n-k}\begin{Bmatrix}n\\k\end{Bmatrix}v_k.$$

Relations avec l'opérateur de dérivation D On démontre à l'aide d'un raisonnement par récurrence que l'on a pour tout entier $n \geq 0$

$$(xD)^n = \sum_k \left\{ n \atop k \right\} x^k D^k$$

et

$$x^n D^n = \sum_k \left[n \atop k \right] (-1)^{n-k} (xD)^k$$

4.3 Congruences vérifiées par les nombres de Stirling

4.3.1 Congruences classiques

Certaines congruences sur les nombres de Stirling se déduisent de résultats obtenus dans les chapitre précédents. Par exemple si p est un nombre premier, on sait d'après les relations 4.8 et 4.9 que

$$\begin{aligned} s(p,1) &= (-1)^{p-1}(p-1)! \\ s(p,2) &= (-1)^p (p-1)! H_{p-1}. \end{aligned}$$

Par le theorème de Wilson, on a

$$(p-1)! \equiv -1 \pmod{p}.$$

Par le théorème de Wolstenholme 73, on sait que pour $p \geq 5$, on a

$$H_{p-1} \equiv 0 \pmod{p^2}.$$

Il en résulte que l'on a

Théorème 130 *Pour tout nombre premier p*

$$s(p,1) = (-1)^{p-1}(p-1)! \equiv -1 \pmod{p}$$

et

$$s(p,2) \equiv 0 \pmod{p^2} \quad \textit{pour } p \geq 5.$$

On sait que pour p premier et $1 \leq k \leq p-1$, le coefficient binomial $\binom{p}{k} \equiv 0 \pmod{p}$. Le Théorème suivant montre que les nombres de Stirling vérifient une propriété analogue :

Théorème 131 *Soit p un nombre premier,alors pour tout entier k tel que $2 \leqslant k \leqslant p-1$, on a*

$$(-1)^{p-k}\begin{bmatrix} n \\ k \end{bmatrix} = s(p,k) \equiv 0 \ (\bmod p) \tag{4.15}$$

et

$$\begin{Bmatrix} p \\ k \end{Bmatrix} = S(p,k) \equiv 0 \ (\bmod p) \tag{4.16}$$

De plus p ne divise aucun des nombres $s(p,1)$, $s(p,p).S(p,1)$ et $S(p,p)$.

Preuve.

1. On a d'une part

$$(x)_p = x(x-1)...(x-p+1) \equiv x^p \ - x \ (\bmod p\mathbb{Z}[x]), \tag{4.17}$$

d'autre part

$$(x)_p = \sum_{k=0}^{n} s(n,k)x^k \tag{4.18}$$

On déduit de (4.17) et(4.18) :

$$\sum_{k=0}^{n} s(n,k)x^k \equiv x^p \ - x \ (\bmod p\mathbb{Z}[x]). \tag{4.19}$$

En comparant les coefficients de x^k , pour $1 \leq k \leq n$ dans (4.19), on obtient (4.15).

2. On sait que

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

Pour $1 \leq j \leq k$ et pour $2 \leqslant k \leqslant p-1$, on a $1 \leq j \leq p-1$, j est donc premier avec p et on a d'après le petit théorème de Fermat

$$j^p \equiv j \ (\bmod p).$$

On a donc

$$k!\begin{Bmatrix} p \\ k \end{Bmatrix} \equiv \sum_{j=1}^{k}(-1)^{k-j}\binom{k}{j}j \ (\bmod p). \tag{4.20}$$

Remarquons alors que l'on a

$$\begin{aligned} \sum_{j=1}^{k}(-1)^{k-j}\binom{k}{j}j &= k\sum_{j=1}^{k}(-1)^{k-j}\binom{k-1}{j-1} \\ &= (-1)^{k-1}k\sum_{i=0}^{k-1}(-1)^i\binom{k-1}{i} \\ &= (-1)^{k-1}k(1+(-1))^{k-1} \\ &= 0 \end{aligned} \tag{4.21}$$

De (4.20) et (4.21), on déduit

$$k!\left\{ {p \atop k} \right\} \equiv 0 \ (\mathrm{mod}\, p). \tag{4.22}$$

Comme $k!$ est premier avec p, la relation (4.22) permet de conclure en remarquant que de plus, on a $\left\{ {p \atop 1} \right\} = \left\{ {p \atop p} \right\} = 1$.

□

Théorème 132 *Pour tout nombre premier p, on a*

$$\begin{bmatrix} p-1 \\ k \end{bmatrix} \equiv 1 \ \ (\mathrm{mod}\, p) \ \textit{pour}\ 1 \leq k \leq p-1 \tag{4.23}$$

et

$$\begin{bmatrix} p-2 \\ k \end{bmatrix} \equiv 2^{p-k-1} - 1 \ \ (\mathrm{mod}\, p) \ \textit{pour}\ 0 \leq k \leq p-2 \tag{4.24}$$

Preuve. On a d'après la relation (4.3) :

$$\begin{bmatrix} p \\ k \end{bmatrix} = (p-1)\begin{bmatrix} p-1 \\ k \end{bmatrix} + \begin{bmatrix} p-1 \\ k-1 \end{bmatrix} \text{ pour } 1 \leq k \leq p-1. \tag{4.25}$$

Or d'après le théorème 131, on a $\begin{bmatrix} p \\ k \end{bmatrix} \equiv 0 \ \ (\mathrm{mod}\, p)$, pour $2 \leq k \leq p-1$. On déduit de (4.25)

$$\begin{bmatrix} p-1 \\ k \end{bmatrix} \equiv \begin{bmatrix} p-1 \\ k-1 \end{bmatrix} \ \ (\mathrm{mod}\, p) \text{ pour } 2 \leq k \leq p-1.$$

On a donc pour $2 \leq k \leq p-1$.

$$\begin{bmatrix} p-1 \\ k \end{bmatrix} \equiv \begin{bmatrix} p-1 \\ k-1 \end{bmatrix} \equiv \cdots \equiv \begin{bmatrix} p-1 \\ 1 \end{bmatrix} = (p-2)! \equiv 1 \ (\mathrm{mod}\, p).$$

Ce qui établit (4.23).

En exploitant de nouveau le relation (4.3), on a

$$\begin{bmatrix} p-1 \\ k \end{bmatrix} = (p-2)\begin{bmatrix} p-2 \\ k \end{bmatrix} + \begin{bmatrix} p-2 \\ k-1 \end{bmatrix} \text{ pour } 1 \leq k \leq p-2. \tag{4.26}$$

Compte tenu de (4.23), on déduit de (4.26) :

$$1 \equiv -2\begin{bmatrix} p-2 \\ k \end{bmatrix} + \begin{bmatrix} p-2 \\ k-1 \end{bmatrix} \ (\mathrm{mod}\, p) \text{pour } 1 \leq k \leq p-2. \tag{4.27}$$

La relation (4.24) s'obtient alors par induction à l'aide de (4.27) après avoir vérifié que l'on a bien

$$\begin{bmatrix} p-2 \\ 0 \end{bmatrix} = 2^{p-1} - 1 \ (\mathrm{mod}\, p) \tag{4.28}$$

La relation 4.28 se verifie directement pour $p = 2$. Pour $p \geq 3$, elle découle du petit théorème d Fermat. □

Plus généralement, on a le

Théorème 133 *Pour tout nombre premier p et pour tous entiers h et m tels que $h > 0$ et $0 \leq m < p$, on a*

$$\begin{bmatrix} hp+m \\ k \end{bmatrix} \equiv \sum \binom{h}{i} (-1)^{h-i} \begin{bmatrix} m \\ k-h-i(p-1) \end{bmatrix} \pmod{p}.$$

Le théorème qui suit va nous être utile dans la preuve du théorème de Von staudt et Clausen que nous énoncerons et démontrerons un peu plus loin

Théorème 134 *Soit p un nombre premier, alors on a*

1. *Pour tous entiers $n > 0$ et $m > 0$:*

$$n \equiv m \pmod{(p-1)} \Longrightarrow \begin{Bmatrix} n \\ p-1 \end{Bmatrix} \equiv \begin{Bmatrix} m \\ p-1 \end{Bmatrix} \pmod{p}.$$

2. *Pour tout entier $n > 0$:*

$$\begin{Bmatrix} n \\ p-1 \end{Bmatrix} \equiv \begin{cases} 1 \pmod{p} & \textit{si } p-1 \textit{ divise } n \\ 0 \pmod{p} & \textit{sinon} \end{cases}.$$

Preuve. Soient p un nombre premier

1. Pour tous entiers $n > 0$ et $m > 0$, tels que $n \equiv m \pmod{(p-1)}$, on a

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

Comme $n > 0$, on a $0^n = 0$ et donc

$$(p-1)! \begin{Bmatrix} n \\ p-1 \end{Bmatrix} = \sum_{j=1}^{p-1} (-1)^{p-1-j} \binom{p-1}{j} j^n. \tag{4.29}$$

De même, on a

$$(p-1)! \begin{Bmatrix} m \\ p-1 \end{Bmatrix} = \sum_{j=1}^{p-1} (-1)^{p-1-j} \binom{p-1}{j} j^m. \tag{4.30}$$

Comme par hypothèse, on a $n \equiv m \pmod{(p-1)}$, il existe $k \in \mathbb{Z}$ tel que

$$n = m + k(p-1). \tag{4.31}$$

Pour $j \in \{1, 2, ..., p-1\}$, j est premier avec p et le petit théorème de Fermat permet d'écrire

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

Par suite, on a avec (4.31)

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

2. Soit
$$j^n \equiv j^m \pmod{p} \tag{4.32}$$
On déduit alors des relations (4.29), (4.30) et (4.32) que
$$(p-1)!\left\{ \begin{matrix} n \\ p-1 \end{matrix} \right\} \equiv (p-1)!\left\{ \begin{matrix} m \\ p-1 \end{matrix} \right\} \pmod{p}.$$
Comme $(p-1)!$ est premier avec p, on en déduit que
$$\left\{ \begin{matrix} n \\ p-1 \end{matrix} \right\} \equiv \left\{ \begin{matrix} m \\ p-1 \end{matrix} \right\} \pmod{p}.$$

3. - Supposons naintenant que $p-1$ divise n.Dans ce cas, on a $n \equiv p-1 \pmod{(p-1)}$. Par suite,
$$\left\{ \begin{matrix} n \\ p-1 \end{matrix} \right\} \equiv \left\{ \begin{matrix} p-1 \\ p-1 \end{matrix} \right\} = 1 \pmod{p}.$$
- Supposons naintenant que $p-1$ ne pas divise n. Soit r le reste de la division euclidienne de n par $p-1$, on a $n \equiv r \pmod{(p-1)}$ avec $0 < r < p-1$. Par suite,
$$\left\{ \begin{matrix} n \\ p-1 \end{matrix} \right\} \equiv \left\{ \begin{matrix} r \\ p-1 \end{matrix} \right\} = 0 \pmod{p}.$$

□

4.3.2 Congruences de Carlitz (1963)

En 1963, L. Carlitz [15] a prouvé de nombreuse congruences pour les nombres de Stirling de deuxième espèce $S(n,k)$ pour $k \equiv r \pmod{m}$.Citons par exemple les relations données dans [87], en page 501.

Théorème 135
$$\begin{cases} S(n,2m) \equiv \binom{n-m-1}{m-1} \pmod{2} \\ S(n,2m+1) \equiv \binom{n-m-1}{m} \pmod{2} \end{cases} \tag{4.33}$$
et
$$\begin{cases} S(n,3m) \equiv \binom{l-1}{m} \pmod{3} \quad (m = n-2l-2) \\ S(m,3m+1) \equiv \binom{l}{m} \pmod{3} \quad (m = 2n-2l-2 \ ou \ n-2l-2) \\ S(m,3m+2) \equiv \binom{l}{m} \pmod{3} \quad (m = n-2l-2\ ) \end{cases}$$

On trouve en pages 501 et 502 de [87] des déductions intéressantes de ces congruences. Par exemple si $\theta_0\ (n)$ désigne le nombre de coefficients $S(n,2m)$ qui sont impairs et $\theta_1\ (n)$ le nombre de coefficients $S(n,2m+1)$ qui sont impairs. Alors avec (4.33), on peut écrire
$$\begin{aligned} \theta_1(n) &= \theta_0(n+1) \\ \theta_0(2n) &= \theta_0(n) + \theta_0(n-1) \\ \theta_0(2n+1) &= \theta_0(n+1) \end{aligned}$$

4.3.3 Congruences de Howard (1990)

En 1990, F. T. Howard [50], a obtenu des congruences pour les nombres de Stirling de première et de deuxième espèce. Ces congruences font intervenir les nombres de Bernoulli et sont une généralisation des congruences obtenues par Glaisher en 1900 ([34]) et Nielsen ([75]) en 1923.

Théorème 136 *Soit p un nombre premier impair et $n \geqslant 1$ un entier. Alors avec $t := v_p(n)$, on a pour $0 < 2r < 2p-2$ et $1 < 2r+1 < 2p-2$*

$$\begin{bmatrix} n \\ n-2r \end{bmatrix} \equiv -\frac{n}{2r}\binom{n-1}{2r} B_{2r} \pmod{p^{2t}}. \tag{4.34}$$

$$\begin{bmatrix} n \\ n-2r-1 \end{bmatrix} \equiv -\frac{n^2(2r+1)}{4r}\binom{n-1}{2r+1} B_{2r} \pmod{p^{3t}}. \tag{4.35}$$

$$\begin{Bmatrix} n+2r \\ n \end{Bmatrix} \equiv \frac{n}{2r}\binom{n+2r}{2r} B_{2r} \pmod{p^{2t}}. \tag{4.36}$$

$$\begin{Bmatrix} n+2r+1 \\ n \end{Bmatrix} \equiv \frac{n^2(2r+1)}{4r}\binom{n+2r+1}{2r} B_{2r} \pmod{p^{3t}}. \tag{4.37}$$

Pour $n = p$ et pour $0 < 2r < p-1$ et $1 < 2r+1 < p-1$, les congruences (4.34) et (4.35) se réduisent aux congruences de Glaisher, et les congruences (4.36) et (4.37) se réduisent aux congruences de Nielsen.

4.3.4 Congruences d'Adelberg (1996)

En étudiant les propriétés des nombres de Bernoulli généralisés $B_n^{(k)}$ (nombres de Bernoulli d'ordre k et de degré n) et en exploitant les congruences de Howard, A. Adelberg[2] a prouvé en 1996 les congruences suivantes relatives aux nombres de Stirling $s(l, l-p)$ et $S(l+p, p)$.

Théorème 137 *Si p est un nombre premier impair et si $l \geqslant 1$ est un entier divisible par p, alors*

$$s(l, l-p) \equiv \frac{l^2}{2}\binom{l-1}{p} \pmod{pl^2}.$$

et

$$S(l+p, p) \equiv (\frac{l}{p}+1)\frac{l^2}{2} \pmod{pl^2}.$$

4.3.5 Congruences de Gertsch (1997) et (1999)

En 1997, A. Gertsch [35] prouve le théorème suivant :

Théorème 138 *A. Gertsch (1997) Pour tout nombre premier $p \geq 5$, on a*

$$\begin{bmatrix} p+1 \\ r+1 \end{bmatrix} \equiv 0 \pmod{p^2} \quad \textit{pour } 0 < r < p-3$$

et

$$\begin{bmatrix} 2p \\ r+2 \end{bmatrix} \equiv 0 \pmod{p^2} \quad \textit{pour } 0 < r < p-1 \textit{ avec } r \textit{ impair}$$

Dans [35], A. Gertsch exploite la relation suivante qui lie les nombres harmoniques généralisés $H(n,r)$ définis par

$$H(n,r) = \sum_{n_0+n_1+\cdots+n_r \leq n} \frac{1}{n_0 n_1 ... n_r}$$

où $r \geq 0$ et $n \geq 1$ sont des entiers. On a

$$H(n,r) = \frac{(r+1)!}{n!} \begin{bmatrix} n+1 \\ r+2 \end{bmatrix}.$$

En 1998, A. Gertsch Hamadene a établi de nombreuses congruences pour les nombres de Stirling. La démonstration de certaines de ces congruences repose sur une congruence connue sous le dénomination de congruence de Bauer généralisée.

Théorème 139 *Pour tout entier $h \geq 1$ et pour tout nombre premier impair p, on a la congruence de Bauer généralisée*

$$(x)_{p^h} \equiv (x^p - x)^{p^{h-1}} \pmod{p^h \mathbb{Z}[x]}.$$

On a aussi

$$(x)_{2^h} \equiv (x^2 - x)^{2^{h-1}} \pmod{2^{h-1} \mathbb{Z}[x]}.$$

A. Gertsch déduit de ce théorème d'intéressantes congruences pour les nombres de Stirling de première espèce.

Théorème 140 *A. Gertsch (1999) Pour tout nombre premier p et pour tout entier $h \geq 1$, on a*

$$s(p^h + j, k) \equiv 0 \pmod{p^h}, \ \textit{pour } 0 \leq k < p^{h-1} \textit{ et } j \in \mathbb{N}.$$

Preuve. Nous suivons dans ce qui suit la preuve de Gertsch. On peut supposer $p \geq 2$ (le cas $p = 2$ se traite de manière analogue). On a

$$(x)_{p^h} = \sum_{k=0}^{p^h} s(p^h, k) x^k$$

En appliquant le théorème 139, on a alors

$$\sum_{k=0}^{p^h} s(p^h,k)x^k \equiv (x^p-x)^{p^{h-1}} \equiv x^{p^{h-1}}(x^{p-1}-1)^{p^{h-1}} \pmod{p^h\mathbb{Z}[x]}. \tag{4.38}$$

La première puissance de x apparaissant dans le membre de gauche de 4.38 est $x^{p^{h-1}}$, ce qui implique que

$$s(p^h,k) \equiv 0 \mod p^h, \text{ pour } 0 \leq k < p^{h-1}.$$

Par induction sur j, on montre alors aisément que pour $j \in \mathbb{N}$, on a

$$s(p^h+j,k) \equiv 0 \pmod{p^h}, \text{ pour } 0 \leq k < p^{h-1}.$$

On utilise pour cela la formule de récurrence bien connue

$$s(n+1,k) = ns(n,k) + s(n,k-1)$$

avec $n = p^h + i$ et pour $k < p^{h-1}$. □

Définition de la factorielle à gauche de n

Définition 141 *Pour tout nombre entier $n \geq 1$, on définit la factorielle à gauche de n notée aussi $!n$ que κ_n en posant*

$$!n = \kappa_n = \sum_{k=0}^{n-1} k!$$

On a

$$(!n)_{n\geq 1} = (1,2,4,10,34,...)$$

En 1999, A. Gertsch [36] a prouvé le theorème suivant

Théorème 142 *Pour tout nombre premier impair p, on*

$$\kappa_p \equiv P_{p-1} \pmod{p},$$

P_{p-1} étant le $p-1$ ième nombre de Bell.

Preuve. On a

$$P_{p-1} = \sum_{k=0}^{p-1} S(p-1,k).$$

Pour $1 \leq k \leq p-1$, on a ,$j^{p-1} \equiv 1 \pmod{p}$ et donc

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

Il en résulte que l'on a

$$P_{p-1} \equiv \sum_{k=0}^{p-1}\frac{(-1)^{k+1}}{k!} \pmod{p}. \tag{4.39}$$

Remarquons alors que d'après le théorème de Wilson, on a

$$(p-1)! = k!\prod_{j=1}^{p-k-1}(p-j) = (-1)^k k!(p-k-1)! \equiv -1 \pmod{p}.$$

On en déduit que

$$\frac{(-1)^{k+1}}{k!} \equiv (p-k-1)! \pmod{p} \tag{4.40}$$

Par conséquent, on déduit de (4.39) et (4.40) que l'on a

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

C'est à dire

$$P_{p-1} \equiv \sum_{k=0}^{p-1}k! = \kappa_p \pmod{p}.$$

□

En page 13 de sa thèse Gertsch [36] observe que l'on a les congruences

$$\begin{bmatrix} n \\ k \end{bmatrix} \equiv \begin{Bmatrix} p-k \\ p-n \end{Bmatrix} \pmod{p}, \text{ pour } 1 \leq n,k \leq p-1,$$

elle démontre ensuite la généralistion de ces congruences.

Théorème 143 *A. Gertsch (1999) Soit p un nombre premier impair ; les congruences*

$$\begin{bmatrix} p^h-j \\ p^h-i \end{bmatrix} \equiv \begin{Bmatrix} i \\ j \end{Bmatrix} \pmod{p^h}$$

sont valables pour $1 \leq i,j \leq p-1$, $h \geq 1$.

La preuve que donne Gertsch de ce théorème repose sur le lemme suivant

Lemme 144 *A. Gertsch (1999) On a* ν

$$\begin{bmatrix} p^h-1 \\ p^h-k \end{bmatrix} \equiv 1 \pmod{p^h},\ 1 \leq k \leq p-1.$$

4.3.6 Congruences de Junod (2003)

La congruence suivante pour les nombres de Stirling de deuxième espèce

$$\left\{ \begin{matrix} m+p^{\upsilon} \\ k \end{matrix} \right\} \equiv \left\{ \begin{matrix} m \\ k-p \end{matrix} \right\} + \left\{ \begin{matrix} m \\ k-p^2 \end{matrix} \right\} + \cdots + \left\{ \begin{matrix} m \\ k-p^{\upsilon} \end{matrix} \right\} + \left\{ \begin{matrix} m+1 \\ k \end{matrix} \right\} \ (\operatorname{mod} p\mathbb{Z}),$$

est donnée en page 44 de [52]. Junod exploite le théorème suivant suivant pour la prouver

Théorème 145 *Pour $\nu \geq 1$ et pour p premier, on a la congruence suivante*

$$P_{m+p^{\upsilon}}(x) \equiv P_{m+1}(x) + (x^p + \cdots + x^{p^{\upsilon}}) P_m(x) \ (\operatorname{mod} p\mathbb{Z}_p[x]) \tag{4.41}$$

Preuve. Nous allons prouver de manière minutieuse ce théorème en suivant la preuve donnée par A. Gertsch et A. M. Robert dans [37]. ce théorème est précisément la proposition 3.1 dans [37]. Cette relation se retrouve dans la thèse de Junod [52], en page 38 (relation 5). □

Dans tout ce qui suit, p désigne un nombre premier impair, et A désigne l'anneau $\mathbb{Z}$, ou l'anneau $\mathbb{Z}_p$ des entiers p-adiques. Soient $f(x)$ et $g(x) \in A[x]$ deux polynômes à une indéterminée x et à coefficients dans l'anneau A. Alors, on a le résultat suivant

Lemme 146 *Si $f(x) \equiv g(x) \mod p^{\upsilon} A[x]$ pour un entier $\nu \geq 1$, alors on a*

$$f(x)^p \equiv g(x)^p \mod p^{\upsilon+1} A[x] \tag{4.42}$$

Preuve. Par hypothèse, on a

$$f(x) = g(x) + p^{\upsilon} h(x), \qquad \text{où } h(x) \in A[x].$$

On a donc

$$\begin{aligned} f(x)^p &= (g(x) + p^{\upsilon} h(x))^p \\ &= (g(x))^p + p^{\upsilon+1} r(x) \qquad \text{avec } r(x) \in A[x]. \end{aligned}$$

Ainrsi, (4.42) est établie. □

Considérons maintenant le produit suivant

$$f(x) f(x-p^{\nu}) \ldots f(x-(p-1)p^{\nu}) = \prod_{k=0}^{p-1} f(x-kp^{\nu}).$$

Nous avons le résultat suivant

Lemme 147 *Pour tout nombre premier p impair, et pour tout entier $\nu \geq 0$, on a la congruence suivante*

$$\prod_{k=0}^{p-1} f(x-kp^{\nu}) \equiv f(x)^p \mod p^{\upsilon+1}A[x]$$

Nous avons pour $0 \leq k \leq p-1$

$$f(x-kp^{\nu}) \equiv f(x) - kp^{\nu}f'(x) \mod p^{2\upsilon}A[x].$$

On en déduit que

$$\begin{aligned}\prod_{k=0}^{p-1} f(x-kp^{\nu}) &\equiv f(x)^p - \sum_{k=0}^{p-1} kp^{\nu}f'(x) \mod p^{2\upsilon}A[x] \\ &\equiv f(x)^p - \frac{p-1}{2}pp^{\nu}f'(x)f(x)^{p-1} \mod p^{2\upsilon}A[x] \\ &\equiv f(x)^p \mod p^{\upsilon+1}A[x].\end{aligned}$$

Rappellons que les polynômes de Pochhammer $(x)_n$ sont définis pour $n \in \mathbb{N}$ par

$$(x)_0 = 1 \qquad \text{et} \qquad (x)_n = x(x-1)...(x-n+1) \quad \text{pour } n \geq 1.$$

Pour tout entier $n \geq 0$, $(x)_n$ est un polynôme unitaire (de coefficient dominant égal à 1), de degré n et à coefficients entiers (ces coefficients sont des nombres de Stirling de première espèce). Cette suite de polynômes $((x)_n)_{n\in\mathbb{N}}$ constitue une base du A module $A[x]$.

Lemme 148 *Pour tout entier $\nu \geq 1$, le polynôme $(x)_{p^{\nu}} = x(x-1)...(x-p^{\nu}+1)$ vérifie la congruence suivante*

$$(x)_{p^{\nu}} \equiv (x^p - x)^{p^{\nu-1}} \mod p^{\upsilon}A[x]. \tag{4.43}$$

Preuve. La preuve s'établit par récurrence sur υ. pour $\nu = 1$, cette congruence s'écrit.

$$x(x-1)...(x-p+1) \equiv x^p - x \mod pA[x].$$

C'est un résultat que l'on a déjà vu. C'est une conséquence immédiate du fait que les deux polynômes unitaires $x^p - x$ et $x(x-1)...(x-p+1)$, de degré p, ayant les mêmes p racines distinctes dans le corps $\mathbf{F}_p$ ne peuvent que coincider dans $\mathbf{F}_p[x]$.

Supposons donc que pour un entier $\nu \geq 1$, on ait $(x)_{p^\nu} \equiv (x^p - x)^{p^{\nu-1}} \mod p^\upsilon A[x]$. Remarquons alors que l'on a, en posant $f(x) = (x)_{p^\nu}$:

$$\begin{aligned}
(x)_{p^{\nu+1}} &= \prod_{k=0}^{p^{\upsilon+1}-1} (x-k) \\
&= \prod_{k=0}^{p^\upsilon-1} (x-k) \prod_{k=0}^{p^\upsilon-1} (x-p^\nu-k) \prod_{k=0}^{p^\upsilon-1} (x-2p^\nu-k) \ldots \prod_{k=0}^{p^\upsilon-1} (x-(p-1)p^\nu-k) \\
&= (x)_{p^\nu}(x-p^\nu)_{p^\nu}(x-2p^\nu)_{p^\nu} \ldots (x-(p-1)p^\nu)_{p^\nu} \\
&= \prod_{k=0}^{p-1} f(x-kp^\nu)
\end{aligned}$$

En appliquant alors le lemme 147 au polynôme $f(x) = (x)_{p^\nu}$, on obtient la congruence

$$(x)_{p^{\nu+1}} \equiv ((x)_{p^\nu})^p \mod p^{\upsilon+1} A[x] \tag{4.44}$$

Or on sait par hypothèse de récurrence que

$$(x)_{p^\nu} \equiv (x^p - x)^{p^{\nu-1}} \mod p^\upsilon A[x]. \tag{4.45}$$

Appliquons le lemme 146, avec $f(x) = (x)_{p^\nu}$ et $g(x) = (x^p - x)^{p^{\nu-1}}$, compte tenu de la congruence (4.45), on obtient

$$((x)_{p^\nu})^p \equiv ((x^p - x)^{p^{\nu-1}})^p \mod p^{\upsilon+1} A[x]$$

Soit

$$((x)_{p^\nu})^p \equiv (x^p - x)^{p^\nu} \mod p^{\upsilon+1} A[x] \tag{4.46}$$

De (4.44) et (4.46), on déduit que

$$(x)_{p^{\nu+1}} \equiv (x^p - x)^{p^\nu} \mod p^{\upsilon+1} A[x].$$

Ce qui prouve que la relation (4.43) est vraie alors vérifiée pour $\nu+1$. La preuve par récurrence est complète. □

La poursuite de la preuve du théorème 145 nécessite quelques rudiments de calcul ombral que nous allons rappeller.

Considérons l'application linéaire

$$\Phi : A[x] \to A[x]$$

définie par ses images sur la base $((x)_n)_{n\in\mathbb{N}}$ de $A[x]$ par

$$\Phi((x)_n) = x^n, \text{ pour tout entier } n \geq 0.$$

Alors, il est facile de constater comme on a la relation

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

et que le n-ième polynôme de Bell noté $P_n(x)$ étant défini par la relation

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

on a aussi

$$\begin{aligned} P_n(x) &= \sum_{k=0}^{n} \left\{ n \atop k \right\} \Phi((x)_k \\ &= \Phi(\sum_{k=0}^{n} \left\{ n \atop k \right\} (x)_k) \\ &= \Phi(x^n). \end{aligned}$$

Ainsi, on obtient cette intéressante relation.

$$P_n(x) = \Phi(x^n).$$

Le n-ième polynôme de Bell $P_n(x)$ est l'image de x^n par Φ. Rappelons que le n-ième nombre de Bell P_n est défini par la relation $P_n = P_n(1)$.

Proposition 149 *Pour $f(x) \in A[x]$ et $n \in \mathbb{N}$, on a*

$$x^n \Phi(f(x)) = \Phi((x)_n f(x-n)), \tag{4.47}$$

$$x\Phi((x+1)^n) = \Phi(x^{n+1}). \tag{4.48}$$

Preuve. On a

$$\begin{aligned} (x)_{n+m} &= \prod_{k=0}^{n+m} (x-k) \\ &= \prod_{k=0}^{n-1} (x-k) \prod_{k=0}^{m-1} (x-n-k) \\ &= (x)_n (x-n)_m. \end{aligned}$$

On en déduit que

$$\begin{aligned} x^{n+m} &= \Phi((x)_{n+m}) \\ &= \Phi((x)_n (x-n)_m). \end{aligned} \tag{4.49}$$

Soit alors $f(x) \in A[x]$, comme $((x)_m)_{m\in\mathbb{N}}$ est une base de $A[x]$, $f(x)$ s'écrit comme une combinaison linéaire des vecteurs de cette base et on a $f(x) = \sum_{m\in I} c_m(x)_m$, I étant une partie finie de $\mathbb{N}$. On a alors

$$\begin{aligned} x^n\Phi(f(x)) &= x^n\Phi(\sum_{m\in I} c_m(x)_m) \\ &= \sum_{m\in I} c_m x^n \Phi((x)_m) \\ &= \sum_{m\in I} c_m x^n x^m \\ &= \sum_{m\in I} c_m x^{n+m} \\ &= \sum_{m\in I} c_m \Phi((x)_{n+m}) \end{aligned}$$

Avec (4.49), on a alors

$$\begin{aligned} x^n\Phi(f(x)) &= \sum_{m\in I} c_m \Phi((x)_n(x-n)_m) \\ &= \Phi(\sum_{m\in I} c_m(x)_n(x-n)_m) \\ &= \Phi((x)_n \sum_{m\in I} c_m(x-n)_m) \\ &= \Phi((x)_n f(x-n)). \end{aligned}$$

On a ainsi établi (4.47).

Pour $n = 1$, (4.47) devient alors

$$x\Phi(f(x)) = \Phi(xf(x-1)).$$

En choisissant le polynôme $f(x) = (x+1)^n$ dans cette dernière égalité, on obtient

$$x\Phi((x+1)^n) = \Phi(xx^n) = \Phi(x^{n+1}).$$

On a ainsi établi (4.48). □

Corollaire 150 *La suite des polynômes de Bell $(P_n(x))_{n\in\mathbb{N}}$ vérifie les relations de récurrence*

$$P_0(x) = 1 \qquad et \qquad P_{n+1}(x) = x\sum_{k=0}^{n} \binom{n}{k} P_k(x), \qquad (n \geq 0)$$

Preuve. Il suffit de remarquer que l'on a, en expoitant (4.48)

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

□

Corollaire 151 *Soit p un nombre premier impair, $\upsilon \geq 1$ un entier et $f(x) \in A[x]$. Alors on a la congruence*

$$\Phi((x^p - x)^{p^{\nu-1}} f(x)) \equiv x^{p^\nu}\Phi(f(x)) \mod p^\upsilon A[x].$$

Preuve. Posons $n = p^\nu$ dans la proposition 149, on obtient

$$x^{p^\nu}\Phi(f(x)) = \Phi((x)_n f(x - p^\nu))$$

Or

$$f(x - p^\nu) \equiv f(x) \mod p^\upsilon A[x].$$

On en déduit que l'on a par linéarité

$$x^{p^\nu}\Phi(f(x)) \equiv \Phi((x)_n f(x)) \mod p^\upsilon A[x].$$

D'autre part, on a d'après la lemme148

$$(x)_{p^\nu} \equiv (x^p - x)^{p^{\nu-1}} \mod p^\upsilon A[x].$$

Nous en concluons que l'on a

$$x^{p^\nu}\Phi(f(x)) \equiv \Phi((x^p - x)^{p^{\nu-1}} f(x)) \mod p^\upsilon A[x],$$

ce qui est bien la relation qu'on voulait démontrer. □

Nous sommes maintenant en mesure de prouver le théorème 145. On a d'après le corollaire (151) la congruence suivante pour p un nombre premier impair, $\upsilon \geq 1$ entier et $f(x) \in A[x]$:

$$\Phi((x^p - x)^{p^{\nu-1}} f(x)) \equiv x^{p^\nu}\Phi(f(x)) \mod p^\upsilon A[x].$$

On a donc pour tout entier $\upsilon \geq 1$

$$\Phi((x^p-x)^{p^{k-1}}f(x)) \equiv x^{p^k}\Phi(f(x)) \mod pA[x].$$

En donnant à k les valeurs $1, 2, ...\upsilon$, on obtient les congruences

$$\begin{aligned}
\Phi((x^p-x)f(x)) &\equiv x^p\Phi(f(x)) \mod pA[x] \\
\Phi((x^p-x)^p f(x)) &\equiv x^{p^2}\Phi(f(x)) \mod pA[x] \\
&\dots \\
\Phi((x^p-x)^{p^{\nu-1}}f(x)) &\equiv x^{p^\nu}\Phi(f(x)) \mod p^\upsilon A[x].
\end{aligned}$$

En additionnant membre à membre ces congruences, on obtient

$$\Phi((\sum_{k=0}^{\nu-1}(x^p-x)^{p^k})f(x)) \equiv (x^p+\cdots+x^{p^\upsilon})\Phi(f(x)) \mod pA[x]. \tag{4.50}$$

En utilisant la relation

$$(x^p-x)^{p^k} \equiv x^{p^{k+1}} - x^{p^k} \mod pA[x],$$

on a

$$\sum_{k=0}^{\nu-1}(x^p-x)^{p^k} \equiv \sum_{k=0}^{\nu-1}(x^{p^{k+1}}-x^{p^k}) \equiv x^{p^\upsilon}-x \mod pA[x]$$

et

$$\Phi((\sum_{k=0}^{\nu-1}(x^p-x)^{p^k})f(x)) \equiv \Phi((x^{p^\upsilon}-x)f(x)) \mod pA[x] \tag{4.51}$$

Par suite, on a avec (4.50) et (4.51)

$$\Phi((x^{p^\upsilon}-x)f(x)) \equiv (x^p+\cdots+x^{p^\upsilon})\Phi(f(x)) \mod pA[x].$$

En choisissant $f(x)=x^n$ dans cette dernière congruence, on obtient

$$\Phi(x^{n+p^\upsilon}-x^{n+1}) \equiv (x^p+\cdots+x^{p^\upsilon})\Phi(x^n) \mod pA[x].$$

Comme $\Phi(x^k)=P_k(x)$, on a bien obtenu la relation

$$P_{m+p^\upsilon}(x) \equiv P_{m+1}(x) + (x^p+\cdots+x^{p^\upsilon})P_m(x) \ (\mathrm{mod}\, p\mathbb{Z}_p[x])$$

La preuve du théorème 145 est complète.

La relation (4.41) de ce théorème s'écrit

$$\sum_{i=0}^{m+p^\upsilon}\left\{{m+p^\upsilon \atop i}\right\}x^j \equiv \sum_{i=0}^{m}\left\{{m \atop i}\right\}(x^{i+p}+x^{i+p^2}+\cdots+x^{i+p^\upsilon}) + \sum_{i=0}^{m+1}\left\{{m+1 \atop i}\right\}x^i \ (\mathrm{mod}\, p\mathbb{Z}_p[x]). \tag{4.52}$$

Les coefficients de x^k dans les membres de gauche et de droite de 4.52 sont entiers et sont donc congrus modolo p. Ce qui s'écrit

$$\left\{ {m+p^v \atop k} \right\} \equiv \left\{ {m \atop k-p} \right\} + \left\{ {m \atop k-p^2} \right\} + \cdots + \left\{ {m \atop k-p^v} \right\} + \left\{ {m+1 \atop k} \right\} \pmod{p\mathbb{Z}}.$$

En exploitant les relations (cf [9])

$$\begin{aligned} S(-n,-k) &= (-1)^{n+k} s(k,n), \\ s(-n,-k) &= (-1)^{n+k} S(k,n), \end{aligned}$$

relations qui se traduisent avec les notations adoptées par Junod par

$$\begin{aligned} \left\{ {-n \atop -k} \right\} &= \left[{k \atop n} \right], \\ \left[{-n \atop -k} \right] &= \left\{ {k \atop n} \right\}, \end{aligned}$$

on obtient (en changent m en $-m$) :

$$\left\{ {p^v-m \atop k} \right\} \equiv \left[{p-k \atop m} \right] + \left[{p^2-k \atop m} \right] + \cdots + \left[{p^v-k \atop m} \right] + \left[{-k \atop m-1} \right] \pmod{p\mathbb{Z}}. \tag{4.53}$$

Comme $\left[{n \atop k} \right] = 0$, pour $k < 0$ et aussi pour $k > n$, on en déduit que pour tout $k, m = 0, 1, ..., p^v$, on a

$$\left\{ {p^v-m \atop p^v-k} \right\} \equiv \left[{k \atop m} \right] \pmod{p\mathbb{Z}}.$$

Remarquons que la relation (4.53) s'écrit aussi

$$\left[{k \atop m-p^v} \right] \equiv \left[{p+k \atop m} \right] + \left[{p^2+k \atop m} \right] + \cdots + \left[{p^v+k \atop m} \right] + \left[{k \atop m-1} \right] \pmod{p\mathbb{Z}}. \tag{4.54}$$

4.3.7 Congruences de DeMaio et Touset (2008)

En 2008, J. DeMaio et S. Touset [25] prouvent la congruence suivante :

Théorème 152 *J. DeMaio and S. Touset, (2008). Si p est un nombre premier,alors p divise $\left\{ {p+1 \atop k+1} \right\}$ pour tout entier k tel que $2 \leqslant k \leqslant p-1$.Autrement dit*

$$\left\{ {p+1 \atop k+1} \right\} \equiv 0 \pmod{p} \text{ pour } 2 \leqslant k \leqslant p-1 \tag{4.55}$$

De plus on a

$$\left\{ {p+1 \atop 2} \right\} \equiv 1 \pmod{p}. \tag{4.56}$$

Preuve. Pour $2 \leqslant k \leqslant p-1$, on a

$$\left\{ {p+1 \atop k+1} \right\} = (k+1)\left\{ {p \atop k+1} \right\} + \left\{ {p \atop k} \right\} \tag{4.57}$$

Pour $2 \leqslant k \leqslant p-2$, p divise $\left\{ {p \atop k+1} \right\}$ et $\left\{ {p \atop k} \right\}$ et par conséquent p divise $\left\{ {p+1 \atop k+1} \right\}$. Pour $k = p-1$, on a

$$\left\{ {p+1 \atop k-1} \right\} = \left\{ {p+1 \atop p} \right\} = p\left\{ {p \atop k+1} \right\} + \left\{ {p \atop p-1} \right\} \equiv \left\{ {p \atop p-1} \right\} \equiv 0 \ (\mathrm{mod}\, p).$$

On a ainsi prouvé (4.55). Pour établir (4.56), il suffit de remarquer que l'on a

$$\begin{aligned} \left\{ {p+1 \atop 2} \right\} &= 2\left\{ {p \atop 2} \right\} + \left\{ {p \atop 1} \right\} \\ &= 2\left\{ {p \atop 2} \right\} + 1 \equiv 1 \ (\mathrm{mod}\, p) \end{aligned} \tag{4.58}$$

Comme p divise $\left\{ {p \atop 2} \right\}$, il résulte de (4.58) que l'on a

$$\left\{ {p+1 \atop 2} \right\} \equiv 1 \ (\mathrm{mod}\, p).$$

□

Nous avons constaté que les nombres de Stirling de première espèce vérifaient aussi une propriété analogue à celle vérifiée par les nombres de Stirling de deuxième espèce établie par J. DeMaio et S. Touset (theorème 152). Nous avons :

Théorème 153 *Si p est un nombre premier,alors p divise $\left[{p+1 \atop k+1} \right]$ pour tout entier k tel que $2 \leqslant k \leqslant p-1$.Autrement dit*

$$\left[{p+1 \atop k+1} \right] \equiv 0 \ (\mathrm{mod}\, p) \ \textit{pour} \ 2 \leqslant k \leqslant p-1 \tag{4.59}$$

De plus on a

$$\left[{p+1 \atop 2} \right] \equiv -1 \ (\mathrm{mod}\, p). \tag{4.60}$$

Preuve. On a pour $2 \leqslant k \leqslant p-1$.

$$\left[{p+1 \atop k+1} \right] = p\left[{p \atop k+1} \right] + \left[{p \atop k} \right] \equiv \left[{p \atop k} \right] \equiv 0 \ (\mathrm{mod}\, p).$$

On a ainsi prouvé (4.59). Quant à (4.60), il suffit de remarquer que l'on a

$$\begin{aligned} \left[{p+1 \atop 2} \right] &= p\left[{p \atop 2} \right] + \left[{p \atop 1} \right] \\ &\equiv (-1)^{p-1}(p-1)! \equiv -1 \ (\mathrm{mod}\, p). \end{aligned} \tag{4.61}$$

□

4.3.8 Congruences de Chan et Manna (2010)

En 2010, O-Y. Chan and D. Manna ([17], theorem2.1) prouvent les congruences suivantes :

Théorème 154 *O-Y. Chan and D. Manna, (2010). Pour des entiers $n \geqslant 1$ et $k \geqslant 1$, on a*

$$\left\{ n \atop k \right\} \equiv 0 \pmod 2 \text{ si } n < k,$$

et

$$\left\{ n \atop k \right\} \equiv \binom{n - \left\lfloor \frac{k}{2} \right\rfloor - 1}{n-k} \pmod 2 \text{ si } n \geqslant k.$$

4.4 Démonstration du théorème de Von staudt et Clausen (1840)

Rappelons l'énoncé du théorème de Von Staudt-Clausen.

Théorème 155 *Von Staudt-Clausen (1840) Pour tout entier $n \geqslant 1$, on a la relation suivante*

$$B_{2n} + \sum_{p-1 \ divise \ 2n} \frac{1}{p} \in \mathbb{Z}. \tag{4.62}$$

La sommation étant étendue à tous les nombres premiers p divisant l'entier $2n$.

La démostration qui va suivre s'inspire largement de celle qu'Edouard Lucas a donné dans son ouvrage Theorie des nombres et dans son article Elle repose sur deux résultats essentiels. D'une part sur une relation simple entre les nombres de Bernoulli et les nombres de Stirling de seconde espèce, et d'autre part sur des propriétés de congruences vérifiées par les nombres de Stirling de deuxième espèce.

Lemme 156 *Pour tout nombre entier $n \geqslant 1$, on a*

$$B_n = \sum_{k=0}^{n} (-1)^k \frac{k!}{k+1} S(n,k). \tag{4.63}$$

Lemme 157 *Pour tout entier naturel $k \neq 3$ tel que $k+1$ soit composé, on a*

$$\frac{k!}{k+1} \in \mathbb{N}$$

Nous prouvons ces deux lemmes 156 et 157 en fin de démonstration du théorème 155.

Preuve du Théorème *On a*

$$B_{2n} = \sum_{k=0}^{2n} (-1)^k \frac{k!}{k+1} S(2n,k),$$

avec

$$S_1 = \sum_{0\leq k\leq 2n \text{ et } k+1 \text{ composé}} (-1)^k \frac{k!}{k+1} S(2n,k)$$

et

$$S_2 = \sum_{0\leq k\leq 2n \text{ et } k+1 \text{ premier}} (-1)^k \frac{k!}{k+1} S(2n,k).$$

Montrons que $S_1 \in \mathbb{Z}$ *et* $S_2 + \sum_{p-1 \text{ divise } 2n} \frac{1}{p} \in \mathbb{Z}$, *le theorème en résultera.*

On a pour $k = 3$

$$(-1)^k \frac{k!}{k+1} S(2n,k) = -\frac{1}{4}(9^n - 3.4^n + 3) \in \mathbb{Z}.$$

Pour $k \neq 3$, et $k+1$ composé, on a aussi $(-1)^k \frac{k!}{k+1} S(2n,k) \in \mathbb{Z}$ car d'après le lemme 157, on a $\frac{k!}{k+1} \in \mathbb{Z}$, dans ce cas. On en conclut que $S_1 \in \mathbb{Z}$.

On a

$$S_2 + \sum_{p-1 \text{ divise } 2n} \frac{1}{p} = \sum_{1\leq p\leq 2n+1 \text{ et } p \text{ premier}} (-1)^{p-1} \frac{(p-1)!}{p} S(2n,p-1) + \sum_{p-1 \text{ divise } 2n} \frac{1}{p}.$$

Or on sait d'après le théorème

$$S(2n,p-1) \equiv \begin{cases} 1 & (\bmod p) \quad \text{si } p-1 \text{ divise } 2n \\ 0 & (\bmod p) \quad \text{sinon} \end{cases}$$

On a donc

$$S_2 + \sum_{p-1 \text{ divise } 2n} \frac{1}{p} \equiv \sum_{p-1 \text{ divise } 2n} \frac{(-1)^{p-1}(p-1)!S(2n,p-1)+1}{p} \ (\bmod 1) \tag{4.64}$$

Or pour p *premier tel que* $p-1$ *divise* $2n$, *on a*

$$(-1)^{p-1}(p-1)!S(2n,p-1)+1 \equiv (-1)^p + 1 \equiv 0 \ (\bmod p). \tag{4.65}$$

Il *résulte des relations (4.64) et (4.65) que* $S_2 + \sum_{p-1 \text{ divise } 2n} \frac{1}{p} \in \mathbb{Z}$.

Pour terminer la preuve du théorème 155, il nous reste à prouver les lemmes 156 et 157

Preuve du lemme 156 *Nous suivrons les indications d'Apostol (, p.).(On a*

$$\begin{aligned}\frac{x}{\exp(x)-1} &= \frac{\log(1+(\exp(x)-1))}{\exp(x)-1}\\ &= \sum_{k=0}^{\infty}(-1)^k\frac{(\exp(x)-1)^k}{k+1}\\ &= \sum_{k=0}^{\infty}(-1)^k\frac{k!}{k+1}\frac{(\exp(x)-1)^k}{k!}\end{aligned}$$

On a alors en désignant par $[x^n]\,((\exp(x)-1)^k)$ *le coefficient de* x^n *dans* $(\exp(x)-1)^k$:

$$\begin{aligned}[x^n]\,(\frac{(\exp(x)-1)^k}{k!}) &= [x^n]\,(\sum S(n,k)\frac{x^n}{n!})\\ &= \frac{1}{n!}S(n,k).\end{aligned}$$

On a alors d'une part

$$\begin{aligned}[x^n]\,\frac{x}{\exp(x)-1} &= [x^n]\,(\sum_{k=0}^{\infty}(-1)^k\frac{k!}{k+1}\frac{(\exp(x)-1)^k}{k!})\\ &= \sum_{k=0}^{\infty}(-1)^k\frac{k!}{k+1}(\frac{1}{n!}S(n,k)).\end{aligned}$$

D'autre part

$$[x^n]\,\frac{x}{\exp(x)-1} = \frac{1}{n!}B_n$$

On en déduit le relation (4.63).

Preuve du lemme (157 *Si* $k=0$, $\frac{k!}{k+1}=1\in\mathbb{N}$, *on peut donc supposer* $k\neq 0$. *Soit donc* k *telque* $k\neq 0$, $k\neq 3$ *et tel que* $k+1$ *soit un nombre composé, alors il est facile de constater que nécessairement* $k\geq 5$. k *étant composé, il existe deux entiers* a *et* b *tels que* $k+1=ab$, a *et* b *appartenant à l'ensemble* $\{1,2,...k\}$. *Si* $a\neq b$, *il est alors évident que* $k!$ *est divible par* $ab=k+1$, *puisque* a *et* b *se retrouvent comme facteurs du produit* $1.2...a...b..k=k!$. *Si* $a=b$, *alors* $k+1=a^2$ *et on a encore* $k!=1.2...a...(2a)...k$ *divisible par* $a^2=k+1$ *; il suffit de s'assurer que* $2a\leq k$; *ou encore que* $2a\leq a^2-1$ *avec* $k=a^2\geq 5$, *ce qui facile à vérifier. En effet, pour* $a\in\mathbb{N}$, *la relation* $a^2\geq 5$ *équivaut à* $a\geq 3$, *on a donc* $(a-1)^2\geq 2$, *relation qui est équivalente à la relation* $2a\leq a^2-1$.

Grace au théorème 155 , on a une caractérisation du dénominateur du nombre de Bernoulli B_{2n} donnée par la corollaire suivant :

Corollaire 158 *Le dénominateur de* B_{2n} *est*

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

Preuve. Soit $n \geq 1$. désignons par $\{p_1, p_2, ...p_m\}$ l'ensemble des nombres premiers p tels que $p-1$ divise $2n$. Posons

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

On sait que $I_{2n} \in \mathbb{Z}$, d'après le théorème 155. On a alors

$$B_{2n} = I_{2n} - \sum_{i=1}^{m} \frac{1}{p_i} = \frac{u}{v}$$

avec

$$u = p_1.p_2...p_m I_{2n} - \sum_{i=1}^{m} \frac{p_1.p_2...p_m}{p_i} \quad \text{et} \quad v = p_1.p_2...p_m.$$

On vérifie facilement que $u \in \mathbb{Z}$, $v \in \mathbb{N}^*$ et $(u, v) = 1$. Le fait que $(u, v) = 1$ résulte du constat que tout nombre premier p_j divise $u - \frac{p_1.p_2...p_m}{p_j} = p_1.p_2...p_m I_{2n} - \sum_{1 \leq i \leq m \text{ et } i \neq j} \frac{p_1.p_2...p_m}{p_i}$ et ne divise pas $\frac{p_1.p_2...p_m}{p_j}$; par conséquent tout nombre premier p_j ne divise pas u. □

Chapitre 5

Quelques Conjectures

"J*e rêve d'un jour où l'égoïsme ne régnera plus dans les sciences, où on s'associera pour étudier, au lieu d'envoyer aux académiciens des plis cachetés, on s'empressera de publier ses moindres observations pour peu qu'elles soient nouvelles et on ajoutera «je ne sais pas le reste».*"

Evariste GALOIS (1811 – 1832).

Zhi-Wei Sun s'est beaucoup investi dans l'étude de certaines congruences et dans l'énoncé de nombreuses conjectures concernant des congruences faisant intervenir des coefficients binomiaux, des nombres de Catalan, des nombres d'Euler, des nombres de Bernoulli, ou encore des nombres de Fibonnacci. Il a aussi écrit de nombreux articles dont un grand nombre se trouve sur arXiv. Dans un de ces articles sur arXiv, dont la première version date du 30 novembre 2009 et comporte 18 pages et la dernière version à ce jour (la 54 ième version) date du 27 janvier 2011 et comporte 83 pages, il énonce dans une partie A une centaine de conjectures non résolues. Dans une partie B, il fait le bilan des conjectures qu'il avait auparavant soumises et qui ont pu être confirmées et donc résolues. Le résumé de son article est le suivant

«We collect here various conjectures on congruences made by the author in a series of papers, some of which involve binary quadratic forms and other advanced theories. Part A consists of 100 unsolved conjectures of the author while conjectures in Part B have been recently confirmed. We hope that this material will interest number theorists and stimulate further research. Number theorists are welcome to work on thoseopen conjectures. »

En introduction de cet article, il affirme

« Congruences modulo primes have been widely investigated since the time of Fermat. However, we find that there are still lots of new challenging congruences that cannot be easily solved. They appeal for new powerful tools or advanced theory.

Here we collect various conjectures of the author on congruences, most of which can be found in the author's papers available from arxiv or his homepage. We use two sections to state conjectures and related remarks. Part A contains 100 unsolved conjectures of the author while PartB consists of conjectures that have been recently confirmed. Most of the congruences here are super congruences in the sense that they happen to hold modulo some higher power of p. The topic of super congruences is related to the p-adic Γ-function, Gauss and Jacobi sums, hypergeometric series, modular forms, Calabi-Yau manifolds, and some sophisticated combinatorial identities involving harmonic numbers (cf. K. Ono's book [O]).The recent theory of super congruences also involves Bernoulli and Euler numbers (see [S09e, S10]) and various series related to (cf. [vH], [S10g] and [T]). Many congruences collected here are about $\sum_{k=0}^{p-1} a_k/m^k$ modulo powers of a prime p, where m is an integer not divisible by p and the quantity a_k is a sum or a product of some binomial coefficients which usually arises from enumerative combinatorics.

For clarity, we often state the prime version of a conjecture instead of the general version.»

Zhi-Wei Sun a démontré le résultat suivant

Théorème 159 *Tout nombre premier impair p vérifie la congruence*

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

Ce qui l'a amené après expérimentation à formuler la conjecture, suivante.(Zhi-Wei Sun affirme avoir vérifié cette conjecture pour $n < 10^4$ à l'aide du logiciel Mathematica. De plus, à sa demande, Quing-Hu Hou de l'université de Nankai a poussé cette vérification pour $n < 10^4$).

Conjecture 160 *(Zhi-Wei Sun,2009) Si un entier impair $n > 1$ vérifie la congruence*

$$\sum_{k=0}^{n-1} \frac{1}{2^k}\binom{2k}{k} \equiv (-1)^{(n-1)/2} \pmod{n^2},$$

alors n est un nombre premier.

Zhi-Wei Sun a énoncé de nombreuses autres conjectures parmi lesquelles on peut citer

Conjecture 161 *Zhi-Wei Sun,2010) Pour tout nombre premier p impair*

$$\sum_{k=0}^{p-1} \binom{2k}{k}^3 \equiv \begin{cases} 4x^2-2p \pmod{p^2} & si\ (\frac{p}{7}) = 1\ \&\ p = x^2+7y^2 \\ 0 \pmod{p^2} & si\ (\frac{p}{7}) = 1, ie., p \equiv 3,5,6 \pmod 7 \end{cases}$$

.

Annexe 1

Nous donnons la preuve de certaines problèmes énoncés au chapitre 1 :

Problème 162 *(Theorie des Nombres de Z. I. Borevitch et I.R. chafarévitch [13],exercices* $1, 2,$ *et* 3 *page* 3*)*

1. *L'équation* $15x^2 - 7y^2 = 9$ *n'a pas de solution en nombres entiers.*
2. *L'équation* $5x^3 + 11y^3 + 13z^3 = 0$ *n'a pas d'autre solution en nombres entiers que la solution triviale* $x = 0$, $y = 0$, $z = 0$.
3. *L'équation* $5x^3 + 11y^3 + 13y^3 = 0$ *n'a pas d'autre solution en nombres entiers que la solution triviale* $x = 0$, $y = 0$, $z = 0$.
4. *Les nombres entiers de la forme* $8n + 7$ *ne peuvent pas s'écrire comme somme de trois carrés de nombres entiers.*

Solution 163 *1. Raisonons par l'absurde. Si léquation* $15x^2 - 7y^2 = 9$ *avait une solution* $(x_0, y_0) \in \mathbb{Z}^2$*, on aurait*

$$15x_0^2 - 7y_0^2 \equiv\ 9 \pmod 5.$$

C"est à dire

$$-2y_0^2 \equiv\ 4 \pmod 5.$$

Soit encore

$$y_0^2 \equiv\ 3 \pmod 5.$$

ou

$$y_0^2 - 3 \equiv\ 0 \pmod 5.$$

Or ceci est impossible. En effet,on sait que

$$y_0 \equiv 0\ ou\ \pm 1\ ou\ \pm 2 \pmod 5,$$

et par conséquent

$$y_0^2 - 3 \equiv 2\ ou\ 3\ ou\ 1 \pmod 5.$$

2. On étudie

$x \searrow y$	0	1	5	8	12
0	0	11	10	3	2
1	5	3	2	8	7
5	1	12	11	4	3
8	12	10	9	2	1
12	8	6	5	11	10

Problème 164 *(exemple 15 de la page 29)_*

$$\frac{1}{\pi}\arctan(\frac{4}{3}) \notin \mathbb{Q}. \tag{5.1}$$

Solution 165 *Voici un lemme utile à le résolution de ce problème*

Lemme 166 *Pour tout nombre réel θ, on a*

$$\frac{\theta}{\pi} \in \mathbb{Q} \Longleftrightarrow \exists n \in \mathbb{N}^*,\ (\cos(\theta) + i\sin(\theta))^n = 1$$

Preuve. En effet montrons tout d'abord l'implication : $\frac{\theta}{\pi} \in \mathbb{Q} \Longrightarrow \exists n \in \mathbb{N}^*$, $(\cos(\theta) + i\sin(\theta))^n = 1$. Supposons que $\frac{\theta}{\pi} \in \mathbb{Q}$, alors il existe deux entiers $r \in \mathbb{Z}$ et $s \in \mathbb{N}^*$tels que $\frac{\theta}{\pi} = \frac{r}{s}$. On a alors $2s\theta = 2r\pi$. Par suite, en posant $n = 2s$, on a $n \in \mathbb{N}^*$ et $\cos(n\theta) + i\sin(n\theta) = 1$, c'est à dire $(\cos(\theta) + i\sin(\theta))^n = 1$.

Réciproquement prouvons que : $\exists n \in \mathbb{N}^*, (\cos(\theta) + i\sin(\theta))^n = 1 \Longrightarrow \frac{\theta}{\pi} \in \mathbb{Q}$. supposons donc qu'il existe un entier naturel non nul n tel que $(\cos(\theta) + i\sin(\theta))^n = 1$, alors on a $\cos(n\theta) + i\sin(n\theta) = 1$. Il existe alors un entier $m \in \mathbb{Z}$ tel que $n\theta = 2m\pi$. On a alors $\frac{\theta}{\pi} = \frac{2m}{n}$ et $\frac{\theta}{\pi} \in \mathbb{Q}$. □

Ainsi en posant

$$\theta = \arctan(\frac{4}{3})$$

prouver que

$$\frac{1}{\pi}\arctan(\frac{4}{3}) \notin \mathbb{Q}.$$

est équivalent à prouver que

$$\forall n \in \mathbb{N}^*,\ (\cos(\theta) + i\sin(\theta))^n \neq 1. \tag{5.2}$$

Or on sait que

$$\begin{aligned} \cos(\theta) &= \cos(\arctan(\frac{4}{3})) \\ &= \frac{1}{\sqrt{1 + (\tan(\arctan(\frac{4}{3})))^2}} = \frac{3}{5} \end{aligned}$$

et

$$\begin{aligned}\sin(\theta) &= \sin(\arctan(\frac{4}{3}) \\ &= \frac{\tan(\arctan(\frac{4}{3}))}{\sqrt{1+(\tan(\arctan(\frac{4}{3})))^2}} = \frac{4}{5}.\end{aligned}$$

La relation (5.2) est équivalente à

$$\forall n \in \mathbb{N}^*,\ (3+4i)^n \neq 5^n. \tag{5.3}$$

La relation (5.3) est facile à prouver à l'aide des congruences modulo 5. Posons pour tout entier $n \geq 1$

$$\begin{aligned}a_n &= \mathrm{Re}((3+4i)^n) \\ b_n &= \mathrm{Im}((3+4i)^n)\end{aligned}$$

On a alors pour tout entier $n \geq 1$

$$a_{n+1} + ib_{n+1} = (3+4i)(a_n + ib_n).$$

D'où

$$\begin{cases} a_1 = 3 \\ b_1 = 4 \\ a_{n+1} = 3a_n - 4b_n,\ n \geq 1 \\ b_{n+1} = 4a_n + 3b_n,\ n \geq 1. \end{cases}$$

A partir de ces relations, il est facile de prouver à l'aide d'un raisonnement par récurrence que pour tout entier $n \geq 1$

$$\begin{aligned}a_n &\equiv 3 \pmod 5 \\ b_n &\equiv 4 \pmod 5.)\end{aligned}$$

Il en resulte que pour tout entier $n \geq 1$, on a

$$\mathrm{Im}(b_n) \neq 0.$$

Ainsi pour tout entier $n \geq 1$, $(3+4i)^n \notin \mathbb{R}$ et donc pour tout entier $n \geq 1$, $(3+4i)^n \neq 5^n$. On a prouvé 5.3, c'est à dire 5.2 et donc 5.1.

Conclusion

"*J'ignore ce que le monde pensera de mes œuvres, mais il me semble n'avoir été qu'un enfant jouant sur une plage trouvant parfois un coquillage d'une beauté inusitée ou un galet étonnamment lisse, tandis que s'étendait devant moi l'immense océan des connaissances.*"

Sir Isaac Newton

"*..De sorte que toute la suite des hommes, pendant le cours de tant de siècles, doit être considérée comme un même homme qui subsiste toujours et qui apprend continuellement...* "

Blaise Pascal

L'écriture de ce mémoire nous a amené à entreprendre une recherche sur le thème des congruences. Pratiquement, celle-ci s'est faite essentiellement par Internet. En effet, cette technologie d'aujourd'hui nous a permis d'avoir accès légalement et gratuitement à de nombreux documents et ouvrages très anciens qui constituent les fonds précieux de certaines bibliothèques et qui ont été numérisés et mis gratuitement à la disposition du grand public sous réserve de respecter certaines clauses. La numérisation des livres anciens est une longue et difficile tâche d'actualité. Ces vieux ouvrages constituent en effet une mine inépuisable de renseignements La numérisation du contenu de grandes bibliothèques européennes ou américaines est devenu un gigantesque chantier, dont l'intérêt n'a pas échappé à des géants de l'informatique comme Google, Yahoo ou Microsoft. Ces initiatives visent aussi à préserver la mémoire de l'humanité pour les générations à venir. Il est vrai que l'ignorance et la bêtise des hommes ont souvent détruit des trésors inestimables. La bibliothèque d'Alexandrie, la plus célèbre bibliothèque de l'Antiquité à Alexandrie en Égypte fondée en -288 , qui recelait de précieux documents souvent en unique exemplaire n'a-t-elle pas a été brulée, et définitivement détruite (au plus tard en l'an 642) . Il n'y a pas si longtemps encore, le 7 juin 1962, la bibliothèque nationale d'Alger avait elle aussi été saccagée, incendiée par des mains criminelles. Des milliers d'ouvrages et de périodiques ont été la proie des flammes ou de l'eau. Aujourd'hui, la technologie ayant évolué, la numérisation constitue une parade adéquate aux risques de pertes des documents scientifiques.

Bien sûr, dans de nombreux cas, nous n'avons pas toujours eu la chance d'avoir accès fa-

cilement aux documents existants, le site exigeant un paiement ou une convention avec un organisme universitaire. L'USTHB a heureusement des conventions avec entre autres Springer Verlag, cela nous a été d'une aide précieuse pour consulter certains documents plus récents et non accessibles pour nous sans cela. Nous avons pu ainsi découvrir et apprécier toute la richesse des écrits mathématiques sur une notion apparemment aussi simple et banale que la notion de congruences. L'origine de cette notion puise ses racines dans la nuit des temps. Le fameux théorème des restes chinois date des tous premiers siècles. Selon Song Y. Yan, ce théorème fut découvert par le mathématicien chinois Sun Tsu qui vivait sans doute avant le début de l'ère chrétienne. Bien plus tard, érigée en théorie des congruences, elle a continué à se développer avec Gauss. Cette recherche continue encore aujourd'hui. Les techniques d'approches ont bien sûr évolué. Tous les domaines des mathématiques (Analyse, Combinatoire...) sont mis à contribution pour mener à bien cette tache. Les logiciels de calcul (calcul formel et numérique) sont un précieux moyen d'investigation. L'approche p-adique que nous a suggéré Monsieur le Professeur Benzaghou, mais que nous n'avons pu qu'esquisser dans ce mémoire est une technique prometteuse pour solutionner certains problèmes difficiles.

En fait, dans ce mémoire, nous n'avons fait que survoler cette immense pays des congruences nous attardant parfois sur certaines d'entre elles, qui nous avaient semblé plus intéressantes ou tout simplement plus accessibles. De nombreuses conjectures découvertes sans doute expérimentalement restent encore à étudier. Pour mesurer l'ampleur de cette tache, on pourrait consulter avec profit le site de Wei Sun où cet éminent Professeur énonce un nombre très appréciable de problèmes restant à solutionner.

Au terme de ce mémoire, nous souhaitons à l'avenir approfondir davantage la technique d'approche p-adique et aussi d'autres techniques pour apporter une réponse à (au moins) une partie de ces nombreuses questions restées en suspens !

Enfin, on conclut ce travail par les nombreuses perspectives de recherche qu'offre l'étude des congruences. De nombreuses conjectures restent encore à prouver. Certaines célébres telles que la conjecture de Giuga et la conjecture d'Agoh.

Conjecture 167 *(Giuga, 1950) Pour tout entier $n \geq 2$, on a l'équivalence*

$$\sum_{k=1}^{n-1} k^{n-1} \equiv -1 \ (\mathrm{mod}\, n) \quad \Longleftrightarrow \quad n \text{ est premier.}$$

Conjecture 168 *(Agoh, 1990) Pour tout entier $n \geq 2$, on a l'équivalence*

$$nB_{n-1} \equiv -1 \ (\mathrm{mod}\, n) \quad \Longleftrightarrow \quad n \text{ est premier.}$$

En 2004, B.C. Kellner [55] a prouvé que ces deux conjectures étaient équivalentes. Depuis, il ne semble pas qu'il y ait eu d'autres avancées. Pour établir ce résultat, B.C. Kellner exploite

des propriétés de congruences des nombres de Stiling de première et deuxième espèce ainsi que certaines congruences vérifiées par les coefficients binomiaux. L'étude de ces congruences de ces familles de nombres remarquables semble donc être une voie prometteuse pour avancer dans la résolution de certaines conjectures.

Signalons toutefois une tentative de résolution de ces deux conjectures en juin 2011 par T. Sauvaget [88]. Cette article comportait une erreur vite signalée par R. Chapman, T. Foo et A. Oller et un rectificatif à l'annonce de cette preuve a été vite fait dans une seconde version le 9 juin 2011 [90].

Bibliographie

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

[2] **A. Adelberg**, *Congruences of p-adic integer order Bernoulli numbers*, J. Number Theory 59(**1996**), 374 − 388.

[3] **C. Aebi and G. Cairns**, Morley's other miracle, Preprint,**2011** http ://www.latrobe.edu.au/mathstats/staff/cairns/papers/morleycong.pdf

[4] **Alhazen** Opuscula

[5] **Y. Amice**, Les nombres p-adiques, Collection SUP, Le Mathématicien, PUF **1975**.

[6] **George .E** .Andrews.Number Theory.

[7] **George .E**. Andrews. q-analogs of the binomial coefficient congruences of Babbage, Wolstenholme and Glaisher. Discrete Math., 204(1) : 15 − 25, **1999**.

[8] **D. Barsky**, *Fonction Gamma p-adique et applications*, Cours à l'USTHB 9 au 14 décembre **2002**

[9] **B Benzaghou and D Barsky**, Extension of classical sequences to negative integers, Discussiones Mathematicae General Algebra and Applications 25(**2005**)75 − 83

[10] **B Benzaghou**, Algèbre de Hurwitz. Fac Math USTHB **2002**.

[11] **C Babbage**, demonstration of a theorem relating to Prime Numbers. Edinburgh philosophical journal vol I**1819**

[12] **M. Bayat**, A generalisation of Wolstenholme's theorem, Amer. Math. Monthly 104(**1997**)557 − 660.

[13] **Z. I. Borévitch et I. R. Chafarévitch** Théorie des Nombres, Gauthier-Villars, Paris, **1967**.

[14] J. Boulanger and J.-L. Chabert, An extension of the Lucas theorem, Acta Arithmetica XCVI.4(**2001**).

[15] **L. Carlitz**, Generating functions and partition problems, Proc. Symp. Pure Math. vol. VIII, American Math. Soc., Providence, **1965**, 144 − 169.

[16] **M. Chamberland and K. Dichler**, A binomial sum related to Wolstenholme's theorem, Journal of Number Theory, Volume 129, Issue 11, (**2009**), 2659 − 2672.

[17] **O-Y. Chan and D. V. Manna**, Congruences for Stirling numbers of the second kind, in Gems in Experimental Mathematics, Contemporary Math. 517, Amer. Math. Soc., (**2010**), $97-111$.

[18] **W. Edwin Clark**. q-analogue of a binomial coefficient congruence. International Journal of Mathematics and Mathematical Sciences, $18(1) : 197-200$, **1995**.

[19] **L. Comtet**, Analyse combinatoire, tomes premier et second, Collection Sup "Le Mathématicien", P.U ;F. **1970**.

[20] **L. Comtet**, Advanced Combinatorics, Reidel, **1974**.

[21] **L. Comtet**, Analyse combinatoire élémentaire, Techniques de l'ingénieur, traité Sciences fondamentales, (**2001**).

[22] **L. Comtet**, Analyse combinatoir avancée, Techniques de l'ingénieur, traité Sciences fondamentales, (**2001**).

[23] **L. Comtet**, Analyse Combinatoire appronfondie, Techniques de l'ingénieur, traité Sciences fondamentales, (**2003**).

[24] **R Chapman and H Pan**. q-analogues of Wilson's theorem. Int. J. Number Theory, $4(4) : 539-547$, **2008**.

[25] **J. DeMaio and S. Touset,** Stirling Numbers of the second Kind and Primality, Proceedings of the 2008 International Conference on Foundations of Computer Science, FCS 2008, July $14-17, 2008$, Las Vegas, Nevada, USA **2008**.

[26] **M Demazure** Cours d'algèbre Cassini

[27] **J. M. De Koninck**, A. Mercier, Introduction à la théorie des nombres, Modulo Editeur **1994**.

[28] **L. E. Dickson**, History of the Theory of Number, Vol. I. Chelsea, Neww York,**1999**.

[29] **K Dilcher**. Determinant expressions for q-harmonic congruences and degenerate Bernoulli numbers. Electron. J. Combin., $15(1)$, **2008**.

[30] **F le Lionnais** (avec la collaboration de Jean Brette) Les nombres remarquables, Hermann, **1983**.

[31] **C.F.Gauss**,Théoria Residuorum Biquadraticorum,Comment.I.soc.reg.sci.Gottingensis rec.6(**1828**); $431-505$

[32] **C .F. Gauss** ; *Recherches arithmétiques,* **1801** *Traduction M. Poullet Delisle Ed. Courcier* **1807**

[33] **Ira M. Gessel**, *Wolstenholme revisited*, Amer. Math. Monthly $105(\mathbf{1998}), 657-658$.

[34] **J. W. L. Glaisher**, On the Residus of the Sums of Products of the First $p-1$ Numbers, and their powers, to Modulo or . Quaterly J. Math. $31(\mathbf{1900}), 321-353$.

[35] **A. Gertsch**, Nombres harmoniques généralisés, C. R. Acad. Sci. Paris, $324(\mathbf{1997})$, Série $1, 7-10$.

[36] **A. Gertsch**, Congruences pour quelques suites classiques de nombres ; sommes de factorielles et calcul ombral, thèse , Université de Neuchatel (Suisse) **1999**

[37] **A. Gertsch**, A. M. Robert, Some congruences concerning the Bell numbers, Bull. Belg. Math. Soc. Simon Stevin Volume 3, Number 4(**1996**).

[38] **H.W.Gould** ,Stirling numbers representation problems .

[39] **F.Q. Gouvea**, p-adic Numbers, An introduction, Second Introduction, Springer-Verlag, **2003**.

[40] **Graham, Knuth, Patashnik**, *Concrete Mathematics*, Addison Wesley (Second Edition), Massachusetts **1994**.

[41] **A. Granville**, Arithmetic Properties of binomial Coefficients I : Binomial coefficients modulo prime powers, in Organic mathematics
(Burnady, BC, 1995), CMS Conf., 20, Amer. Math. Soc., Providence, RI ; **1997**, pp. $253 - 276$.

[42] **A. Granville**,Binomial coefficients modulo prime powers, School of Mathematics at the Institute for Advanced Study, http ://www.dms.umontreal.ca/~andrew/PDF/BinCoeff.pdf.

[43] **A. Granville**, *The square of the Fermat quotient*, Integers : Electronic J. of Combinatorial Number Theory 4(**2004**), # A22(electronic)

[44] **R. K. Guy**, Unsolved Problems in Number Théory, Springer, New York, **1981**.

[45] **G.H. Hardy & E. M. Wright**, introduction à la théorie des nombres, traduction de François Sauvaegeot, Vuibert Spinger **2007**.

[46] **C.Helou and G.Terjanian** On Wolstenholme's theorem and its converse ,J.Number Theory 128 (**2008**), $475 - 499$.

[47] **T Herriot**,http ://echo.mpigw-berlin.mpg.de/content/
scientific_revolution/harriot/harriot/medium.html

[48] **L.Euler** Opuscule Anal tome $1p - 329$

[49] **J. M. Holte**, A Lucas-type theorem for binomial-coefficient residues, Fibonacci Quart. 32(**1994**), $60 - 68$.

[50] **F.T.Howard**,Extensions of congruences of Glaisher and Nielsen concerning Stirling numbers ,Fib.Quart.28(**1990**),n $4, 355 - 362$.

[51] **Ch.Jordan**, *Calculus of finite Differences* (second edition,New York,**1952**, $652p$).

[52] **A. Junod**, *Congruences par l'analyse p−adique et le calcul symbolique*, Thèse de doctorat, **2003**.

[53] **G. S. Kazandzidis**, Congruences on the binomial coefficients, Bull. Soc. Math. rce (N.S.) 9(**1968**), fasc. 1, pp. $1 - 12$.

[54] **G. S. Kazandzidis**, On congruences in number –théory, Bull. Soc., Bull. Soc. Math. rce (N.S.) 10(**1969**), fasc. 1, pp. $35-40$

[55] **B. C. Kellner**, The equivalence of Giuga's and Agoh's Conjectures, arXiv :math/0409259v [math.NT] 15Sep **2004**

[56] **N. Koblitz**, *p-adic Numbers, p-adic Analysis, and Zeta-Functions, Second Edition*, Springer-Verla, **1984**.

[57] **D. E. Knuth and H. S. Wi l f**, The power of a prime that divides a generalized binomial coefficient, J. Reine Angew. Math. 396(**1989**), $212-219$.

[58] **M. Janjić**, On a non-combinatorial definition of Stirling numbers, ArXiv !0806.2366v1, **2008**.

[59] **A. M. Legendre** Essai sur la théorie des nombres, Paris, $1797-1798$ (2è éd. 1808, 3è éd. 1830), 2 vol.

[60] **J L Lagrange** ,Oeuvres de Lagrange ,tome $IIIpp425-438$.Nouveau Mémoires de l'Académie royale des sciences et belles lettres de Berlin,année **1771**.

[61] **E. Lehmer**, on congruences involving Bernoulli number and the quotients of Fermat and Wilson, Annals of Math., 39(**1938**), $350-360$.

[62] **E. Lucas**, Théorie des nombres, Gauthier-Villars 1891, rééd. Jacques Gabay **1991**).

[63] **N Mahloul** Sur une congruence de Morley préprint **2012**

[64] **R.J.McIntosh**,On the converse of Wolstenholme's theorem,Acta Arithmetica LXX1.4(**1995**).

[65] **R.Méstrovic**,On the mod p^7 determination of $\binom{2p-1}{p-1}$,Arxiv :1108.1174v1.04 Aout **2011**.

[66] **R.Méstrovic**,Congruences for Wolstenholme primes,Arxiv :1108.4178v1.21 Aout **2011**.

[67] **R.Méstrovic**,An extension of a congruence by Kohnen Arxiv :1109.2340v3 19 Oct **2011**.

[68] **R.Méstrovic**,Wolstenholme theorem's :Its generalisations and extentions in the last hundred and fifty years$(1862-2012)$.Arxiv :1111.3057v2.25 Déc **2011**.

[69] **D.S.Mitrinovic -R.S.Mitrinovic**,Tableaux qui fournissent des polynômes de Stirling .N 34(**1960**).

[70] **D.S.Mitrinovic-R.S.Mitrinovic**,Sur une classe de nombres se rattachant aux nombres de Stilring .N 60 (**1961**).

[71] **D.S.Mitrinovic-R.S.Mitrinovic**,Tableaux d'une classe de nombres reliés aux nombres de Stirling .N 77 (**1962**).

[72] **Y. Morita**, *A p-adic analog of the* $\Gamma-$*fonction*, Journal Faculty of Science University of Tokyo, 22(**1975**), $255-266$.

[73] **F. Morley**, *Note on the Congruence* $2^{4n} \equiv (-1)^n(2n)!/(n!)^2$, *where* $2n+1$ *is a prime*, Ann. Math. $9-$**1895**), $168-170$.

[74] **J. Neukirch** The p-Adic Numbers,

[75] **N. Nielsen**, *Recherches sur les polynômes de Bernoulli*, Danske Vidensk. Selsk. Skr. (7)10(**1913**), $285-366$.

[76] **N. Nielsen**, *Traité élémentaire des nombres de Bernoulli, Paris,* **1923**.

[77] **N. Nielsen**, *Recherches sur les polynômes de Stirling*, Det Kgl. Danske Videnskabernes Selseskab. Mathematisk-fysiske Meddelelser. $II, 12,$ **1920**.

[78] **Hao Pan**. A q-analogue of Lehmer's congruence. Acta Arith., $128(4) : 303-318,$ **2007**.

[79] **C. Pisot**, *L'analyse p-adique en théorie des nombres*, Séminaire Delane-Pisot-Poitou. Théorie des nombres, tome 5(**1963 − 1964**), ex. n°1.$p1-6$.

[80] **Léon.Pomey**,Trois démonstrations des théorèmes de Fermat et Wilson ,Nouvelles annales de mathématiques 4 ^{eme}série tome 19(**1919**) p $373-380$.

[81] **E.Prouhet**,Note sur les nombres associés :généralisation du théorème de Wilson,Nouvelles annales de mathématiques 1^{re} série tome 4(**1845**) p $273-278$.

[82] **R Rashed**,Entre arithmétique et algèbre :recherches sur l'histoire des mathématiques arabes .Paris :les belles lettres ;**1984**,In-8, 324 pages (Sciences et philosophie arabe).

[83] **P. Ribenboim**, the book of Prime Number Records, 2nd ed., Springer, New York, **1989**.

[84] **S. Roman**, The harmonic loarithms and the binomial formula, J. Combbin. Theory, Serie A, 63 (**1993**), $143-163$.

[85] **A. Robert**, *A Course in p-adic Analysis*, TM 198, Spiner-Verla (**2000**).

[86] **P. Samuel**, Théorie alébrique des nombres, Collection Méthodes, Hermann **1997**.

[87] **J. Sándor and B. Crstici** Handbook of number theory II, Kluwer Academic Publisher, **2005**.

[88] **T. Sauvaget**, elementary proof of the Giuga-Agoh conjecture, arxiv : 1106.1627v1 [math NT] 8 juin **2011**

[89] **J stirling** , Methodus Differentialis ;Sive Tractatus de Summations et Interpolatione ,Serierum Infinitarum.Auctore Jacobo Stirling ,R.S.S.**1730** .

[90] Retraction of " elementary proof of the Giuga-Agoh conjecture", arxiv : 1106.1627v2 [math NT] 9 juin **2011**

[91] **Ling-Ling Shi and H Pan**. A q-analogue of Wolstenholme's harmonic series congruence. Amer. Math. Monthly, $114(6) : 529-531,$ **2007**.

[92] **W. H. Schikhof** "Ultrametric calculus An introduction to p-adic analysis", Cambrie University Press, **2006**, (First edition 1984).

[93] **N. J. A. Sloane**, On-Line Encyclopaedia of Integer Sequence,http ://oeis.org/

[94] **A Straub**, A q-analog of Ljunggren's binomial congruence, arXiv : 1103.3258v116 mars 2011.

[95] **Terquem**,Théorème de Wilson d'après M.Gauss , Nouvelles annales de mathématiques ,1^{re} série ,tome 2 (**1843**), $p193 - 195$.

[96] **V.Trevisan and K.Weber**,Testing the controverse of Wolstenholme's theorem ,Matematica Contemporânea $21(\mathbf{2001}), 275 - 286$.

[97] **C. Tweedie**, The Stirling Numbers and Polynomials, EMS Proceedings and Notes, Vol $37(\mathbf{1918})2 - 25$.

[98] **C. Tweedie** ,JAMES STIRLING ,A Sketch of his life and works Along with his Scientif Correspondance .Oxford ,AT THE CLARENDON PRESS.(**1922**)

[99] **E. Waring**.Meditationes algebraicoeab Eduardo Waring,Matheseos Professore Lucasiano .Cantabrigiae (**1770**), $p - 218$.

[100] **P. Xu and H. Pan**, Note on acongruence involving products of binomial coefficients, Electronic Journal of combinatorial Number Theory 7(**2007**), #A04.

[101] **J. Zhao**, Bernoulli Numbers, Wolstenholme's Theorem, and p^5 Variations of Lucas'Theorem, Arxiv :math/0303332v310 Feb **2006**.

[102] **Zhi-Hong Sun**, Congruences concerning Bernoulli numbers and Bernoulli polynomials, Discrete Applied Mathematics $105(\mathbf{2000})192 - 233$.

[103] **Zhi Wei Sun**, On congruences related to central binomial coefficients preprint arXiv : 0911.2415, 15 Sep **2010**.

[104] **Zhi Wei Sun**, *Open conjectures on congruences,* Preprint arXiv : 0911.5665 v54, 27 Jan **2011**. http ://arxiv.org/abs/0911.5665

[105] **Zhi Wei Sun**, Binomial coefficients, *Catalan numbers and Lucas quotients*, preprint arXiv : **0909**.