REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE
MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE
UNIVERSITE DE DJILALI BOUNAÂMA-KHEMIS MILIANA
Faculté des Sciences et de la Technologie
Département de Mathématiques et Informatique

Mémoire

Pour obtenir

Le diplôme de master en mathématiques
Spécialité : Analyse Mathématique et Applications

Présenté par

BOUAICH Ibtissem

Étude de certaines généralisations des congruences de Wolstenholme de Morley

---

Soutenue publiquement le 23 juin 2018 devant les membres du jury :

Mr. M. HACHAMA	*Univ. de Khemis Miliana*	**Président**
Mr. M. HOUASNI	*Univ. de Khemis Miliana*	**Encadrant**
Mr. M. KARRAS	*Univ. de Khemis Miliana*	**Examinateur**
Mr. B. CHAOUCHI	*Univ. de Khemis Miliana*	**Examinateur**

Année Universitaire : ***2017-2018***

Résumé

Ce mémoire est consacré à une étude approfondie de certaines congruences célèbres relatives à des coefficients binomiaux et à des sommes harmoniques. Il s'agit de congruences dûes à J. Wolstenholme (1862), F. Morley (1895).

Nous étudions les preuves de ces congruences ainsi que des généralisations et améliorations successives de ces congruences jusqu'à nos jours dont les plus récentes datent de 2016.

Ce mémoire comporte trois chapitres. Le premier chapitre est consacré à des rappels et à des compléments utiles à la compréhension des nombreux articles que l'on a du étudier. Dans le second chapitre nous étudions les congruences de J. Wolstenholme et de F. Morley et quelques unes de ses améliorations et extensions. Le troisième chapitre est consacré à une congruence dûe à F. Bencherif et R. Boumahdi et quelques unes de ses résultats.

Abstract

This memoir is devoted to an in-depth study of some famous congruences relating to binomial coefficients and harmonic sums. These are congruences due to J. Wolstenholme (1862), F. Morley (1895).

We study the proofs of these congruences and some of its generalizations and successive improvements until our days.

This memoir has three chapters. The first one is devoted to reminders useful for understanding the many articles that we have to study. In the second chapter we study the congruences of J. Wolstenholme and F. Morley and some of its improvements and extensions. The third chapter is devoted to a congruence due to F. Bencherif and R. Boumahdi and some of its results.

Table des matières

Dédicaces

à ma chère maman

Aucun dédicace ne saurrait exprimer mon espoir, mon amour étérnel et ma considération pour les sacrifices que vous avez consenti pour mon instruction et mon bien être.

je vous remercie pour tout le soutien et l'amour que vous me portez depuis mon enfance et j'éspère que votre bénédiction m'accompagne toujours.

Je fais un dédicace a $Hamza$ *qui a crus à moi tout au long de mon parcours scolaire.*

Remerciements

La première personne que je tiens à remercier est mon encadrant Mr M. HOUASNI, pour l'orientation, la confiance, la patience qui ont constitué un apport considérable sans lequel ce travail n'aurait pas pu être mené au bon port. Qu'il trouve dans ce travail un hommage vivant à sa haute personnalité.

J'exprime toute ma reconnaissance à Monsieur M. HACHAMA pour avoir bien voulu accepter de présider le jury de ce mémoire. Que Monsieur B. CHAOUCHI et Monsieur M. KARRAS, des professeurs à l'université de Djilali Bounaama de Khemis Miliana , trouvent ici l'expression de mes vifs remerciements pour avoir bien voulu juger ce travail.

Je tiens à exprimer mes sincères remerciements aussi à tous les professeurs qui nous ont enseigné et qui par leurs compétences nous ont soutenu dans la poursuite de nos études.

Enfin, on remercie tous ceux qui, de près ou de loin, ont contribué à la réalisation de ce travail.

A ma chère maman Nadia, pour tous ses sacrifices, son amour, sa tendresse, son soutien et ses prières tout au long de mes études,

A mon cher frère Abdelghani pour son encouragement permanent, et son soutien moral.

Je rends hommage aussi à mon papa Djelloul, mon héros mon inspirtation, tu resteras dans mon cœur à jamais, que Dieu t'accueille dans son vaste paradis.

Je remercie particulièrement Hamza qui m'a fait encouragé et m'a donné des conseils, sans oublié mes beaux parents et mes grands parents pour leurs soutien et leurs confiance qui m'ont fait a moi,

A toute ma famille pour leur soutien tout au long de mon parcours universitaire, mes tante (Mazori,Hamida amina,Samira et Fouzia) et Amo Boualem, Amo Amar et tout mes oncles et Khalil qui m'a fait aider, mes cousins et mes cousines,

A tout mes collègues surtout Ahlem et Asmaa,

Enfin, on remercie tous ceux qui, de près ou de loin, ont contribué à la réalisation de ce travail.

Merci d'être toujours là pour moi.

Notations

1. $\mathbb{N}$, $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ et $\mathbb{C}$ désignent respectivement les ensembles des entiers naturels, des entiers relatifs, des rationnels, des réels et des complexes.
2. $\deg(P(x))$ *: degré du polynôme* $P(x)$.
3. $a \mid b$ où a et b sont deux entiers signifie : "a divise b".
4. $a \nmid b$ où a et b sont deux entiers signifie : "a ne divise pas b"
5. Pour $x \in \mathbb{Q}$, $\text{denom}(x)$ désigne le dénominateur de x. $\text{denom}(x) := \min\{n \in \mathbb{N}^* / \ nx \in \mathbb{Z}\}$.
6. La lettre p désigne toujours un nombre premier.
7. Pour $x \in \mathbb{Z} - \{0\}$, $v_p(x) := \max\{m \in \mathbb{N} \ / \ p^m | x\}$, $v_p(x)$ est appelé valuation p-adique de x.
8. Pour $x = \frac{a}{b} \in \mathbb{Q} - \{0\}$, avec $a, b \in \mathbb{Z} - \{0\}$, $v_p(x) := v_p(a) - v_p(b)$, $v_p(x)$ est appelé valuation p-adique de x.
9. Pour $x \in \mathbb{Q}$, $\text{num}(x)$ désigne le numérateur de x. $\text{num}(x) := x\,\text{denom}(x)$.
10. $\mathbb{Z}_{(n)}$ désigne l'anneau des n-entiers, un n-entier étant un nombre rationnel dont le dénominateur (de sa forme réduite) est premier avec n.
11. Pour $a \in \mathbb{Q}$ et $b \in \mathbb{Q}$ et $n \in \mathbb{N}^*$, $n \geq 2$, $a \equiv b \pmod{n}$ signifie que $a - b \in n\mathbb{Z}_{(n)}$ et se lit : a congru à b modulo n.
12. Pour $a \in \mathbb{Q}$ et $b \in \mathbb{Q}$ et $n \in \mathbb{N}^*$, $n \geq 2$, $a \not\equiv b \pmod{n}$ signifie que $a - b \notin n\mathbb{Z}_{(n)}$ et se lit : a est non congru à b modulo n.
13. $\binom{n}{k}$ coefficient binomial, tel que n et k deux entier où $0 \leq k \leq n$.
14. $B_n(x)$: n-ième polynôme de Bernoulli.
15. B_n : n-ième nombre de Bernoulli : $B_n = B_n(0)$.
16. $P_m(n) = 0^m + 1^m + 2^m + \cdots + n^m$.
17. Pour tout nombre réel x :

    $[x]$ désigne la partie entiére de x, c'est à dire l'unique nombre entier k vérifiant $x - 1 < k \leq x$.

Introduction

Le théorème connu sous le nom de théorème de Wilson (1770) affirme que si p est un nombre entier supérieur ou égal à 2, alors p est premier si et seulement si

$$(p-1)! \equiv -1 \pmod{p}.$$

Dans une recherche d'une caractérisation des nombres premiers analogue au théorème de Wilson, C. Babage [2] établit en 1819 la congruence suivante.

$$\binom{2p-1}{p-1} \equiv 1 (\mathrm{mod}\, p^2) \quad (p \geq 3).$$

En 1862, J. Wolstenholme [35] améliora la congruence de Babbage en prouvant que si p est premier, alors

$$\binom{2p-1}{p-1} \equiv 1 (\mathrm{mod}\, p^3) \quad (p \geq 5). \tag{1}$$

Pour établir ce résulat, J. Wolstenholme avait d'abord prouvé les congruences suivantes concernant certains nombres harmoniques

$$1 + \frac{1}{2} + \cdots + \frac{1}{p-1} \equiv 0 \pmod{p^2} \quad (p \geq 5),$$

$$1 + \frac{1}{2^2} + \cdots + \frac{1}{(p-1)^2} \equiv 0 \pmod{p} \quad (p \geq 5).$$

Les congruences de Babbage et de Wolstenholme furent le point de départ d'une intense recherche, qui continue de nos jours, sur les congruences pour certains coefficinets binomiaux et certaines sommes harmoniques. Ainsi, en 1861, J.J. Sylvester [1] prouva la congruence suivante, pour tout nombre premier p

$$\sum_{k=1}^{(p-1)/2} \frac{1}{k} \equiv -2q \pmod{p}, \text{ où } q = \frac{2^{p-1}-1}{p}. \ (p \geq 5). \tag{2}$$

En 1895, F. Morley [24] prouva par une méthode surprenante, en exploitant des relations trigonométriques, la congruence suivante

$$(-1)^{\frac{p-1}{2}} \binom{p-1}{\frac{p-1}{2}} \equiv 4^{p-1} \pmod{p^3} \quad (p \geq 5). \tag{3}$$

En 2016, F. Bencherif et R. Boumahdi [7] ont trouvé une généralisation de (1), pour tout p-entier $\alpha \geq 1$ et pour tout nombre premier impair p, on a

$$\binom{\alpha p - 1}{p-1} \equiv 1 - \alpha(\alpha-1)(\alpha^2-\alpha-1)p\sum_{k=1}^{p-1}\frac{1}{k} + \alpha^2(\alpha-1)^2p^2\sum_{1\leq i<j\leq p-1}\frac{1}{ij} \pmod{p^m}. \quad (4)$$

où $m = 7$ si $p \neq 7$ et $m = 6$ si $p = 7$.

Ce mémoire est consacré à une étude des preuves et amélioartions successives des congruences de Wolstenholme (1) et de Morley (3). Il comporte trois chapitres. Le premier chapitre est consacré à des rappels de certains théorèmes classiques d'arihmétique et à une brêve étude des congruences dans l'anneau $\mathbb{Z}_{(p)}$ des p-entiers. Dans ce chapitre, nous définissons les nombres et polynômes de Bernoulli et étudions certaines de leurs propriétés. Au second chapitre nous étudions le théorème de J. Wolstenholme et quelques unes de ses généralisations et extensions. Au troisième chapitre, nous étudions une généralisation plus fortes des congruences de J. Wolstenholme et de F. Morley dûe à F. Bencherif et R. Boumahdi [7].

Chapitre 1

Généralités

1.1 Introduction

Dans ce chapitre, nous rappelons les principales propriétés de la congruence modulo n dans l'anneau $\mathbb{Z}$, n étant un entier et $n \geq 2$. Nous citons les principaux théorèmes classiques d'arithmétique : théorème de Fermat, d'Euler, de Von-Staudt et Clausen, de Wolstenholme et de Glaisher. Nous précisons ensuite la notion de congruence modulo n entre nombres rationnels. Nous nous intéresserons plus particulièrement au cas où n est un nombre premier (ou une puissance d'un nombre premier). Nous rappelons aussi la définition et quelques propriétés des coefficients binomiaux. Nous définissons les nombres et les polynômes de Bernoulli. Nous prouvons la formule de Faulhaber qui permet d'exprimer la somme des puissances m-ièmes des n premiers entiers à l'aide du $(m+1)$-ième polynôme de Bernoulli. A la fin de ce chapitre, nous présentons les congruences de Kummer concernant les nombres de Bernoulli et certaines de ses généralisations et applications.

1.2 Congruences dans $\mathbb{Z}$

Historiquement, la notion de congruence sur les entiers relatives a été introduite par Gauss vers 1801. Si a et b sont deux entiers et si $n \geq 2$ est un entier, on convient d'écrire :
$a \equiv b \,(\mathrm{mod}\, n)$ si et seulement si $a - b \in n\mathbb{Z}$. On dit alors que les entiers a et b sont congrus modulo n. La relation de congruence modulo n ainsi définie est une relation d'équivalence définie sur l'anneau $\mathbb{Z}$, compatible avec l'addition et la multiplication définies sur $\mathbb{Z}$. Voici maintenant les principaux théorèmes d'arithmétique qui nous seront utiles. Nous commençons par un théorème de Lagrange qui nous permettra de prouver aisément le théorème de Wilson, le petit théorème de Fermat et qui nous fournira d'intéressantes relations sur des sommes d'entiers

1.3 Théorème de Lagrange

Le théorème 1 qui suit va nous être très utile pour prouver un théorème établi par Lagrange en 1768.

Théorème 1 *Pour tout nombre premier p et pour tout $k \in \{1, 2, \ldots, p-1\}$, $p \mid \binom{p}{k}$*

Preuve. Soit $k \in \{1, 2, \ldots, p-1\}$. On a

$$p! = k!\,(p-k)!\binom{p}{k}. \tag{1.1}$$

Nous constatons alors que le nombre premier $p \mid p!$, p divise donc le premier membre de (1.1). On en déduit que p divise le second membre de (1.1). Autrement dit, $p \mid k!\,(p-k)!\binom{p}{k}$. Comme de plus, le nombre premier $p \nmid k!\,(p-k)!$ car $k \in \{1, 2, \ldots, p-1\}$, on a $(p, k!(p-k)!) = 1$. Le théorème bien connu de Gauss permet d'affirmer que $p \mid \binom{p}{k}$. □

Théorème 2 *Soit $p \geq 3$ un nombre premier et $f(x) = (x+1)(x+2)\cdots(x+p-1)$. Alors, dans le développement de $f(x)$*

$$f(x) = x^{p-1} + a_1 x^{p-2} + \cdots + a_{p-2}x + a_{p-1,} \tag{1.2}$$

les coefficients $a_1, a_2, \ldots, a_{p-2}$ sont divisibles par p.

Preuve. On constate que l'on peut écrire

$$(x+p)\,f(x) = (x+1)\,f(x+1),$$

on en déduit que

$$pf(x) = (x+1)\,f(x+1) - xf(x).$$

Autrement dit, en posant $a_0 = 1$, on a

$$\sum_{k=0}^{p-1} pa_k x^{p-1-k} = \sum_{k=0}^{p-1} a_k \left((x+1)^{p-k} - x^{p-k}\right). \tag{1.3}$$

En identifiant les coefficients de x^{p-1-k} dans chacun des deux membres de (1.3), on obtient pour $1 \leq k \leq p-1$

$$pa_k = \binom{p}{k+1} + a_1\binom{p-1}{k} + \cdots + a_{k-1}\binom{p-2}{2} + a_k\binom{p-k}{1}, \tag{1.4}$$

on en déduit que

$$pa_k - a_k\binom{p-k}{1} = \binom{p}{k+1} + a_1\binom{p-1}{k} + \cdots + a_{k-1}\binom{p-2}{2},$$

ainsi, on a

$$ka_k = \binom{p}{k+1} + a_1\binom{p-1}{k} + \cdots + a_{k-1}\binom{p-2}{2}. \tag{1.5}$$

On en déduit que pour $k = 1$

$$a_1 = \binom{p}{2}. \tag{1.6}$$

Comme d'après le théorème 1, $p \mid \binom{p}{k}$ pour $1 \leq k \leq p-1$, on déduit de (1.6) que $p \mid a_1$. On peut alors raisonner par récurrence. En effet, la relation (1.5) montre que si a_1, a_2, ..., a_{k-1} sont divisibles par p, alors il est de même pour a_k, pour $2 \leq k \leq p-2$. La preuve du théorème de Lagrange est complète. □

Remarquons qu'on déduit de ce qui précède que

$$a_{p-1} = (p-1)! \equiv -1 \pmod{p}.$$

Ce résultat nous permet de prouver le célèbre théorème de Wilson suivant

Théorème 3 *Pout tout entier $p \geq 2$, on a l'équivalence suivante*

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

Nous allons maintenant reformuler le théorème 2 d'une autre manière. Pour cela, nous utilisons les polynômes symétriques de $\mathbb{C}[x_1, x_2, ..., x_n]$ suivants. Soit $s \in \mathbb{N}^*$, on peut les définir par

$$P_m := P_m(x_1, x_2, ..., x_s) = x_1^m + x_2^m + + \cdots + x_s^m, \ (m \geq 0), \tag{1.7}$$

$$A_m := A_m(x_1, x_2, ..., x_s) = \sum_{1 \leq i_1 < i_2 < \cdots < i_m \leq s} x_{i_1} x_{i_2} \cdots x_{i_m} \ \ (1 \leq m \leq s) \ \text{ et } A_0 := 1. \tag{1.8}$$

Nous posons

$$G(x) := (x + x_1)(x + x_2) \cdots (x + x_s),$$
$$H(x) := (x - x_1)(x - x_2) \cdots (x - x_s).$$

On a alors les résultats bien connus suivants

$$(x + x_1)(x + x_2) \cdots (x + x_s) = x^n + A_1 x^{n-1} + A_2 x^{n-2} + \cdots + A_n,$$

$$(x - x_1)(x - x_2) \cdots (x - x_s) = x^n - A_1 x^{n-1} + A_2 x^{n-2} + \cdots + (-1)^n A_n.$$

En particulier, on a

$$(x+1)(x+2) \cdots (x + (p-1)) = x^n + a_1 x^{n-1} + a_2 x^{n-2} + \cdots + a_{p-2} x + a_{p-1},$$

avec

$$a_r = A_r(1, 2, ..., p-1) = \sum_{1 \leq i_1 < i_2 < \cdots < i_r \leq p-1} i_1 i_2 \cdots i_r.$$

Le théorème de Lagrange s'énonce donc aussi de la manière suivante

Théorème 4 *Pour tout $p \geq 3$ et tout entier r tel que $1 \leq r \leq p-2$, on a*

$$a_r := \sum_{1 \leq i_1 < i_2 < \cdots < i_r \leq p-1} i_1 i_2 \cdots i_r \equiv 0 \pmod{p}.$$

1.4 Congruences dans $\mathbb{Z}[x]$ et petit théorème de Fermat

Soit $n \geq 2$ un entier On dit que deux polynômes $A(x)$ et $B(x)$ de $\mathbb{Z}[x]$ sont congrus modulo n et on écrit alors $A(x) \equiv B(x) \pmod{n}$ si et seulement si le polynôme $A(x) - B(x) \in n\mathbb{Z}[x]$. Ainsi, si $A(x) = \sum_{k=0}^{m} a_k x^k$, on a $A(x) \equiv 0 \pmod{n}$ si et seulement si $a_k \equiv 0 \pmod{n}$ pour tout k compris entre 0 et m. On vérifie que la relation de congruence ainsi définie sur l'anneau $\mathbb{Z}[x]$ est une relation d'équivalence compatible avec l'addition et la multiplication des polynômes. Remarquons aussi que si deux polynômes $A(x)$ et $B(x)$ de $\mathbb{Z}[x]$ sont congrus modulo n, alors pour tout entier $a \in \mathbb{Z}$, les entiers $A(a)$ et $B(a)$ sont aussi congrus modulo n. Grâce à cette définition, on peut déduire des théorème de Lagrange et de Wilson les résultats suivants

Théorème 5 *Pour tout nombre premier p, on a la congruence suivante entre polynômes de $\mathbb{Z}[x]$*

$$(x-1)(x-2)\cdots(x-(p-1)) \equiv x^{p-1} - 1 \pmod{p}.$$

Preuve. Pour $p = 2$, le résulat est immédait et pour $p \geq 3$, il traduit les théorèmes de Lagrange et Wilson. □

Le petit théorème de Fermat qui suit est un corollaire immédait au théorème 5

Théorème 6 *Pour tout nombre premier p et tout entier a premier avec p, on a*

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

Preuve. Soit a un entier premier avec p. Alors $a \equiv r \pmod{p}$ avec $r \in \{1, 2, \ldots, p-1\}$. On a donc

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

or d'après le théorème 5, on a $r^{p-1} - 1 \equiv 0 \pmod{p}$, il en résulte qu'on a bien $a^{p-1} \equiv 1 \pmod{p}$. □

Remarquons qu'on peut aussi énoncer le petit théorème de Fermat sous la forme équivalente suivante

Théorème 7 *Pour tout nombre p et pour tout entier a, on a*

$$a^p \equiv a \pmod{p}.$$

Le théorème d'Euler que nous prouvons au paragraphe suivant est une généralisation du petit théoème de Fermat.

1.5 Fonction indicatrice φ d'Euler et théorème d'Euler

1.5.1 Fonction indicatrice φ d'Euler

On appelle fonction arithmétique toute fonction définie sur l'ensemble des entiers naturels non nuls $\mathbb{N}^*$ à valeurs dans l'ensemble des nombres complexes $\mathbb{C}$. La fonction indicatrice d'Euler que l'on note φ, est une fonction arithmétique importante. Elle est définie comme suit

$$\varphi(n) = \text{Card}\left\{m \in \mathbb{N}^*/1 \leq m \leq n \text{ et } \text{pgcd}(n,m) = 1\right\}.$$

Notation 8 *Notons par $U(\mathbb{Z}/n\mathbb{Z}), n \in \mathbb{N}$, l'ensemble des éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$.*

Remarque 9 *On dit que $a \in \mathbb{Z}/n\mathbb{Z}$ est inversible si $\exists b \in \mathbb{Z}/n\mathbb{Z}$ tels que : $a \times b = \overline{1}$.*

$$U(\mathbb{Z}/n\mathbb{Z}) = \{\overline{k} \in \mathbb{Z}/n\mathbb{Z} : (k,n) = 1\}$$

Pour tout entier $n \geq 2$, $\varphi(n)$ est égal au nombre d'entiers naturels compris entre 1 et n et premiers avec n. On démontre que

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

On montre que si $\text{pgcd}(n,m) = 1$, alors les anneaux $\mathbb{Z}/nm\mathbb{Z}$ et $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ sont isomorphes. On en déduit que l'on a alors [25]

$$(n,m) = 1 \Longrightarrow \varphi(nm) = \varphi(n)\varphi(m)\cdot$$

On a pour tout nombre premier p et pour tout entier $\alpha \geq 0$, on a

$$\begin{aligned} \varphi(p^\alpha) &= p^\alpha - p^{\alpha-1} \\ &= p^\alpha \left(1 - \frac{1}{p}\right), \end{aligned}$$

il en résulte que l'on a pour tout entier $n \geq 2$

$$\varphi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right),$$

le produit étant étendu à tous les nombres premiers p divisant n.

1.5.2 Théorème d'Euler

Théorème 10 *Pour tout entier $n \geq 2$ et pour tout entier a, tel que $(a, n) = 1$, on a*

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

Preuve. Soit a un entier tel que $(a, n) = 1$. Alors $\overline{a} \in U(\mathbb{Z}/n\mathbb{Z})$. Comme $U(\mathbb{Z}/n\mathbb{Z})$ est un groupe multiplicatif d'ordre $\varphi(n)$, on a

$$\overline{a}^{\varphi(n)} = \overline{1}$$

c'est à dire $a^{\varphi(n)} \equiv 1 \pmod{n}$. □

Soit p un nombre premier. Alors $\varphi(p) = p - 1$. L'application du théorème d'Euler dans le cas particulier où n est un nombre premier p fournit le petit théorème de Fermat.iUne étude de la fonction d'Euler permet de prouver le théorème suivant

Théorème 11 *Pour tout nombre premier p, le groupe multiplicative $U(\mathbb{Z}/p\mathbb{Z}) = (\mathbb{Z}/p\mathbb{Z})^*$ est un groupe cyclique d'ordre $p - 1$·*

Preuve. cf [14]. □

Définition 12 *Soit m et a deux entiers tels que $m \geq 2$ et $(a, m) = 1$. Le plus petit entier $d \geq 1$ tel que $a^d \equiv 1 \pmod{m}$ est appelé ordre de a modulo m. On appelle racine primitive de l'unité modulo m tout entier a premier avec m dont l'ordre est égal à $\varphi(m)$.*

Remarque 13 *Il résulte du théorème 11 et de la définition 12 que pour tout nombre premier p, il existe au moins une racine primitive modulo p, c'est à dire un entier g dont l'ordre est égal à $\varphi(p) = p - 1$. Il suffit pour cela que $\overline{g}$ soit un générateur du groupe cyclique $(\mathbb{Z}/p\mathbb{Z})^*$.*

1.5.3 Formules de Newton

Rappelons qu'on a déjà définit les polynômes symétriques de $\mathbb{C}[x_1, x_2, ..., x_s]$ (1.7) et (1.8), alors on a

Théorème 14 *Pour tout entier naturel non nul n et $s \in \mathbb{N}^*$, on a*

1. *Pour $n \geq s$*

$$P_n - A_1 P_{n-1} + A_2 P_{n-2} + \cdots + (-1)^s A_s P_{n-s} = 0. \tag{1.9}$$

2. Pour $n \leq s$

$$P_n - A_1 P_{n-1} + A_2 P_{n-2} + \cdots + (-1)^{n-1} A_{n-1} P_1 + (-1)^n n A_n = 0. \tag{1.10}$$

Preuve. Considérons le polynôme $Q(x) = (x - x_1)(x - x_2) \cdots (x - x_s)$. On a

$$Q(x) = \prod_{n=1}^{s} (x - x_n) = x^s - A_1 x^{s-1} + A_2 x^{s-2} + \cdots + (-1)^s A_s = \sum_{k=0}^{s} (-1)^k A_k x^{s-k}. \tag{1.11}$$

1. Si $n \geq s$, en multipliant par x_i^{n-s} la relation $Q(x_i) = 0$, on obtient

$$\sum_{k=0}^{s} (-1)^k A_k x_i^{n-k} = 0 \quad \text{pour } i = 1...s. \tag{1.12}$$

En ajoutant membre à membre les relations obtenues en donnant à i les valeurs de 1 à s, dans (1.12), on trouve

$$\sum_{k=0}^{s} (-1)^k A_k P_{n-k} = 0,$$

c'est à dire

$$P_n - A_1 P_{n-1} + A_2 P_{n-2} + \cdots + (-1)^s A_s P_{n-s} = 0.$$

La relation (1.9) est ainsi prouvée.

2. Prouvons maintenant la relation (1.10), remarquons tout d'abord que pour tout $1 \leq \ell \leq s$, on a $Q(x_\ell) = 0$ et que par conséquent, on a

$$\begin{aligned} \frac{Q(x)}{x - x_\ell} &= \frac{Q(x) - Q(x_\ell)}{x - x_\ell} \\ &= \sum_{k=0}^{s} (-1)^k A_k \frac{x^{s-k} - x_\ell^{s-k}}{x - x_\ell}. \end{aligned}$$

En remarquant encore que pour tout entier naturel m, on a

$$\frac{x^m - x_\ell^m}{x - x_\ell} = \sum_{\substack{i+j=m-1 \\ i,j \geq 0}} x^i x_\ell^j,$$

on en déduit que

$$\frac{Q(x)}{x - x_\ell} = \sum_{k=0}^{s} (-1)^k A_k \sum_{\substack{i+j=s-k-1 \\ i,j \geq 0}} x^i x_\ell^j. \tag{1.13}$$

Compte tenu de cette remarque, la dérivée du polynôme $Q(x)$ peut s'exprimer de deux manières. D'une part, avec la règle de dérivation d'un produit, on a

$$Q'(x) = \sum_{\ell=0}^{s} \frac{Q(x)}{x - x_\ell}.$$

Compte tenu des relations (1.13) et (1.7), on a alors

$$Q'(x) = \sum_{k=0}^{s}(-1)^k A_k \sum_{\substack{i+j=s-k-1 \\ i,j\geq 0}} x^i P_j. \tag{1.14}$$

D'autre part, en dérivant l'expression développée (1.11) de $Q(x)$, on obtient

$$Q'(x) = \sum_{\ell=0}^{s-1}(-1)^\ell (s-\ell)x^{s-1-\ell}A_\ell. \tag{1.15}$$

En égalant les deux expressions $Q'(x)$ obtenues (1.14) et (1.15), on obtient

$$\sum_{k=0}^{s}(-1)^k A_k \sum_{\substack{i+j=s-k-1 \\ i,j\geq 0}} x^i P_j = \sum_{\ell=0}^{s-1}(-1)^\ell (s-\ell)x^{s-1-\ell}A_\ell. \tag{1.16}$$

En égalant les coefficients de x^{s-1-n} dans chacun des deux membres de (1.16), on obtient

$$\sum_{k=0}^{n}(-1)^k A_k P_{n-k} = (-1)^n (s-n)A_n.$$

Comme on a $P_0 = s$, on en déduit que

$$(-1)^n sA_n + P_n + \sum_{\ell=1}^{n-1}(-1)^\ell A_l P_{n-\ell} = (-1)^n (s-n)A_n.$$

Ainsi $P_n - A_1P_{n-1} + A_2P_{n-2} + \cdots + (-1)^n nA_n = 0$.La relation (1.10) est ainsi prouvée.

□

1.5.4 Congruences dans le groupe $\mathbb{Q}$ et dans l'anneau $\mathbb{Z}_{(p)}$

Tout nombre rationnel x s'écrit de manière unique $x = \frac{u}{v}$ avec $(u, v) \in \mathbb{Z}\times\mathbb{N}^*$ et $\text{pgcd}(u, v) = 1$. Cette écriture unique est appelée forme réduite de x, u et v sont respectivement le numérateur et le dénominateur de x. Nous notons

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

Pour tout entier $n \geq 2$, nous dirons que deux nombres rationnels x et y sont congrus modulo n et nous écrirons alors " $x \equiv y \pmod n$" si et seulement si le numérateur de $x - y$ est divisible par n (dans $\mathbb{Z}$). Ainsi

$$x \equiv y \pmod n \iff \text{num}(x-y) \in n\mathbb{Z}. \tag{1.17}$$

Il est facile de constater que la relation de congruence modulo n définie sur $\mathbb{Q}$ prolonge à $\mathbb{Q}$ la relation de congruence définie sur $\mathbb{Z}$. En effet, si x et y sont entiers, alors $\text{num}(x-y) = x-y$ et la relation (1.17) définie dans $\mathbb{Q}$ est exactement la défintion de la congruence modulo n définie dans $\mathbb{Z}$. De plus la relation de congruence modulo n définie dans $\mathbb{Q}$ est une relation d'équivalence compatible avec l'addition du groupe $\mathbb{Q}$, mais non compatible avec la multiplication définie sur $\mathbb{Q}$. Nous allons maintenant examiner quelques propriétés des congruences modulo n définies dans $\mathbb{Q}$.

Désignons par $\mathbb{Z}_{(n)}$ l'ensemble des nombres rationnels dont le dénominateur est premier avec n. Autrement dit

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

Un élément de $\mathbb{Z}_{(n)}$ est appelé un n- entier. Remarquons que $\mathbb{Z} \subset \mathbb{Z}_{(n)} \subset \mathbb{Q}$. De plus si $\{q_1, q_2, ..., q_r\}$ désigne l'ensemble des diviseurs premiers de n, alors $\mathbb{Z}_{(n)} = \mathbb{Z}_{(q_1 q_2 ... q_r)}$. Remarquons aussi que pour qu'un nombre rationnel x soit un élément de $\mathbb{Z}_{(n)}$, il faut et il suffit qu'il puisse s'écrire comme le quotient de deux entiers p et q, $x = \frac{p}{q}$, q étant un entier premier avec n, $\frac{p}{q}$ n'étant pas nécessairement la forme réduite de x. Cette dernière remarque permet de prouver aisément que $\mathbb{Z}_{(n)}$ est un sous anneau de $\mathbb{Q}$. Il est aussi facile de constater que le groupe des unités de cet anneau est

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

Dans le cas où $n = p^m$, p étant un nombre premier et m un entier naturel non nul, on a

$$\mathbb{Z}_{(p^m)} = \mathbb{Z}_{(p)},$$

$$\mathbb{Z}_{(p^m)} = \{x \in \mathbb{Q}/ \ p \nmid \text{denom}(x)\},$$
$$U(\mathbb{Z}_{(p^m)}) = \{x \in \mathbb{Q}/ \quad p \nmid \text{num}(x) \text{ et } \ p \nmid \text{denom}(x)\}.$$

1.5.5 Congruences pour les sommes de puissances $\sum_{k=1}^{p-1} k^m$, $m \in \mathbb{Z}$

Dans tout ce qui suit, p désigne un nombre premier. L'étude des sommes de Newton nous permet d'obtenir aisément le résulat suivant

Théorème 15 *Pour tout nombre premier p et pour tout entier $r \in \{0, 1, 2, \ldots, p-2\}$, on a*

$$\sum_{k=1}^{p-1} k^r \equiv \begin{cases} -1 \pmod p & \text{si } r = p-1 \\ 0 \pmod p & \text{si } 1 \leq r \leq p-2 \end{cases}$$

Preuve. Si $r = 0$, le résulat est immédiat.

Si $1 \leq r \leq p-2$, alors avec $s = p-1$ et $x_k = k$, les expressions (1.7) et (1.8)) deviennent.

$$\begin{aligned} P_m &= 1^m + 2^m + + \cdots + (p-1)^m, \ (m \geq 0), \\ A_m &= a_m = \sum_{1 \leq i_1 < i_2 < \cdots < i_m \leq p-1} i_1 i_2 \cdots i_m \ \ (1 \leq m \leq p-1) \end{aligned}$$

la formule de Newton (1.10) s'écrit

$$P_n - a_1 P_{n-1} + a_2 P_{n-2} + \cdots (-1)^{n-1} a_{n-1} P_1 + (-1)^n n a_n = 0 \quad \text{pour } n \leq p-1. \tag{1.18}$$

Le théorème 4 affirme que pour tout $p \geq 3$ et tout entier r tel que $1 \leq r \leq p-2$, on a

$$a_r := \sum_{1 \leq i_1 < i_2 < \cdots < i_r \leq p-1} i_1 i_2 \cdots i_r \equiv 0 \pmod{p}. \tag{1.19}$$

On déduit de (1.18) et (1.19) que si $r \in \{1, 2, ...p-2\}$, alors

$$\sum_{k=1}^{p-1} k^m \equiv P_r \equiv 0 \pmod{p}.$$

Le théorème 15 admet la généralisation suivante □

Théorème 16 *Soit p un nombre premier et $m \in \mathbb{Z}$, on a*

$$\sum_{k=1}^{p-1} k^m \equiv \begin{cases} -1 \pmod{p} & \textit{si } p-1 \mid m, \\ 0 \pmod{p} & \textit{si } p-1 \nmid m. \end{cases} \tag{1.20}$$

Preuve. Soit $m \in \mathbb{Z}$. La division euclidienne de m par $p-1$ s'écrit

$$m = q(p-1) + r \quad \text{avec} \ \ r \in \{0, 1, 2, ...p-2\}.$$

On a alors, pour $1 \leq k \leq p-1$, k est un p-entier, et on a d'après le petit théorème de Fermat

$$k^m = \left(k^{p-1}\right)^q k^r \equiv k^r \pmod{p}.$$

Il en résulte que

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

L'application du théorème (15) permet de conclure. □

Nous pouvons déduire du théorème 16 un corollaire qui nous sera untile pour prouver d'autres résultats dont le théorème de Wolstenholme.

Corollaire 17 *Pour tout nombre premier $p \geq 5$, on a*

$$\sum_{k=1}^{p-1} \frac{1}{k^2} \equiv 0 \pmod{p}, \tag{1.21}$$

$$\sum_{k=1}^{p-1} \frac{1}{k} \equiv 0 \pmod{p^2}, \tag{1.22}$$

$$\sum_{1 \leq k < \ell \leq p-1} \frac{1}{k\ell} \equiv 0 \pmod{p}. \tag{1.23}$$

Preuve. Soit $p \geq 5$ un nombre premier, en appliquant le théorème 16, on a

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

pourvu que le nombre $p-1 \nmid (-2)$, ce qui est vérifiée pour $p \geq 5$. La relation (1.21) est établie.

Prouvons (1.22). On a pour $p \geq 5$ et en exploitant la relation (1.21) qu'on vient de prouver

$$\begin{aligned}
\sum_{k=1}^{p-1} \frac{1}{k} &= \frac{1}{2} \sum_{k=1}^{p-1} \left(\frac{1}{k} + \frac{1}{p-k} \right) \\
&= \frac{p}{2} \sum_{k=1}^{p-1} \frac{1}{k(p-k)} \\
&\equiv -\frac{p}{2} \sum_{k=1}^{p-1} \frac{1}{k^2} \\
&\equiv 0 \pmod{p^2}.
\end{aligned}$$

La relation (1.22) est ainsi prouvée. Signalons que cette relation (1.22) a été prouvée par Wolstenholme en 1862 [35].

Enfin, en remarquant que pour $p \geq 5$, on a

$$\begin{aligned}
\sum_{1 \leq k < \ell \leq p-1} \frac{1}{k\ell} &= \frac{1}{2} \left(\sum_{k=1}^{p-1} \frac{1}{k} \right)^2 - \frac{1}{2} \sum_{k=1}^{p-1} \frac{1}{k^2} \\
&\equiv 0 \pmod{p}.
\end{aligned}$$

on en déduit que

$$\sum_{1 \leq k < \ell \leq p-1} \frac{1}{k\ell} \equiv 0 \pmod{p}.$$

□

Remarque 18 *Remarquons que si $h \in \mathbb{N}^*$, on a, d'après le théorème d'Euler*

$$k^{\varphi(p^h)} \equiv 1 \pmod{p^h}, \text{ avec } \varphi(p^h) = p^{h-1}(p-1).$$

On en déduit que pour $n \in \mathbb{N}$

$$\frac{1}{k^n} \equiv k^{\varphi(p^h)-n} \pmod{p^h}, \text{ où } \varphi(p^h) = p^{h-1}(p-1).$$

Par suite

$$\sum_{k=1}^{p-1} \frac{1}{k^n} \equiv \sum_{k=1}^{p-1} k^{\varphi(p^h)-n} \pmod{p^h}. \tag{1.24}$$

1.6 Les nombres et polynômes de Bernoulli

C'est à Jacques Bernoulli qu'on doit l'introduction d'une suite de nombres rationnels qu'Abraham de Moivre a désigné par "nombres de Bernoulli". Ces nombres ont été introduit par Jacques Bernoulli pour pouvoir écrire une formule générale exprimant la somme,

$\sum_{k=0}^{n-1} k^m = 0^m + 1^m + \cdots + (n-1)^m$ comme un polynôme en n. Cette formule que nous établirons dans ce chapitre porte aujourd'hui de nom de formule de Faulhaber.

1.6.1 Les nombres de Bernoulli

Définition 19 *[5] On appelle suite des nombres de Bernoulli la suite $(B_n)_{n\in\mathbb{N}}$ des nombres rationnels définie par la relation de récurrence suivante*

$$B_0 = 1 \text{ et } B_n = -\frac{1}{n+1}\sum_{k=0}^{n-1}\binom{n+1}{k}B_k \text{ pour } n \geq 1. \tag{1.25}$$

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

On montre facilement que la définition précédente est équivalente à définir la suite $(B_n)_{n\in\mathbb{N}}$ des nombres de Bernoulli par la realtion suivante dans l'anneau $\mathbb{C}[z]$

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

Les premiers valeurs des nombres de Bernoulli de $n = 1$ a $n = 14$ sont

n	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
B_n	1	$-\frac{1}{2}$	$\frac{1}{6}$	0	$-\frac{1}{30}$	0	$\frac{1}{42}$	0	$-\frac{1}{30}$	0	$\frac{5}{66}$	0	$-\frac{691}{2730}$	0	$\frac{7}{6}$

Théorème 20 *Pour tout entier $n \geq 1$, on a $B_{2n+1} = 0$.*

Preuve. Il suffit de remarquer que la série formelle de la fonction suivante $\frac{z}{e^z-1}+\frac{1}{2}z = \frac{z}{2\tanh(\frac{z}{2})}$ est paire. □

1.6.2 Les polynômes de Bernoulli

Définition 21 *[6] La suite des polynômes de Bernoulli, notée $(B_n(x))_{n\in\mathbb{N}}$, est définie par la relation*

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

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

Théorème 22 *Pour tout entier naturel n, on a*

$$B_n(x) = \sum_{k=0}^{n} \binom{n}{k} B_k x^{n-k}. \tag{1.26}$$

Preuve. En effet, d'après le produit de Cauchy de deux séries entières, on a

$$\sum_{n=0}^{\infty} \frac{B_n(x)}{n!} z^n = \left(\sum_{n=0}^{\infty} \frac{B_n}{n!} z^n\right)\left(\sum_{n=0}^{\infty} \frac{x^n}{n!} z^n\right), \tag{1.27}$$

en identifiant le coefficient de z^n dans chacun des deux membres de (1.27), on obtient

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

ce qui permet d'obtenir la relation (1.26). Les premières valeurs des polynômes de Bernoulli sont

n	$B_n(x)$
0	1
1	$x-\frac{1}{2}$
2	$x^2-x+\frac{1}{6}$
3	$x^3-\frac{3}{2}x^2+\frac{1}{2}x$
4	$x^4-2x^3+x^2-\frac{1}{30}$
5	$x^5-\frac{5}{2}x^3+\frac{5}{3}x^3-\frac{1}{6}x$
6	$x^6-3x^5+\frac{5}{2}x^4-\frac{1}{2}x^2+\frac{1}{42}$

□

Théorème 23 *On a, pour tout nombre entier positif n où $n \geqslant 1$*

$$B_n(x+1) - B_n(x) = nx^{n-1}. \tag{1.28}$$

Preuve. On a

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

Ainsi, on a

$$\sum_{n=0}^{\infty} \frac{B_n(x+1) - B_n(x)}{n!} z^n = \sum_{n=0}^{\infty} \frac{nx^{n-1}}{n!} z^n. \tag{1.29}$$

On obtient ainsi la relation recherchée en identifiant les coefficients de z^n dans chacun des deux membres de (1.29). □

1.6.3 La formule de Faulhaber

La formule de Faulhaber, nommée en l'honneur de Johann Faulhaber (1580-1635) exprime la somme $P_m(n) = \sum_{k=1}^{n} k^m$ où $n, m \in \mathbb{N}$ à l'aide d'un polynôme en n de degré $m+1$. Faulhaber ne connaissait pas la formule sous la forme que nous connaissons aujourd'hui mais il connaissait des expressions de $P_m(n)$ pour $1 \leq m \leq 17$. Jacques Bernoulli, dans son Academia Algebrae, publié en 1631 donne les coefficients de ce polynôme.

Commençons par la première application historique, la relation de la formule de Faulhaber avec les nombres de Bernoulli.

Théorème 24 *[8](formule de **Faulhaber**) Pour tout entiers $n \geq 1$ et $m \geq 0$, on a*

$$\sum_{k=1}^{n-1} k^m = \frac{1}{m+1} \sum_{k=0}^{m} \binom{m+1}{k} B_k n^{m+1-k}. \tag{1.30}$$

Preuve. En exploitant les formules (1.28) et (1.26), on obtient

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

□

Remarque 25 *On utilise le fait que*

$$\binom{m+1}{k} = \frac{m+1}{m-k+1}\binom{m}{k}$$

la relation (1.30) devient

$$P_m(n-1) = \sum_{k=0}^{m} \binom{m}{k} B_k \frac{n^{m+1-k}}{m-k+1}.$$

Maintenant, on utilise aussi le fait que $\binom{m}{k} = \binom{m}{m-k}$, nous obtenons

$$\begin{aligned}
\sum_{k=1}^{n} k^m &= \sum_{k=0}^{m} \binom{m}{k} B_{m-k} \frac{n^{k+1}}{k+1} \\
&= \sum_{k=0}^{m} \binom{m}{k} B_{m-k} \frac{n^{k+1}}{k+1} \\
&= \sum_{r=1}^{m+1} \frac{1}{r}\binom{m}{r-1} B_{m-r+1} n^r,
\end{aligned}$$

donc on a

$$\sum_{k=1}^{n} k^m = \sum_{r=1}^{m+1} \frac{1}{r}\binom{m}{r-1} B_{m-r+1} n^r. \tag{1.31}$$

1.6.4 Théorème de Von-Staudt et Clausen

Introduction

En 1840, Karl Georg Von Staudt [27] et Thomas Clausen [9] découvrent indépendamment l'un de l'autre une remarquable propriété des nombres de Bernoulli. Cette propriété est aujourd'hui appelée théorème de **Von-Staudt et Clausen.**

Théorème 26 *[17] Théorème de* ***Von-Staudt et Clausen*** *(1840) : pour tout entier pair n où $n \geq 2$ et p un nombre premier on a*

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

Corollaire 27 *[17] Pour tout entier positif n et p un nombre premier on a $pB_n \in \mathbb{Z}_{(p)}$, et si $p-1 \nmid n$ on a*

$$B_{2n} \in \mathbb{Z}_{(p)} \quad et \quad \frac{B_{2n}}{2n} \in \mathbb{Z}_{(p)}.$$

Le dénominateur du nombre B_{2n}

Les nombres de Bernoulli sont des nombres rationnels i.e. $B_{2n} = \frac{N_n}{D_n}$

Les numérateurs N_n ont un rôle important dans la théorie des nombres en grande partie grâce à leur connexion avec le dernier théorème de Fermat.

Les dénominateurs D_n ont joué un rôle moins important en mathématique même si elles peuvent être décrites clairement. Von Staudt et Clausen stipulent que D_n est le produit de tous les nombres premiers p avec $p-1 \mid n$, où n est pair.

Une conséquence intéressante est que D_n est sans carré pour tout n.

Corollaire 28 *Pour tout entier pair n, $n \geq 2$ on a*

$$\operatorname{denom}(B_{2n}) = \prod_{p-1 \mid 2n} p. \tag{1.32}$$

Preuve. C'est une conséquence de théorème de **Von-Staudt et Clausen**
Soient $p_1, p_2, \ldots, p_m$ les nombres premiers tels que pour tout $i = 1, 2, \ldots, m$ on a $p_i - 1 \mid 2n$.

$B_{2n} + \sum_{p-1 \mid 2n} \frac{1}{p} \in \mathbb{Z}$ alors il existe un $N \in \mathbb{Z}$ tel que : $B_{2n} + \sum_{p-1 \mid 2n} \frac{1}{p} = N$

On remarque alors que

$$\begin{aligned} B_{2n} &= N - \sum_{p-1 \mid 2n} \frac{1}{p}, \quad \text{où } N \in \mathbb{Z} \\ &= N - \left(\frac{1}{p_1} + \frac{1}{p_2} + \cdots + \frac{1}{P_m}\right) \\ &= \frac{p_1 p_2 \cdots p_m N - \sum_{i=1}^{m} \prod_{j=1, j\neq i}^{m} p_j}{p_1 p_2 \cdots p_m} \\ &= \frac{M}{p_1 p_2 \cdots p_m}. \end{aligned}$$

Comme $(M, p_i) = 1$ on obtient

$$\operatorname{denom}(B_n) = p_1 p_2 \cdots p_m.$$

Ceci complète la preuve. □

1.6.5 Théorème de Kummer

Les congruences de Kummer décrivent les propriétés arithmétiques les plus importantes des nombres de Bernoulli qui donnent une relation modulaire entre ces nombres.

Théorème 29 *[15] Page 239. Pour tout nombre premier impair p et tout nombre entier pair $m \geq 2$ où $p - 1 \nmid m$, on définit $C_m = (1 - p^{m-1})B_m/m$. Si $m \equiv m'(\operatorname{mod} \varphi(p^n))$, $n \in \mathbb{N}^*$, alors*

$$C_m \equiv C_{m'}(\operatorname{mod} p^n)$$

Preuve. cf [15] □

Corollaire 30 *Soient p un nombre premier impair, m, m' et n sont des entiers tels que m, m' sont pairs, $n \leq m' - 1 \leq m - 1$ et $p - 1 \nmid m$. Si $m \equiv m'(\operatorname{mod} \varphi(p^n))$, où*

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

Alors

$$\frac{B_m}{m} \equiv \frac{B_{m'}}{m'}(\operatorname{mod} p^n). \tag{1.33}$$

Preuve. On utilise le fait que $p^{m-1} \equiv p^{m'-1} \equiv 0(\operatorname{mod} p^n)$ (car $n \leq m' - 1 \leq m - 1$) dans le théorème 29. □

1.6.6 Généralisation du théorème de Kummer

Théorème 31 *[30] p.193. Pour tout nombre premier impair p et tout nombre entier pair b où $p-1 \nmid b$ on a*

$$\frac{B_{k(p-1)+b}}{k(p-1)+b} \equiv k\frac{B_{p-1+b}}{p-1+b} - (k-1)\left(1-p^{b-1}\right)\frac{B_b}{b} \pmod{p^2} \quad \textit{pour } k \in \mathbb{N}^*. \tag{1.34}$$

1.6.7 Application du théorème de Kummer

Lemme 32 *On a pour tout nombre premier p*

$$pB_{\varphi(p^3)-k} \equiv \begin{cases} kp\left(\frac{B_{2p-2-k}}{2p-2-k} - 2\frac{B_{p-1-k}}{p-1-k}\right) \pmod{p^3} & \textit{si } \ k < p-3, \\ (p-3)\,p\left(\frac{B_{p+1}}{p+1} - 2(1-p)\frac{B_2}{2}\right) \pmod{p^3} & \textit{si } \ k = p-3. \end{cases} \tag{1.35}$$

Preuve. On a d'après la formule (1.34) du théorème généralisé de Kummer 31 si on remplace k par p^2-1 et b par $p-1-k$ on obtient

$$\begin{aligned} \frac{B_{\varphi(p^3)-k}}{\varphi(p^3)-k} &= \frac{B_{p^2(p-1)-k}}{p^2(p-1)-k} = \frac{B_{(p^2-1)(p-1)+p-1-k}}{(p^2-1)(p-1)+p-1-k} \\ &\equiv \left(p^2-1\right)\frac{B_{2p-2-k}}{2p-2-k} - \left(p^2-2\right)\left(1-p^{p-2-k}\right)\frac{B_{p-1-k}}{p-1-k} \\ &\equiv -\frac{B_{2p-2-k}}{2p-2-k} + 2\left(1-p^{p-2-k}\right)\frac{B_{p-1-k}}{p-1-k} \pmod{p^2}, \end{aligned}$$

donc on a deux cas
si $p-2-k \geq 2$ c'est à dire, $k < p-3$ on a

$$B_{\varphi(p^3)-k} \equiv -k\left(-\frac{B_{2p-2-k}}{2p-2-k} + 2\frac{B_{p-1-k}}{p-1-k}\right) \pmod{p^2} \quad \text{car } p^{p-2-k} \equiv 0 \pmod{p^2}, \tag{1.36}$$

et si $k = p-3$ on a

$$B_{\varphi(p^3)-k} \equiv (p-3)\left(\frac{B_{p+1}}{p+1} - 2(1-p)\frac{B_2}{2}\right) \pmod{p^2}. \tag{1.37}$$

En multipliant les deux nombres des formules (1.36) et (1.37) par p on obtient

$$pB_{\varphi(p^3)-k} \equiv \begin{cases} kp\left(\frac{B_{2p-2-k}}{2p-2-k} - 2\frac{B_{p-1-k}}{p-1-k}\right) \pmod{p^3} & \text{si } \ k < p-3, \\ (p-3)\,p\left(\frac{B_{p+1}}{p+1} - 2(1-p)\frac{B_2}{2}\right) \pmod{p^3} & \text{si } \ k = p-3. \end{cases}$$

□

Chapitre 2

Congruences de Wostenholme et de Morley

2.1 Introduction :

Dans tout ce chapitre p désigne un nombre premier.

En 1819, C.Babbage [2] prouva que

$$\left(\begin{array}{c} 2p-1 \\ p-1 \end{array} \right) \equiv 1(\mathrm{mod}\, p^2) \quad (p \geq 3).$$

En 1862 ; J. Wolstenholme (1829-1891) améliora ce résultat en prouvant que :

$$\left(\begin{array}{c} 2p-1 \\ p-1 \end{array} \right) \equiv 1(\mathrm{mod}\, p^3) \quad (p \geq 5).$$

En 1895, F. Morley [1] prouva sa congruence célèbre, pour tout $p \geq 5$

$$(-1)^{\frac{p-1}{2}} \binom{p-1}{\frac{p-1}{2}} \equiv 4^{p-1} \ (\mathrm{mod}\, p^3), \tag{2.1}$$

Dans ce qui suit dans ce mémoire nous nous intéréssons à des généralisations et extensions de ces deux dernières congruences depuis 1862 jusqu'à nos jours.

2.2 Congruence de Wolstenholme et de Morley

2.2.1 Théorème de Wostenholme

Théorème 33 *pour tout $p \geq 5$ on a cette congruence :*

$$\left(\begin{array}{c} 2p-1 \\ p-1 \end{array} \right) \equiv 1 (\mathrm{mod}\, p^3) \tag{2.2}$$

Preuve. On sait que :

$$\left(\begin{array}{c} 2p-1 \\ p-1 \end{array} \right) = (-1)^{p-1} \frac{(1-2p)(2-2p)...((p-1)-2p)}{1.2...(p-1)} = \prod_{i=1}^{p-1} (1 - \tfrac{2p}{i})$$

$$\equiv 1 - 2p \sum_{1 \leq k \leq l \leq p-1} \tfrac{1}{k} + 4p^2 \left(\sum_{1 \leq k \leq l \leq p-1} \tfrac{1}{kl} \right) \pmod{p^3}$$

En utilisant les relations (1.22) et (1.23) pour terminer la preuve de (2.2), alors :

$$\left(\begin{array}{c} 2p-1 \\ p-1 \end{array} \right) \equiv 1 (\mathrm{mod}\, p^3)$$

□

En 1900 ; **Glaisher** généralisa le théorème de Wolstenholme comme suit :

2.2.2 Théorème de Glaisher

Théorème 34 *Pour tout nombre premier $p \geq 5$ et tout entier $n \geq 1$ on a :*

$$\binom{np-1}{p-1} \equiv 1 \left(\mathrm{mod}\, p^3\right) \tag{2.3}$$

Le lemme suivant nous sera utile pour prouver le théorème de Glaisher.

Lemme 35 *Pour tout nombre premier p, pour tout entier $k \epsilon \{1, 2, ..., p\}$ et pour tout entier $n \geq 1$ on a :*

$$\binom{np-1}{k-1} \equiv (-1)^{k-1} \left(1 - np \sum_{i=1}^{k-1} \frac{1}{i} + n^2 p^2 \sum_{1 \leq i \leq j \leq k-1} \frac{1}{ij} \right) (\mathrm{mod}\, p^3)$$

Preuve. En posant pour $r \epsilon \{1, 2, ..., k-1\}$

$$A_r = A_r\left(\frac{1}{1}, \frac{1}{2}, ..., \frac{1}{k-1}\right) = \sum_{1\leq i_1<i_2<...<i_r\leq k-1} \frac{1}{i_1 i_2 ... i_r},$$

en remarquant que les A_r sont alors des p-entiers, donc :

$$\begin{aligned}
\binom{np-1}{k-1} &= \frac{(np-1)(np-2)...(np-j)...(np-(k-1))}{1.2...j...(k-1)} \\
&= \left(\frac{np}{1}-1\right)\left(\frac{np}{2}-1\right)...\left(\frac{np}{j}-1\right)...\left(\frac{np}{k-1}-1\right) \\
&= (-1)^{k-1}\left(1-\frac{np}{1}\right)\left(1-\frac{np}{2}\right)...\left(1-\frac{np}{j}\right)...\left(1-\frac{np}{k-1}\right) \\
&= (-1)^{k-1}\left(1-npA_1+n^2p^2A_2+...+(-1)^{k-1}(np)^{k-1}A_n\right) \\
&= (-1)^{k-1}(1-np\sum_{i-1}^{k-1}\frac{1}{i}+n^2p^2\sum_{1\leq i<j\leq k-1}\frac{1}{ij})(\mathrm{mod}\, p^3)
\end{aligned}$$

□

Preuve du théorème de Glaisher. Dans le cas où $k = p$ avec $p \geq 5$ et p premier, le lemme précédent implique

$$\begin{aligned}
\binom{np-1}{p-1} &\equiv (-1)^{p-1}\left(1-np\sum_{i=1}^{p-1}\frac{1}{i}+n^2p^2\sum_{1\leq i<j\leq p-1}\frac{1}{ij}\right) \qquad (2.4) \\
&\equiv 1-np\sum_{i=1}^{p-1}\frac{1}{i}+n^2p^2\sum_{1\leq i<j\leq p-1}\frac{1}{ij}(\mathrm{mod}\, p^3)
\end{aligned}$$

Or, on sait d'aprés le corollaire 17 que l'on a $\sum_{i=1}^{p-1}\frac{1}{i} \equiv 0(\mathrm{mod}\, p^2)$ et $\sum_{1\leq i<j\leq p-1}\frac{1}{ij} \equiv p(\mathrm{mod}\, p)$, donc le théorème de Glaisher résulte de *(2.4)* de manière immédiate. □

2.2.3 Théorème de Morley

Théorème 36 *Pour tout nombre premier $p \geq 5$ on a*

$$(-1)^{\frac{p-1}{2}}\binom{p-1}{\frac{p-1}{2}} \equiv 4^{p-1}\ (\mathrm{mod}\, p^3). \qquad (2.5)$$

Le lemme suivant nous sera utile pour la preuve, considérons la notation suivante ;

$$S = \sum_{0<i<p}\frac{1}{i},\ S_a = \sum_{\substack{0<i<p \\ i\equiv a(\mathrm{mod}\, 2)}}\frac{1}{i}\ et\ \ S_{ab} = \sum_{\substack{0<i<j<p \\ i\equiv a\ ,\ j\equiv b(\mathrm{mod}\, 2)}}\frac{1}{ij}$$

Lemme 37 *Soit p un nombre premier impair, on a*

1. $S_0 \equiv -S_1 (\mathrm{mod}\, p^2)$.
2. $S_0^2 \equiv -S_{01} - S_{10} (\mathrm{mod}\, p)$.
3. $S_{00} \equiv S_{11} (\mathrm{mod}\, p)$.
4. $2S_{00} \equiv -S_{01} (\mathrm{mod}\, p)$.

Preuve.

1. D'après la relation (1.22) de Wolstenholme, on obtient

$$S = \sum_{0<i<p} \frac{1}{i} = S_0 + S_1 \equiv 0 \ (\mathrm{mod}\, p^2),$$

alors

$$S_0 \equiv -S_1 \ (\mathrm{mod}\, p^2).$$

2. On a

$$\begin{aligned} S_0^2 &\equiv S_0(-S_1) \equiv \left(\sum_{\substack{0<i<p \\ i\equiv 0 (\mathrm{mod}\, 2)}} \frac{1}{i} \right) \cdot \left(- \sum_{\substack{0<i<p \\ j\equiv 1 (\mathrm{mod}\, 2)}} \frac{1}{i} \right) \\ &\equiv - \sum_{\substack{0< i\ ,\ j\ <p \\ i\equiv 0\ ,\ j\equiv 1 (\mathrm{mod}\, 2)}} \frac{1}{ij} \equiv - \sum_{\substack{0<i<j<p \\ i\equiv 0\ ,\ j\equiv 1 (\mathrm{mod}\, 2)}} \frac{1}{ij} - \sum_{\substack{0<j<i<p \\ i\equiv 0\ ,\ j\equiv 1 (\mathrm{mod}\, 2)}} \frac{1}{ij} \\ &\equiv -S_{01} - S_{10} \ (\mathrm{mod}\, p). \end{aligned}$$

3. On sait que $i \equiv i - p \ (\mathrm{mod}\, p)$, donc

$$\begin{aligned} S_{00} &= \sum_{\substack{0<i<j<p \\ i\equiv 0\ ,\ j\equiv 0 (\mathrm{mod}\, 2)}} \frac{1}{ij} \equiv \sum_{\substack{0<i<j<p \\ i\equiv 0\ ,\ j\equiv 0 (\mathrm{mod}\, 2)}} \frac{1}{(i-p)(j-p)} \\ &\equiv \sum_{\substack{0<i<j<p \\ i\equiv 0\ ,\ j\equiv 0 (\mathrm{mod}\, 2)}} \frac{(-1)(-1)}{(p-i)(p-j)}\ ,\ (\ p-i = k \equiv 1 (\mathrm{mod}\, 2),\ p-j = l \equiv 1 (\mathrm{mod}\, 2)) \\ &\equiv \sum_{\substack{0<k<l<p \\ k\equiv 1\ ,\ l\equiv 1 (\mathrm{mod}\, 2)}} \frac{1}{kl} \equiv S_{11} \ (\mathrm{mod}\, p). \end{aligned}$$

4. on a

$$\begin{aligned} S_{00} &= \sum_{\substack{0<i<j<p \\ i\equiv 0\ ,\ j\equiv 0 (\mathrm{mod}\, 2)}} \frac{1}{ij} \equiv \sum_{\substack{0<i<j<p \\ i\equiv 0\ ,\ j\equiv 0 (\mathrm{mod}\, 2)}} \frac{1}{i(j-p)} \\ &\equiv - \sum_{\substack{0<i<j<p \\ i\equiv 0\ ,\ j\equiv 0 (\mathrm{mod}\, 2)}} \frac{1}{i(p-j)}, \end{aligned}$$

Posons $p-j=k$ donc $k\equiv 1(\mathrm{mod}\,2)$. On a $i<j$ donc $p-i>p-j$, $p-i>k$, alors $p>i+k$.
Ainsi, nous obtenons

$$\begin{aligned} S_{00} &= -\sum_{\substack{0<i<i+k<p\\ i\equiv 0\ ,\ k\equiv 1(\mathrm{mod}\,2)}} \frac{1}{ik} \equiv -\sum_{\substack{0<k<l<p\\ k\equiv 1\ ,\ l\equiv 1(\mathrm{mod}\,2)}} \frac{1}{k(l-k)} \\ &\equiv -\sum_{\substack{0<k<l<p\\ k\equiv 1,\ l\equiv 1(\mathrm{mod}\,2)}} \left(\frac{1}{kl}+\frac{1}{(l-k)l}\right) \\ &\equiv -\sum_{\substack{0<k<l<p\\ k\equiv 1,\ l\equiv 1(\mathrm{mod}\,2)}} \frac{1}{kl} - \sum_{\substack{0<m<l<p\\ m\equiv 0,\ l\equiv 1(\mathrm{mod}\,2)}} \frac{1}{ml} \\ &\equiv -S_{11}-S_{01}(\mathrm{mod}\,p). \end{aligned}$$

□

Remarque 38 *1. Soient a_i, x, des nombres réels, i et n sont des entiers où $1\leq i\leq n$, on a cette relation ;*

$$(1+a_1x)(1+a_2x).....(1+a_nx)=1+A_1x+A_2x^2+...+A_nx^n, \tag{2.6}$$

où ;

$$A_1=\sum_{1\ \leq i\leq\ n} a_i,\ A_2=\sum_{1\ \leq i<j\leq\ n} a_ia_j,\ A_3=\sum_{1\ \leq i<j<k\leq\ n} a_ia_ja_k,...,\ A_n=\prod_{i=1}^{n} a_i.$$

2. Pour i,j deux entiers on a

$$2\sum_{1\leq i<j\leq p-1}\frac{1}{ij}=\left(\sum_{i=1}^{p-1}\frac{1}{i}\right)^2-\sum_{1\leq i\leq p-1}\frac{1}{i^2} \tag{2.7}$$

Preuve du théorème de Morley. On sait que

$$\binom{p}{i}=\frac{p.(p-1).(p-2)...(p-(i-1))}{i.1.2...(i-1)},$$

donc

$$\binom{p}{i}=(-1)^{i-1}.\frac{p}{i}.\left(1-\frac{p}{1}\right).\left(1-\frac{p}{2}\right).\left(1-\frac{p}{3}\right)...\left(1-\frac{p}{i-1}\right).$$

En appliquant la relation (2.6) de la remarque 38, on obtient

$$\binom{p}{i}\equiv(-1)^i\left(-\frac{p}{i}+p^2\sum_{j=1}^{i-1}\frac{1}{ij}\right)\ (\mathrm{mod}\,p^3).$$

Puisque

$$2^p = 2 + \sum_{i=1}^{p-1} \binom{p}{i}, \text{ alors}$$

d'après *1* et *3* du lemme 37 , nous déduisons

$$\begin{aligned} 2^{p-1} &\equiv 1 - \frac{p}{2} \sum_{1\leq i\leq p-1} \frac{(-1)^i}{i} + \frac{p^2}{2} \sum_{1\leq j<i\leq p-1} \frac{(-1)^i}{ij} \\ &\equiv 1 - pS_0 + \frac{p^2}{2}(S_{10} - S_{01}) (\mathrm{mod}\, p^3), \end{aligned}$$

l'application de *2* et *4* du lemme 37, donne

$$\begin{aligned} 4^{p-1} &\equiv 1 - 2pS_0 + p^2(S_{10} - S_{01} + S_0^2) \\ &\equiv 1 - 2pS_0 + 2p^2(-S_{01}) \\ &\equiv 1 - 2pS_0 + 4p^2 S_{00} \ (\mathrm{mod}\, p^3), \end{aligned}$$

par ailleurs

$$\begin{aligned} (-1)^{\frac{p-1}{2}} \binom{p-1}{\frac{p-1}{2}} &= (-1)^{\frac{p-1}{2}} \left(1 - \frac{p}{1}\right)\left(1 - \frac{p}{2}\right) ... \left(1 - \frac{p}{\frac{p-1}{2}}\right) \\ &\equiv 1 - p \sum_{1\leq i\leq \frac{p-1}{2}} \frac{1}{i} + p^2 \sum_{1\leq j<i\leq \frac{p-1}{2}} \frac{1}{ij} (\mathrm{mod}\, p^3), \end{aligned}$$

mais

$$S_{00} = \sum_{\substack{1\ \leq j<i\leq\ p-1 \\ i\equiv 0(\mathrm{mod}\,2) \\ j\equiv 0(\mathrm{mod}\,2)}} \frac{1}{ij} = \sum_{1\ \leq 2J<2I\leq\ p-1} \frac{1}{2I2J} = \frac{1}{4} \sum_{1\ \leq j<i\leq\ \frac{p-1}{2}} \frac{1}{ij} \quad \text{et,}$$

$$S_0 = \sum_{\substack{1\ \leq i\leq\ p-1 \\ i\equiv 0(\mathrm{mod}\,2)}} \frac{1}{i} = \sum_{1\ \leq 2I\leq\ p-1} \frac{1}{2I} = \frac{1}{2} \sum_{1\ \leq i\leq\ \frac{p-1}{2}} \frac{1}{i} \quad \text{alors;}$$

$$\begin{aligned} (-1)^{\frac{p-1}{2}} \binom{p-1}{\frac{p-1}{2}} &\equiv 1 - p \sum_{1\leq i\leq \frac{p-1}{2}} \frac{1}{i} + p^2 \sum_{1\leq j<i\leq \frac{p-1}{2}} \frac{1}{ij} \\ &\equiv 1 - 2pS_0 + 4p^2 S_{00} \ (\mathrm{mod}\, p^3), \end{aligned}$$

nous terminons la preuve, alors

$$(-1)^{\frac{p-1}{2}} \binom{p-1}{\frac{p-1}{2}} \equiv 4^{p-1} \ (\mathrm{mod}\, p^3).$$

□

2.2.4 Certaines extensions

En 1900, J.W.L. Glaisher [17] trouva que pour tout $p \geq 5$ on a

$$\binom{2p-1}{p-1} \equiv 1 + 2p \sum_{k=1}^{p-1} \frac{1}{k} (\mathrm{mod}\, p^4) \tag{2.8}$$

En 1995, R.J. McIntosh [17] établit une généralisation de (2.8) modulo p^5 ; il prouva que si $p \geq 7$ alors

$$\binom{2p-1}{p-1} \equiv 1 - p^2 \sum_{k=1}^{p-1} \frac{1}{k^2} (\mathrm{mod}\, p^5) \tag{2.9}$$

En 2007, J. Zhao [34] trouva une autre congruence modulo p^5 comme suit,

$$\binom{2p-1}{p-1} \equiv 1 + 2p \sum_{k=1}^{p-1} \frac{1}{k} (\mathrm{mod}\, p^5) \tag{2.10}$$

En 2010, R. Tauraso [31] prouva que pour tout $p \geq 5$

$$\binom{2p-1}{p-1} \equiv 1 + 2p \sum_{k=1}^{p-1} \frac{1}{k} + \frac{2p^3}{3} \sum_{k=1}^{p-1} \frac{1}{k^3} (\mathrm{mod}\, p^6), \tag{2.11}$$

aussi on peut ecrire (2.11) comme suit [20]

$$\binom{2p-1}{p-1} \equiv 1 - 2p \sum_{k=1}^{p-1} \frac{1}{k} - 2p^2 \sum_{k=1}^{p-1} \frac{1}{k^2} (\mathrm{mod}\, p^6) \tag{2.12}$$

En 2014 ; R. Meštrovi´c [20] a amélioré (2.12) avec une méthode claire, il prouva que pour tout

$p \geq 11$ on a :

$$\binom{2p-1}{p-1} \equiv 1 - 2p \sum_{k=1}^{p-1} \frac{1}{k} + 4p^2 \sum_{1 \leq i < j \leq p-1} \frac{1}{ij} (\mathrm{mod}\, p^7). \tag{2.13}$$

Dans ce qui suit, nous expliquons particulièrement cette méthode et donnons plusieurs congruences de Wolstenholme modulo p^k où $k \epsilon \{5, 6, 7\}$ concernant des nombres de Bernoulli.

2.3 Extension de la congruence de Wolstenholme modulo p^7

Posons

$$R_n(p)=\sum_{i=1}^{p-1}\frac{1}{i^n},\ \text{et}\ H_n(p)=\sum_{1\leq i_1<i_2<i_3\ldots<i_n\leq p-1}\frac{1}{i_1i_2i_3\ldots i_n}.$$

Si pas de confusion, on écrit R_n et H_n.

Lemme 39 *[17] Pour tout premier $p\geq 5$ et $n\in\mathbb{N}^*$ où $n\leq p-3$, on a*

$$R_n\equiv\begin{cases}0\pmod p & si\ 2\mid n,\\ 0\pmod{p^2} & si\ 2\nmid n.\end{cases}\tag{2.14}$$

Lemme 40 *Pour tout premier $p\geq 7$, on a*

$$H_3\equiv\frac{R_3}{3}-\frac{R_1R_2}{2}(\mathrm{mod}\,p^6)\tag{2.15}$$

$$H_4\equiv-\frac{R_4}{4}+\frac{R_2^2}{8}(\mathrm{mod}\,p^4)\tag{2.16}$$

En particulier, $p^2|H_3$,$p|H_2$ et $p|H_4$.

Preuve. On sait que

$$3H_3=R_3-R_1R_2+H_2R_1,\ \text{où}\ H_2=(R_1^2-R_2)/2,$$

donc

$$3H_3=R_3-R_1R_2+\frac{R_1^3}{2}-\frac{R_1R_2}{2}=R_3-\frac{3R_1R_2}{2}+\frac{R_1^3}{2},$$

Alors

$$H_3=\frac{R_3}{3}-\frac{R_1R_2}{2}+\frac{R_1^3}{6}\equiv\frac{R_3}{3}-\frac{R_1R_2}{2}(\mathrm{mod}\,p^6),$$

ainsi, $p^2|H_3$.

De même, par la formule de Newton (2.21),on a

$$4H_4=-R_4+H_1R_3-H_2R_2+H_3R_1.$$

Par ailleurs, par le lemme 39, $p^4|R_1R_3=H_1R_3$ (car $R_1=H_1$), et puisque $p^2|H_3$ on a aussi $p^4|H_3R_1$,

par suite

$$\begin{aligned} 4H_4 &= -R_4 + H_1R_3 - H_2R_2 + H_3R_1 \\ &\equiv -R_4 - H_2R_2 \\ &\equiv -R_4 - \frac{R_2R_1^2}{2} + \frac{R_2^2}{2} (\mathrm{mod}\, p^4), \end{aligned}$$

puisque, par le lemme 39, $p^5 | R_2R_1^2$, alors on peut enlever le terme $\frac{R_2R_1^2}{2}$ de la congruence précédente pour obtenir (2.16), ainsi $p|H_4$. □

Lemme 41 *Pour tout premier p et $r \in \mathbb{N}^*$, on a*

$$2R_1 \equiv -\sum_{i=1}^{r} p^i R_{i+1} (\mathrm{mod}\, p^{r+1}) \tag{2.17}$$

Preuve. En multipliant l'égalité

$$1 + \frac{p}{i} + \frac{p^2}{i^2} + ... + \frac{p^{r-1}}{i^{r-1}} = \frac{p^r - i^r}{i^{r-1}(p-i)}$$

Par $\frac{-p}{i^2} (1 \leq i \leq p-1)$, nous obtenons

$$\frac{-p}{i^2}(1 + \frac{p}{i} + \frac{p^2}{i^2} + ... + \frac{p^{r-1}}{i^{r-1}}) = \frac{-p^{r+1} + pi^r}{i^{r+1}(p-i)} \equiv \frac{p}{i(p-i)} (\mathrm{mod}\, p^{r+1}),$$

donc

$$\frac{1}{i} + \frac{1}{p-i} \equiv -\left(\frac{p}{i^2} + \frac{p^2}{i^3} + ... + \frac{p^r}{i^{r+1}} \right) (\mathrm{mod}\, p^{r+1}),$$

alors

$$\sum_{i=1}^{p-1} \frac{1}{i} + \frac{1}{p-i} \equiv -\left(\frac{p}{i^2} + \frac{p^2}{i^3} + ... + \frac{p^r}{i^{r+1}} \right) (\mathrm{mod}\, p^{r+1}),$$

ainsi

$$2R_1 \equiv -\sum_{i=1}^{r} p^i R_{i+1} (\mathrm{mod}\, p^{r+1}).$$

□

Lemme 42 *Pour $p \geq 7$, on a*

$$2R_1 \equiv -pR_2 (\mathrm{mod}\, p^4), \tag{2.18}$$

et pour $p \geq 11$, on a

$$2R_3 \equiv -3pR_4 (\mathrm{mod}\, p^4).$$

Preuve. Notons que, par le lemme 41

$$2R_1 \equiv -pR_2 - p^2R_3 - p^3R_4 (\mathrm{mod}\, p^4),$$

puisque, par le lemme 39 on a, $p^2|H_3$, et $p|H_4$ pour tout $p \geq 7$, alors

$$2R_1 \equiv -pR_2 (\mathrm{mod}\, p^4).$$

Par suite, pour tout $1 \leq k \leq p-1$, on a

$$\frac{1}{k^3} + \frac{1}{(p-k)^3} = \frac{p^3 - 3p^2k + 3pk^2}{k^3(p-k)^3},$$

ainsi

$$2R_3 = \sum_{k=1}^{p-1} \left(\frac{1}{k^3} + \frac{1}{(p-k)^3} \right) \tag{2.19}$$

$$= p^3 \sum_{k=1}^{p-1} \frac{1}{k^3(p-k)^3} - 3p^2 \sum_{k=1}^{p-1} \frac{1}{k^2(p-k)^3} + 3p \sum_{k=1}^{p-1} \frac{1}{k(p-k)^3},$$

en appliquant le lemme 39, pour $p \geq 11$

$$\sum_{k=1}^{p-1} \frac{1}{k^3(p-k)^3} \equiv -\sum_{k=1}^{p-1} \frac{1}{k^6} \equiv 0 (\mathrm{mod}\, p). \tag{2.20}$$

Par ailleurs $\frac{1}{p-k} \equiv -\frac{p+k}{k^2} (\mathrm{mod}\, p^2)$, et pour tout $p \geq 11$, $p|R_6$ et $p^2|R_5$, par le lemme 39 on a

$$\sum_{k=1}^{p-1} \frac{1}{k^2(p-k)^3} = \sum_{k=1}^{p-1} \frac{1}{k^3(p-k)^2} \equiv \sum_{k=1}^{p-1} \frac{(p+k)^2}{k^7} \tag{2.21}$$

$$\equiv \sum_{k=1}^{p-1} \frac{2p}{k^6} + \sum_{k=1}^{p-1} \frac{1}{k^5} \equiv 0 (\mathrm{mod}\, p^2),$$

En rempalçant (2.20) et (2.21) dans (2.19), nous trouvons :

$$2R_3 \equiv 3p \sum_{k=1}^{p-1} \frac{1}{k(p-k)^3} (\mathrm{mod}\, p^4) \tag{2.22}$$

Maintenant, par l'égalité

$$\frac{1}{k(p-k)^3} + \frac{1}{k^4} = \frac{p^3}{k^4(p-k)^3} - \frac{3p^2}{k^3(p-k)^3} + \frac{3p}{k^2(p-k)^3},$$

pour $k = 1, 2, 3, ..., p-1$, nous obtenons

$$\frac{1}{k(p-k)^3} + \frac{1}{k^4} = \frac{3p^2}{k^6} + \frac{3p}{k^2(p-k)^3} (\mathrm{mod}\, p^3),$$

d'après la sommation de $k = 1$ à $p-1$, la congruence précédente donne

$$\sum_{k=1}^{p-1} \frac{1}{k(p-k)^3} + R_4 \equiv 3p^2 R_6 + 3p \sum_{k=1}^{p-1} \frac{1}{k^2(p-k)^3} (\mathrm{mod}\, p^3),$$

puisque, par le lemme 39, $p|R_6$, pour $p \geq 11$ et d'après (2.21), cette congruence devient

$$\sum_{k=1}^{p-1} \frac{1}{k(p-k)^3} \equiv -R_4 (\mathrm{mod}\, p^3),$$

On remplace ceci dans (2.22), donc

$$2R_3 \equiv -3pR_4 (\mathrm{mod}\, p^4).$$

Ceci complète la preuve. □

Théorème 43 *Soit* $p \geq 11$ *un nombre premier, alors*

$$\binom{2p-1}{p-1} \equiv 1 - 2p \sum_{k=1}^{p-1} \frac{1}{k} + 4p^2 \sum_{1 \leq i < j \leq p-1} \frac{1}{ij} (\mathrm{mod}\, p^7) \tag{2.23}$$

Preuve. Pour tout premier $p \geq 11$ on a

$$\begin{aligned}
\binom{2p-1}{p-1} &= \frac{(p+1)(p+2)...(p+k)...(p+(p-1))}{1.2.3...p-1} \\
&= (\frac{p}{1}+1)(\frac{p}{2}+1)...(\frac{p}{k}+1)...(\frac{p}{p-1}+1) \\
&= 1 + \sum_{i=1}^{p-1} \frac{p}{i} + \sum_{1 \leq i_1 < i_2 \leq p-1} \frac{p^2}{i_1 i_2} + ... + \sum_{i \leq i_1 < i_2 < ... j_k \leq p-1} \frac{p^k}{i_1 i_2 ... i_k} + ... + \frac{p^{p-1}}{(p-1)!} \\
&= 1 + \sum_{k=1}^{p-1} p^k H_k = 1 + \sum_{k=1}^{6} p^k H_k + \sum_{k=7}^{p-1} p^k H_k, \qquad (2.24)
\end{aligned}$$

par les lemmes 39, et 40, on a $R_1 \equiv R_3 \equiv R_5 \equiv H_3 \equiv 0 (\mathrm{mod}\, p^2)$, et $R_2 \equiv R_4 \equiv R_6 \equiv H_4 \equiv 0 (\mathrm{mod}\, p)$ pour $p \geq 11$.

Par ailleurs, la formule de Newton (1.10) donne

$$5H_5 = R_5 + \sum_{i=1}^{4}(-1)^i H_i R_{5-i} \text{ ,et } 6H_6 = -R_6 - \sum_{k=1}^{5}(-1)^i H_i R_{6-i},$$

Ceci implique que, $p^2|H_5$ et $p|H_6$, donc :

$$p^7|\sum_{i=5}^{p-1} p^k H_k = p^5 H_5 + p^6 H_6 + \sum_{i=7}^{p-1} p^k H_k, \text{ pour } p \geq 11,$$

ainsi, le coefficient bilomial $\binom{2p-1}{p-1}$ devient

$$\binom{2p-1}{p-1} \equiv 1 + pH_1 + p^2 H_2 + p^3 H_3 + p^4 H_4 (\mathrm{mod}\, p^7). \tag{2.25}$$

Rappelons que, $H_1 = R_1$, et $H_2 = (R_1^2 - R_2)/2$, les congruences du lemme 40 donnent

$$\begin{aligned} H_3 &\equiv \frac{R_3}{3} - \frac{R_1 R_2}{2} (\mathrm{mod}\, p^4), \\ H_4 &\equiv -\frac{R_4}{4} + \frac{R_2^2}{8} (\mathrm{mod}\, p^3), \end{aligned}$$

alors

$$\binom{2p-1}{p-1} \equiv 1 + pR_1 + \frac{p^2}{2}(R_1^2 - R_2) + \frac{p^3}{6}(2R_3 - 3R_1 R_2) + \frac{p^4}{8}(R_2^2 - 2R_4) (\mathrm{mod}\, p^7).$$

Par ailleurs, le lemme 42 donne

$$2R_1 \equiv -pR_2 (\mathrm{mod}\, p^4), \tag{2.26}$$

$$\text{et } 2R_3 \equiv -3pR_4 (\mathrm{mod}\, p^4), \tag{2.27}$$

En multipliant (2.26) par $p^3 R_2$, et (2.27) par p^3

$$\begin{aligned} p^4 R_2^2 &\equiv -2P^3 R_1 R_2 (\mathrm{mod}\, p^7) \text{ ,} \\ \text{et } p^4 R_4 &\equiv -\frac{2}{3} p^3 R_3 (\mathrm{mod}\, p^7) \text{ ,} \end{aligned}$$

Ceci implique que

$$\binom{2p-1}{p-1} \equiv 1 + pR_1 + \frac{p^2}{2}(R_1^2 - R_2) - \frac{3p^3}{4} R_1 R_2 + \frac{p^3}{2} R_3 (\mathrm{mod}\, p^7) \tag{2.28}$$

Maintenant, il nous reste d'enlever R_3 à partir de (2.28).

Par le lemme 41, on a

$$2R_1 \equiv -pR_2 - p^2R_3 - p^3R_4 - p^4R_5 - p^5R_6 \pmod{p^6},$$

Puisque $p^2|R_5$ et $p|R_6$, alors

$$2R_1 \equiv -pR_2 - p^2R_3 - p^3R_4 - p^4R_5 - p^5R_6 \pmod{p^6}, \tag{2.29}$$

Encore, on utilise (2.27) pour obtenir

$$p^3R_4 \equiv -\frac{2}{3}p^2R_3 \pmod{p^6},$$

donc (2.29) devient

$$2R_1 \equiv -pR_2 - \frac{1}{3}p^2R_3 \pmod{p^6},$$

En multipliant par $3p$, ceci implique que

$$p^3R_3 \equiv -6pR_1 - 3p^2R_2 \pmod{p^7}, \tag{2.30}$$

On remplace ceci dans (2.28), nous déduisons

$$\binom{2p-1}{p-1} \equiv 1 - 2pR_1 - 2p^2R_2 + \frac{p^2}{4}R_1(2R_1 - 3pR_2) \pmod{p^7}. \tag{2.31}$$

Nous écrivons (2.26) sous la forme suivante

$$2R_1 - 3pR_2 \equiv 8R_1 \pmod{p^4},$$

En multipliant la congruence précédente par $\frac{1}{4}p^2R_1$, et on utilise le fait que $p^2|R_1$ donc $p^4|p^2R_1$, nous trouvons

$$\frac{p^2}{4}R_1(2R_1 - 3pR_2) \equiv 2p^2R_1^2 \pmod{p^7},$$

On remplace par ce résultat dans (2.31), nous obtenons

$$\left(\begin{array}{c} 2p-1 \\ p-1 \end{array}\right) \equiv 1 - 2pR_1 + 2p^2(R_1^2 - R_2) \pmod{p^7}, \tag{2.32}$$

mais $R_1^2 - R_2 = 2H_2$, alors

$$\left(\begin{array}{c} 2p-1 \\ p-1 \end{array}\right) \equiv 1 - 2pR_1 + 4p^2H_2 \pmod{p^7},$$

ceci complète la preuve. □

Corollaire 44 *Soit $p \geq 5$ un premier, on a*

$$\binom{2p-1}{p-1} \equiv 1 - 2p\sum_{k=1}^{p-1}\frac{1}{k} - 2p^2\sum_{k=1}^{p-1}\frac{1}{k^2} \equiv 1 + 2p\sum_{k=1}^{p-1}\frac{1}{k} + \frac{2p^3}{3}\sum_{k=1}^{p-1}\frac{1}{k^3} \pmod{p^6}.$$

Preuve. La première congruence du corollaire 44 pour $p \geq 11$ est immédiate à partir de (2.32), en utilisant le fait que $p^2|R_1$ et donc $p^6|p^2R_1^2$.

D'après (2.30) nous avons

$$p^2R_2 \equiv -2pR_1 - \frac{p^3}{3}R_3 \pmod{p^6}, \tag{2.33}$$

l'insertion de cette dernière dans la première congruence du corollaire 44 donne immédiatement

$$\binom{2p-1}{p-1} \equiv 1 + 2p\sum_{k=1}^{p-1}\frac{1}{k} + \frac{2p^3}{3}\sum_{k=1}^{p-1}\frac{1}{k^3} \pmod{p^6}.$$

□

Corollaire 45 *Soit $p \geq 7$ un premier, on a*

$$\binom{2p-1}{p-1} \equiv 1 + 2p\sum_{k=1}^{p-1}\frac{1}{k} \equiv 1 - p^2\sum_{k=1}^{p-1}\frac{1}{k^2} \pmod{p^5}.$$

Preuve. Par le corollaire 44 on a

$$\binom{2p-1}{p-1} \equiv 1 - 2pR_1 - 2p^2R_2 \pmod{p^5}. \tag{2.34}$$

Mais, d'après (2.18) du lemme 42 on a

$$2R_1 \equiv -pR_2 \pmod{p^4},$$

l'insertion de cette dernière dans (2.34) donne

$$\binom{2p-1}{p-1} \equiv 1 + 2p\sum_{k=1}^{p-1}\frac{1}{k} \equiv 1 - p^2\sum_{k=1}^{p-1}\frac{1}{k^2} \pmod{p^5}.$$

□

Dans ce qui suit on étude certaines congruences concernant des nombres de Bernoulli.

Rappelons que, d'après la relation (1.24) de la remarque 18 et la relation (1.31), on a

Théorème 46 *Pour tout premier p, et $h, n \in \mathbb{N}$, avec $h \geq 1$,*

$$R_n \equiv P_{\varphi(p^h)-n} (\mathrm{mod}\, p^h) \ \textit{et}$$

$$P_m = P_m(p-1) = \sum_{r=1}^{m+1} \frac{1}{r} \binom{m}{r-1} B_{m-r+1} p^r. \tag{2.35}$$

D'après (1.32) on peut déduire que : $\upsilon_p(B_k) \geq -1$ si $k \in \mathbb{N}$, et $\upsilon_p(B_k) \geq 0$ si $(p-1) \nmid k$ [13].

Donc pour tout $m \in \mathbb{N}$,

$$\begin{aligned} \upsilon_p \left(\frac{1}{r} \binom{m}{r-1} p^r B_{m-r+1} \right) &= r - \upsilon_p \left(\binom{m}{r-1} \right) + \upsilon_p(B_{m-r+1}) \\ &\geq r - \upsilon_p(r) - 1, \end{aligned}$$

ainsi

$$P_m \equiv \sum_{r-\upsilon_p(r) \leq h} \frac{1}{r} \binom{m}{r-1} B_{m-r+1} p^r \ (\mathrm{mod}\, p^h). \tag{2.36}$$

Où la sommation sur tous les entiers $1 \leq r \leq m+1$ tels que $r - \upsilon_p(r) \leq h$.

Lemme 47 *Pour tout premier $p \geq 11$ on a*

(i) $R_1(p) \equiv -\frac{p^2}{2} B_{p^4-p^3-2} - \frac{p^4}{4} B_{p^2-p-4} + \frac{p^5}{6} B_{p-3} + \frac{p^5}{20} B_{p-5} \pmod{p^6}$

(ii) $R_1^2(p) \equiv \frac{p^4}{9} B_{p^4-p^3-2} + p^3 B_{p^4-p^3-4} \pmod{p^5}$

(iii) $R_2(p) \equiv p B_{p^4-p^3-2} + p^3 B_{p^4-p^3-4} \pmod{p^5}$

Preuve. D'après la relation (2.36), on a

$$P_m \equiv \sum_{r-\upsilon_p(r) \leq 6} \frac{1}{r} \binom{m}{r-1} B_{m-r+1} p^r (\mathrm{mod}\, p^6).$$

Pour $1 \leq r \leq m+1$, soit $s = \upsilon_p(r)$ et $r = up^s$, avec $u \neq 0$,$s \in \mathbb{N}$, et $p \nmid u$ alors $r - \upsilon_p(r) \leq 6$ ssi $up^s \leq s+6$, ceci implique que $p^s \leq s+6$, mais $p^s > s+6$ pour $s \geq 1$, nous déduisons alors que $s = 0$, donc $r - \upsilon_p(r) \leq 6$ ssi $1 \leq r \leq 6$, alors

$$P_m = \sum_{r=1}^{6} \frac{1}{r} \binom{m}{r-1} B_{m-r+1} p^r \pmod{p^6}, \text{ pour } m = 1, 2, ...$$

Posons $m = p^5(p-1|) - 1$, puisque $B_k = 0$ pour tout impair $k \geq 3$, et $m+1 = p^5(p-1)$ est pair >3, alors $B_{m-r+1} = 0$ pour $r = 1, 3, 5$.

Aussi ,par le corollaire 28, $p^6 \nmid denom(B_{p^5(p-1)-6})$ donc $p^6 | p^6 B_{p^5(p-1)-6}$ pour $p \geq 11$, ainsi

$$P_m \equiv \frac{1}{2}(p^6-p^5-1)p^2 B_{p^6-p^5-2} + \frac{1}{4}\frac{(p^6-p^5-1)(p^6-p^5-2)(p^6-p^5-3)}{6} p^4 B_{p^6-p^5-4} (\mathrm{mod}\, p^6),$$

alors, par la relation (1.24) de la remarque 18, c'est à dire $P_{\varphi(p^6)-1} \equiv R_1 (\mathrm{mod}\, p^6)$ on a

$$R_1 \equiv P_m \equiv -\frac{p^2}{2} B_{p^6-p^5-2} - \frac{p^4}{4} B_{p^6-p^5-4} \pmod{p^6}. \tag{2.37}$$

Mais, par (1.33) de Kummer, on a

$$B_{p^6-p^5-2} \equiv \frac{p^6-p^5-2}{p^4-p^3-2} B_{p^4-p^3-2} \equiv \frac{2B_{p^4-p^3-2}}{p^3+2} \equiv \left(1 - \frac{p^3}{2}\right) B_{p^4-p^3-2} \left(\mathrm{mod}\, p^4\right)$$

et

$$B_{p^4-p^3-2} \equiv \frac{2}{3} B_{p-3} \left(\mathrm{mod}\, p\right),$$

donc (2.37) devient

$$R_1 \equiv -\frac{p^2}{2} B_{p^4-p^3-2} + \frac{p^5}{6} B_{p-3} - \frac{p^4}{4} B_{p^6-p^5-4} \quad \left(\mathrm{mod}\, p^6\right). \tag{2.38}$$

et

$$B_{p^6-p^5-4} \equiv \frac{p^6-p^5-4}{p^2-p-4} B_{p^2-p-4} \equiv \frac{4B_{p^2-p-4}}{p+4} \equiv \left(1 - \frac{p}{4}\right) B_{p^2-p-4} \quad \left(\mathrm{mod}\, p^2\right),$$

En remplaçant cette congruence dans (2.38), nous obtenons :

$$R_1 \equiv -\frac{p^2}{2} B_{p^4-p^3-2} + \frac{p^5}{6} B_{p-3} - \frac{p^4}{4} B_{p^2-p-4} + \frac{p^5}{16} B_{p^2-p-4} \pmod{p^6}, \tag{2.39}$$

Finalement, on sait que :

$$B_{p^4-p^3-4} \equiv \frac{4}{5} B_{p-5} \pmod{p},$$

D'après cette dernière et (2.39), On trouve **(i)**.

Aussi, (2.39) donne immédiatement :

$$R_1^2 \equiv \frac{p^4}{4} B_{p^4-p^3-2}^2 \left(\mathrm{mod}\, p^5\right),$$

Ceci implique que :

$$R_1^2 \equiv \frac{p^4}{9} B_{p-3}^2 \pmod{p^5}, \quad \text{C'est à dire } \textbf{(ii)}.$$

Afin de prouver la congruence **(iii)**, notons que si $p-1 \nmid (m-4)$, alors, par le corollaire 28,pour $m \geq 6$ pair, et $p \geq 11$ on a $p^5 | p^5 B_{m-4} t$, ainsi que $B_{m-1} = B_{m-s} = 0$ pour tout m.

Donc pour tout $m \geq 2$ pair, la relation (2.36) donne

$$P_m \equiv pB_m + \frac{P^3}{6} m(m-1) B_{m-2} \pmod{p^5}.$$

En particulier, $m = \varphi(p^4) - 2$. On applique la relation (1.24) de la remarque 18, c'est à dire

$$P_{\varphi(p^4)-2} \equiv R_2 \pmod{p^4}.$$

Nous trouvons :

$$R_2 \equiv pB_{p^4-p^3-2} + p^3 B_{p^4-p^3-4} \pmod{p^5}, \text{ C'est à dire } \textbf{(iii)}.$$

□

D'après le théorème 43 et le lemme précédent on a le corollaire suivant :

Corollaire 48 *Soit $p \geq 11$ un premier, donc*

$$\begin{aligned} \binom{2p-1}{p-1} &\equiv 1 - p^3 B_{p^4-p^3-2} + p^5 \left(\frac{1}{2} B_{p^2-p-4} - 2B_{p^4-p^3-4} \right) \\ &\quad + p^6 \left(\frac{2}{9} B_{p-3}^2 - \frac{1}{3} B_{p-3} - \frac{1}{10} B_{p-5} \right) \pmod{p^7}. \end{aligned} \tag{2.40}$$

Preuve. Il est un résultat immédiat d'inserer les congruences (i) ; (ii) et (iii) du lemme précédent dans (2.23) du théorème 43.

En effet, on a :

$$\begin{aligned} \binom{2p-1}{p-1} &\equiv 1 - 2p \sum_{k=1}^{p-1} \frac{1}{k} + 4p^2 \sum_{1 \leq i < j \leq p-1} \frac{1}{ij} \\ &\equiv 1 - 2p \left(-\frac{p^2}{2} B_{p^4-p^3-2} - \frac{p^4}{4} B_{p^2-p-4} + \frac{p^5}{6} B_{p-3} + \frac{p^5}{20} B_{p-5} \right) \\ &\quad + 2p^2 \left(\frac{p^4}{9} B_{p-3}^2 - pB_{p^4-p^3-2} - p^3 B_{p^4-p^3-4} \right) \\ &\equiv 1 - p^3 B_{p^4-p^3-2} + p^5 \left(\frac{1}{2} B_{p^2-p-4} - 2B_{p^4-p^3-4} \right) \\ &\quad + p^6 \left(\frac{2}{9} B_{p-3}^2 - \frac{1}{3} B_{p-3} - \frac{1}{10} B_{p-5} \right) \pmod{p^7}. \end{aligned}$$

□

Chapitre 3

Généralisation des congruences de Wolstenholme et de Morley

3.1 Introduction :

Dans ce chapitre, nous présentons une congruence qui généralise les congruences de Wolstenholme(2.2), Morley(2.5), Glaisher(2.8), McIntosh(2.9), Tauraso(2.11) et Mestrovic(2.13). Elle permet aussi de retrouver simplement des congruences dûes à Glaisher et Zhao. On commence ce chapitre par des lemmes utiles pour la preuve de cette congruence.

3.2 Lemmes

Lemme 49 *Pour tout entier $n \geq 1$ on a :*

$$(-1)^n \binom{2n}{n} = 4^{2n} \binom{n-\frac{1}{2}}{2n} \tag{3.1}$$

Preuve. On a

$$4^{2n}\binom{n-\frac{1}{2}}{2n} = \frac{4^{2n}}{(2n)!}\frac{(n-\frac{1}{2})(n-\frac{3}{2})...(n-(2n+\frac{1}{2})+1)(n-(2n+\frac{1}{2}))!}{1.2.3...(n-(2n+\frac{1}{2}))}$$

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

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

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

ce qui nous donne

$$4^{2n} \binom{n-\frac{1}{2}}{2n} = (-1)^n \frac{2^{2n}}{(2n)!} \left(\prod_{j=1}^{n} (2j-1) \right)^2 \tag{3.2}$$

On constate alors que

$$\prod_{k=1}^{n} (2j-1) = \frac{\prod_{j=1}^{n} (2j) . \prod_{j=1}^{n} (2j-1)}{\prod_{j=1}^{n} (2j)} = \frac{(2n)!}{2^n n!} \tag{3.3}$$

il resulte de (3.2) et (3.3) que

$$4^{2n} \binom{n-\frac{1}{2}}{2n} = (-1)^n \frac{2^{2n}}{(2n)!} \left(\frac{(2n)!}{2^n n!} \right)^2$$

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

Pour tout nombre premier p et pour tout entier k, nous définissons les nombres harmoniques généralisés H_m par :

$$H_m = \sum_{1 \leq k_1 < \ldots < k_m \leq p-1} \frac{1}{k_1 \ldots k_m}, \qquad \text{pour} \;\; 1 \leq m \leq p-1$$

et par convention

$$H_0 = 1 \quad \text{et} \quad H_m = 0 \quad \text{pour} \;\; m \geq p \tag{3.4}$$

Soit $P(x)$ le polynome défini par

$$P(x) = \frac{(x-1)(x-2)\ldots(x-(p-1))}{(p-1)!} \tag{3.5}$$

On a alors

$$\begin{aligned} P(x) &= (-1)^{p-1} \prod_{k=1}^{p-1} \frac{k-x}{k} \\ &= \prod_{i=1}^{p-1} (1 - \frac{x}{k}) \end{aligned}$$

On utilise la même technique que la relation (1.11), donc en deduit que

$$P(x) = \sum_{k=0}^{p-1} (-1)^k H_k x^k \tag{3.6}$$

□

Lemme 50 *Pour tout nombre premier p impair et pour tout entier $m \geq 1$, on a :*

1.
$$H_{2m-1} - mpH_{2m} = \frac{1}{2}p^2 \sum_{k=2m+1}^{p-1} (-1)^k \begin{pmatrix} k \\ 2m-1 \end{pmatrix} p^{k-(2m-1)} H_k \tag{3.7}$$

2.
$$H_m \equiv 0(\mathrm{mod}\, p) \quad \textit{pour } m \neq p-1 \tag{3.8}$$

3.
$$H_m \equiv 0(\mathrm{mod}\, p^2) \quad \textit{pour } m \textit{ impair et } m \neq p-2 \tag{3.9}$$

4.
$$H_{2m-1} - mpH_{2m} \equiv 0(\mathrm{mod}\, p^4), \quad \textit{pour } 2m+1 \neq p-2 \tag{3.10}$$

Preuve.

1. La relation (3.5), nous permet d'obtenir qu'on a :

$$P(x) = P(p-x)$$

Ce qui peut s'ecrire en exploitent la relation (3.6) et la convention (3.4) :

$$\sum_{k\geq 0}(-1)^k H_k x^k = \sum_{k\geq 0}(-1)^k H_k (p-x)^k \tag{3.11}$$

en identifiant les coefficients de x^{2m-1} dans chacun des deux membres de (3.11), on obtient :

$$\begin{aligned} (-1)^{2m-1} H_{2m-1} x^{2m-1} &= \sum_{k\geq 2m-1} (-1)^k H_k (p-x)^{2m-1} \\ -H_{2m-1} x^{2m-1} &= \sum_{k\geq 2m-1} (-1)^k H_k \binom{2m-1}{k} p^{2m-1-k} (-x)^k \end{aligned}$$

et puis, on fixe le k qui est egale a $2m-1$, on trouve :

$$-H_{2m-1} = \sum_{k\geq 2m-1} (-1)^k H_k \binom{k}{2m-1} p^{k-2m+1} (-1)^{2m-1}$$

$$-H_{2m-1} = -\sum_{k\geq 2m-1} (-1)^k \binom{k}{2m-1} p^{k-2m+1} H_k$$

$$-H_{2m-1} = H_{2m-1} - 2mpH_{2m} - p^2 \sum_{k=2m+1}^{p-1} (-1)^k \binom{k}{2m-1} p^{k-2m+1} H_k$$

$$-2H_{2m-1} = -2mpH_{2m} - p^2 \sum_{k=2m+1}^{p-1} (-1)^k \binom{k}{2m-1} p^{k-2m+1} H_k$$

$$H_{2m-1} - mpH_{2m} = \frac{1}{2}p^2 \sum_{k=2m+1}^{p-1} (-1)^k \binom{k}{2m-1} p^{k-2m+1} H_k$$

2. Il s'agit d'utiliser un résultat bien connu qu'on peut déduire facilement du fait que le polynome considéré comme un polynome a coefficients dans le corps $(\mathbb{Z}/p\mathbb{Z})$, et grace au théoreme de Wilson et le théoreme 5 on a

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

en multipliant par $\frac{1}{(p-1)!}$

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

$$P(x) \equiv 1 - x^{p-1} (\mathrm{mod}\, p)$$

car

$$(p-1)! \equiv -1 (\mathrm{mod}\, p) \qquad \text{(Wilson)}$$

On en déduit aussi que

$$H_{p-1} = \frac{1}{(p-1)!} \equiv -1 (\mathrm{mod}\, p)$$

3. D'aprés la relation (3.7) on a :

$$H_{2m-1} \equiv mpH_{2m} \pmod{p^2} \tag{3.12}$$

on a alors

$$H_{2m-1} \equiv 0 (\mathrm{mod}\, p^2) \qquad \text{pour } 2m-1 \neq p-2$$

parcequ'on a

$$H_{2m} \equiv 0 (\mathrm{mod}\, p)$$

Remarquons que si

$$2m-1 \neq p-2 \quad \Leftrightarrow \quad m = \frac{p-1}{2}$$

Donc

$$H_{2m-1} = H_{p-2} \equiv \frac{p-1}{2} p H_{p-1} \equiv \frac{p}{2} \pmod{p^2}$$

4. D'aprés la relation (3.7) on a

$$H_{2m-1} - mpH_{2m} \equiv -\frac{1}{2}p^2 \binom{2m+1}{2} H_{2m+1} + \frac{1}{2}p^3 \binom{2m+2}{3} H_{2m+2} \pmod{p^4} \tag{3.13}$$

Si $2m+1 \neq p-2$, on alors $2m+2 \neq p-1$ et on déduit de (3.9) et (3.8) que $H_{2m+1} \equiv 0 (\mathrm{mod}\, p^2)$ et $H_{2m+2} \equiv 0 (\mathrm{mod}\, p)$, En tenant compte de ces deux dernières congruences dans (3.13).

□

Lemme 51 *Pour tout entier $m \geq 1$, on a :*

1. $$\sum_{k=1}^{p-1} \frac{1}{k^m} \equiv \begin{cases} 0 \pmod p & si\ p-1 \nmid m \\ -1 \pmod p & si\ p-2 \mid m \end{cases}$$

2. $$\sum_{k=1}^{p-1} \frac{1}{k^m} \equiv \begin{cases} 0 \pmod{p^2} & si\ m\ est\ impair\ et\ p-1 \nmid m+1 \\ \frac{1}{2}mp \pmod{p^2} & si\ m\ est\ impair\ et\ p-1 \mid m+1 \end{cases}$$

3. *Pour m impair, on a :*

$$2\sum_{k=1}^{p-1} \frac{1}{k^m} + mp\sum_{k=1}^{p-1} \frac{1}{k^{m+1}} \equiv \begin{cases} 0 \pmod{p^3} & \\ 0 \pmod{p^4} & si\ \ p-1 \nmid m+3 \\ -\frac{1}{12}m(m+1)(m+2)p^3 \pmod{p^4} & si\ \ p-1 \mid m+3 \end{cases} \tag{3.14}$$

4. *Pour m impair, on a :*

$$\sum_{k=1}^{p-1} \frac{1}{k^m} + \frac{1}{2}mp\sum_{k=1}^{p-1} \frac{1}{k^{m+1}} + \frac{m(m+1)}{12}p^2\sum_{k=1}^{p-1} \frac{1}{k^{m+2}} \equiv 0 (\mathrm{mod}\, p^6) \qquad si\ \ p-1 \nmid m+5 \tag{3.15}$$

Preuve.

1. Soit $g \in \mathbb{Z}$ tel que $\overline{g}$ soit un générateur du groupe cyclique $(\mathbb{Z}/p\mathbb{Z})^*$. L'application $x \longrightarrow x^{-1}$ de $(\mathbb{Z}/p\mathbb{Z})^*$ dans lui meme étant bijective, on a :

$$\sum_{k=1}^{p-1} \frac{1}{k^m} \equiv \sum_{k=1}^{p-1} k^m \equiv \sum_{j=0}^{p-2} (g^j)^m \equiv \sum_{j=0}^{p-2} (g^m)^j \equiv 0 (\mathrm{mod}\, p)$$

   On a alors :

$$(g^m-1)\sum_{k=1}^{p-1} \frac{1}{k^m} \equiv (g^m-1)\sum_{j=0}^{p-2} (g^m)^j \equiv (g^m)^{p-1} - 1 \equiv 0 (\mathrm{mod}\, p)$$

   Ce qui implique que :

   (a) Si $p-1 \nmid m$, on a $g^m - 1$ ne congrus pas 0 modulo p et $\sum_{k=1}^{p-1} \frac{1}{k^m} \equiv 0 (\mathrm{mod}\, p)$

   (b) Si $p-1 \mid m$, on a $\frac{1}{k^m} \equiv 1 (\mathrm{mod}\, p)$ pour $1 \leq k \leq p-1$ et $\sum_{k=1}^{p-1} \frac{1}{k^m} \equiv \sum_{k=1}^{p-1} 1 = p-1 \equiv -1 (\mathrm{mod}\, p)$

2. Pour m impair, on a :

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

$$=\frac{1}{2}\sum_{k=1}^{p-1}\frac{(p-k)^m+k^m}{k^m(p-k)^m}\equiv-\frac{1}{2}mp\sum_{k=1}^{p-1}\frac{1}{k^{m+1}}(\mathrm{mod}\,p^2) \tag{3.16}$$

Ce qui implique :

(a) Si $p-1\nmid m+1$, on a

$$\sum_{k=1}^{p-1}\frac{1}{k^{m+1}}\equiv 0(\mathrm{mod}\,p) \text{ et (3.16) donne } \sum_{k=1}^{p-1}\frac{1}{k^m}\equiv 0(\mathrm{mod}\,p^2)$$

(b) Si $p-1\mid m+1$, on a

$$\sum_{k=1}^{p-1}\frac{1}{k^{m+1}}\equiv -1(\mathrm{mod}\,p) \text{ et (3.16) donne } \sum_{k=1}^{p-1}\frac{1}{k^m}\equiv \frac{1}{2}mp(\mathrm{mod}\,p^2)$$

3. Pour $1\leq k\leq p-1$

$$\frac{1}{(1-\frac{p}{k})^m}\equiv 1+m\frac{p}{k}+\frac{m(m+1)}{2}\frac{p^2}{k^2}+\frac{m(m+1)(m+2)}{6}\frac{p^3}{k^3}(\mathrm{mod}\,p^4)$$

Pour m impair, on a :

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

$$\equiv\sum_{k=1}^{p-1}\left(-\frac{1}{k^m}-m\frac{p}{k^{m+1}}-\frac{m(m+1)}{2}\frac{p^2}{k^{m+2}}-\frac{m(m+1)(m+2)}{6}\frac{p^3}{k^{m+2}}\right)(\mathrm{mod}\,p^4)$$

Cela nous donne

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

$$\equiv -mp\sum_{k=1}^{p-1}\frac{1}{k^{m+1}}-\frac{m(m+1)}{2}p^2\sum_{k=1}^{p-1}\frac{1}{k^{m+2}}-\frac{m(m+1)(m+2)}{6}p^3\sum_{k=1}^{p-1}\frac{1}{k^{m+3}}(\mathrm{mod}\,p^4) \tag{3.17}$$

Or $m+2$ est impair. On a donc $p-1\nmid m-2$ et $\sum_{k=1}^{p-1}\frac{1}{k^{m+2}}\equiv 0(\mathrm{mod}\,p)$.
Dans ce cas, d'aprs (3.17) on déduit que

$$2\sum_{k=1}^{p-1}\frac{1}{k^m}+mp\sum_{k=1}^{p-1}\frac{1}{k^{m+1}}\equiv 0(\mathrm{mod}\,p^3)$$

Si $p-1 \nmid m+3$ on a à la fois $\sum_{k=1}^{p-1} \frac{1}{k^{m+2}} \equiv 0(\mathrm{mod}\, p^2)$ et $\sum_{k=1}^{p-1} \frac{1}{k^{m+3}} \equiv 0(\mathrm{mod}\, p)$. Dans ce cas, on déduit de (3.17)

$$2\sum_{k=1}^{p-1} \frac{1}{k^m} \equiv -mp \sum_{k=1}^{p-1} \frac{1}{k^{m+1}} (\mathrm{mod}\, p^4)$$

Si $p-1 \nmid m+3$ on a $\sum_{k=1}^{p-1} \frac{1}{k^{m+2}} \equiv \frac{1}{2}(m+2)p \ (\mathrm{mod}\, p^2)$ et $\sum_{k=1}^{p-1} \frac{1}{k^{m+3}} \equiv 1(\mathrm{mod}\, p)$. Dans ce cas, on déduit de (3.17) que

$$\begin{aligned} 2\sum_{k=1}^{p-1} \frac{1}{k^m} + mp \sum_{k=1}^{p-1} \frac{1}{k^{m+1}} &\equiv -\frac{m(m+1)(m+2)}{4} p^3 + \frac{m(m+1)(m+2)}{6} p^3 \\ &\equiv -\frac{1}{12} m(m+1)(m+2) \ (\mathrm{mod}\, p^4). \end{aligned}$$

4. Si m impair et si $p-1 \nmid m+5$, on a :

$$2\sum_{k=1}^{p-1} \frac{1}{k^m} \equiv -mp \sum_{k=1}^{p-1} \frac{1}{k^{m+1}} - \frac{m(m+1)}{2} p^2 \sum_{k=1}^{p-1} \frac{1}{k^{m+2}} - \frac{m(m+1)(m+2)}{6} p^3 \sum_{k=1}^{p-1} \frac{1}{k^{m+3}} (\mathrm{mod}\, p^4) \tag{3.18}$$

On a aussi d'aprés (3.14) :

$$2p^2 \sum_{k=1}^{p-1} \frac{1}{k^{m+2}} + (m+2)p^3 \sum_{k=1}^{p-1} \frac{1}{k^{m+3}} \equiv 0(\mathrm{mod}\, p^6). \tag{3.19}$$

En déduisant que d'aprés (3.18) et (3.19) :

$$2\sum_{k=1}^{p-1} \frac{1}{k^m} \equiv -mp \sum_{k=1}^{p-1} \frac{1}{k^{m+1}} - \frac{m(m+1)}{2} p^2 \sum_{k=1}^{p-1} \frac{1}{k^{m+2}} + \frac{m(m+1)}{3} p^2 \sum_{k=1}^{p-1} \frac{1}{k^{m+2}} (\mathrm{mod}\, p^4)$$

□

3.3 Généralisation des congruences de Wolstenholme et de Morley

3.3.1 Théorème

Théorème 52 *Pour tout nombre premier impair p et pour tout p-entier α , on a :*

$$\binom{\alpha p - 1}{p-1} \equiv 1 - \alpha(\alpha-1)(\alpha^2-\alpha-1)p \sum_{k=1}^{p-1} \frac{1}{k} + \alpha^2(\alpha-1)^2 p^2 \sum_{1 \le i < j \le p-1} \frac{1}{ij} \ (\mathrm{mod}\, p^m) \tag{3.20}$$

où $m = 7$ si $p \neq 7$ et $m = 6$ si $p = 7$.

Preuve. D'aprés la relation (3.5), on a

$$\binom{\alpha p - 1}{p-1} = P(\alpha p) = \sum_{k=0}^{p-1} (-\alpha)^k H_k p^k$$

On déduit que

$$\binom{\alpha p - 1}{p-1} = \sum_{k=0}^{4} (-\alpha)^k H_k p^k + (-\alpha)^5 H_5 p^5 + (-\alpha)^6 H_6 p^6 (\mathrm{mod}\, p^7) \tag{3.21}$$

Or, d'aprés les relations (3.8) et (3.9), on a

$$(-\alpha)^5 H_5 p^5 \equiv 0 (\mathrm{mod}\, p^7) \quad \text{et} \quad (-\alpha)^6 H_6 p^6 \equiv 0 (\mathrm{mod}\, p^7) \tag{3.22}$$

Pourvu que $5 \neq p-2$ et $6 \neq p-1$, c.à.d $p \neq 7$. Il suffit donc de choisir $p \geq 11$ pour réaliser ces conditions. Ainsi pour $p \geq 11$, Il résulte des relations (3.21) et (3.22) que l'on a

$$\binom{\alpha p - 1}{p-1} = \sum_{k=0}^{4} (-\alpha)^k H_k p^k (\mathrm{mod}\, p^7) \tag{3.23}$$

Pour $\alpha = 1$, on déduit d'aprés la relation (3.23) que

$$\sum_{k=1}^{p-1} (-\alpha)^k H_k p^k \equiv 0 (\mathrm{mod}\, p^7) \tag{3.24}$$

D'autre part, le fait que $p \geq 11$, on a d'aprés (3.10) du lemme 50,

$$p^3 H_3 - 2p^4 H_4 \equiv 0 (\mathrm{mod}\, p^7) \tag{3.25}$$

Des relations (3.23),(3.24) et (3.25), on déduit que pour tout p-entiers λ et μ, on a :

$$\binom{\alpha p - 1}{p-1} \equiv \sum_{k=0}^{4} (-\alpha)^k H_k p^k + \lambda \left(\sum_{k=1}^{4} (-\alpha)^k H_k p^k \right) + \mu (p^3 H_3 - 2p^4 H_4) (\mathrm{mod}\, p^7) \tag{3.26}$$

Autrement dit, on a :

$$\binom{\alpha p - 1}{p-1} \equiv \sum_{k=0}^{4} A_k H_k p^k (\mathrm{mod}\, p^7)$$

avec

$$\begin{aligned} A_0 &= 1 \\ A_1 &= -\alpha - \lambda \\ A_2 &= \alpha^2 + \lambda \\ A_3 &= -\alpha^3 - \lambda + \mu \\ A_4 &= \alpha^4 + \lambda - 2\mu \end{aligned}$$

Choisissons λ et μ tels que : $A_3 = A_4 = 0$, on obtient :

$$\lambda = \alpha^4 - 2\alpha^3 \qquad \text{et} \qquad \mu = \alpha^4 - \alpha^3$$

Avec ce choix de λ et μ , la relation (3.26) devient :

$$\binom{\alpha p - 1}{p-1} \equiv 1 - (\alpha^4 - 2\alpha^3 + \alpha)pH_1 + (\alpha^4 - 2\alpha^3 + \alpha^2)p^2H_2 \pmod{p^7}$$

Ce qui nous fournit bien la relation (3.20), si $p = 7$, aprés un calcul on obtient

$$\begin{aligned}\binom{\alpha p - 1}{p-1} - \left(1 - \alpha(\alpha-1)(\alpha^2-\alpha-1)p\sum_{k=1}^{p-1}\frac{1}{k} + \alpha^2(\alpha-1)^2p^2\sum_{1\le i<j\le p-1}\frac{1}{ij}\right) &= \\ \frac{\alpha^3(\alpha-1)^3}{720}7^6 &\equiv 0(\bmod 7^6)\end{aligned}$$

□

3.3.2 Quelques corollaires

Le théorème 52 permet d'en déduire les résultats suivants

Corollaire 53 *Pour tout nombre premier impair, on a*

$$\binom{2p-1}{p-1} \equiv 1 - 2p\sum_{k=1}^{p-1}\frac{1}{k} + 4p^2\sum_{1\le i<j\le p-1}\frac{1}{ij} \pmod{p^m} \tag{3.27}$$

$$(-1)^{\frac{p-1}{2}}\binom{p-1}{\frac{p-1}{2}} \equiv 4^{p-1}\left(1 - \frac{5}{16}p\sum_{k=1}^{p-1}\frac{1}{k} + \frac{1}{16}p^2\sum_{1\le i<j\le p-1}\frac{1}{ij}\right) \pmod{p^m} \tag{3.28}$$

où $m = 7$ et $p \neq 7$ et $m = 6$ si $p = 7$

On constate ainsi que le théoreme 52 est bien une généralisation des congruences de Wostenholme (2.2) et de Morley(2.5).

En effet ces deux congruences se deduisent respectivement de (3.27) et (3.28) en observant qu'on a d'aprés (3.9) pour $m = 1$ et (3.8) pour $m = 2$

$$\sum_{k=1}^{p-1}\frac{1}{k} \equiv 0(\bmod p^2) \quad \text{et} \quad \sum_{1\le i<j\le p-1}\frac{1}{ij} \equiv 0(\bmod p), \;\; p \ge 5 \tag{3.29}$$

En déduisant d'apres le theoreme 52 et de (3.29) le corollaire suivant qui généralise aux p-entiers, la congruence de Glaisher (2.3).

Corollaire 54 *Pour tout p−entier α, on a*

$$\binom{\alpha p-1}{p-1} \equiv 1(\mathrm{mod}\, p^3) \quad p \geq 5 \tag{3.30}$$

On en deduit du theoreme 52 les deux relations suivantes

$$\binom{2p-1}{p-1} \equiv 1 - 2p\sum_{k=1}^{p-1}\frac{1}{k} + 4p^2 \sum_{1\leq i<j\leq p-1}\frac{1}{ij}(\mathrm{mod}\, p^6) \tag{3.31}$$

$$(-1)^{\frac{p-1}{2}}\binom{p-1}{\frac{p-1}{2}} \equiv 4^{p-1}\left(1 - \frac{5}{16}\sum_{k=1}^{p-1}\frac{1}{k} + \frac{1}{16}p^2\sum_{1\leq i<j\leq p-1}\frac{1}{ij}\right)(\mathrm{mod}\, p^6) \tag{3.32}$$

Comme on a

$$\sum_{1\leq i<j\leq p-1}\frac{1}{ij} = \frac{1}{2}\left(\sum_{k=1}^{p-1}\frac{1}{k}\right)^2 - \frac{1}{2}\sum_{k=1}^{p-1}\frac{1}{k^2}$$

On en déduit de (3.29) que

$$p^2\sum_{1\leq i<j\leq p-1}\frac{1}{ij} \equiv -\frac{1}{2}p^2\sum_{k=1}^{p-1}\frac{1}{k^2}(\mathrm{mod}\, p^6)$$

Corollaire 55 *Pour tout p-entier α, on a*

$$\binom{\alpha p-1}{p-1} \equiv 1 + \alpha(\alpha-1)p\sum_{k=1}^{p-1}\frac{1}{k}(\mathrm{mod}\, p^5) \quad p \geq 7 \tag{3.33}$$

$$\binom{\alpha p-1}{p-1} \equiv 1 - \frac{1}{2}\alpha(\alpha-1)p^2\sum_{k=1}^{p-1}\frac{1}{k^2}(\mathrm{mod}\, p^5) \quad p \geq 7 \tag{3.34}$$

Pour $\alpha = 2$ la relation (3.34) nous permet de retrouver la congruence de R.J McIntosh (2.9) et la relation (3.33) permet de retrouver la congruence de Zhao (2.10).

Bibliographie

[1] C. Aebi et G. Cairns, Sylvester's, Wolstenholme's, Morley's and lehmer's congruences theorems revisited, arXiv :1201.6559v4[math.HO] 2 Jul 2012.

[2] C. Babbage, « Demonstration of a theorem relating to prime numbers », The Edinburgh philosophical journal, vol. 1, 1819, p. 46–49.[2]

[3] F. Bencherif, La congruence dans l'anneau des p-entiers. Cours de post-graduation a l'école supérieure de Kouba (2011/2012).

[4] F. Bencherif, Amélioration d'une congruence d'Emma Lehmer, Congrès des Mathématiciens Algériens, CMA'2014, Tlemcen, 11-13 Mai 2014.

[5] André JOYAL, Les nombres de Bernoulli, 2003.

[6] Tom M. Apostol, Introduction to Analytic Number Theory, 1976, Springer-Verlag, New York, chap. 12.11.

[7] F. Bencherif et R. Boumahdi, Généralisation des congruences de Wolstenholme et de Morley, https ://arxiv.org/abs/1607.00700, 3 Jul 2016.

[8] G. Bisson, Autour des nombres et polynômes de Bernoulli (d'après un cours de Don Zagier) (2005/2006).

[9] Clausen, Thomas (1840), "Theorem", Astronomische Nachrichten 17 (22) : 351–352, doi :10.1002/asna.18400172204.

[10] L. Calitz, A theorem of Glaisher, Canadian J. Math.5 (1953), 306-316.

[11] A. Derbal, Nombres et polynômes de Bernoulli. Cours de post-graduation a l'école normale supérieure de Kouba (2011/2012).

[12] K. Dilcher, «Sums of reciprocals modulo composite integers ». Disponible sur <http ://www.cs.uleth.ca/~cnta2012/slides-cnta12/Karl-Dilcher.pdf >.

[13] L. EL Khiri, Sur certaines super-congruences dans l'anneau $\mathbb{Z}_{(p)}$, mémoire de Magister. ENS (2014).

[14] G-H Hardy, E-M Wright, An introduction to the theory of Numbers, (5th edition, collection "Oxfor Science Publications", Oxfor University Presss, Grande Bretagne, 1979. (first edition :1938).

[15] K. Irland and M. Rosen, A classical Introduction to modern numbres Theory (graduates texts in math. ;84),2nd ed.,Springer,New York,(1990).

[16] N. Jacobson, Basic Algebra I, 2nd Edition,W.H.Freeman Publishing company, New York,(1985).

[17] L. Khaldi, Etude de certaines propriétés des nombres et pollynômes de Bernoulli et d'Euler, mémoire de Magister. ENS (2013).

[18] E. Lehmer, On congruences involving Bernoulli numbers and the quotients of Fermat and Wilson, Annals of Mathematics. Second Series, 1938, Vol 39, pg 350-360.

[19] R. J. McIntosh, On the converse of Wolstenholme's Theorem, Acta Arith. 71 (1995), 381–389.

[20] R.J. McIntosh and E.L. Roettger, A search for Fibonacci-Wieferich and Wolstenholme primes, Math. Comp. 76 (2007), 2087–2094.

[21] R. Meštrović, Congruences for Wolstenholme prime, ArXiv.11O8.4178v1[Math.NT] (2011).

[22] R. Meštrović, On the mod p^7 determination of $\binom{2p-1}{p-1}$, la revue Rocky Mountain J. Math. Volume 44, Number 2 (2014), 633-648.

[23] R. Meštrović, Wolstenholme's theorem :its generalisations and extentions in the last hundred and fifty yearss (1862-2012), ArXiv 1111.3057v2[Math.NT] (2011).

[24] F. Morley, Note on the congruence $2^{4n}(-)^n(2n)!/(n!)^2$, where $2n+1$ is a prime, Annals of Mathematics, Vol 9, 1894/95, pg 168-170

[25] J. P. Margirier et C.Vadot Nickel : le DEUG dans la poche et la prépa sans stress ISBN 2711724786.Vuibert supèrier

[26] H. Pan, On a generalization of Carlitz's congruence, Int. J. Mod. Math.4 (2009), 87–93.

[27] von Staudt, Ch. (1840), "Beweis eines Lehrsatzes, die Bernoullischen Zahlen betreffend", Journal für Reine und Angewandte Mathematik 21 : 372–374, ISSN 0075-4102, JFM 021.0672cj

[28] Cheung Park-Hong,Ko Tsz-Mel,Leung Tat-Wing,Li Kin-Yin et NG Keng-Po Roger. Mathematical Excalibur,Volume 16,Number1 (2011).

[29] Z. H. Sun, Congruence for Bernoulli numbers and Bernoulli polynomials. Discrete Mathematics 163 (1997). 153-163

[30] Z. H. Sun, Congruences concerning Bernolli numbers and Bernoulli polynomials, Discrete applied Mathematics 105 (1-3) :193-223 (2000).

[31] Z. W. Sun et R.Tauraso, New congruences for central binomial coefficients, Adv. in Applied Mathematics 45,125-148.(2010).

[32] J. J. Sylvester, Note relative aux communications faites dans les séances du 28 Janvier et 4 Février 1861. C. R. Acad. Sci. Paris, Vol 52, 1861, pg 307-308.

[33] R. Tauraso, More congruences for central binomial coefficients,J, Nomber Theory 130 (2010), 2639-2649.

[34] R. Tauraso, Private correspondence, November 2011.

[35] J. Wolstenholme, On certain properties of prime numbers, Quart.J.Appl.Math.5, 35-39 (1862).

[36] J. Zhao, Bernoulli numbers, Wolstenholme's Theorem , and p^5 Variations of Lucas' Theorem, J. Number theory 123 (2007), 18-26