N^{0}= 10/2015 – M/MT

REPUPLIQUE ALGÉRIENNE DEMOGRATIQUE ET POPULAIRE
MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET LA RECHERCHE SCIENTIFIQUE
UNIVERSITE DES SCIENCES ET DE LA TECHNOLOGIE HOUARI BOUMEDIENE
FACULTÉ DE MATHÉMATIQUES

MÉMOIRE

Présenté pour l'obtention du diplôme de MAGISTER

EN MATHÉMATIQUES

Spécialité : Arithmétique, Codage et Combinatoire : Théorie des nombres

Par

BOUNEBIRAT Fouad

Sujet :

Autour des quotients de Fermat

Soutenu publiquement le 19/02/2015, devant le jury composé de :

M. BENSBAA Boualem	Maitre de Conférence / A,	à l'USTHB	Président
M.BENCHERIF Farid	Professeur,	à l'USTHB	Directeur de mémoire
Mme. CHERCHEM Leila	Maitre de Conférence / A,	à l'USTHB	Examinatrice

Table des matières

Remerciements

Je remercie mon directeur de mémoire, monsieur le professeur Bencherif Farid pour l'intéressant sujet de mémoire qu'il m'a proposé.

Je remercie madame la professeure Cherchem Leïla et monsieur le professeur Benseba pour avoir bien voulu examiner ce mémoire et faire partie du Jury de soutenance.

Je suis particulièremant honoré que monsieur le professeur Benseba ait aussi accepté de présider ce Jury.

Notations

1. $\mathbb{N}$: ensemble des nombres entiers naturels.
2. $\mathbb{N}^*$: ensemble des nombres entiers naturels non nuls.
3. $\mathbb{Z}$: ensemble des nombres entiers relatifs .
4. $\mathbb{Q}$: ensemble des nombres rationnels.
5. $\mathbb{R}$: ensemble des nombres réels.
6. $\mathbb{C}$: ensemble des nombres complexes.
7. La lettre p désigne toujours un nombre premier (sauf mention contraire).
8. $\binom{n}{k}$ coefficient binomial, où n et k deux entiers où $0 \leq k \leq n$.
9. (a, b) désigne le plus grand commun diviseur de a et b $((pgcd(a, b))$, a et b étant des entiers.
10. $a \mid b$ où a et b sont deux entiers signifie : " a divise b ".
11. $a \nmid b$ où a et b sont deux entiers signifie : " a ne divise pas b ".
12. $\mathbb{Z}_n$ désigne l'anneau des n-entiers, un n- entier étant un nombre rationnel dont le dénominateur est premier avec $n \in \mathbb{N}$.
13. $\mathbb{Z}_p$ désigne l'anneau des p-entiers, p étant un nombre premier, un p-entier est alors un nombre rationnel dont le dénominateur est premier avec p.
14. $H_n := 1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n}$ le $n - ième$ nombre harmonique.
15. $q_p(a)$ quotient de Fermat défini pour p premier et pour $a \in \mathbb{Z} - p\mathbb{Z}$ par : $q_p(a) = \frac{a^{p-1}-1}{p}$.
16. w_p quotient de Wilson défini pour $p \in \mathbb{Z}$ par $w_p = \frac{(p-1)!+1}{p}$.
17. φ fonction indicatrice d'Euler.
18. 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 est congru à b modulo n.
19. 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.

Introduction

Ce mémoire est consacré à une étude approfondie de nombreux articles concernant des propriétés des quotients de Fermat. Rappelons que pour un nombre premier p et un entier a non divisible par p, on appelle quotient de Fermat le nombre $q_p(a)$ exprimé par la formule suivante :

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

On sait, d'après le petit théorème de Fermat que $q_p(a) \in \mathbb{Z}$.

Cette étude est composé de quatre chapitres que nous allons détailler successivement.

Le premier chapitre de ce mémoire est consacré à des rappels utiles à la compréhension des articles qu'on étudie aux chapitres 3 et 4. Dans ce chapitre, nous commençons par rappeler de nombreuses définitions et propriétés des coefficients binomiaux et des congruences définies sur un anneau commutatif. Nous étudions plus particulièrement les propriétés des congruences définies dans l'anneau $\mathbb{Z}_{(p)}$ des p-entiers et plus précisément des congruences concernant des sommes comportant des sommes harmoniques.

Dans le deuxieme chapitre, nous nous intéressons à l'étude du quotient de Fermat en base $a = 2$,

$$q_p(2) = \frac{2^{p-1} - 1}{p} \in \mathbb{Z}.$$

Nous prouvons certains resultats célèbres concernant des nombres harmoniques tels que celui découvert par Eisenstien, en 1850. Nous étudions de nombreuses propriétés du quotient de Fermat telles que la relation suivante qui lie le quotient de Wilson à une somme de quotients de Fermat

$$\sum_{a=1}^{p-1} q_p(a) \equiv w_p \pmod{p}.$$

Dans ce chapitre, nous rappelons aussi le célèbre critère établi en 1909 par Wieferich[24] concernant le premier cas du dernier théorème de Fermat :

$$(p \nmid xyz \quad \text{et} \quad x^p + y^p + z^p = 0\ ) \quad \Longrightarrow \quad \frac{2^{p-1} - 1}{p^2} \in \mathbb{Z}.$$

Les deux derniers chapitres de ce mémoire sont consacrés à l'étude de trois articles. Plus précisément, le troisième chapitre est une étude approfondie de la congruence suivante :

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

Nous y prouvons la relation précédente en détaillant les preuves données de ce résulat dans deux articles différents, le premier article étant celui d'Andrew Granville [10]intitulé : " The square of the Fermat quotient" et le deuxiéme étant celui de Romeo Mestrovic [17] intitulé : " An elementary proof of congruence by Skula and Granville".

Enfin au quatrième et dernier chapitre de ce mémoire, nous détaillons la preuve de la congruence suivante donnée en 2006 par Karl Dilcher et Ladislav Skula dans leur article [6] intitulé "The cube of the Fermat quotient" :

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

Signalons que cette dernière congruence est équivlente à la congruence suivante :

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

Chapitre 1

Généralités

1.1 Introduction

Ce chapitre est consacré à de nombreux rappels. Nous commençons par rappeler la définition et les propriétés des coefficients binomiaux. Nous étudions ensuite l'anneau des n-entiers $\mathbb{Z}_{(n)}$ et certaines propriétés de cet anneau. Nous précisons la notion de p-entier et la définition des congruences dans l'anneau $\mathbb{Z}_{(p)}$. Nous étudions plus particulièrement les congruences modulo p et modulo p^2 pour les nombres harmoniques d'indice $p-1$.

Dans tout ce qui suit, nous désignons par $\mathbb{K}$ l'un des corps $\mathbb{Q}$, $\mathbb{R}$ ou $\mathbb{C}$ et par A un anneau non nécessairement commutatif.

1.2 Coefficients binomiaux

1.2.1 Définition et propriétés

Pour tous entiers naturels n et k, on définit le coefficient binomial $\binom{n}{k}$ de manière suivante

$$\binom{n}{k} = \begin{cases} \frac{\alpha(\alpha-1)(\alpha-2)\ldots(\alpha-k+1)}{k!} & pour \quad n \geq k, \\ 0 & pour \quad k > n. \end{cases}$$

Rappelons la formule du binôme qui affirme que si a et b sont deux éléments d'un anneau qui commutent, alors pour tout entier $n \in \mathbb{N}$, on a

$$\forall n \in \mathbb{N} \quad (a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k.$$

Les coefficients binomiaux vérifient les propriétés suivantes et le théorème rappelé ci-dessous, nous sera utile aux chapitres 2 et 3.

Théorème 1 *Pour tous entiers naturels n et k, on a*

1. *Pour $n \geq k \geq 0$,*
$$\binom{n}{k} = \binom{n}{n-k}. \tag{1.1}$$
2. *Pour $n \geq k \geq 0$,*
$$\frac{1}{n}\binom{n}{k} = \frac{1}{k}\binom{n-1}{k-1}. \tag{1.2}$$
3. *Pour tous entiers naturels n, k et j tel que $n \geq k$, on a*
$$\sum_{j=k}^{n} \binom{j}{k} = \binom{n+1}{k+1}. \tag{1.3}$$

Preuve.

1. Pour tous entiers naturels n et k tel que $0 \leq k \leq n$, on a
$$\binom{n}{k} = \frac{n!}{k!(n-k)!} = \frac{n!}{(n-k)!(n-(n-k))!} = \binom{n}{n-k}.$$
2. Pour tous entiers naturels n et k tel que $n \geq k$, on a
$$\begin{aligned}\frac{1}{n}\binom{n}{k} &= \frac{1}{n}\frac{n!}{(n-k)!k!} = \frac{1}{n}\frac{n(n-1)!}{(n-k)!k(k-1)!} \\ &= \frac{1}{k}\frac{(n-1)!}{(k-1)!(n-1-(k-1))!} = \frac{1}{k}\binom{n-1}{k-1}.\end{aligned}$$
3. Nous allons prouver (1.3) en raisonnant par récurrence sur n, qu'on a :
   - Pour $n = k$, on a : $\sum_{j=k}^{n} \binom{j}{k} = \binom{k}{k} = 1$ et $\binom{k+1}{k+1} = 1$, donc la formule est vrai pour $n = k$.
   - Supposons la formule vraie pour $n \in \mathbb{N}$ fixé tel que $n \geq k$.
     On a alors :
$$\begin{aligned}\sum_{j=k}^{n+1} \binom{j}{k} &= \sum_{j=k}^{n} \binom{j}{k} + \binom{n+1}{k} \\ &= \binom{n+1}{k+1} + \binom{n+1}{k} \\ &= \binom{(n+1)+1}{k+1},\end{aligned}$$
     ce qui montre la formule est vraie pour $n+1$. On conclut, par récurrence sur n, que pour tout $(n,k) \in \mathbb{N}^2$ tel que $n \geq k$, on a $\sum_{j=k}^{n} \binom{j}{k} = \binom{n+1}{k+1}$.

Ce qui établit par récurrence la relation (1.3). □

1.3 Etude de l'anneau $\mathbb{Z}_{(n)}$ des n-entiers

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

Pour tout entier rationnel x, où $x = \frac{a}{b}$ avec $a \in \mathbb{Z}$ et $b \in \mathbb{Z}^*$, définissons "le dénominateur" de x, noté dénom(x) et le numérateur" de x, noté num(x) par :

$$a = \text{dénom}(x) \quad \text{et} \quad b = \text{num}(x).$$

Dans le cas où a et b sont premiers entre eux, x s'écrit de manière unique sous la forme (appelée forme réduite de x).

Définition 2 *Pour tout entier $n \geq 2$, on appelle n-entier tout nombre rationnel dont le dénominateur est premier avec n. On désigne par $\mathbb{Z}_{(n)}$ l'ensemble des n-entiers. Autrement dit :*

$$\mathbb{Z}_{(n)} = \{\ x \in \mathbb{Q}\ /\quad pgcd(n, dénom(x)) = 1\ \}.$$

Remarquons que pour qu'un nombre rationnel $x \in \mathbb{Z}_{(n)}$, il faut et il suffit qu'il puisse s'écrire comme le quotient de deux entiers a et b, $x = \frac{a}{b}$ avec $\text{pgcd}(n, b) = 1$, $\frac{a}{b}$ n'étant pas nécessairement la forme irréductible de x. Cette propriété permet de prouver facilement les propriétés de $\mathbb{Z}_{(n)}$ données dans le théorème suivant :

Théorème 3 .

1. *L'ensemble $\mathbb{Z}_{(n)}$ est un sous-anneau de $\mathbb{Q}$.*
2. *$\mathbb{Z} \subset \mathbb{Z}_{(n)}$.*
3. *$\mathbb{Z}_{(n)}$ est un anneau principal. De plus :*
   - *Pour $n \geq 2$, les idéaux non nuls de $\mathbb{Z}_{(n)}$ sont les $m\mathbb{Z}$ où $m = q_1^{\alpha_1} q_2^{\alpha_2} ... q_r^{\alpha_r}$, $q_1, q_2, ..., q_r$, désignent les diviseurs premiers avec n, $\alpha_1, \alpha_2, ..., \alpha_r$ étant des entiers naturels,*
4. *Le groupe des unités de l'anneau $\mathbb{Z}_{(n)}$ est*

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

La preuve du théorème précédent est bien détaillée dans le mémoire, de R. Chellal dirigé par le professeur F. Bencherif [5].

Le corollaire suivant est un cas particulier du théorème (3).

Corollaire 4 *[3]Pour $n = p$, p étant un nombre premier,*

$$\mathbb{Z}_{(p)} = \left\{x \in \mathbb{Q} \quad / \ p \text{ ne divise pas dénom}(x)\ \right\},$$
$$U(\mathbb{Z}_{(p)}) = \left\{x \in \mathbb{Q} \quad / \ p \nmid \ num(x) \ \ et\ p \nmid \ dénom(x)\right\}.$$

De plus $\mathbb{Z}_{(p)}$ est un anneau principal et tout idéal non nul de $\mathbb{Z}_{(p)}$ sont les $p^m\mathbb{Z}_{(p)}$, où m un entier naturel.

1.4 Congruences dans $\mathbb{Z}$ et dans $\mathbb{Z}_p$

1.4.1 Congruences dans $\mathbb{Z}$

On sait que tout idéal I de $\mathbb{Z}$ peut s'écrire $I = m\mathbb{Z}$, où m est un entier naturel. La congruence modulo l'idéal $m\mathbb{Z}$ s'énonce ainsi, x et y étant deux entiers :

$$x \equiv y \pmod{m} \Longleftrightarrow x - y \in m\mathbb{Z}.$$

Nous allons maintenant rappeler les principaux théorèmes classiques d'arithmétique : Théorème de Wilson, de Fermat, d'Euler.

Théorème de Wilson

Ibn al-Haytham (Bassorah, 965 -Le Caire, 1039) est un mathématicien, philosophe et physicien d'origine Perse. C'est le premier mathématicien connu pour avoir énoncer le théorème suivant appelé théorème de Wilson.

Théorème 5 *[20] Pour tout nombre premier $p \geq 2$, on a l'équivalence suivante :*

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

Théorème de Fermat

Le théorème suivant est appelé " petit théorème de Fermat", il date de 1640.

Théorème 6 *[20]Pour tout nombre premier p et pour tout entier a premier avec p, on a*

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

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

$$a^p \equiv a \pmod{p} \quad \text{pour } p \text{ premier et } a \in \mathbb{Z}\cdot$$

Théorème d'Euler

Le théorème d'Euler qui suit est une généralisation du petit théorème de Fermat. Ce théorème fait intervenir la fonction indicatrice phi d'Euler notée φ. Cette fonction est définie pour tout entier $n \geq 1$ par

$$\varphi(n) = \operatorname{card}\{a \in \mathbb{N} : a < n \text{ et } (a, n) = 1\},$$

$\varphi(n)$ s'appelle aussi l'indicateur d'Euler de n. Le théorème établi en 1760 par Euler s'énonce alors comme suit :

Théorème 7 *[8] Pour tout entier $n \geq 2$, et pour $a \in \mathbb{Z}$, on a*

$$(a, n) = 1 \Longrightarrow a^{\varphi(n)} \equiv 1 \pmod{n},$$

avec

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

1.4.2 Congruences dans $\mathbb{Z}_p$ des p-entiers

Les idéaux de $\mathbb{Z}_{(p)}$ sont les $p^m\mathbb{Z}_{(p)}$, où m un entier naturel ; la congruence modulo l'déal $p^m\mathbb{Z}_{(p)}$ s'énonce ainsi : x et y étant deux p-entiers, on a :

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

Nous allons établir maintenant un important théorème de congruence :

Théorème 8 *Pour tout nombre premier $p \geq 3$, on a*

$$1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{p-1} \equiv 0 \pmod{p}. \tag{1.4}$$

Preuve. On a

$$\begin{aligned} 1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{p-1} &= \sum_{k=1}^{\frac{p-1}{2}} \left(\frac{1}{k} + \frac{1}{p-k}\right), \\ &= p \sum_{k=1}^{\frac{p-1}{2}} \frac{1}{k(p-k)}, \end{aligned} \tag{1.5}$$

pour $1 \leq k \leq \frac{p-1}{2}$, on a $\frac{1}{k(p-k)} \in \mathbb{Z}_{(p)}$ et donc $\sum_{k=1}^{\frac{p-1}{2}} \frac{1}{k(p-k)} \in \mathbb{Z}_{(p)}$.Il résulte de la relation (1.5) que l'on a bien $1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{p-1} \in p\mathbb{Z}_{(p)}$.
La relation (1.4) est prouvée. □

Nous allons maintenant établir des congruences modulo p et modulo p^2 concernant les nombres harmoniques et des sommes particulières dans l'anneau $\mathbb{Z}_p$ des p-entiers.

Pour cela on commence par étudier des congruences modulo p sur les sommes de puissances $\sum_{k=0}^{p-1} k^m$. Les congruences obtenues vont nous permettre de prouver de nombreux résultats dans ce mémoire.

Théorème 9 *Pour tout nombre premier $p \geq 3$ et pour tout entier $m \in \mathbb{Z}$, on a*

$$1^m + 2^m + ... + (p-1)^m \equiv \begin{cases} -1 & si \quad p-1 \mid m, \\ 0 & si \quad p-1 \nmid m. \end{cases} \tag{1.6}$$

Pour prouver ce théorème, on va utiliser les deux propriétés suivantes :

- Le corollaire du petit théorème de Fermat ; pour p premier et pour $m \in (p-1)\mathbb{Z}$, on a pour tout entier k tel que $1 \leq k \leq p-1$
$$(p-1) \text{ divise } m \Longrightarrow k^m \equiv 1 \pmod{p}$$
- Le groupe multiplicatif $(\mathbb{Z}/p\mathbb{Z})^*$ est cyclique [12].

Preuve.

- Si $p-1 \mid m$. On a alors :
$$1^m + 2^m + ... + (p-1)^m \equiv 1 + 1 + ... + 1 = p - 1 \equiv -1 \pmod{p}.$$
- Si $p-1 \nmid m$. Soit alors g un entier tel que $\bar{g}$ engendre $(\mathbb{Z}/p\mathbb{Z})^*$ on a $g^m - 1 \not\equiv 0 \pmod{p}$ et
$$\begin{aligned} 1^m + 2^m + ... + (p-1)^m &\equiv 1 + g^m + (g^2)^m + ... + (g^{p-2})^m \\ &= 1 + g^m + (g^m)^2 + ... + (g^m)^{p-2} \\ &= \frac{(g^m)^{p-1} - 1}{g^m - 1} \\ &= \frac{(g^{p-1})^m - 1}{g^m - 1} \\ &\equiv 0 \pmod{p}. \end{aligned}$$

Le théorème (9) est prouvé. □

Théorème de Wolstenholme et congruences modulo p pour $\sum_{k=1}^{p-1} \frac{1}{k^m}$.

En 1862, Joseph Wolstenholme (1829- 1891) a énoncé le résultat suivant :

Théorème 10 *[25]Pour tout nombre premier $p \geq 5$, on a*

$$\sum_{k=1}^{p-1} \frac{1}{k} \equiv 0 \ (\mathrm{mod} p^2) \tag{1.7}$$

Preuve. On a pour $p \geq 5$ et en exploitant les deux théorèmes (8) et (9) qu'on vient de prouver :

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

La relation (1.7) est prouvée. □

Théorème 11 *[13] On a pour tout nombre premier p impair et pour $m \in \mathbb{N}$, on a*

$$\sum_{k=1}^{p-1} \frac{1}{k^m} \equiv \begin{cases} -1 & si \quad p-1 \mid m, \\ 0 & si \quad p-1 \nmid m. \end{cases} \tag{1.8}$$

Preuve.

- Si $p-1 \mid m$, on a d'après le petit théorème de Fermat :$k^m \equiv 1 \pmod{p}$ pour $1 \leq k \leq p-1$ et comme k^m est une unité de $\mathbb{Z}_p$, on a aussi $\frac{1}{k^m} \equiv 1-p \equiv -1 \pmod{p}$ ce qui implique $\sum_{k=1}^{p-1} \frac{1}{k^m} \equiv p-1 \equiv -1 \pmod{p}$.
- Si $p-1 \nmid m$. Considérons g comme une racine primitive modulo p. On sait qu'on a alors $g^l \equiv 1 \pmod{p}$si et seulement si $p-1 \mid l$. Ainsi $g^m \not\equiv 1 \pmod{p}$ Notons que l'ensemble $\{g, 2g, \ldots, (p-1)\, g\}$ est équivalent modulo p à l'ensemble $\{1, 2, \ldots, (p-1)\}$. Ainsi nous obtenons

$$\left(\frac{1}{g^m} - 1\right) \sum_{k=1}^{p-1} \frac{1}{k^m} = \sum_{k=1}^{p-1} \frac{1}{(gk)^m} - \sum_{k=1}^{p-1} \frac{1}{k^m} \equiv \sum_{k=1}^{p-1} \frac{1}{k^m} - \sum_{k=1}^{p-1} \frac{1}{k^m} = 0 \pmod{p},$$

et comme $\frac{1}{g^m} - 1 = \frac{1-g^m}{g^m} \not\equiv 0 \pmod{p}$, nous en déduisons : $\sum_{k=1}^{p-1} \frac{1}{k^m} \equiv 0 \pmod{p}$.

□

Chapitre 2

Le quotient de Fermat

2.1 Introduction

Dans ce chapitre, nous commençons tout d'abord par énoncer la définition des quotients de Fermat, nous citons ensuite quelques propriétés importantes : propriétés de Gotthold Max Eisenstein ([7], 1850), propriétés des quotients de Fermat et des quotients de Wilson([21], 1905) et le critère de Wieferich([24] ,1909) pour le premier cas du dernier théorème de Fermat.

2.2 Définition des quotients de Fermat

Définition 12 *Pour tout nombre premier p et pour tout entier $a \in \mathbb{Z}$ tel que $(a,p) = 1$ on définit $q_p(a)$ le quotient de Fermat en base a par*

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

On sait, d'après le petit théorème de Fermat que $q_p(a) \in \mathbb{Z}$.

A l'aide de cette définition nous pouvons calculer les congruences suivantes pour les valeurs de a. On trouve

$$q_p(1) \equiv 0 \pmod{p}.$$
$$q_p(-a) \equiv q_p(a) \pmod{p}.$$

Notation 13 *q_a est fonction de p. On note aussi $q_p(a)$ quand cela est nécéssaire.*

2.3 Propriétés des quotients de Fermat

2.3.1 Propriétés de Gotthold Max Eisenstein

1. En 1850, Gotthold Max Eisenstein(1823-1852)[7], énonça et démontra les propriétés suivantes :

$$q_p(a-1) \equiv 1 \pmod{p}. \tag{2.1}$$
$$q_p(a+1) \equiv -1 \pmod{p}. \tag{2.2}$$
$$q_p(a+p) \equiv q_p(a) - \frac{1}{a} \pmod{p}. \tag{2.3}$$

Nous citons les propriétés apparentées au logarithme :

$$q_p(a^r) \equiv r q_p(a) \pmod{p}. \tag{2.4}$$
$$q_p(\frac{1}{a}) \equiv -q_p(a) \pmod{p}. \tag{2.5}$$
$$q_p(\frac{a}{b}) \equiv q_p(a) - q_p(b) \pmod{p}. \tag{2.6}$$
$$q_p(ab) \equiv q_p(a) + q_p(b) \pmod{p}. \tag{2.7}$$

2. G. Eisenstein établit aussi que le quotient de Fermat $q_2 = \frac{2^{p-1}-1}{p}$ peut s'exprimer comme une somme faisant intervenir les inverses des entiers compris entre 1 et $p-1$,

$$q_p(2) \equiv \frac{1}{2} \sum_{k=1}^{p-1} \frac{(-1)^{k-1}}{k} \pmod{p}. \tag{2.8}$$
$$q_p(2) \equiv -\frac{1}{2} \sum_{k=1}^{\frac{p-1}{2}} \frac{1}{k} \pmod{p}. \tag{2.9}$$

On peut aussi citer[4] :

$$q_p(2) \equiv \sum_{\substack{1 \le k \le p-1 \\ k \nmid 2}} \frac{1}{k} \pmod{p}. \tag{2.10}$$
$$q_p(2) \equiv \frac{1}{2} \sum_{k=\frac{p+1}{2}}^{p-1} \frac{1}{k} \pmod{p}. \tag{2.11}$$

3. On a aussi les propriétés suivantes dues à Dmitry Mirimanoff (1895)[18] :

$$q_p(a+np) \equiv q_p(a) - n\frac{1}{a} \pmod{p}. \tag{2.12}$$
$$q_p(a+np^2) \equiv -q_p(a) \pmod{p}. \tag{2.13}$$

La preuve des relations

Relation(2.1). On a

$$\begin{aligned} q_p(p+1) &= \frac{(p+1)^{p-1}-1}{p} \\ &= (p-1)+\sum_{k=2}^{p-1}\binom{p-1}{k}p^{k-1} \\ &= -1+p+p\sum_{k=2}^{p-1}\binom{p-1}{k}p^{k-2} \\ &\equiv -1 \pmod{p}, \quad \text{ce qui établit (2.1).} \end{aligned}$$

Relation(2.2). La preuve de cette relation est analogue à la preuve de (2.1).

Relation(2.3). On sait, d'après le petit théorème de Fermat et comme $a \nmid p$, on peut écrire :

$$\begin{aligned} q_p(a+p) &= \frac{(a+p)^{p-1}-1}{p} \\ &= \frac{a^{p-1}-1+p\binom{p-1}{1}a^{p-2}+\sum_{k=2}^{p-1}\binom{p-1}{k}a^{p-1-k}p^k}{p} \\ &= q_p(a)-a^{p-2}+pa^{p-2}+\sum_{k=2}^{p-1}\binom{p-1}{k}a^{p-1-k}p^{k-1} \\ &= q_p(a)-\frac{a^{p-1}}{a}+p.\left(a^{p-2}+\sum_{k=2}^{p-1}\binom{p-1}{k}a^{p-1-k}p^{k-2}\right) \\ &\equiv q_p(a)-\frac{1}{a} \pmod{p}, \quad \text{ce qui établit (2.3).} \end{aligned}$$

Relation(2.4). D'après le petit théorème de Fermat $a^{p-1} \equiv 1 \pmod{p}$, on a

$$\begin{aligned} q_p(a^r) &= \frac{(a^r)^{p-1}-1}{p} = \frac{(a^{p-1})^r-1}{p} \\ &= \frac{(a^{p-1}-1)((a^{p-1})^{r-1}+(a^{p-1})^{r-2}+\cdots+1)}{p} \\ &= q_p(a)\left((a^{p-1})^{r-1}+(a^{p-1})^{r-2}+\cdots+1\right) \\ &\equiv q_p(a)\left((1)^{r-1}+(1)^{r-2}+...+1\right) \\ &= q_p(a)(1+1+...+1) \\ &= r.q_p(a) \pmod{p}, \quad \text{ce qui établit (2.4).} \end{aligned}$$

Relation(2.5). D'après la définition même des quotients de Fermat, on a $a^{p-1} = pq_p(a)+1$. Il en résulte que :

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

alors :

$$\frac{1}{a^{p-1}} = \frac{1 - pq_p(a)}{(1 - p^2 q_p(a)^2)}, \tag{2.14}$$

en ajoutant (-1) aux deux membres de (2.14), on en conclut

$$\left(\frac{1}{a}\right)^{p-1} - 1 = \frac{-pq_p(a) + p^2 q_p(a)}{1 - p^2 q_p(a)^2}, \tag{2.15}$$

en divisant par p les deux membres de (2.15), on obtient

$$\begin{aligned} q_p(1/a) &= \frac{q_p(a)(p-1)}{1 - p^2 q_p(a)^2}, \\ &\equiv -q_p(a) \pmod{p}, \quad \text{ce qui établit (2.5).} \end{aligned}$$

Relation(2.6). D'après la définition même des quotients de Fermat, on a $a^{p-1} = pq_p(a) + 1$ et $b^{p-1} = pq_p(b) + 1$. Il en résulte que :

$$\begin{aligned} \left(\frac{a}{b}\right)^{p-1} &= \frac{pq_p(a) + 1}{pq_p(b) + 1} = \left(\frac{pq_p(a) + 1}{pq_p(b) + 1}\right)\left(\frac{1 - pq_p(b)}{1 - pq_p(b)}\right) \\ &= \frac{pq_p(a) - pq_p(b) - p^2 q_p(a) q_p(b) + 1}{1 - p^2 q_p(b)^2}, \end{aligned}$$

alors :

$$\left(\frac{a}{b}\right)^{p-1} = \frac{pq_p(a) - pq_p(b) - p^2 q_p(a) q_p(b) + 1}{1 - p^2 q_p(b)^2}, \tag{2.16}$$

en ajoutant (-1) aux deux membres de (2.16), on trouve

$$\left(\frac{a}{b}\right)^{p-1} - 1 = \frac{pq_p(a) - pq_p(b) - p^2 q_p(a) q_p(b) + p^2 q_p(b)}{1 - p^2 q_p(b)^2}, \tag{2.17}$$

en divisant par p les deux membres de (2.17), on trouve

$$\begin{aligned} q_p\left(\frac{a}{b}\right) &= \frac{q_p(a) - q_p(b) - pq_p(a) q_p(b) + pq_p(b)}{1 - pq_p(b)^2} \\ &\equiv q_p(a) - q_p(b) \pmod{p}, \quad \text{ce qui établit (2.6).} \end{aligned}$$

Relation(2.7). D'après la définition même des quotients de Fermat, on a $a^{p-1} = pq_p(a) + 1$ et $b^{p-1} = pq_p(b) + 1$. Il en résulte que :

$$(ab)^{p-1} = p^2 q_p(a) q_p(b) + pq_p(a) + pq_p(b) + 1, \tag{2.18}$$

en ajoutant (-1) aux deux membres de (2.18), on obtient

$$(ab)^{p-1} - 1 = p^2 q_p(a) q_p(b) + q_p(a) + q_p(b), \tag{2.19}$$

et en divisant par p les deux membres de (2.19), on trouve

$$\begin{aligned} q_p(ab) &= pq_p(a)q_p(b) + pq_p(a) + pq_p(b) \\ &\equiv q_p(a) + q_p(b) \pmod{p}, \qquad \text{ce qui établit (2.7).} \end{aligned}$$

Relation(2.8). On a, $2^p = (1+1)^p = \sum_{k=0}^{p} \binom{p}{k} = \sum_{k=1}^{p-1} \binom{p}{k} + 2$ alors $2^p - 2 = \sum_{k=1}^{p-1} \binom{p}{k}$, d'où l'on éduit : $q_2 = \frac{1}{2.p} \sum_{k=1}^{p-1} \binom{p}{k}$, alors on peut écrire :

$$q_p(2) = \frac{1}{2.p} \sum_{k=1}^{p-1} \binom{p}{k} = \frac{1}{2} \sum_{k=1}^{p-1} \frac{(p-1)(p-2)...(p-(k-1))}{k.1.2...(k-1)},$$

pour $p \neq 2$, donc $\forall p \geq 3$. On a

$$\begin{aligned} &\equiv \frac{1}{2} \sum_{k=1}^{p-1} \frac{(-1)(2)...(k-1)}{1.2...(k-1)k} \pmod{p}, \\ &\equiv \frac{1}{2} \sum_{k=1}^{p-1} \frac{(-1)^{k-1}}{k} \pmod{p}, \qquad \text{ce qui établit (2.8).} \end{aligned}$$

Relation(2.9). En exploitant (2.8) et en ajoutant aussi la quantité nulle : $-\frac{1}{2} \sum_{k=1}^{p-1} \frac{1}{k} \equiv 0 \pmod{p}$ tel que $p \neq 2$, on obtient

$$\begin{aligned} q_p(2) &\equiv \frac{1}{2}\left(\frac{1}{1} - \frac{1}{2} + ... - \frac{1}{p-1}\right) - \frac{1}{2}\left(\frac{1}{1} + \frac{1}{2} + ... + \frac{1}{p-1}\right) \\ &\equiv \left(-\frac{1}{2} - \frac{1}{4} - ... - \frac{1}{(p-1)}\right) = -\frac{1}{2}\left(\frac{1}{1} + \frac{1}{2} + ... + \frac{1}{(p-1)/2}\right) \\ &\equiv -\frac{1}{2} \sum_{k=1}^{\frac{p-1}{2}} \frac{1}{k} \pmod{p}, \quad \text{ce qui établit (2.9).} \end{aligned}$$

Relation(2.10). En exploitant (2.8) et en ajoutant aussi la quantité nulle : $\frac{1}{2} \sum_{k=1}^{p-1} \frac{1}{k} \equiv 0 \pmod{p}$ tel que $p \neq 2$, on obtient

$$\begin{aligned} q_p(2) &\equiv \frac{1}{2}\left(\frac{1}{1} - \frac{1}{2} + \frac{1}{3} + ... - \frac{1}{p-1}\right) + \frac{1}{2}\left(\frac{1}{1} + \frac{1}{2} + \frac{1}{3} + ... + \frac{1}{p-1}\right) \\ &\equiv \left(\frac{1}{1} + \frac{1}{3} + \frac{1}{5} + ... + \frac{1}{(p-2)}\right) \\ &\equiv \sum_{\substack{1 \leq k \leq p-1 \\ k \nmid 2}} \frac{1}{k} \pmod{p}, \quad \text{ce qui établit (2.10).} \end{aligned}$$

Relation(2.11). En écrivant la relation (2.9) sous la forme : $q_p(2) \equiv \sum_{k=1}^{p-1} \frac{1}{k} - \sum_{k=(p+1)/2}^{p-1} \frac{1}{k}$, on obtient :

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

Si $p \neq 2$, on a la quantité : $-\frac{1}{2}\sum_{k=1}^{p-1} \frac{1}{k} \equiv 0 \pmod p$ est nulle. On peut donc écrire :

$$q_p(2) \equiv \frac{1}{2}\sum_{k=(p+1)/2}^{p-1} \frac{1}{k} \pmod p, \quad \text{ce qui établit (2.11).}$$

Relation(2.12). On a

$$\begin{aligned} q_p(a+np) &= \frac{(a+np)^{p-1}-1}{p} \\ &= \frac{\sum_{k=0}^{p-1} \binom{p-1}{k} a^{p-1-k}(np)^k - 1}{p} \\ &= \frac{a^{p-1} - 1 + np(p-1)a^{p-2} + np\sum_{k=2}^{p-1} \binom{p-1}{k} a^{p-1-k}(np)^{k-1}}{p} \\ &= q_p(a) - n\frac{a^{p-1}}{a} + pna^{p-2} + pn^2 \sum_{k=2}^{p-1} \binom{p-1}{k} a^{p-1-k}(np)^{k-2} \\ &\equiv q_p(a) - n\frac{1}{a} \pmod p, \quad \text{ce qui établit (2.12).} \end{aligned}$$

Relation(2.13). On a

$$\begin{aligned} q_p(a+np^2) &= \frac{(a+np^2)^{p-1}-1}{p} \\ &= \frac{\sum_{k=0}^{p-1} \binom{p-1}{k} a^{p-1-k}(np^2)^k - 1}{p} \\ &= \frac{a^{p-1} - 1 + np^2\sum_{k=1}^{p-1} \binom{p-1}{k} a^{p-1-k}(np^2)^{k-1}}{p} \\ &= q_p(a) + np\sum_{k=2}^{p-1} \binom{p-1}{k} a^{p-1-k}(np^2)^{k-1} \\ &\equiv q_p(a) \pmod p, \quad \text{ce qui établit (2.13).} \end{aligned}$$

2.3.2 Propriétés des quotients de Fermat et des quotients de Wilson

Définition 14 *Pour tout nombre premier p, on appelle quotient de Wilson le nombre entier w_p défini par*

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

En 1905, M. Lerch [21] énonça et démontra le théorème suivant :

Théorème 15 *Pour tout nombre premier p impair, on a*

$$\sum_{k=1}^{p-1} q_k \equiv w_p \pmod{p}. \tag{2.20}$$

Preuve.
Nous allons calculer le nombre $((p-1)!)^{p-1}$ modulo p^2, par deux méthodes différentes :

– La premiere méthode se base sur la définition des quotients de Wilson, on a

$$\begin{aligned}((p-1)!)^{p-1} = (pw_p - 1)^{p-1} &= \sum_{k=0}^{p-1} \binom{p-1}{k} (pw_p)^k (-1)^{p-k-1} \\ &= (-1)^{p-1} + \binom{p-1}{1} pw_p (-1)^{p-2} + p^2 \sum_{k=2}^{p-1} \binom{p-1}{k} p^{k-2} (w_p)^k (-1)^{p-k-1} \\ &\equiv 1 - (p-1)pw_p \ (\mathrm{mod} p^2) \\ &\equiv 1 + pw_p \ (\mathrm{mod} p^2). \end{aligned} \tag{2.21}$$

– La deuxième méthode par la définition des quotients de Fermat, on a

$$\begin{aligned}((p-1)!)^{p-1} &= \prod_{k=1}^{p-1} k^{p-1} \\ &= \prod_{k=1}^{p-1} (pq_k + 1) \\ &\equiv 1 + p \sum_{k=1}^{p-1} q_k \ (\mathrm{mod} p^2). \end{aligned} \tag{2.22}$$

En exploitant les relations (2.21) et (2.22). On déduit de ce résultat que :

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

finalement on obtient :

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

La preuve du théorème (15) est complète. □

2.3.3 Critère de Wieferich dans le premier cas du dernier théorème de Fermat

Le dernier théorème de Fermat

Le théorème suivant appelé "dernier théorème de Fermat " ou " grand théorème de Fermat", a été énoncé par Fermat([11], 1637) ; et est resté conjecture pendant 350 ans jusqu'à sa démonstration par le Mathématicien Andrew Wiles en 1995. Aujourd'hui il est souvent appelé à juste raison "théorème de Fermat Wiles."

Théorème 16 *Il n'est pas possible de trouver pour un entier $n \geq 2$, des entiers x, y, et z non nuls tel que*

$$x^n + y^n = z^n.$$

Cet énoné équivaut aussi à affirmer il n'est pas possible de trouver pour un entier $n \geq 2$, des entiers x, y, et z non nul tels que

$$x^n + y^n + z^n = 0.$$

Critère de Wieferich

En 1909, Arthur Wieferich prouva son célèbre critère pour le premier cas du dernier théorème de Fermat, c'est à dire dans le cas où le produit $x.y.z$ n'est pas divisible par p. Dans un article [24] intitulé : " Zum letzten Fermat'schen Theorem ", le résultat obtenu donne le théorème suivant :

Théorème 17 *Pour tout nombre premier impair p, si l'équation $x^p + y^p + z^p = 0$ est possible en nombres entiers premiers à p, alors $(2^{p-1} - 1)$ est divisible par p^2. Ce qu'on peut énoncer comme suit en terme de quotient de Fermat "Pour tout nombre premier impair p, si l'équation $x^p + y^p + z^p = 0$ est possible en nombres entiers premiers à p, alors $q_2 = \frac{2^{p-1}-1}{p}$ est divisible par p." Autrement dit :*

$$(p \nmid xyz \quad et \quad x^p + y^p + z^p = 0\ ) \quad \Longrightarrow \quad \frac{2^{p-1} - 1}{p^2} \in \mathbb{Z}.$$

Dans la même année (1909), Mirimanoff [19] prouva l'impossibilité de l'équation de Fermat en nombres entiers premiers à p est donc établie pour tous les nombres premiers p tel que $(2^{p-1} - 1)$ ne soit pas divisible par p^2, c'est-à-dire pour tous les nombres premiers p tel que $q_p(2) = \frac{2^{p-1}-1}{p} \not\equiv 0 \pmod{p}$.

En 1910, Mirimanoff a démontré le théorème (17) pour $a = 3$, avec p premier impair comme suivant : "Pour tout nombre premier impair p, si l'équation $x^p + y^p + z^p = 0$ est possible en nombres entiers à p, alors $q_3 = \frac{3^{p-1}-1}{p}$ est divisible par p."

Les nombres premiers de Wieferich

Définition 18 *On appelle nombre premier de Wieferich un nombre premier p tel que p^2 divise $(2^{p-1}-1)$ c'est à dire que :*

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

Les seuls nombres premiers de Wieferich connus aujourd'hui sont :
- $p = 1093$ trouvé en 1913 par Meissner [16].
- $p = 3511$ trouvé en 1922 par N. Beeger[2].

Critère généralisé de Wieferich

Définition 19 *Si l'équation $x^p + y^p + z^p = 0$ est possible en nombres entiers premiers à p, alors pour un certain nombre entier m, on a le quotient de $(m^{p-1}-1)$ par p est divisible par p.*
Autrement dit :

$$(p \nmid xyz \quad et \quad x^p + y^p + z^p = 0\ ) \quad \Longrightarrow \quad \frac{m^{p-1}-1}{p^2} \in \mathbb{Z}.$$

Signalons que ce critère à été prouvé par de nombreux auteurs pour m premier avec $m \leq 41$ comme D. H et Emma Lehmer dans ([14], 1941), A.Granville et M. B. Monagan dans ([11], 1988) quand m est un des 24 nombres premiers $p_1 = 2,\ p_2 = 5, ...,\ p_{24} = 89$.

Chapitre 3

Le carré du quotient de Fermat

3.1 Introduction

Dans ce chapitre, nous allons nous intéresser à une étude approfondie d'une congruence modulo p, conjecturée par Skula et qui s'énone de la manière suivante : pour tout nombre premier $p \geq 5$, on a

$$\left(\frac{2^{p-1}-1}{p}\right)^2 \equiv -\left(\frac{2^1}{1^2}+\frac{2^2}{2^2}+...+\frac{2^{p-1}}{(p-1)^2}\right) \pmod{p}. \tag{3.1}$$

Nous y prouvons la congruence précédente en détaillant les preuves données de ce résulat dans deux articles différents, le premier article étant celui d'Andrew Granville[10] intitulé : "The square of the Fermat quotient" et le deuxième étant celui de Romeo Meštrović [17] intitulé : "An elementary proof of congruence by Skula and Granville".

3.2 Première démonstration d'Andrew Granville(2004)

Andrew Granville définit d'abord les trois fonctions suivantes [15] :

$$q(x) = \frac{x^p-(x-1)^p-1}{p}.$$

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

$$G(x) = \sum_{k=1}^{p-1} \frac{x^k}{k^2}.$$

Propriétés : on peut remarquer que les fonctions précédentes vérifient quelques propriétés intéressantes, en particulier :

$$q(x) = q(1-x). \tag{3.2}$$

$$G'(x) = \frac{g(x)}{x}. \tag{3.3}$$

$$q(2) = 2.q_p(2). \tag{3.4}$$

On a aussi :

$$G(-1) \equiv 0 \pmod{p}. \tag{3.5}$$

$$g(x) \equiv -x^p g(\frac{1}{x}) \pmod{p}. \tag{3.6}$$

$$q(x) \equiv -g(x) \pmod{p}. \tag{3.7}$$

Preuve.
Relation(3.2). Pour p un nombre premier impair, on a

$$q(1-x) = \frac{(1-x)^p - (-x)^p - 1}{p} = \frac{x^p - (x-1)^p - 1}{p} = q(x).$$

Relation(3.3). D'après la dérivée de $G(x)$, on a

$$G'(x) = \sum_{k=1}^{p-1} k.\frac{x^{k-1}}{k^2} = \sum_{k=1}^{p-1} \frac{x^{k-1}}{k} = \frac{1}{x}\sum_{k=1}^{p-1} \frac{x^k}{k} = \frac{g(x)}{x}.$$

Relation(3.4). Pour p un nombre premier tel que $p \geq 3$, on a

$$q(2) = \frac{(2)^p - (2-1) - 1}{p} = \frac{2^p - 2}{p} = 2.\frac{2^{p-1} - 1}{p} = 2.q_p(2).$$

Relation(3.5). Pour p un nombre premier tel que $p \geq 3$, on a

$$\begin{aligned} G(-1) &= \sum_{k=1}^{p-1} \frac{(-1)^k}{k^2} \\ &= -\frac{1}{1^2} + \frac{1}{2^2} - \frac{1}{3^2} + ... + \frac{1}{(p-1)^2} \\ &= \sum_{k=1}^{\frac{p-1}{2}} \frac{1}{(2k)^2} - \sum_{k=1}^{\frac{p-1}{2}} \frac{1}{(p-2k)^2} \\ &\equiv \sum_{k=1}^{\frac{p-1}{2}} \frac{1}{(2k)^2} - \sum_{k=1}^{\frac{p-1}{2}} \frac{1}{(2k)^2} \\ &\equiv 0 \pmod{p}, \quad \text{ce qui établit (3.5).} \end{aligned}$$

Relation(3.6). On a

$$\begin{aligned} g(x) &= \sum_{k=1}^{p-1} \frac{x^k}{k} = x^p \sum_{k=1}^{p-1} \frac{x^k}{k.x^p} \\ &= x^p \sum_{k=1}^{p-1} \frac{1}{k.x^{p-k}} = x^p \sum_{k=1}^{p-1} \frac{1}{(p-k)x^k}, \end{aligned}$$

et comme $(p-k) \equiv -k \pmod{p}$, on trouve

$$g(x) \equiv -x^p g(\frac{1}{x}) \pmod{p}, \quad \text{ce qui établit (3.6).}$$

Relation(3.7). La dérivée de $q(x)$, donne :

$$\begin{aligned} q'(x) &= x^{p-1} - (x-1)^{p-1} \\ &= x^{p-1} - \sum_{j=0}^{p-1} \binom{p-1}{j} (-1)^j x^{(p-1)-j} \\ &= -\sum_{j=1}^{p-1} \binom{p-1}{j} (-1)^j x^{(p-1)-j}, \end{aligned}$$

et comme $\binom{p-1}{j} = \frac{(p-1)(p-2)...(p-j)}{j!} \equiv \frac{(-1)(-2)...(-j)}{1.2...j} \equiv (-1)^j \pmod{p}$, on en déduit que

$$q'(x) \equiv -\sum_{j=1}^{p-1} x^{(p-j)-1} = -\sum_{j=1}^{p-2} x^j = -g'(x) \pmod{p}.$$

Ainsi, $q(x) + g(x) \equiv c_0 \pmod{p}$ mais, en faisant $x = 0$ la constante d'intégration c_0 est nulle, d'où : $q(x) + g(x) \equiv 0 \pmod{p}$, finalement on obtient

$$q(x) \equiv -g(x) \pmod{p}, \quad \text{ce qui établit (3.7).}$$

□

À partir des propriétés ci-dessus, on peut déduire un corollaire qui nous sera utile pour prouver le lemme (21) et détailler d'autres relations de ce mémoire.

Corollaire 20 *Pour tout nombre premier p tel que $p \geq 5$, on a*

1. *D'après les relations (3.7) et (3.2), on a*

$$g(x) \equiv -q(x) = -q(1-x) \equiv g(1-x) \pmod{p},$$

ce qui implique

$$g(x) \equiv g(1-x) \pmod{p}. \tag{3.8}$$

2. *D'après les relations (3.7) et (3.8), on a*

$$-g(x) \equiv x^p g(\frac{1}{x}) \equiv x^p g(1-\frac{1}{x}) \pmod{p},$$

ce qui implique

$$g(x) \equiv -x^p g(1-\frac{1}{x}) \pmod{p}. \tag{3.9}$$

3. *Si on remplace x par 2 dans (3.7) et (3.4), on a*

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

ce qui implique

$$q_p(2) \equiv -\frac{1}{2}\sum_{k=1}^{p-1} \frac{2^k}{k} \pmod{p}, \quad \textit{puisque} \quad p \neq 2. \tag{3.10}$$

Signalons que la congruence(3.10)a été publiée en 1900 *par James Glaisher [9], son article intitulé : "On the residues of the sums of the inverse powers of a number in arithmetical progression"*

Première démonstration de la conjecture de Skula par d'Andrew Granville (2004).

Cette démonstration repose sur le lemme suivant :

Lemme 21 *Soit p un nombre premier tel que $p \geq 5$, on a*

$$q(x)^2 \equiv -2x^p G(x) - 2(1-x^p)G(1-x) \pmod{p}. \tag{3.11}$$

Preuve. D'après la dérivée de la fonction $q(x)^2$, on a

$$\begin{aligned}\frac{d}{dx}q(x)^2 &= 2q(x)q'(x)\\ &= 2q(x)\left(x^{p-1} - \sum_{j=0}^{p-1}\binom{p-1}{j}(-1)^j x^{(p-1)-j}\right),\end{aligned}$$

et comme $\binom{p-1}{j}(-1)^j \equiv 1$, on peut écrire

$$\begin{aligned}\frac{d}{dx}q(x)^2 &= -2g(x)\left(x^{p-1} - \sum_{j=0}^{p-1} x^{(p-1)-j}\right)\\ &= -2x^p\frac{g(x)}{x} + 2g(x)(x^{p-1}+x^{p-2}+...+x+1)\\ &= -2x^p\frac{g(x)}{x} + 2g(x)\left(\frac{x^p-1}{x-1}\right) = -2x^p\frac{g(x)}{x} + 2(1-x^p)\frac{g(x)}{(1-x)},\end{aligned}$$

D'après la relations (3.8) et (3.3), on obtient

$$\begin{aligned}\frac{d}{dx}q(x)^2 &\equiv -2x^p\frac{g(x)}{x} - 2(1-x^p)\frac{g(1-x)}{(1-x)}\\ &\equiv -2x^pG'(x) - 2(1-x^p)G'(1-x)\\ &\equiv \frac{d}{dx}\left(-2x^pG(x) - 2(1-x^p)G(1-x)\right) \pmod p.\end{aligned}$$

D'où :

$$q(x)^2 + 2.x^p.G(x) + 2.(1-x^p).G(1-x) \equiv c_2 + c_3.x^p \pmod p.$$

Pour déterminer les constantes c_2 et c_3 il suffit de prendre $x = 0$ et $x = 1$, on trouve que les deux constantes c_2 et c_3 sont nulles. Finalement on en déduit que :

$$q(x)^2 \equiv -2x^pG(x) - 2(1-x^p)G(1-x) \pmod p. \tag{3.12}$$

Par suite, en faisant $x = 2$ dans (3.12), on a

$$q(2)^2 \equiv -2.2^pG(2) - 2(1-2^p)G(-1) \pmod p,$$

en exploitant les congruences de $G(-1) \equiv 0 \pmod p$, petit théorème de Fermat $a^p \equiv a \pmod p$ et on a aussi $q(2) = 2.q_p(2)$, on obtient directement :

$$q_p(2)^2 \equiv -G(2) \pmod p.$$

On en déduit que :

$$\left(\frac{2^{p-1}-1}{p}\right)^2 \equiv -\left(\frac{2^1}{1^2} + \frac{2^2}{2^2} + ... + \frac{2^{p-1}}{(p-1)^2}\right) \pmod p.$$

□

3.3 Deuxième démonstration de Romeo Meštrović(2011)

3.3.1 Lemmes préliminaires

Cette démonstration repose sur les lemmes suivants :

Lemme 22 *Soit p un nombre premier tel que $p \geq 5$, on a*

$$q_p(2)^2 \equiv \sum_{k=1}^{p-1}(2^k + \frac{1}{2^k})\frac{H_k}{k+1} \pmod p. \tag{3.13}$$

Preuve. En exploitant le résultat de Glaicher (3.10) , on peut donc écrire :

$$q_p(2)^2 \equiv \left(-\frac{1}{2}\sum_{k=1}^{p-1}\frac{2^k}{k}\right)^2 = \frac{1}{4}\left(\sum_{k\ =1}^{p\ -1}\frac{2^{p-k}}{p-k}\right)^2 = \frac{1}{4}\left(2\sum_{k\ =1}^{p\ -1}\frac{2^{(p-1)-k}}{p-k}\right)^2 \pmod p,$$

on sait d'après le petit théorème de Fermat que $2^{p\ -1} \equiv 1 \pmod p$ et comme $p-k \equiv -k \pmod p$, on obtient

$$q_p(2)^2 \equiv \frac{1}{4}\left(2\sum_{k\ =1}^{p\ -1}\frac{2^{-k}}{-k}\right)^2 = \left(\sum_{k\ =1}^{p\ -1}\frac{2^{-k}}{k}\right)^2 = \left(\sum_{k\ =1}^{p\ -1}\frac{1}{k.2^k}\right)^2 \pmod p.$$

Par suite, on suppose que tous les entiers positifs i et j tel que $i \leq p-1$ et $j \leq p-1$. Alors :

$$\begin{aligned} q_p(2)^2 &= \left(\sum_{k\ =1}^{p\ -1}\frac{1}{k\ 2^k}\right)\left(\sum_{k\ =1}^{p\ -1}\frac{1}{k\ 2^k}\right) = \left(\sum_{i\ =1}^{p\ -1}\frac{1}{i\ 2^i}\right)\left(\sum_{j\ =1}^{p\ -1}\frac{1}{j\ 2^j}\right) \\ &= \sum_{i\ +j\ <p}\frac{1}{ij\ 2^{i+j}} + \sum_{i\ +j\ >p}\frac{1}{ij\ 2^{i\ +j}} + \sum_{i\ +j\ =p}\frac{1}{ij\ 2^{i\ +j}} \\ &= \sum_{i\ +j\ \leq p}\frac{1}{ij\ 2^{i\ +j}} + \sum_{i\ +j\ \geq p}\frac{1}{ij\ 2^{i\ +j}} - \sum_{i\ +j=p}\frac{1}{ij\ 2^{i\ +j}} \pmod p. \end{aligned}$$

Pour simplifier les calculs, nous désignons par :

$$S_1 = \sum_{i\ +j\ \leq p}\frac{1}{ij2^{i\ +\ j}},\ S_2 = \sum_{i\ +j\ \ \geq\ p}\frac{1}{ij2^{i\ \ +\ j}} \text{ et } S_3 = \sum_{i\ +j\ \ =p}\frac{1}{ij2^{i\ \ +\ j}}.$$

– On commence par S_1 ; comme $p \geq 5$ et $i+j \leq p$, $i+j \in \{2,3,...p\}$, on a

$$\begin{aligned} S_1 &= \sum_{i+j\leq p}\frac{1}{ij2^{i+j}} = \sum_{k=2}^{p}\sum_{i+j=k}\frac{1}{ij2^k} \\ &= \sum_{k=2}^{p}\frac{1}{2^k}\sum_{i+j=k}\frac{1}{i}(\frac{1}{k-i}) = \sum_{k=2}^{p}\frac{1}{2^k}\sum_{i=1}^{k-1}\frac{1}{k}(\frac{1}{i}+\frac{1}{k-i}) \\ &= \sum_{k=2}^{p}\frac{1}{2^k}\frac{1}{k}(\sum_{i=1}^{k\ -1}\frac{1}{i}+\sum_{i=1}^{k-1}\frac{1}{k-i}) = \sum_{k=2}^{p}\frac{1}{2^k k}(H_{k-1}+H_{k-1}) \\ &= \sum_{k=2}^{p}\frac{2H_{k-1}}{2^k k} = \sum_{k=2}^{p}\frac{H_{k-1}}{2^{k-1}k} = \sum_{k=1}^{p-1}\frac{H_k}{(k+1)2^k}. \end{aligned}$$

On en déduit que :

$$S_1 = \sum_{k=2}^{p-1}\frac{H_k}{(k+1)2^k} \pmod p. \tag{3.14}$$

– Nous allons maintenant calculer S_2 ; pour $p \geq 5$ et en posant $i+j=k$ avec $k \in \{p, p+1, ...(2p-2)\}$ alors :
$(p-i)+(p-j) = 2p-(i+j) \leq p$, et :

$$S_2 = \sum_{i+j \geq p} \frac{1}{ij2^{i+j}} = \sum_{(p-i)+(p-j) \geq p} \frac{1}{(p-i)(p-j)2^{2p-(i+j)}},$$

d'après le petit théorème de Fermat $2^{2p} \equiv 2^2 \pmod{p}$ et comme $p-i \equiv -i \pmod{p}$ et $p-j \equiv -j \pmod{p}$, on obtient :

$$\begin{aligned} S_2 &\equiv \sum_{i+j \leq p} \frac{1}{ij2^2 2^{-(i+j)}} = \frac{1}{4} \sum_{i+j \leq p} \frac{2^{(i+j)}}{ij} \\ &= \frac{1}{4} \sum_{k=2}^{p} \sum_{i+j=k} \frac{2^k}{ij} = \frac{1}{4} \sum_{k=2}^{p} \frac{2^k}{k} \sum_{i=1}^{k-1} (\frac{1}{i} - \frac{1}{k-i}) \\ &= \frac{1}{4} \sum_{k=2}^{p} \frac{2^k}{k} (\sum_{i=1}^{k-1} \frac{1}{i} + \sum_{i=1}^{k-1} \frac{1}{k-i}) = \frac{1}{4} \sum_{k=2}^{p} \frac{2^k}{k} (H_{k-1} + H_{k-1}) \\ &= \frac{1}{4} \sum_{k=2}^{p} \frac{2^k 2H_{k-1}}{k} = \sum_{k=2}^{p} \frac{2^{k-1} H_{k-1}}{k} = \sum_{k=1}^{p-1} \frac{2^k H_k}{k} \pmod{p}. \end{aligned}$$

On en déduit que :

$$S_2 \equiv \sum_{k=1}^{p-1} \frac{2^k H_k}{k+1} \pmod{p}. \tag{3.15}$$

– Enfin nous calculons S_3 ; pour $p \geq 5$ et pour $i+j=p$ et comme $j=p-i$, on obtient

$$\begin{aligned} S_3 &= \sum_{i+j=p} \frac{1}{ij2^{i+j}} = \sum_{i=1}^{p-1} \frac{1}{i(p-i)2^p} \\ &= \frac{1}{2^p.p} \sum_{i=1}^{p-1} (\frac{1}{i} + \frac{1}{p-i}) = \frac{1}{2^p.p} \left(\sum_{i=1}^{p-1} \frac{1}{i} + \sum_{i=1}^{p-1} \frac{1}{p-1} \right) \\ &= \frac{1}{2^p.p} \left(H_{p-1} + H_{_{p-1}} \right) = \frac{2.H_{p-1}}{2^p.p} = \frac{1}{2^{p-1}} \left(\frac{H_{p-1}}{p} \right), \end{aligned}$$

en exploitant les congruences de Wolstenholme (10) et le petit théorème de Fermat $a^{p-1} \equiv 1 \pmod{p}$, on en déduit :

$$S_3 = \frac{1}{2^{p-1}} \left(\frac{H_{p-1}}{p} \right) \equiv 0 \pmod{p}. \tag{3.16}$$

Finalement, d'après les relations précédentes :(3.14), (3.15) et (3.16). Il en résulte : $q_p(2)^2 = S_1 + S_2 - S_3$, d'où :

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

Ce qui achève la démonstration du lemme (22).

□

Lemme 23 *[22] Soit p un nombre premier et $k \in \{1, 2, 3...p-2\}$, on a*

$$H_k \equiv H_{p-k-1} \pmod{p}. \tag{3.17}$$

Preuve. Comme $1 \leq k \leq p-2$ alors $1 \leq p-k-1 \leq p-2$, on a

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

ce qui implique :

$$H_k = H_{p-1} - \sum_{i=1}^{p-k-1} \frac{1}{(p-i)},$$

et comme $H_{p-1} \equiv 0 \pmod{p}$, on obtient

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

Les deux lemmes précédents (22) et (23) nous permettent de prouver le lemme suivant : □

Lemme 24 *Soit p un nombre premier $p \geq 5$, alors :*

$$q_p(2)^2 \equiv \sum_{k=1}^{p-1} \frac{H_k}{k.2^k} - \sum_{k=1}^{p-1} \frac{2^k}{k^2} \pmod{p}. \tag{3.18}$$

Preuve. D'après le lemme (22), on peut écrire

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

Nous désignons par : $T_1 = \sum_{k=1}^{p-1} \frac{H_k}{(k+1)2^k}$ et $T_2 = \sum_{k=1}^{p-1} \frac{2^k H_k}{k+1}$.

– Nous allons commencer par T_1 ; en exploitant les congruences de Wolstenholme et le petit théorème de Fermat, on déduit que :

$$T_1 = \sum_{k=1}^{p-1} \frac{H_k}{(k+1)2^k} = \frac{1}{2^{p-1}}.\left(\frac{H_{p-1}}{p}\right) + \sum_{k=1}^{p-2} \frac{H_k}{(k+1)2^k} \equiv \sum_{k=1}^{p-2} \frac{H_k}{(k+1)2^k} \pmod{p},$$

et comme $H_k = H_{k+1} - \frac{1}{k+1}$, on trouve

$$T_1 = 2\sum_{k=1}^{p-2} \frac{H_{k+1} - \frac{1}{k+1}}{(k+1)2^{k+1}} = 2\sum_{k=1}^{p-2} \frac{H_{k+1}}{(k+1)2^{k+1}} - 2\sum_{k=1}^{p-2} \frac{1}{(k+1)^2 2^{k+1}}$$
$$= 2\sum_{k=1}^{p-1} \frac{H_k}{k2^k} - 2\sum_{k=1}^{p-1} \frac{1}{k^2 2^k} = 2\sum_{k=1}^{p-1} \frac{H_k}{k2^k} - 2\sum_{k=1}^{p-1} \frac{1}{(p-k)^2 2^{p-k}},$$

d'où :

$$T_1 = 2\sum_{k=1}^{p-1} \frac{H_k}{k2^k} - \sum_{k=1}^{p-1} \frac{2^k}{k^2} \pmod{p}. \tag{3.19}$$

– Nous allons maintenant calculer T_2, en utilisant les congruences de Wolstenholme et le petit thérème de Fermat, on a :

$$T_2 = \sum_{k=1}^{p-1} \frac{2^k H_k}{k+1} = 2^{p-1}.\left(\frac{H_{p-1}}{p}\right) + \sum_{k=1}^{p-2} \frac{2^k H_k}{k+1} \equiv \sum_{k=1}^{p-2} \frac{2^k H_k}{k+1} \pmod{p},$$

d'après le lemme(23), on obtient

$$T_2 \equiv \sum_{k=1}^{p-2} \frac{2^{p-k-1} H_{p-k-1}}{p-k} \equiv -\sum_{k=1}^{p-2} \frac{H_k}{k.2^k} \equiv -\sum_{k=1}^{p-1} \frac{H_k}{k.2^k} \pmod{p},$$

d'où :

$$T_2 \equiv -\sum_{k=1}^{p-1} \frac{H_k}{k.2^k} \pmod{p}. \tag{3.20}$$

D'après les relations (3.19) et (3.20), on trouve directement :

$$q_p(2)^2 \equiv \sum_{k=1}^{p-1} \frac{H_k}{k2^k} - \sum_{k=1}^{p-1} \frac{2^k}{k^2} \pmod{p}.$$

□

Lemme 25 *Soit p un nombre premier $p \geq 5$, on a*

$$\sum_{k=1}^{p-1} \frac{H_k}{k2^k} \equiv \frac{1}{2} \sum_{1 \leq i \leq j \leq p-1} \frac{2^i - 1}{ij} \pmod{p}. \tag{3.21}$$

Signalons qui en 2012, Zhi-Wei Sun prouve dans son article intitulé"Aritmetic theory of harmonic numbers " [23] que pour tout nombre premier $p > 3$, on a $\sum_{k=1}^{p-1} \frac{H_k}{k2^k} \equiv 0 \pmod{p}$

Preuve. En remarquant que l'on a

$$\left(\sum_{k=1}^{p-1} \frac{1}{k}\right)\left(\sum_{k=1}^{p-1} \frac{1}{k.2^k}\right) = \sum_{1 \leq i < j \leq p-1} \frac{1}{ij.2^j} + \sum_{1 \leq j < i \leq p-1} \frac{1}{ij.2^j} + \sum_{k=1}^{p-1} \frac{1}{k^2.2^k}, \tag{3.22}$$

et comme on a la congruence $\sum_{k=1}^{p-1} \frac{1}{k} \equiv 0 \pmod{p}$, alors donc la relation (3.22) devient

$$\sum_{1\leq i<j\leq p-1} \frac{1}{ij.2^j} + \sum_{1\leq j<i\leq p-1} \frac{1}{ij.2^j} + \sum_{k=1}^{p-1} \frac{1}{k^2.2^k} \equiv 0 \pmod{p},$$

Par suite, on obtient :

$$\begin{aligned}
\sum_{1\leq i<j\leq p-1} \frac{1}{ij.2^j} + \sum_{k=1}^{p-1} \frac{1}{k^2.2^k} &\equiv - \sum_{1\leq j<i\leq p-1} \frac{1}{ij.2^j} \\
&\equiv - \sum_{1\leq j<i\leq p-1} \frac{2^{p-1}}{ij.2^j} \pmod{p} \\
&\equiv - \sum_{1\leq i\leq j\leq p-1} \frac{1}{2} \frac{2^{(p-j)}}{(p-i)(p-j)} \pmod{p} \\
&\equiv -\frac{1}{2} \sum_{1\leq i<j\leq p-1} \frac{2^j}{ij} \pmod{p}.
\end{aligned}$$

On en déduit que :

$$\sum_{1\leq i<j\leq p-1} \frac{1}{ij.2^j} + \sum_{k=1}^{p-1} \frac{1}{k^2.2^k} \equiv -\frac{1}{2} \sum_{1\leq i<j\leq p-1} \frac{2^j}{ij} \pmod{p}. \tag{3.23}$$

D'une part, on remarque aussi que :

$$\begin{aligned}
\sum_{k=1}^{p-1} \frac{H_k}{k.2^k} &= \sum_{k=1}^{p-1} \frac{H_{k-1} + \frac{1}{k}}{k.2^k} = \sum_{k=1}^{p-1} \frac{H_{k-1}}{k.2^k} + \sum_{k=1}^{p-1} \frac{1}{k^2.2^k} \\
&= \sum_{k=1}^{p-2} \frac{1}{k} \sum_{k=1}^{p-1} \frac{1}{k.2^k} + \sum_{k=1}^{p-1} \frac{1}{k^2.2^k} = \sum_{1\leq i<j\leq p-1} \frac{1}{i.j.2^j} + \sum_{k=1}^{p-1} \frac{1}{k^2.2^k}.
\end{aligned}$$

On en déduit que :

$$\sum_{k=1}^{p-1} \frac{H_k}{k.2^k} = \sum_{1\leq i<j\leq p-1} \frac{1}{i.j.2^j} + \sum_{k=1}^{p-1} \frac{1}{k^2.2^k}. \tag{3.24}$$

D'après la relation (3.23) et la relation (3.24). Il en résulte que :

$$\sum_{k=1}^{p-1} \frac{H_k}{k.2^k} = -\frac{1}{2} \sum_{1\leq i<j\leq p-1} \frac{2^j}{ij} \pmod{p}. \tag{3.25}$$

D'autre part, on a aussi

$$\left(\sum_{k=1}^{p-1} \frac{1}{k}\right) \left(\sum_{k=1}^{p-1} \frac{2^k}{k}\right) = \sum_{1\leq j\leq i\leq p-1} \frac{2^j}{ij} + \sum_{1\leq i<j\leq p-1} \frac{2^j}{ij}, \tag{3.26}$$

et comme $\sum_{k=1}^{p-1} \frac{1}{k} \equiv 0 \pmod{p}$, alors la relation (3.26) devient :

$$\sum_{1\leq j\leq i\leq p-1} \frac{2^j}{ij} + \sum_{1\leq i<j\leq p-1} \frac{2^j}{ij} \equiv 0 \pmod{p},$$

Par suite, on a

$$\sum_{1\leq j\leq i\leq p-1} \frac{2^j}{ij} \equiv -\sum_{1\leq i<j\leq p-1} \frac{2^j}{ij} \pmod{p}, \tag{3.27}$$

pour $p \neq 2$, en multipliant les deux membres de la relation (3.27) par $\frac{1}{2}$, on obtient

$$\frac{1}{2}\sum_{1\leq j\leq i\leq p-1} \frac{2^j}{ij} \equiv -\frac{1}{2}\sum_{1\leq i<j\leq p-1} \frac{2^j}{ij} \pmod{p}, \tag{3.28}$$

D'après la relation (3.25) et la relation (3.28), on peut écrire :

$$\sum_{k=1}^{p-1} \frac{H_k}{k.2^k} \equiv \frac{1}{2}\sum_{1\leq j\leq i\leq p-1} \frac{2^j}{ij} \pmod{p}$$

ce qui implique

$$\begin{aligned}\sum_{k=1}^{p-1} \frac{H_k}{k.2^k} &\equiv \frac{1}{2}\sum_{1\leq j\leq i\leq p-1} \frac{2^j}{ij} \\ &= \frac{1}{2}\sum_{1\leq j\leq i\leq p-1} \frac{2^{p-i}}{(p-i)(p-j)} \\ &\equiv \frac{1}{2}\sum_{1\leq i\leq j\leq p-1} \frac{2^i}{ij} \pmod{p},\end{aligned}$$

et comme la congruence : $\sum_{1\leq i\leq j\leq p-1} \frac{1}{ij} = \frac{1}{2}((\sum_{k=1}^{p-1} \frac{1}{k})^2 + \sum_{k=1}^{p-1} \frac{1}{k^2}) \equiv 0 \pmod{p}$, on obtient :

$$\begin{aligned}\sum_{k=1}^{p-1} \frac{H_k}{k.2^k} &\equiv \frac{1}{2}\sum_{1\leq i\leq j\leq p-1} \frac{2^i}{ij} - \sum_{1\leq i\leq j\leq p-1} \frac{1}{ij} \\ &\equiv \frac{1}{2}\sum_{1\leq i\leq j\leq p-1} \frac{2^i-1}{ij} \pmod{p}.\end{aligned}$$

On en déduit que :

$$\sum_{k=1}^{p-1} \frac{H_k}{k.2^k} \equiv \frac{1}{2}\sum_{1\leq i\leq j\leq p-1} \frac{2^i-1}{ij} \pmod{p}.$$

□

Lemme 26 *Pour tout entier naturel n non nul, on a*

$$\sum_{1\leq i\leq j\leq n}\frac{2^i-1}{ij}=\sum_{k=1}^{n}\frac{1}{k^2}\binom{n}{k}.$$

Preuve. On a,

$$\sum_{1\leq i\leq j\leq n}\frac{2^i-1}{ij}=\sum_{1\leq i\leq j\leq n}\frac{(1+1)^i-1}{ij}=\sum_{1\leq i\leq j\leq n}\frac{1}{i.j}\sum_{k=1}^{i}\binom{i}{k},$$

en exploitant la relation (1.2) du théotème (1), on peut écrire :

$$\begin{aligned}\sum_{1\leq i\leq j\leq n}\frac{2^i-1}{ij}&=\sum_{1\leq i\leq j\leq n}\frac{1}{j}\sum_{k=1}^{i}\frac{1}{i}\binom{i}{k}=\sum_{1\leq i\leq j\leq n}\frac{1}{j}\sum_{k=1}^{n}\frac{1}{k}\binom{i-1}{k-1}\\&=\sum_{k=1}^{n}\frac{1}{k}\sum_{1\leq i\leq j\leq p-1}\frac{1}{j}\binom{i-1}{k-1}=\sum_{k=1}^{n}\frac{1}{k}\sum_{j=1}^{n}\frac{1}{j}\sum_{i=k}^{j}\binom{i-1}{k-1}.\end{aligned}$$

Par suit, en exploitant aussi la relation (1.3) du théotème (1), on trouve :

$$\begin{aligned}\sum_{1\leq i\leq j\leq n}\frac{2^i-1}{ij}&=\sum_{k=1}^{n}\frac{1}{k}\sum_{j=i}^{n}\frac{1}{j}\binom{j}{k}=\sum_{k=1}^{n}\frac{1}{k}\sum_{j=i}^{n}\frac{1}{k}\binom{j-1}{k-1}\\&=\sum_{k=1}^{n}\frac{1}{k^2}\sum_{j=k}^{n}\binom{j-1}{k-1}=\sum_{k=1}^{n}\frac{1}{k^2}\binom{n}{k}.\end{aligned}$$

La démonstration du lemme (25) est complète. □

Deuxième démonstration par Romeo Meštrović (2011)

D'après le lemme (24), on a donc

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

Par suite, on sait que d'après les lemmes (25) et (26), on a $\sum_{k=1}^{p-1}\frac{H_k}{k2^k}\equiv\frac{1}{2}\sum_{1\leq i\leq j\leq p-1}\frac{2^i-1}{ij}=\sum_{k=1}^{n}\frac{1}{k^2}\binom{n}{k}\pmod p$ ce qui implique :

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

Si on remplace n par $(p-1)$, on obtient

$$q_p(2)^2 \equiv \sum_{k=1}^{p-1} \frac{1}{k^2} \binom{p-1}{k} - \sum_{k=1}^{p-1} \frac{2^k}{k^2} \pmod{p}, \tag{3.29}$$

et comme $\binom{p-1}{k} \equiv (-1)^k \pmod{p}$ alors la relation (3.29) devient

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

en utilisant la congruence (3.5) qui affirme que $G(-1) = \sum_{k=1}^{p-1} \frac{(-1)^k}{k^2} \equiv 0 \pmod{p}$, on obtient :

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

Ainsi la démonstration de Romeo Maštrović est complète.

Chapitre 4

Le cube du quotient de Fermat

4.1 Introduction et théorème principal

Ce chapitre est consacré à une réformulation détaillée des preuves des nombreux résultats de l'article de Karl Dilcher et Ladislav Skula [6] intitulé *" The cube of the Fermat quotient "*. Ces résultats sont résumés dans le théorème suivant :

Théorème 27 *Pour tout nombre premier p, $p \geq 5$, on a*

$$q_p(2)^3 \equiv \sum_{j=1}^{p-1} \frac{2^j}{j^3} + \frac{7}{4} \sum_{j=1}^{p-1} \frac{(-1)^j}{j^3} \pmod{p}. \tag{4.1}$$

Signalons que cette dernière congruence est équivlente à la congruence suivante :

$$q_p(2)^3 \equiv -3 \sum_{j=1}^{p-1} \frac{2^j}{j^3} + \frac{7}{16} \sum_{j=1}^{\frac{p-1}{2}} \frac{1}{j^3} \pmod{p}. \tag{4.2}$$

L'obtention de ces résultats nécessite de nombreux calculs ainsi que l'utilisation de la congruence d'Andrew Granville [10], que nous avons énoncé au troisième chapitre. Dans ce chapitre nous allons particulièrement nous intéresser à la prermière congruence autre pouvant se démontrer de la même manière en utilisant les mêmes résultats intermédiaires.

4.2 La preuve de Karl Dichler et de Ladislav Skula (2006)

Avant de prouver le principal théorème de ce chapitre, nous allons d'abord prouver des résultats qui nous seront nécessaires.

On commence par définir la fonction suivante qui affirme que pour tout nombre premier p tel que $p \geq 5$ et $j \in \{1, 2, ..., p-1\}$, on a

$$G_3(x) = \sum_{j=1}^{p-1} \frac{x^j}{j^3}. \tag{4.3}$$

Elle présente quelques propriétés intéressantes, en particulier :

$$G_3'(x) = \frac{G(x)}{x}. \tag{4.4}$$

$$G_3(1) \equiv 0 \pmod{p}. \tag{4.5}$$

$$x^p G_3(\frac{1}{x}) \equiv -G_3(x) \pmod{p}. \tag{4.6}$$

Preuve.
Relation4.4. On sait d'après la définition de $G(x)$ que nous avons énoncé au troisième chapitre, on peut écrire

$$G_3'(x) = \sum_{j=1}^{p-1} \frac{x^{j-1}}{j^2} = \frac{1}{x} \sum_{j=1}^{p-1} \frac{x^j}{j^2} = \frac{G(x)}{x},$$

Relation4.5. On utilise le corollaire (**??**), on obtient

$$G_3(1) = \sum_{j=1}^{p-1} \frac{1}{j^3} \equiv 0 \pmod{p}.$$

Relation4.6. On a

$$\begin{aligned} x^p G_3(\frac{1}{x}) &= x^p \sum_{j=1}^{p-1} \frac{1}{j^3.x^j} \\ &= \sum_{j=1}^{p-1} \frac{x^{p-j}}{j^3} = \sum_{j=1}^{p-1} \frac{x^j}{(p-j)^3}, \end{aligned}$$

et comme $p - j \equiv -j \pmod{p}$, on a donc

$$x^p G_3(\frac{1}{x}) \equiv -\sum_{j=1}^{p-1} \frac{x^j}{j^3} = -G_3(x) \pmod{p}.$$

□

Le lemme suivant nous sera utile pour donner la preuve du théorème (29) qui suit ce lemme

Lemme 28 *[10] Soit p un nombre premier tel que $p \geq 5$, on a*

$$G(x) \equiv G(1-x) + x^p G(1 - \frac{1}{x}) \pmod{p}.$$

Preuve. Considérons la dérivée de membre de gauche, alors on peut écrire

$$\frac{d}{dx}\left(G(1-x)+x^pG(1-\frac{1}{x})\right)=-\frac{g(1-x)}{(1-x)}+px^{p-1}G(1-\frac{1}{x})+x^p\frac{g(1-\frac{1}{x})}{x^2(1-\frac{1}{x})},$$

et comme le terme $px^{p-1}G(1-\frac{1}{x})$ est nul puisque p est en facteur, on trouve

$$\begin{aligned}\frac{d}{dx}\left(G(1-x)+x^pG(1-\frac{1}{x})\right)&\equiv\frac{g(1-x)}{(x-1)}+x^p\frac{g(1-\frac{1}{x})}{x(x-1)}=\frac{xg(1-x)+x^pg(1-\frac{1}{x})}{x(x-1)}\\&\equiv\frac{xg(x)-g(x)}{x(x-1)}=\frac{g(x)(x-1)}{x(x-1)}=\frac{g(x)}{x}\\&\equiv G'(x)\pmod p,\end{aligned}$$

d'où

$$G(x)-G(1-x)-x^pG(1-\frac{1}{x})\equiv C_0\pmod p,$$

où C_0 est une constante, en faisant $x=1$ et on a aussi d'après le théorème (11) que $G(1)=\sum_{k=1}^{p-1}\frac{1}{k^2}\equiv 0\pmod p$, ce qui implique :

$$C_0\equiv 0\pmod p.$$

On obtient directement :

$$G(x)-G(1-x)-x^pG(1-\frac{1}{x})\equiv 0\pmod p.$$

La preuve du lemme est complète. □

Théorème 29 *Si p est un nombre premier tel que $p\geq 5$, alors :*

$$\begin{aligned}\frac{1}{6}q(x)^3\equiv x^pG_3(x)-(1-x^p)G_3(1-x)-x^{2p}(1-x^p)G_3(1-\frac{1}{x})\\+C_1x^p(1-x^p)\pmod p.\end{aligned}\tag{4.7}$$

où C_1 est une constante.

Preuve. On considère la dérivée de $q(x)^3$:

$$\frac{d}{dx}q(x)^3=3.q(x)^2.q'(x),\tag{4.8}$$

On considère maintenant la dérivée de $q(x)$:

$$\begin{aligned}q'(x)&=x^{p-1}-(x-1)^{p-1}\\&=x^{p-1}-\sum_{j=0}^{p-1}\binom{p-1}{j}(-x)^j,\end{aligned}$$

et, comme $\binom{p-1}{j} = (-1)^j \pmod p$, donc on a

$$q'(x) \equiv x^{p-1} - \sum_{j=0}^{p-1} x^j \pmod p. \tag{4.9}$$

On a aussi $\sum_{j=0}^{p-1} x^j = \frac{1-x^p}{1-x}$, alors la relation (4.9) devient :

$$q'(x) = x^{p-1} - \frac{1-x^p}{1-x}, \tag{4.10}$$

en exploitant la relation (4.10) et la congruence $(q(x)^2 \equiv -2x^pG(x) - 2(1-x^p)G(1-x))$ du lemme (21), on peut ecrire :

$$\begin{aligned}
\frac{d}{dx}q(x)^3 &\equiv 3.\left(-2x^pG(x) - 2(1-x^p)G(1-x)\right)\left(x^{p-1} - \frac{1-x^p}{1-x}\right) \\
&= -6x^{2p-1}G(x) + 6(1-x^p)^2\frac{G(1-x)}{1-x} + 6x^p(1-x^p)\frac{G(x)}{1-x} - 6x^p(1-x^p)\frac{G(1-x)}{x} \\
&= -6x^{2p}\frac{G(x)}{x} + 6(1-x^p)^2\frac{G(1-x)}{1-x} \\
&+ 6x^p(1-x^p)\left(\frac{G(x)}{1-x} - \frac{G(1-x)}{x}\right) \pmod p.
\end{aligned} \tag{4.11}$$

On a d'une part, et d'après le lemme (28) :

$$G(x) \equiv G(1-x) + x^pG(1-\frac{1}{x}) \pmod p, \tag{4.12}$$

en multipliant les deux membres de (4.12) par $(1/1-x)$, on trouve

$$\begin{aligned}
\frac{G(x)}{1-x} &\equiv \frac{G(1-x) + x^pG(1-\frac{1}{x})}{1-x} \\
&= \frac{G(1-x)}{1-x} - x^p\frac{1}{x}\frac{G(1-\frac{1}{x})}{1-\frac{1}{x}} \pmod p,
\end{aligned} \tag{4.13}$$

en multipliant aussi les deux membres de (4.12) par $-1/x$, on trouve

$$\begin{aligned}
-\frac{G(1-x)}{x} &\equiv -\frac{G(x) - x^pG(1-\frac{1}{x})}{x} \\
&= -\frac{G(x)}{x} + x^p\left(\frac{1}{x} - \frac{1}{x^2}\right)\frac{G(1-\frac{1}{x})}{1-\frac{1}{x}} \\
&= -\frac{G(x)}{x} + x^p\frac{1}{x}\frac{G(1-\frac{1}{x})}{1-\frac{1}{x}} - x^p\frac{1}{x^2}\frac{G(1-\frac{1}{x})}{1-\frac{1}{x}} \pmod p,
\end{aligned} \tag{4.14}$$

ajoutant, membre à membre les relations (4.13) et (4.14), on trouve

$$\frac{G(x)}{1-x}-\frac{G(1-x)}{x}=\frac{G(1-x)}{1-x}-\frac{G(x)}{1-x}-x^p\frac{1}{x^2}\frac{G(1-\frac{1}{x})}{1-\frac{1}{x}}. \tag{4.15}$$

En utilisant (4.15) et (4.11), on peut écrire :

$$\begin{aligned}
\frac{d}{dx}q(x)^3 &= -6x^{2p}\frac{G(x)}{x}+6(1-x^p)^2\frac{G(1-x)}{1-x}\\
&\quad+6x^p(1-x^p)\left(\frac{G(1-x)}{1-x}-\frac{G(x)}{x}-x^p\frac{1}{x^2}\frac{G(1-\frac{1}{x})}{1-\frac{1}{x}}\right)\\
&=6(-x^{2p}-x^p+x^{2p})\frac{G(x)}{x}-6(x^p+1-x^p)(1-x^p)\frac{G(1-x)}{1-x}\\
&\quad-6.x^{2p}(1-x^p)\frac{1}{x^2}\frac{G(1-\frac{1}{x})}{1-\frac{1}{x}}\\
&=6.\left(-x^p\frac{G(x)}{x}-(1-x^p)\frac{G(1-x)}{1-x}-x^{2p}(1-x^p)\frac{1}{x^2}\frac{G(1-\frac{1}{x})}{1-\frac{1}{x}}\right)\\
&\equiv 6.\left(-x^p.G_3'(x)-(1-x^p)G_3'(1-x)-x^{2p}(1-x^p)G_3'(1-\frac{1}{x})\right)\pmod p.
\end{aligned}$$

D'où :

$$\begin{aligned}
\frac{1}{6}q_(x)^3 &\equiv -x^pG_3(x)-(1-x^p)G_3(1-x)-x^{2p}(1-x^p)G_3(1-\frac{1}{x})\\
&\quad+C_0+C_1x^p+C_2x^{2p}\pmod p,
\end{aligned}$$

où C_0, C_1et C_2 sont des constantes ; en faisant $x=0$ et comme $q(0)=0$ et $G_3(1)\equiv 0 \pmod p$, on établit que :

$$C_0\equiv 0 \pmod p$$

par suite, en faisant $x=1$ et comme $q(1)=0$ et $G_3(0)=0$, on établit que

$$C_2\equiv -C_1 \pmod p$$

ce qui implique

$$\begin{aligned}
\frac{1}{6}q(x)^3 &\equiv -x^pG_3(x)-(1-x^p)G_3(1-x)-x^{2p}(1-x^p)G_3(1-\frac{1}{x})\\
&\quad+C_1x^p(1-x^p)\pmod p.
\end{aligned} \tag{4.16}$$

□

La preuve du théorème (29) est complète. Nous allons maintenant nous intéresser à la détermination modulo p de la constante C_1.

Détermination de la constante C_1

On considère le polynôme suivant :

$$p(x) = x^2 - x + 1.$$

C'est un polynôme irréductible dans $\mathbb{Q}[\mathbb{X}]$, puisqu'il possède deux racines dans $\mathbb{C}$, il est unitaire car le coefficient de x^2 est égale 1, ce qui signifie un polynôme minimale, soit a comme élément primitif d'ordre 6. Pour cela on peut écrire :

$$\begin{cases} a^0 = 1, \\ a^1 = a, \\ a^2 = a - 1, \\ a^3 = a.a^2 = -1, \\ a^4 = a.a^3 = a(-1) = -a, \\ a^5 = a.a^4 = a(-a) = -a^2 = -(a-1) = 1 - a, \\ a^6 = a.a^5 = a(1-a) = a - a^2 = a - (a-1) = a - a + 1 = 1. \end{cases} \tag{4.17}$$

Remarque 30 *D'après l'écriture de (4.17), on peut calculer $q(a)$.*

$$\begin{aligned} q(a) &= \frac{a^p - (a-1)^p - 1}{p} \\ &= \frac{a^p - (a^2)^p - 1}{p} = \frac{-((a^p)^2 - a + 1)}{p} = 0. \end{aligned}$$

Ce qui établit : $q(a) = 0$.

Revenons à la relation (4.16), si on remplace x par a, on obtient

$$-a^p G_3(a) - (1-a^p)G_3(1-a) - a^{2p}(1-a^p)G_3(1-\frac{1}{a}) + c_1 a^p(1-a^p) \equiv 0 \pmod{p},$$

en remarquant qu'on peut écrire : $a = 1 - \frac{1}{a}$ même aussi $a^p(1-a^p) = 1$, on a donc

$$-a^p.G_3(a) - (1-a^p).G_3(1-a) - a^p.G_3(a) + C_1 \equiv 0 \pmod{p},$$

ce qui implique

$$C_1 \equiv 2a^p.G_3(a) + (1-a^p).G_3(1-a) \pmod{p}.$$

Il est facile de constater que : $a.\underbrace{(a-1)}_{\bar{a}} = 1$ et $a^p.\underbrace{(1-a^p)}_{\bar{a}^p} = 1$, on en déduit que l'on a la congruence suivante :

$$a^p.G_3(a) \equiv \bar{a}^p.G_3(\bar{a}) \pmod{p},$$

enfin, on obtient

$$C_1 \equiv 3.a^p.G_3(a) \pmod{p}.$$

Nous allons maintenant nous intéresser à la détermination modulo p de $a^pG_3(a)$, pour cela, on définit la somme suivante : pour tout entier r et $j \in \{1, 2, ..., (p-1)\}$, on a

$$t(r) = \sum_{\substack{j=1 \\ j\equiv r(mod6)}}^{p-1} \frac{1}{j^3}. \tag{4.18}$$

Si : $r \equiv l \pmod 6$, on a $t(r) = t(l)$, alors on peut écrire $G_3(-1)$:

$$\begin{aligned} G_3(-1) &= \sum_{j=1}^{p-1} \frac{(-1)^j}{j^3} = \sum_{j=0}^{5} (-1)^j t(j) \\ &= t(0) - t(1) + t(2) - t(3) + t(4) - t(5) \\ &\equiv 2(t(0) + t(2) + t(4)). \end{aligned} \tag{4.19}$$

D' autre part, on a

$$\begin{aligned} t(0) + t(2) + t(4) &= \frac{1}{2^3} + \frac{1}{4^3} + \frac{1}{6^3} + ... + \frac{1}{(p-1)^3} \\ &= 3^3 \left(\frac{1}{6^3} + \frac{1}{12^3} + \frac{1}{18^3} + ... + \frac{1}{(3p-3)^3} \right) = \sum_{\substack{j=1 \\ j\equiv 0 \pmod 6}}^{3p-1} \frac{1}{j^3} \\ &= 3^3 \sum_{i=0}^{2} \sum_{\substack{j=ip+1 \\ j\equiv 0 \pmod 6}}^{(i+1)p} \frac{1}{j^3} = 3^3 \sum_{i=0}^{2} \sum_{\substack{k=1 \\ j\equiv -ip \pmod 6}}^{p} \frac{1}{j^3} \\ &\equiv 27(t(0) + t(-p) + t(-2p)) \pmod{p} \end{aligned}$$

d'après la définition de (4.18), on a $t(j) \equiv -t(p-j) \pmod p$, alors on peut distinguer deux cas : le cas où $p \equiv 1 \pmod 6$ et le cas $p \equiv -1 \pmod 6$

1. **Premier cas :** $p \equiv 1 \pmod 6$**.**

   On sait d'après la congruence $t(j) \equiv t(p-j) \pmod p$ qui montre que $t(-p) \equiv -t(2p) = -t(2) \pmod p$ et $t(-2p) \equiv t(4) \pmod p$. On trouve :

   $$t(0) + t(2) + t(4) \equiv 27(t(0) - 2t(2) + t(4)) \pmod{p}. \tag{4.20}$$

   D'une part, on a

   $$\begin{aligned} a^pG_3(a) &= \sum_{j=0}^{5} a^{p+j} t(j) = a^p t(0) + a^{p+1} t(1) + a^{p+2} t(2) + a^{p+3} t(3) a^{p+4} t(4) + a^{p+5} t(5) \\ &\equiv a^1 t(0) + a^2 t(1) + a^3 t(2) + a^4 t(3) + a^5 t(4) + a^6 t(5), \end{aligned} \tag{4.21}$$

on sait d'après la congruence $t(j) \equiv t(p-j) \pmod p$ qui montre que $t(1) \equiv -t(0) \pmod p$, $t(3) \equiv -t(4) \pmod p$ et $t(5) \equiv -t(2) \pmod p$, la relation (4.21) devient :

$$\begin{aligned} a^p G_3(a) &\equiv a^1 t(0) - a^2 t(0) + a^3 t(2) - a^4 t(4) + a^5 t(4) - a^6 t(2) \\ &\equiv t(0)(a - a^2) + t(2)(a^3 - a^6) + t(4)(a^5 - a^4), \end{aligned}$$

d'après la relation (4.17), on a $(a - a^2) = 1$, $(a^3 - a^6) = -2$ et $(a^5 - a^4) = 1$, on peut alors écrire :

$$\begin{aligned} a^p G_3(a) &= t(0) - 2t(2) + t(4) \\ &= \frac{3}{2}(t(0) - t(2) + t(4)) - \frac{1}{2}(t(0) + t(2) + t(4)), \end{aligned}$$

en utilisant les relations (4.20) et (4.19), on en déduit que :

$$\begin{aligned} a^p G_3(a) &\equiv \frac{1}{18}(t(0) + t(2) + t(4)) - \frac{1}{2}(t(0) + t(2) + t(4)) \\ &\equiv -\frac{4}{9}((t(0) + t(2) + t(4))) \\ &\equiv -\frac{2}{9} G_3(-1) \pmod p. \end{aligned}$$

Ce qui établit $C_1 \equiv -\frac{2}{3} G_3(-1) \pmod p$.

2. **Deuxième cas :** $p \equiv -1 \pmod 6$**.**

On sait la congruence $t(j) \equiv -t(p-j) \pmod p$ que $t(-p) \equiv -t(2p) = -t(2) \pmod p$ et $t(-2p) \equiv t(2) \pmod p$. On trouve :

$$t(0) + t(2) + t(4) \equiv 27(t(0) + 2t(2) - t(4)) \pmod p. \tag{4.22}$$

D'une part, on a

$$\begin{aligned} a^p G_3(a) &= \sum_{j=0}^{5} a^{p+j} t(j) = a^p t(0) + a^{p+1} t(1) + a^{p+2} t(2) + a^{p+3} t(3) a^{p+4} t(4) + a^{p+5} t(5) \\ &\equiv a^5 t(0) + a^1 t(1) + a^2 t(2) + a^3 t(3) + a^4 t(4) + a^5 t(5), \end{aligned} \tag{4.23}$$

on sait la congruence $t(j) \equiv t(p-j) \pmod p$ que $t(1) \equiv -t(4) \pmod p$, $t(3) \equiv -t(2) \pmod p$ et $t(5) \equiv -t(0) \pmod p$, la relation (4.23) est devient :

$$\begin{aligned} a^p G_3(a) &\equiv a^1 t(0) - a^2 t(0) + a^3 t(2) - a^4 t(4) + a^5 t(4) - a^6 t(2) \\ &\equiv t(0)(a^5 - a^4) + t(2)(a - a^2) + t(4)(a^3 - a^0), \end{aligned}$$

d'après la relation (4.17) $(a^5 - a^4) = 1$, $(a - a^2) = 1$, et $(a^3 - a^0) = -2$, on peut écrire :

$$\begin{aligned} a^p G_3(a) &= t(0) + t(2) - 2t(4) \\ &= \frac{3}{2}(t(0) + t(2) - 2t(4)) - \frac{1}{2}(t(0) + t(2) + t(4)), \end{aligned}$$

en utilisant les relations de (4.19) et (4.22), on en déduit que

$$\begin{aligned} a^p G_3(a) &\equiv \frac{1}{18}(t(0) + t(2) + t(4)) - \frac{1}{2}(t(0) + t(2) + t(4)) \\ &\equiv -\frac{4}{9}((t(0) + t(2) + t(4))) \\ &\equiv -\frac{2}{3}G_3(-1) \pmod{p}. \end{aligned}$$

Ce qui établit $C_1 \equiv -\frac{2}{3}G_3(-1) \pmod{p}$.

4.2.1 Démonstration du théorème principal

Daprès le (29) et sachant que $C_1 \equiv -\frac{2}{3}G_3(-1)$, on a

$$\begin{aligned} \frac{1}{6}q(x)^3 \equiv &-x^p G(x) - (1 - x^p)G(1 - x) - x^{2p}(1 - x^p)G(1 - \frac{1}{x}) \\ &- \frac{2}{3}G_3(-1)x^p(1 - x^p) \pmod{p}, \end{aligned}$$

en faisant $x = 2$, alors :

$$\begin{aligned} \frac{1}{6}q(2)^3 \equiv &-2^p G(2) - (1 - 2^p)G(-1) - 2^{2p}(1 - 2^p)G(1 - \frac{1}{2}) \\ &- \frac{2}{3}G_3(-1)2^p(1 - 2^p) \pmod{p}. \end{aligned}$$

Puisque : $x^p G_3(1/x) \equiv -G_3(x) \pmod{p}$ et la relation (3.4) montre que :

$$\begin{aligned} q_p(2)^3 &\equiv -\frac{3}{2}G_3(2) + \frac{3}{4}G_3(-1) - \frac{3}{2}G_3(2) + G_3(-1) \\ &= -3G_3(2) + \frac{7}{4}G_3(-1) \\ &\equiv -3G_3(2) + \frac{7}{4}\sum_{j=1}^{p-1}\frac{(-1)}{j^3} \pmod{p}. \end{aligned}$$

Ainsi la congruence (4.1) est prouvée et la preuve du théorème principal est maintenant complète.

Conclusion

Dans ce mémoire, nous avons pu constater que le quotient de Fermat intervient dans de nombreuses congruences dont certaines comportent des nombres harmoniques. Notre mémoire a porté sur l'étude des puissances des quotients de Fermat $q_p^n(2)$ pour $n = 1$, $n = 2$ et $n = 3$. Nous avons détaillé la preuve des congruences suivantes :

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

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

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

cette dernière congruence s'écrivant aussi de manière équivalente

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

Ces congruences sont dues à Eisenstein (1850), Glaisher (1905) [9], Andrew Granville (2004)[10], Karl Dilcher et Ladislav Skula (2006) [6] ainsi qu'à Romeo Meštrović(2011) [17].

Les congruences faisant intervenir la puissance quatrième du quotient de Fermat $q_p^4(2)$ ne semblent pas avoir fait l'objet d'une étude particulière et approfondie à ce jour. Il nous semble qu'une étude sur ce sujet représente une intéressante perspective de recherche pour poursuivre le travail que nous avons réalisé dans ce mémoire.

Bibliographie

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

[2] N. Beeger, On a New Case of the congruence $2^{p-1} \equiv 1(modp^2)$, Messenger of Mathematics, pages 149–150, (1922)volume 51.

[3] F. Bencherif, La congruence dans l'anneau des p-entiers. Cours de post-graduation, Fac Math USTHB (2011/2012).

[4] R. Bernard, Quotient de Fermat et relation avec le Grand Théorème (25 mai 2013).

[5] R. Chellal, Autour De Certaines Propriétés Arithmétiques des Nombre de Bernoulli, mémoire de Magister, 2012.

[6] K. Dilcher and L. Skula, The cube of The Fermat Quotient, Electronic Journal of Combinatorial Number Theory 4, (30 novembre 2006).

[7] G. Eisenstein, Academie der Wessenschaften zu berlin, "Neue Gattung Zahlentheoret. Funkionen, die v. 2 Elementen abhangen und durch guwisse Lineare funktional-gattungen definirt werden, " bericht ubre die zur bekanntmachung geeigneten verhandlungen der konigl. Preuβ, pages 36–42(1850).

[8] L. Elhiri, Etude de certaines super congruences dans l'anneau $\mathbb{Z}_p$, mémoire de Magister. ENS (2014).

[9] J.W.L. Glaisher, On the residues of the sums of the inverse powers of numbre in arithmetical progression, Q. J. Math. pages 271–288 volume (32), 2012.

[10] A. Granville, The square Of The Fermat Quotient. Electronic Journal Of Combinatroial Number Theory 4,A22, (30 novembre 2004).

[11] A. Granville and M. B. Monagan, The First Case of Fermat's Last theorem is true for all prime exponents up. to 714. 416.091.389. Trans. Amer. Math. Soc., 306(1988).

[12] G-H Hardy, E-M Wright, An introduction to the theory of Numbres, (5th edition, collection "Oxfor Science Publication", Oxfod University Press, Grand Bretagne, 1979 (first edition : 1938).

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

[14] D.H.Lehma and Emma Lehmer, On the first case of Fermat's last theorem, Bull. Amer. Math. Soc 47(1941). 139-142.MR 00003657, (5,250f),http ://dz. doi org / 10.1090/ S0002-9904-1941-07393-3.

[15] S. Matharei and R. Tauraso, Congruences for central binomial sums and finite polylogarithms, arXiv : 1012.1308v6[Math. Net], (22 sep 2011).

[16] W. Meissner, Uber die Teilbarkeit von 2^{p-1} durch das quadrat der primzahl $p = 1093$, sitz ungsberichte der Akademie der wissenschaften, Berlin pages 663–667, (1913)volume 35.

[17] R. Mestrovic, An elementary proof of congruence by Skula and Granville, arXiv : 1108.2361v1 [math.NT](11 octobre 2011).

[18] D. Mirimanoff, Sur la congruence $(q_p(r) = (r^{p-1} - 1)/p(modp)$, journal fur die reine und angewandte Mathematik(1895), pages295–300, volume 115.

[19] D. Mirimanoff, "Sur le dernier théorème de Fermat et le Critérium de M. A. Wieferich "(1910), volume 11(1909), pages 455–459.

[20] L. Pomey, Nouvelles annales de mathématiques, trois demonstrations des théorèmes de Fermat et de Wilson 4 ème serie, (1919)volume 19, pages 373–380.

[21] J. Sondow, Lerch Quotient, Lerch primes, Fermat- Wilson Quotients, and the Wieferich - non - Wilson Primes 2,3, 14771, arXiv : 1110. 3113v5[math.NT](6 Dec 2012).

[22] Z.W. Sun, Arithmetic theory of harmonic numbers, Proc. Amer. Math. Soc., article in press ; preprint arXiv : 0911. 4433v3 [math. NT](2009).

[23] Z.W.Sun, Arithmetic theory of Harmonic numbers.Proc.Amer.Maths.Soc.140, no.2,415-428.(2012).

[24] A. Wieferich,"Zum letzten Fermat'schen Theorem", journal fur die reine und angewandte Mathematics(1919), volume 136(3/6), pages 293– 302.

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