TER de L3 :
Identité de Kesava Menon et congruences de Ramanujan.

Dorian Perrot
Sous la direction de J.Riou

Année universitaire 2020/2021

Table des matières

1 Présentation du sujet.

Le TER est en deux parties. La première regroupe les chapitres 2, 3 et 4 et la seconde les chapitres 5 et 6.

La première partie est constituée de trois chapitres et a pour but de démontrer l'identité de Kesava Menon donnée à la page 2 de l'article [1] :

$$\forall n \in \mathbb{N}^*, \qquad \sum_{\overline{k} \in \mathbb{U}_n} (k-1) \wedge n = \varphi(n)\tau(n)$$

où $\mathbb{U}_n = (\mathbb{Z}/n\mathbb{Z})^\times$ désigne l'ensemble des inversibles de l'anneau $\mathbb{Z}/n\mathbb{Z}$,
φ est la fonction indicatrice d'Euler
et τ la fonction nombre de diviseurs.
On montrera aussi l'une de ses généralisation donnée à la page 2 de l'article [2] :

$$\forall n \in \mathbb{N}^*, \forall f \in \mathbb{Z}[X], \qquad \sum_{\overline{k} \in \mathbb{U}_n} (f(k) \wedge n) = \varphi(n) \cdot \sum_{d|n} \#\{r \in \mathbb{U}_d, f(r) = 0 \pmod d\}$$

Pour obtenir ces relations, il est nécessaire d'introduire le produit de convolution de Dirichlet (chapitre 2) et de voir ou revoir des résultats sur les anneaux $\mathbb{Z}/n\mathbb{Z}$ (chapitre 3). Une fois ceci terminé, on démontrera les relations dans le chapitre 4.

La seconde partie est constituée de deux chapitres qui se veulent indépendants et a pour objectif de démontrer une des congruences de Ramanujan de l'article [7] :

$$\forall k \in \mathbb{N}, \qquad p(5k+4) \equiv 0 \pmod 5$$

où $p(n)$ désigne le nombre de partition de l'entier n.
Le chapitre 5 a pour but d'introduire des notations, définitions et de comprendre des relations utilisées dans la partie suivante. En particulier, on reprendra des calculs effectués dans [5] et [6]. Enfin le chapitre 6 a pour objectif de démontrer la congruence de Ramanujan présentée ci-dessus.

2 Convolution de Dirichlet.

2.1 Définitions

♣ **Définition.** Une fonction arithmétique f est une application définie sur l'ensemble des entiers strictement positifs et à valeur dans l'ensemble des nombres complexes.

♣ **Définition.** La convolution de Dirichlet des fonctions arithmétiques f et g est la fonction :

$$f * g : n \in \mathbb{N}^* \mapsto \sum_{d|n} f(d) g\left(\frac{n}{d}\right) = \sum_{ab=n} f(a)g(b) \in \mathbb{C}$$

Remarque (1) : La fonction $f * g$ est arithmétique et donc $*$ définie une loi de composition interne sur l'ensemble des fonctions arithmétiques.

Remarque (2) : Comme la multiplication est commutative dans $\mathbb{C}$ et dans $\mathbb{N}^*$ alors pour tout entier n strictement positifs on a $(f*g)(n) = (g*f)(n)$ et donc $f*g = g*f$, autrement dit la loi $*$ est commutative.

Proposition 2.1
La loi $*$ est associative.

Démonstration : Soit f, g, h des fonctions arithmétiques et $n \in \mathbb{N}^*$. On a les égalités suivantes :

$$((f*g)*h)(n) = \sum_{dc=n} (f*g)(d)h(c) = \sum_{dc=n} \sum_{ab=d} f(a)g(b)h(c) = \sum_{abc=n} f(a)g(b)h(c)$$

Or par un calcul identique on montre que $(f*(g*h))(n) = \sum_{abc=n} f(a)g(b)h(c)$ ce qui permet de conclure.■

2.2 Fonctions multiplicatives

♣ **Définition.** Une fonction arithmétique f est dite multiplicative si $f(1) = 1$ et si pour tous entiers n, m premiers entre eux on a : $f(mn) = f(m)f(n)$.

Proposition 2.2 (produit de deux fonctions multiplicatives)
Si f et g sont deux fonctions multiplicatives alors $f * g$ est multiplicative.

Démonstration : soit $m, n \in \mathbb{N}^*$ avec $m \wedge n = 1$, on a :

$$\begin{aligned}
(f*g)(mn) &= \sum_{d|mn} f(d)g\left(\frac{mn}{d}\right) \\
&= \sum_{\substack{d|m \\ d'|n}} f(dd')g\left(\frac{m}{d}\frac{n}{d'}\right) && \text{car } m \wedge n = 1 \\
&= \sum_{\substack{d|m \\ d'|n}} f(d)f(d')g\left(\frac{m}{d}\right)g\left(\frac{n}{d'}\right) && \text{car } f \text{ et } g \text{ sont multiplicatives} \\
&= \left(\sum_{d|m} f(d)g\left(\frac{m}{d}\right)\right)\left(\sum_{d'|n} f(d')g\left(\frac{n}{d'}\right)\right) \\
&= [(f*g)(m)]\,[(f*g)(n)]
\end{aligned}$$

■

2.3 Inversion de Möbius

Dans la suite, on désigne par :

- $\mathbf{1}$ la fonction constante égale à 1.
- id la fonction identité.
- χ_1 la fonction tel que $\chi_1(1) = 1$ et pour tout $n > 1, \chi_1(n) = 0$.

La fonction χ_1 est l'élément neutre de $*$. Autrement dit, pour toute fonction arithmétique g on a $g * \chi_1 = \chi_1 * g = g$.

♣ **Définition.** La fonction de Möbius $\mu : \mathbb{N} \longrightarrow \mathbb{C}$ est la fonction multiplicative telle que $\mu(1) = 1$ et pour tout nombre premier p et tout entier strictement positif k on ait $\mu(p^k) = -1$ si $k = 1$ et $\mu(p^k) = 0$ sinon.

Example : On a ainsi $\mu(1) = 1$; $\mu(5) = -1$; $\mu(15) = 1$ etc...

Théorème 2.1 (Inversion de Möbius)
On a l'égalité suivante : $\mathbf{1} * \mu = \chi_1$.

Démonstration : La fonction χ_1 est multiplicative et comme les fonctions $\mathbf{1}$ et μ le sont aussi alors la fonction $\mathbf{1} * \mu$ est multiplicative. Il suffit donc de vérifier l'égalité annoncée seulement sur 1 et les puissances de nombres premiers.
Soit p un nombre premier et $k \in \mathbb{N}^*$, on a

$$(\mathbf{1} * \mu)(p^k) = \sum_{i=0}^{k} \mu(p^i) = \mu(1) + \mu(p) = 1 - 1 = 0 = \chi_1(p^k)$$

et $(\mathbf{1} * \mu)(1) = \mu(1) = 1 = \chi_1(1)$. ■

Grâce à ce théorème et à l'associativité du produit de convolution $(*)$, on peut énoncer le résultat suivant qui nous servira plus tard dans le chapitre (4).

Proposition 2.3
Pour tous $x \in \mathbb{N}^*$ on a

$$x = \sum_{d|x} (id * \mu)(d)$$

Démonstration : En utilisant l'inversion de Möbius, l'associativité et la commutativité de la loi $*$, il vient :

$$id = id * \chi_1 = id * (\mu * \mathbf{1}) = (id * \mu) * \mathbf{1}$$

En appliquant à x on a exactement $x = \sum_{d|x} (id * \mu)(d)$. ∎

3 Approfondissement des anneaux $\mathbb{Z}/n\mathbb{Z}$

3.1 Sous-groupes de $\mathbb{Z}/n\mathbb{Z}$

Proposition 3.1
Pour tout diviseur d de $n \geq 2$, il existe un unique sous-groupe de cardinal d de $\mathbb{Z}/n\mathbb{Z}$: l'ensemble $\{\overline{0}, \overline{e}, \overline{2e}, \cdots, \overline{(d-1)e}\} =< e >$ où $e = \frac{n}{d}$.

Démonstration : Soit d un diviseur de n.
Notons $e := \frac{n}{d}$ et $H := \{\overline{0}, \overline{e}, \cdots, \overline{(d-1)e}\}$. Comme $\overline{e}$ est d'ordre d alors H est un sous-groupe de cardinal d de $\mathbb{Z}/n\mathbb{Z}$, ce qui prouve l'existence.
Pour l'unicité, si F est un sous-groupe de $\mathbb{Z}/n\mathbb{Z}$ de cardinal d. Soit $\overline{a} \in F$, par le théorème de Lagrange $\overline{da} = \overline{0}$ donc il existe un entier k tel que $da = nk$. En divisant par d, on constate que $\overline{a}$ appartient à H. Par suite, $F \subset H$ et donc $H = F$ par égalité des cardinaux. ∎

Donnons un exemple d'application de la proposition précédente et de l'inversion de Möbius en montrant l'identité d'Euler. On a besoin de définir la fonction indicatrice d'Euler. [1]

♣ **Définition.** La fonction indicatrice d'Euler est la fonction notée φ définie par :

$$\begin{aligned} \varphi : \mathbb{N}^* &\to \mathbb{N}^* \\ n &\mapsto \#\{u \in \{1, \cdots, n\}; u \wedge n = 1\} \end{aligned}$$

Lemme 3.1 (identité d'Euler) *On a :*

$$\varphi = id * \mu$$

Démonstration : Soit $n \in \mathbb{N}^*$, on se place dans $\mathbb{Z}/n\mathbb{Z}$ alors :
$n = \sum_{d=1}^{n} \#\{k \in \mathbb{Z}/n\mathbb{Z}, ord(k) = d\} = \sum_{d|n} \#\{k \in \mathbb{Z}/n\mathbb{Z}, ord(k) = d\}$ car d'après le théorème de Lagrange l'ordre d'un élément d'un groupe fini divise l'ordre du groupe.
Soit d un diviseur de n, il n'y a qu'un seul sous-groupe H de cardinal d dans $\mathbb{Z}/n\mathbb{Z}$ et il est cyclique (proposition 3.1). Ainsi, $x \in \mathbb{Z}/n\mathbb{Z}$ est d'ordre d si et seulement s'il engendre H. Il y a donc $\varphi(d)$ éléments d'ordre d dans $\mathbb{Z}/n\mathbb{Z}$. On en déduit l'identité d'Euler : $n = \sum_{d|n} \varphi(d) = (\varphi * \mathbf{1})(n)$.
On a montré que $id = \varphi * \mathbf{1}$ et donc par inversion de Möbius que $id * \mu = \varphi$. ∎

Nous allons maintenant trouver le nombre de sous-groupes de $\mathbb{Z}/n\mathbb{Z}$. Pour cela nous avons besoin de définir la fonction "nombre de diviseurs".

♣ **Définition.** La fonction nombre de diviseurs est la fonction notée τ définie par :

$$\begin{aligned} \tau : \mathbb{N}^* &\to \mathbb{N}^* \\ n &\mapsto \#\{d \in \mathbb{N};\ \ d|n\} \end{aligned}$$

1. Pour plus de détail sur cette fonction, allez à la sous-section suivante (cf 3.2).

Remarque : On a $\tau = \mathbf{1} * \mathbf{1}$ et comme la fonction $\mathbf{1}$ est multiplicative alors la fonction τ l'est aussi d'après le chapitre 2.

Proposition 3.2 (Nombre de sous-groupes de $\mathbb{Z}/n\mathbb{Z}$)
Soit $n \geq 1$, il y a exactement $\tau(n)$ sous-groupes dans $\mathbb{Z}/n\mathbb{Z}$

Démonstration : L'application

$$\begin{aligned} \{\text{sous-groupes de } \mathbb{Z}/n\mathbb{Z}\} &\to \{\text{diviseurs de n}\} \\ H &\mapsto \#H \end{aligned}$$

est bien définie d'après le théorème de Lagrange et est une bijection d'après la proposition 3.1. Ainsi, $\tau(n)$ est exactement le nombre de sous-groupes de $\mathbb{Z}/n\mathbb{Z}$. ∎

3.2 Théorème des restes chinois et inversibles

Théorème 3.1 (théorème des restes chinois)
Soit $m, n \in \mathbb{N}^*$.
Si m est premier avec n alors l'application f définie par :

$$\begin{aligned} f : \mathbb{Z}/mn\mathbb{Z} &\to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \\ a \pmod{mn} &\mapsto (a \pmod{m}, a \pmod{n}) \end{aligned}$$

est un isomorphisme d'anneaux.

Démonstration : On vérifie que f est un morphisme d'anneaux et que $\#(\mathbb{Z}/mn\mathbb{Z}) = \#(\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z})$. Ainsi pour montrer que f est un isomorphisme il suffit de montrer que f est injective.
Soit $(x \pmod{mn}) \in \ker(f)$. En particulier, m divise x et n divise x. Or m et n sont premier entre eux et donc mn divise x. Mais alors $x = 0 \pmod{mn}$ et donc $\ker(f) = \{0\}$. Ainsi, f est un isomorphisme. ∎

Remarque : On peut vérifier que le morphisme réciproque de f est l'application $\psi : \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/mn\mathbb{Z}$ définie par $\psi(a \pmod{m}, b \pmod{n}) \mapsto (anv + bmu) \pmod{mn}$ où (u, v) est un couple d'entiers relatifs tel que $mu + nv = 1$ (qui existe d'après le théorème de Bézout).

♣ **Définition.** Si $n \geq 2$, on note $(\mathbb{Z}/n\mathbb{Z})^\times := \{u \in \mathbb{Z}/n\mathbb{Z}; \quad \exists v \in \mathbb{Z}/n\mathbb{Z}, uv = 1\}$ l'ensemble des inversibles de $\mathbb{Z}/n\mathbb{Z}$.

Proposition 3.3 (Inversibles de $\mathbb{Z}/n\mathbb{Z}$)
Soit $n \geq 2$. L'ensemble $(\mathbb{Z}/n\mathbb{Z})^\times$ est exactement l'ensemble $\{\overline{u} \in \mathbb{Z}/n\mathbb{Z}; \quad u \wedge n = 1\}$.

Démonstration : On a les équivalences suivantes :

$$\begin{aligned} \overline{u} \in (\mathbb{Z}/n\mathbb{Z})^\times &\Leftrightarrow \exists v \in \mathbb{Z}, \quad \overline{u} \cdot \overline{v} = 1 \\ &\Leftrightarrow \exists v \in \mathbb{Z}, \quad \overline{uv} = 1 \\ &\Leftrightarrow \exists v, k \in \mathbb{Z}, \quad uv = 1 + kn \\ &\Leftrightarrow u \wedge n = 1 \end{aligned}$$

∎

Remarque : On vient de montrer que de manière équivalente, on aurait pu définir la fonction indicatrice d'Euler comme : $\varphi : n \in \mathbb{N}^* \mapsto \#(\mathbb{Z}/n\mathbb{Z})^\times \in \mathbb{N}^*$.

Proposition 3.4
La fonction indicatrice d'Euler est multiplicative.

Démonstration : Soit $m, n \in \mathbb{N}^*$ tels que $m \wedge n = 1$.
D'après le théorème des restes chinois (3.1), il existe un isomorphisme de l'anneau $\mathbb{Z}/mn\mathbb{Z}$ vers l'anneau $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$. En particulier, les groupes $(\mathbb{Z}/mn\mathbb{Z})^\times$ et $(\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z})^\times$ sont isomorphes. On a aussi un isomorphisme entre $(\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z})^\times$ et $(\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times$. En passant au cardinal, on en déduit que $\varphi(mn) = \varphi(m)\varphi(n)$. ∎

Remarque : Alternativement, on a montré que $\varphi = id * \mu$. Comme id et μ sont multiplicatives alors φ l'est aussi.

3.3 Lemmes de relèvement

Dans ce qui suit, $\mathbb{U}_n$ désigne l'ensemble $(\mathbb{Z}/n\mathbb{Z})^\times$.

Lemme 3.2 (lemme de relèvement 1) *Soit $n \in N^*$ et d un diviseur de n, alors le morphisme canonique $\mathbb{U}_n \twoheadrightarrow \mathbb{U}_d, \quad \overline{x} \mapsto \overline{x}$ est surjective.*

Démonstration : Une récurrence sur le nombre de facteurs de $\frac{n}{d}$ permet de se ramener au cas où $\frac{n}{d} = p$ est premier.
Soit $u \in \{1, \cdots, d\}$ qui est premier avec d et $\frac{n}{d} = p$ premier, on distingue deux cas :
Soit $\frac{n}{d}$ divise d. Alors u qui est premier avec d l'est aussi avec n (car $\frac{n}{d}$ est supposé premier).
Soit $\frac{n}{d}$ ne divise pas d. Il se peut alors que u ne soit pas premier avec n (si $\frac{n}{d}$ divise u). Dans ce cas on pose $u' := u + d$ qui donne le même inversible que u modulo d. De plus $\frac{n}{d}$ ne divise pas u' et donc u' est inversible modulo n. ∎

Lemme 3.3 (lemme de relèvement 2) *Soit d un diviseur de $n \in \mathbb{N}^*$ et $l \in \mathbb{U}_d$ alors*

$$\#\{k \in \mathbb{U}_n, k = l \pmod d\} = \frac{\varphi(n)}{\varphi(d)}$$

Démonstration : D'après le lemme 3.2 le morphisme $f : (k \pmod n) \in \mathbb{U}_n \mapsto (k \pmod d) \in \mathbb{U}_d$ est surjectif donc tous les éléments de $\mathbb{U}_d$ ont le même nombre d'antécédents par f, et ce nombre est égal à $\#ker(f)$.
Par suite, $\#\{k \in \mathbb{U}_n, k = l \pmod d\} = \#f^{-1}(l) = \#kerf = \frac{\varphi(n)}{\varphi(d)}$ ∎

3.4 Formule de Burnside

♣ **Définition.** Soit G est un groupe opérant sur un ensemble X. Pour tout $g \in G$, on note $\mathrm{Fix}(g)$ l'ensemble défini par : $\mathrm{Fix}(g) = \{x \in X, \ \ g \cdot x = x\}$.

Remarque (1) : On note aussi cet ensemble $\mathrm{Fix}_X(g)$ ou encore X^g.

Remarque (2) : Si on note e l'élément neutre de G alors $\mathrm{Fix}(e) = X$.

Avant d'énoncer et démontrer la formule de Burnside, il faut se remémorer un résultat sur les actions de groupe.

Lemme 3.4 *Soit G un groupe opérant sur un ensemble X et $x \in X$. Pour tout y appartenant à l'orbite de x (noté $\omega(x)$) on a $\#\,\mathrm{Stab}(y) = \#\,\mathrm{Stab}(x)$.*

Démonstration : Soit $y \in \omega(x)$, il existe $g' \in G$ tel que $g' \cdot x = x$. On a les équivalences suivantes :

$$\begin{aligned} g \in \mathrm{Stab}(y) &\Leftrightarrow g \cdot y = y \\ &\Leftrightarrow g \cdot (g' \cdot x) = g' \cdot x \\ &\Leftrightarrow gg' \cdot x = g' \cdot x \\ &\Leftrightarrow g'^{-1} \cdot (gg' \cdot x) = g'^{-1} \cdot (g' \cdot x) \\ &\Leftrightarrow g'^{-1}gg' \cdot x = x \\ &\Leftrightarrow g'gg'^{-1} \in \mathrm{Stab}(x) \\ &\Leftrightarrow g \in g'\,\mathrm{Stab}(x)g'^{-1} \end{aligned}$$

On a donc montré que $\mathrm{Stab}(y) = g'\,\mathrm{Stab}(x)g'^{-1}$. En passant au cardinal, on a montré que pour tout y dans l'orbite de x, $\#\,\mathrm{Stab}(y) = \#\,\mathrm{Stab}(x)$. ∎

Théorème 3.2 (Formule de Burnside)
Soit G un groupe fini opérant sur un ensemble fini X. Le nombre d'orbites sous l'action de G est donné par la formule suivante :

$$\#\left(X/G\right) = \frac{1}{\#G}\sum_{g\in G}\#\operatorname{Fix}(g)$$

Démonstration : Posons $F := \{(g,x) \in G\times X; g\cdot x = x\}$ et introduisons les projections $p : (g,x) \in F \mapsto g \in G$ et $q : (g,x) \in F \mapsto x \in X$.

Comme p et q sont définies sur F on a : $F = \bigsqcup_{x\in X} q^{-1}(\{x\}) = \bigsqcup_{g\in G} p^{-1}(\{g\})$.
On peut donc calculer le cardinal de F de deux façons.

D'une part, $F = \bigsqcup_{g\in G} p^{-1}(\{g\})$. Comme pour tout $g \in G$ les ensembles $p^{-1}(\{g\})$ et $\operatorname{Fix}(g)$ sont en bijection, alors $\#p^{-1}(\{g\}) = \#\operatorname{Fix}(g)$ pour tout $g \in G$ et donc $\#F = \sum_{g\in G}\#\operatorname{Fix}(g)$.
D'autre part, $F = \bigsqcup_{x\in E} q^{-1}(\{x\})$ Comme pour tout $x \in X$ les ensembles $q^{-1}(\{x\})$ et $\operatorname{Stab}(x)$ sont en bijection, alors $\#q^{-1}(\{x\}) = \#\operatorname{Stab}(x)$ pour tout $x \in X$ et donc $\#F = \sum_{x\in X}\#\operatorname{Fix}(g)$. En utilisant le lemme précédent, on peut réécrire cette somme :

$$\#F = \sum_{\overline{x}\in X/G}\ \sum_{y\in\omega(x)}\#\operatorname{Stab}(x)$$

Par suite,

$$\#F = \sum_{\overline{x}\in X/G}\#\omega(x)\#\operatorname{Stab}(x) = \sum_{\overline{x}\in X/G}\#G = \#\left(X/G\right)\#G$$

On a donc montré que $\#\left(X/G\right)\#G = \#F = \sum_{g\in G}\#\operatorname{Fix}(g)$. La formule de Burnside s'en déduit. ∎

4 Identité de Kesava Menon

4.1 Énoncé et première démonstration

L'identité de Kesava Menon peut être appréhendée avec le lemme de Burnside. C'est ce qui est rapidement fait dans [1, p.2] et que nous allons détailler maintenant.

Théorème 4.1 (Identité de Kesava Menon)
Pour tout n dans $\mathbb{N}^*$ on a :

$$\sum_{\overline{k}\in\mathbb{U}_n}(k-1)\wedge n = \varphi(n)\tau(n) \tag{1}$$

Démonstration : Soit $n \in \mathbb{N}^*$, on fait agir le groupe $\mathbb{U}_n = (\mathbb{Z}/n\mathbb{Z})^\times$ sur $\mathbb{Z}/n\mathbb{Z}$ par $(k,a) \in \mathbb{U}_n \times \mathbb{Z}/n\mathbb{Z} \longmapsto ka \in \mathbb{Z}/n\mathbb{Z}$. La formule de Burnside donne alors :

$$\#\left(\mathbb{Z}/n\mathbb{Z}\ \middle/\ \mathbb{U}_n\right) = \frac{1}{\#\mathbb{U}_n}\sum_{k\in\mathbb{U}_n}\#\operatorname{Fix}\left(k\right) \tag{2}$$

• On sait que $\#\mathbb{U}_n = \varphi(n)$ par définition de φ.

• Déterminons $\#\left(\mathbb{Z}/n\mathbb{Z}\ \middle/\ \mathbb{U}_n\right)$, c'est-à-dire le nombre d'orbites pour l'action de $\mathbb{U}_n$ sur $\mathbb{Z}/n\mathbb{Z}$.

Notons $\omega(x)$ l'orbite de x et montrons que l'application

$$\begin{array}{rcl} \psi : \mathbb{Z}/n\mathbb{Z} \Big/ \mathbb{U}_n & \to & \{\text{diviseurs de } n\} \\ \omega(x) & \mapsto & \#<x> \end{array}$$

est une bijection.
Pour commencer, ψ est bien définie car si $b \in \omega(a)$ ($a \in \mathbb{Z}/n\mathbb{Z}$), il existe $k \in \mathbb{U}_n$ tel que $b = ka$ donc $<b> \subset <a>$. Or $k \wedge n = 1$ donc l'application $x \in \mathbb{Z}/n\mathbb{Z} \mapsto kx \in \mathbb{Z}/n\mathbb{Z}$ est un automorphisme, donc a et $ka = b$ ont le même ordre. Comme $<b> \subset <a>$ alors $<b> = <a>$.
Par le théorème de Lagrange, ψ est bien à valeurs dans l'ensemble des diviseurs de n.
D'après la proposition 3.1, ψ est surjective.
Enfin montrons que ψ est injective. Supposons que $\psi(\omega(a)) = \psi(\omega(b)) =: l$ alors d'après la proposition 3.1 $<a> = <b>$. Ainsi, il existe $k \in \mathbb{Z}/l\mathbb{Z}$ tel que $b = ka$. On a $k \wedge l = 1$ car b est d'ordre l dans $<a>$ qui est de cardinal l, donc $k \in \mathbb{U}_l$. Pour terminer, il faut relever k (qui est défini modulo l) dans $\mathbb{Z}/n\mathbb{Z}$ en un élément inversible. Ce qui est toujours possible (car l divise n) d'après le lemme de relèvement (3.2). Par suite, il existe $\overline{k} \in \mathbb{U}_n$ tel que $b = \overline{k}a$ et donc $\omega(a) = \omega(b)$.
En conclusion ψ est une bijection est donc $\#\left(\mathbb{Z}/n\mathbb{Z} \Big/ \mathbb{U}_n\right) = \tau(n)$.

• Enfin, déterminons pour $k \in \mathbb{U}_n$ le cardinal de $\mathrm{Fix}(k) = \{x \in \mathbb{Z}/n\mathbb{Z}; (k-1)x = 0\}$. Notons $d := (k-1) \wedge n$, $(k-1)' := (k-1)/d$ et $n' := n/d$. On a les équivalences suivantes :

$$\begin{array}{rcll} x \in \mathrm{Fix}(k) & \Leftrightarrow & (k-1)x = 0 \pmod{n} & \\ & \Leftrightarrow & (k-1)'x \in <n'> & \\ & \Leftrightarrow & x \in <n'> & \text{car } (k-1)' \wedge n' = 1. \end{array}$$

On en déduit que $\#\,\mathrm{Fix}(k) = \#<n'> = d = (k-1) \wedge n$.

En injectant ces résultats sur les cardinaux dans l'équation (2), on trouve le résultat souhaité. ∎

4.2 Une approche personnelle

Dans cette section, je propose une autre démonstration de l'identité de Kesava Menon (théorème 4.1) que j'ai rédigée et qui n'utilise pas la formule de Burnside.
On commence par montrer que la fonction qui suit (notée F) est multiplicative. Comme les fonctions φ et τ le sont aussi, pour démontrer le théorème 4.1 il suffira de le montrer juste pour les puissances de nombres premiers.

Lemme 4.1 *La fonction $F : \mathbb{N}^* \mapsto \mathbb{N}$ définie par $F(n) = \sum_{\overline{k} \in \mathbb{U}_n} (k-1) \wedge n$ est multiplicative.*

Démonstration : Soit a, b des entiers strictement positifs et premiers entre eux.
En particulier, pour tout entier k, on a $k \wedge ab = (k \wedge a) \cdot (k \wedge b)$. On en déduit que :

$$F(ab) = \sum_{\overline{k} \in \mathbb{U}_{ab}} (k-1) \wedge ab = \sum_{\overline{k} \in \mathbb{U}_{ab}} ((k-1) \wedge a) \cdot ((k-1) \wedge b)$$

Si on note $\overline{k_1} = \overline{k} \pmod{a}$ et $\overline{k_2} = \overline{k} \pmod{b}$ alors $(k \wedge a) \cdot (k \wedge b) = (k_1 \wedge a) \cdot (k_2 \wedge b)$.
De plus, grâce au théorème des restes chinois (3.1) on avait montré dans la proposition 3.4 que les groupes $(\mathbb{Z}/ab\mathbb{Z})^\times$ et $(\mathbb{Z}/a\mathbb{Z})^\times \times (\mathbb{Z}/b\mathbb{Z})^\times$ étaient isomorphes. On en déduit que :

$$\begin{aligned} F(ab) &= \sum_{\overline{k} \in \mathbb{U}_{ab}} ((k_1 - 1) \wedge a) \cdot ((k_2 - 1) \wedge b) \\ &= \left(\sum_{\overline{k_1} \in \mathbb{U}_a} ((k_1 - 1) \wedge a \right) \left(\sum_{\overline{k_2} \in \mathbb{U}_b} ((k_2 - 1) \wedge b \right) \\ &= F(a)F(b) \end{aligned}$$

∎

En conservant les notations du lemme, on peut écrire une autre démonstration de l'identité de Kesava Menon dont on rappelle l'énoncé :

Théorème 4.2 (Identité de Kesava Menon)
Pour tout n dans $\mathbb{N}^*$ on a :

$$F(n) = \sum_{\overline{k} \in \mathbb{U}_n} (k-1) \wedge n = \varphi(n)\tau(n)$$

Démonstration (méthode alternative) : D'après le lemme précédent et de ce qui précède, les fonctions F, φ et τ sont multiplicatives. Ainsi, pour démontrer l'identité voulue il suffit de la montrer seulement pour les puissances de nombres premiers. Soit p un nombre premier et a un entier strictement positif.
D'une part, on a $\tau(p^a)\varphi(p^a) = (a+1)(p^a - p^{a-1})$
D'autre part, $F(p^a) = \sum_{\overline{k} \in \mathbb{U}_{p^a}} (k-1) \wedge p^a$. On cherche à comprendre quelles sont les termes de cette dernière somme. Plus exactement, il faut trouver quelles sont les termes "manquants" par rapport à $\sum_{\overline{k} \in \mathbb{Z}/p^a\mathbb{Z}} (k-1) \wedge p^a$. Or on a :

$$\sum_{\overline{k} \in \mathbb{Z}/p^a\mathbb{Z}} (k-1) \wedge p^a = \sum_{\overline{k} \in \mathbb{U}_{p^a}} (k-1) \wedge p^a + \sum_{\substack{\overline{k} \in \mathbb{Z}/p^a\mathbb{Z} \\ p|k}} \underbrace{(k-1) \wedge p^a}_{=1} = \sum_{\overline{k} \in \mathbb{U}_{p^a}} (k-1) \wedge p^a + p^{a-1} \tag{3}$$

Enfin, on a aussi par ré-indexation et calcul explicite :

$$\sum_{\overline{k} \in \mathbb{Z}/p^a\mathbb{Z}} (k-1) \wedge p^a = \sum_{\overline{k} \in \mathbb{Z}/p^a\mathbb{Z}} k \wedge p^a$$

On décompose la somme selon les valeurs p^{a-i} du pgcd :

$$\begin{aligned} &= p^a + \sum_{i=1}^{a-1} (p^i - p^{i-1}) p^{a-i} + \varphi(p^a) \\ &= p^a + \sum_{i=1}^{a-1} (p^a - p^{a-1}) + (p^a - p^{a-1}) \\ &= (a-1)(p^a - p^{a-1}) + 2p^a - p^{a-1} \end{aligned}$$

On en déduit avec (3) que

$$\sum_{\overline{k} \in \mathbb{U}_{p^a}} (k-1) \wedge p^a = (a-1)(p^a - p^{a-1}) + 2p^a - 2p^{a-1} = (a+1)(p^a - p^{a-1}) = \tau(p^a)\varphi(p^a)$$

.
De fait, pour tout nombre premier p et entier strictement positif a, on a bien $\sum_{\overline{k} \in \mathbb{U}_{p^a}} (k-1) \wedge p^a = \varphi(p^a)\tau(p^a)$
ce qui termine la preuve. ∎

4.3 Une généralisation

L'article de M.Richards [2, p.2] donne une formule plus générale de l'identité de Kesava Menon (théorème 4.1), en voici l'énoncé :

Théorème 4.3
Soit $n \in \mathbb{N}^*$ et $f \in \mathbb{Z}[X]$ alors :

$$\sum_{\overline{k} \in \mathbb{U}_n} (f(k) \wedge n) = \varphi(n) \cdot \sum_{d|n} \#\{r \in \mathbb{U}_d, f(r) = 0 \pmod d\} \tag{4}$$

Grâce au livre de V.Sita Ramaiah [4], on peut comprendre et extraire une démonstration de ce théorème qui est donnée dans l'article de P.Haukkanen et J.Wang [3] où une formule beaucoup plus générale est établie.

Démonstration : Soit n un entier strictement positif et $f \in \mathbb{Z}[X]$.
Si $k \in \mathbb{N}^*$, alors la proposition 2.3 appliquée à $x = f(k) \wedge n$ et le lemme 3.1 permettent d'affirmer que $f(k) \wedge n = \sum_{\substack{d|f(k) \\ d|n}} \varphi(d)$ car d divise $f(k) \wedge n$ si et seulement si d divise $f(k)$ et d divise n. On en déduit que :

$$\sum_{\overline{k} \in \mathbb{U}_n} f(k) \wedge n = \sum_{\overline{k} \in \mathbb{U}_n} \sum_{\substack{d|f(k) \\ d|n}} \varphi(d) \tag{5}$$

Si on note $D(n)$ l'ensemble des diviseurs (positifs) de n, alors dans le membre de droite on somme sur l'ensemble $\{(\overline{k}, d) \in \mathbb{U}_n \times D(n), d|f(k)\}$ par rapport à $\overline{k} \in \mathbb{U}_n$. Si on somme par rapport à $d \in D(n)$ on en déduit que :

$$\sum_{\overline{k} \in \mathbb{U}_n} \sum_{\substack{d|f(k) \\ d|n}} \varphi(d) = \sum_{d|n} \sum_{\substack{\overline{k} \in \mathbb{U}_n \\ d|f(k)}} \varphi(d) = \sum_{d|n} \varphi(d) \#\{\overline{k} \in \mathbb{U}_n, f(k) = 0 \pmod d\} \tag{6}$$

On continue en fixant un d (diviseur positif de n). On remarque que si $k = l \pmod d$ alors $f(k) = f(l) \pmod d$. On a donc les égalités ensemblistes :

$$\begin{aligned} \{\overline{k} \in \mathbb{U}_n, f(k) = 0 \pmod d\} &= \bigsqcup_{\overline{l} \in \mathbb{Z}/l\mathbb{Z}} \{\overline{k} \in \mathbb{U}_n, \quad k = l \pmod d \text{ et } f(l) = 0 \pmod d\} \\ &= \bigsqcup_{\substack{\overline{l} \in \mathbb{U}_d \\ d|f(l)}} \{\overline{k} \in \mathbb{U}_n, k = l \pmod d\} \end{aligned}$$

Ainsi, en passant au cardinal puis en utilisant le lemme 3.3 on a :

$$\#\{\overline{k} \in \mathbb{U}_n, f(k) = 0 \pmod d\} = \sum_{\substack{\overline{l} \in \mathbb{U}_d \\ d|f(l)}} \#\{\overline{k} \in \mathbb{U}_n, k = l \pmod d\} = \frac{\varphi(n)}{\varphi(d)} \#\{\overline{l} \in \mathbb{U}_d, f(l) = 0 \pmod d\}$$

En injectant dans l'égalité (6) combinée avec (5), on trouve que :

$$\sum_{\overline{k} \in \mathbb{U}_n} f(k) \wedge n = \varphi(n) \sum_{d|n} \#\{\overline{l} \in \mathbb{U}_d, f(l) = 0 \pmod d\}$$ ∎

Remarque : En prenant le polynôme $f(X) = X - 1$, on retrouve exactement l'identité de Kesava Menon (théorème 4.1).

5 Congruence de Ramanujan : début de la démonstration

Cette section et la suivante sont indépendantes. Ce chapitre a pour but d'introduire des notations et de comprendre les relations présentées au début de la partie suivantes (sous-section 6.1).

5.1 Énoncé

♣ **Définition (partition d'un entier, $p(n)$).** Soit $n \in \mathbb{N}$, une partition de n consiste en la donnée d'un entier naturel l et d'un l-uplet $(a_1, a_2, \cdots, a_l)$ d'entiers strictement positifs tels que $a_1 \geq a_2 \geq \cdots \geq a_l$ et $a_1 + a_2 + \cdots + a_l = n$.
On note $p(n)$ le nombre de partitions de l'entier n. On convient de poser $p(n) = 0$ pour $n < 0$.

Voici le tableau des onze premières valeurs de $p(n)$:

n	0	1	2	3	4	5	6	7	8	9	10
$p(n)$	1	1	2	3	5	7	11	15	22	30	42

On remarque que $p(4)$ et $p(9)$ sont divisibles par 5 et que $4 = 5 \times 0 + 4$ et $9 = 5 \times 1 + 4$. En fait pour tout $k \in \mathbb{N}$, tout les $p(5k+4)$ sont divisibles par 5 : c'est une des congruences de Ramanujan. C'est ce que nous allons démontrer.

Théorème 5.1 (Congruence Ramanujan)
Pour tout entier naturel k, on a :

$$p(5k+4) \equiv 0 \pmod 5$$

5.2 Notations

5.2.1 Les séries formelles $\Phi_{r,s}$

♣ **Définition.** Pour tout couple $(r,s) \in \mathbb{N}^2$, on note $\Phi_{r,s} = \sum_{m\geq 1, n\geq 1} m^r n^s X^{mn} \in \mathbb{Z}[[X]]$.

En utilisant [5, exercice 1], on montre que la famille définissant $\Phi_{r,s}$ est bien sommable et les propriétés suivantes :

Proposition 5.1
1. $\forall (r,s) \in \mathbb{Z}^2 : \Phi_{r,s} = \Phi_{s,r}$
2. $\forall s \geq 0 : \Phi_{0,s} = \sum_{n=1}^{\infty} \frac{n^s X^n}{1-X^n}$
3. $\forall s \geq 0 : \Phi_{1,s} = \sum_{n=1}^{\infty} \frac{n^s X}{(1-X^n)^2}$
4. $\forall (r,s) \in \mathbb{Z}^2 : X\Phi'_{r,s} = \Phi_{r+1,s+1}$

Démonstration : 1. Il suffit d'échanger le rôle des indices m et n au niveau de la somme.

2. On a $\Phi_{0,s} = \sum_{n=1}^{\infty} n^s \sum_{m=1}^{\infty} (X^n)^m = \sum_{n=1}^{\infty} \frac{n^s X^n}{1-X^n}$

3. On a : $\Phi_{1,s} = \sum_{n=1}^{\infty} n^s \sum_{m=1}^{\infty} m(X^n)^m = \sum_{n=1}^{\infty} n^s \frac{X^n}{(1-X^n)^2}$.
   La dernière égalité vient du fait que $\sum_{m=1}^{\infty} mY^m = Y\frac{d}{dY}\left(\sum_{m=1}^{\infty} Y^m\right) = Y\frac{d}{dY}\left(\frac{Y}{1-Y}\right) = \frac{Y}{(1-Y)^2}$.

4. On a $X\Phi'_{r,s} = X \sum_{m\geq 1, n\geq 1} m^r n^s (mn) X^{mn-1} = \sum_{m\geq 1, n\geq 1} m^{r+1} n^{s+1} X^{mn} = \Phi_{r+1,s+1}$ ∎

Remarque : Plus précisément, on montre dans [5, exercice 1] que si $r \geq s$ alors $\Phi_{r,s} = \sum_{k=1}^{\infty} \left(k^s \sum_{m|k} m^{r-s} \right) X^k$.

5.2.2 Les nombres B_n

Posons $h : x \in \mathbb{R}^* \mapsto \frac{x}{e^x - 1}$ qui est prolongeable en 0 et est développable en série entière au voisinage de 0. Notons H sa série de Taylor en 0.

♣ **Définition.** Pour tout entier naturel n, on note B_n le n-ième nombre de Bernoulli. La série génératrice exponentielle des nombres de Bernoulli est donnée par H. Autrement dit, $H = \sum_{n=0}^{\infty} B_n \frac{x^n}{n!}$.

Voici les onze premiers nombres de Bernoulli :

n	0	1	2	3	4	5	6	7	8	9	10
B_n	1	$-\frac{1}{2}$	$\frac{1}{6}$	0	$-\frac{1}{30}$	0	$\frac{1}{42}$	0	$-\frac{1}{30}$	0	$\frac{5}{66}$

Il existe un lien entre les nombres de Bernoulli et la fonction cotangente dont on rappelle la définition.

♣ **Définition.** La fonction cotangente est la fonction notée cotan définie par :

$$\begin{aligned} \text{cotan} : \mathbb{R} - \pi\mathbb{Z} &\to \mathbb{R} \\ x &\mapsto \frac{\cos(x)}{\sin(x)} \end{aligned}$$

Remarque : Géométriquement, si on note A le point de coordonnées $(\cos(x), \sin(x))$. Alors $\text{cotan}(x)$ désigne l'abscisse du point d'intersection entre la droite d'équation $y = 1$ et la droite dirigée par le vecteur directeur $\overrightarrow{OA}$.

Proposition 5.2

1. *Pour tout $n \geq 1$, $B_{2n+1} = 0$*

2. *Il existe $\epsilon > 0$ tel que pour tout $\theta \in]-\epsilon, \epsilon[-\{0\}$, on ait :*

$$\frac{\theta}{2}\text{cotan}\left(\frac{\theta}{2}\right) = \sum_{n=0}^{\infty}(-1)^n \frac{B_{2n}\theta^{2n}}{(2n)!} \tag{7}$$

3. *Il existe $\epsilon > 0$ tel que pour tout $\theta \in]-\epsilon, \epsilon[-\{0\}$, on ait :*

$$\left(\frac{\theta}{2}\text{cotan}\left(\frac{\theta}{2}\right)\right)^2 = 1 - \frac{\theta^2}{4} + \sum_{n=1}^{\infty}(-1)^{n+1} \frac{B_{2n}\theta^{2n}}{(2n)(2n-2)!} \tag{8}$$

Démonstration (idée) : 1. On commence par montrer que :

$$(H(X) - B_1X - [H(-X) - B_1(-X)])\underbrace{(e^X - 1)}_{\neq 0} = 0$$

Ainsi $H(X) - B_1X = H(-X) - B_1(-X)$ donc $H(X) - B_1X$ est pair, d'où le résultat.

2. On commence par montrer que les fonctions $y \mapsto \cos(y/2)$ et $y \mapsto \frac{y/2}{\sin(y/2)}$ sont développables en série entière au voisinage de 0. On note respectivement $A = \frac{1}{2}(e^{iX/2} + e^{-iX/2})$ et $B = iX(e^{iX/2} - e^{-iX/2})^{-1}$ leur série de Taylor en 0. Ainsi, AB est la série de Taylor en 0 de la fonction $y \mapsto \frac{y}{2}\text{cotan}\left(\frac{y}{2}\right)$. De plus :

$$\begin{aligned} AB &= \frac{iX}{2}\frac{e^{iX}+1}{e^{iX}-1} \\ &= \frac{iX}{2(e^{iX}-1)}(e^{iX}+1) \\ &= \frac{1}{2}H(iX)(e^{iX} - 1 + 2) \\ &= H(iX) - \left(-\frac{iX}{2}\right) \end{aligned}$$

Or $B_1 = -\frac{1}{2}$ et d'après le point 1, tout les termes impairs de $H(iX) - \left(-\frac{iX}{2}\right)$ sont nulles. On considère donc que les termes pairs de la somme.
Enfin, si θ appartient au domaine de convergence des séries définies plus haut (ce qui permet de définir notre $\epsilon > 0$) , alors :

$$\frac{\theta}{2}\text{cotan}\left(\frac{\theta}{2}\right) = \sum_{n=0}^{\infty}(-1)^n \frac{B_{2n}\theta^{2n}}{(2n)!}$$

3. On considère le même $\epsilon > 0$ qu'au point précédent et on conclut en utilisant l'égalité (7) et en remarquant que $\text{cotan}'(x) = -(1 + \text{cotan}^2(x))$. ∎

Remarque : Pour plus de détail sur cette démonstration et de relations sur les nombres de Bernoulli, on regardera [5, exercice 2].

5.3 Relations cruciales

5.3.1 Les C_n et relation fonctionnelle

Proposition 5.3
Il existe une famille sommable $(C_n)_{n\geq 0}$ de séries formelles appartenant à $\mathbb{Q}[[X]]$ telles que pour tout $\theta \in \mathbb{R} - \pi\mathbb{Z}$, on ait l'égalité suivante dans $\mathbb{R}[[X]]$:

$$\left(\frac{1}{4}\text{cotan}\left(\frac{\theta}{2}\right) + \sum_{n=1}^{\infty}\frac{\sin(n\theta)X^n}{1-X^n}\right)^2 = \frac{1}{16}\text{cotan}^2\left(\frac{\theta}{2}\right) + \sum_{n\in\mathbb{N}}\cos(n\theta)C_n \tag{9}$$

Démonstration (idée) : Soit $\theta \in \mathbb{R} - \pi\mathbb{Z}$.
Posons $A(\theta) := \frac{1}{4}\text{cotan}\left(\frac{\theta}{2}\right) + \sum_{n=1}^{\infty}\frac{\sin(n\theta)X^n}{1-X^n} \in \mathbb{R}[[X]]$. On commence par développer $A^2(\theta)$:

$$\begin{aligned} A^2(\theta) &= \frac{1}{16}\text{cotan}^2\left(\frac{\theta}{2}\right) + \frac{1}{2}\text{cotan}\left(\frac{\theta}{2}\right)\sum_{n=1}^{\infty}\frac{\sin(n\theta)X^n}{1-X^n} + \left(\sum_{n=1}^{\infty}\frac{\sin(n\theta)X^n}{1-X^n}\right)^2 \\ &= \frac{1}{16}\text{cotan}^2\left(\frac{\theta}{2}\right) + \sum_{n=1}^{\infty}\frac{\frac{1}{2}\text{cotan}\left(\frac{\theta}{2}\right)\sin(n\theta)X^n}{1-X^n} + \sum_{n\geq 1, m\geq 1}\frac{\sin(n\theta)\sin(m\theta)X^{n+m}}{(1-X^n)(1-X^m)} \end{aligned}$$

L'idée est de retirer tout les cotan et sin dans les deux sommes pour n'avoir que des cos. C'est possible car on sait que :

$$\forall\theta \in \mathbb{R}, \forall n, n' \in \mathbb{Z} : \sin(n\theta)\sin(n'\theta) = \frac{1}{2}\left(\cos((n-n')\theta) - \cos((n+n')\theta)\right)$$

et que :

$$\forall\theta \in \mathbb{R} - \pi\mathbb{Z}, \forall n \in \mathbb{N}^* : \text{cotan}\left(\frac{\theta}{2}\right)\sin(n\theta) = 1 + 2\sum_{k=1}^{n-1}\cos(k\theta) + \cos(n\theta)$$

On injecte ensuite ces expressions dans les sommes précédentes afin de n'avoir que des cosinus dans celles-ci. Pour obtenir les C_n, il suffit alors de regrouper les termes en $\cos(n\theta)$.
On trouve que : $C_0 = \frac{1}{2}\sum_{n=1}^{\infty}\frac{X^n}{(1-X^n)^2} = \frac{1}{2}\Phi_{1,0} = \frac{1}{2}\Phi_{0,1} = \frac{1}{2}\sum_{n=1}^{\infty}\frac{nX^n}{1-X^n}$.
et pour tout $n \geq 1 : C_n = \frac{1}{2}\frac{X^n}{1-X^n} + \sum_{k=1}^{\infty}\frac{X^{n+k}}{1-X^{n+k}} + \sum_{k=1}^{\infty}\frac{X^{n+2k}}{(1-X^k)(1-X^{n+k})} - \frac{1}{2}\sum_{k=1}^{n-1}\frac{X^n}{(1-X^k)(1-X^{n-k})}$
Ce qui précède montre l'existence de la famille sommable $(C_n)_{n\geq 0}$. Maintenant on va simplifier l'expression des C_n pour $n \geq 1$.
On commence par montrer que pour $n \geq 1$:

$$\frac{(1-X^n)C_n}{X^n} = \frac{1}{2} + \sum_{k=1}^{\infty}\left(\frac{X^k}{1-X^k} - \frac{X^{n+k}}{1-X^{n+k}}\right) - \frac{1}{2}\sum_{k=1}n - 1\left(1 + \frac{X^k}{1-X^k} + \frac{X^{n-k}}{1-X^{n-k}}\right)$$

Pour cela on utilise que si $a, b \in X\mathbb{R}[[X]]$ alors d'une part :

$$\frac{(1-a)b}{1-ab} + \frac{(1-a)b^2}{(1-b)(1-ab)} = \frac{b}{(1-b)} - \frac{ab}{1-ab}$$

et d'autre part :

$$\frac{1-ab}{(1-a)(1-b)} = 1 + \frac{a}{1-a} + \frac{b}{1-b}$$

On déduit que pour tout $n \geq 1$, on a $C_n = \frac{X^n}{(1-X^n)^2} - \frac{nX^n}{2(1-X^n)}$. ∎

Remarque (1) : On a $\sum_{n=1}^{\infty} C_n = \Phi_{1,0} - \frac{1}{2}\Phi_{0,1} = \frac{1}{2}\Phi_{0,1} = C_0$.

Remarque (2) : Pour un calcul légèrement plus détaillé on regardera [5, exercice 3] ou [6, p.177-178].

5.3.2 Les séries formelles S_n et P, Q, R

Pour tout entier naturel n, on définit $S_n := \Phi_{0,n} - \frac{B_{n+1}}{2n+2} \in \mathbb{Q}[[X]]$. En particulier, les $(S_n)_{n\geq 0}$ permettent de relier les $\Phi_{0,n}$ avec les B_{n+1}.
On définit aussi P, Q et R comme :

$$P := -24S_1 = 1 - 24\Phi_{0,1}$$
$$Q := 240S_3 = 1 + 240\Phi_{0,3}$$
$$R := -504S_5 = 1 - 504\Phi_{0,5}$$

A la fin de ce chapitre, on verra comment sont reliés les P, Q et R entre eux. Pour cela, il faut trouver des relations entre les S_n. C'est l'objet des prochaines propositions.

Proposition 5.4
Pour tout entier pair n non nul on a :

$$\frac{n+3}{2(n+1)} S_{n+1} - \Phi_{1,n} = \sum_{\substack{i+j=n \\ i,j \text{ impairs}}} \binom{n}{i} S_i S_j \tag{10}$$

Démonstration (idée) : En utilisant la valeur des $(C_n)_{n\in\mathbb{N}}$ dans l'équation (9) on a :

$$\left(\frac{1}{4}\operatorname{cotan}\left(\frac{\theta}{2}\right) + \sum_{n=1}^{\infty} \frac{\sin(n\theta)X^n}{1-X^n}\right)^2 = \frac{1}{16}\operatorname{cotan}^2\left(\frac{\theta}{2}\right) + \sum_{n=1}^{\infty} \frac{X^n\cos(n\theta)}{(1-X^n)^2} + \frac{1}{2}\left(\sum_{n=1}^{\infty} \frac{nX^n}{1-X^n}(1-\cos(n\theta))\right)$$

Multiplions les deux membres de l'égalité précédente par θ^2 afin d'obtenir une égalité dans $\mathbb{R}[[X]]$ valable pour tout θ appartenant à un certain intervalle ouvert I contenant 0. On développe les $\sin(n\theta), \cos(n\theta)$, $\frac{\theta}{2}\operatorname{cotan}\left(\frac{\theta}{2}\right)$ et $\frac{\theta^2}{4}\operatorname{cotan}^2\left(\frac{\theta}{2}\right)$ en série entière (on utilise (7) et (8)). Notons l'identité obtenue par :

$$A^2(\theta) = B(\theta)$$

En fait, on peut penser à cette identité comme à une égalité entre les séries formelles A et B dont les coefficients sont des fonctions de θ. Ainsi, il existe des fonctions $\mathcal{C}^\infty$ de I dans $\mathbb{R}$, a_n et b_n telles que pour tout $\theta \in I$, on ait l'égalité suivante dans $\mathbb{R}[[X]]$:

$$A(\theta) = \sum_{n=0}^{\infty} a_n(\theta)X^n \qquad B(\theta) = \sum_{n=0}^{\infty} b_n(\theta)X^n$$

On a donc $A, B \in \mathcal{C}^\infty(I, \mathbb{R})[[X]]$.
Ensuite on considère le morphisme $g \in \mathcal{C}^\infty(I,\mathbb{R}) \mapsto \hat{g} \in \mathbb{R}[[T]]$ qui à $g \in \mathcal{C}^\infty(I,\mathbb{R})$ associe sa série de Taylor en 0. Ainsi :

$$\widehat{A} = \sum_{n=0}^{\infty} \widehat{a_n}X^n \qquad \widehat{B} = \sum_{n=0}^{\infty} \widehat{b_n}X^n$$

On a $\widehat{A}, \widehat{B} \in \mathbb{R}[[T]][[X]]$. Or $\mathbb{R}[[T]][[X]] = \mathbb{R}[[T,X]] = \mathbb{R}[[X]][[T]]$. On peut donc regarder le coefficient devant T^k dans l'égalité $\left(\widehat{A}\right)^2 = \widehat{B}$. On obtient exactement l'égalité souhaitée. ∎

Proposition 5.5
Pour tout entier pair $n \geq 4$ on a :

$$\frac{(n-2)(n+5)}{12(n+1)(n+2)} S_{n+3} = \sum_{\substack{i+j=n \\ i\geq 2, j\geq 2 \\ i,j \text{pairs}}} \binom{n}{i} S_{i+1} S_{j+1} \tag{11}$$

Démonstration (idée) : C'est le même raisonnement que la démonstration de la proposition précédente mais il ne faut pas partir de l'équation (9) mais de l'identité :

$$\left(\frac{1}{12} + \frac{1}{8}\operatorname{cotan}^2\left(\frac{\theta}{2}\right) + \sum_{n=1}^{\infty} \frac{nX^n}{1-X^n}(1-\cos(n\theta))\right)^2 = \left(\frac{1}{12} + \frac{1}{8}\operatorname{cotan}^2\left(\frac{\theta}{2}\right)\right)^2 + \frac{1}{12}\left(\sum_{n=1}^{\infty} \frac{n^3X^n}{1-X^n}(5+\cos(n\theta))\right)$$

Pour plus de détail, on regardera [6, p.178-179]. ∎

En particulier, si dans l'équation (11) on prend $n = 4$, on trouve que :

$$1 + 480\Phi_{0,7} = Q^2$$

En prenant successivement $n = 1, 3, 5$ dans l'équation (10), on trouve que [2] :

$$\begin{aligned} 288\Phi_{1,2} &= Q - P^2 \\ 720\Phi_{1,4} &= PQ - R \\ 1008\Phi_{1,6} &= Q^2 - PR \end{aligned}$$

6 Congruence de Ramanujan : fin de la démonstration

6.1 Formulaire

6.1.1 Résumé de la partie précédente

Dans la section précédente, on avait les relations suivantes dans $\mathbb{Q}[[X]]$:

$$\begin{aligned} S_n &:= \Phi_{0,n} - \frac{B_{n+1}}{2n+2} \qquad \text{pour tout } n \geq 0 \\ P &:= -24S_1 = 1 - 24\Phi_{0,1} \\ Q &:= 240S_3 = 1 + 240\Phi_{0,3} \\ R &:= -504S_5 = 1 - 504\Phi_{0,5} \end{aligned}$$

On a aussi :

$$1 + 480\Phi_{0,7} = Q^2 \tag{12}$$
$$288\Phi_{1,2} = Q - P^2 \tag{13}$$
$$720\Phi_{1,4} = PQ - R \tag{14}$$
$$1008\Phi_{1,6} = Q^2 - PR \tag{15}$$

Enfin en dérivant les P, Q et R et en utilisant ces dernières égalités, on trouve que :

$$X\frac{dP}{dX} = \frac{1}{12}(P - Q^2) \tag{16}$$
$$X\frac{dQ}{dX} = \frac{1}{3}(PQ - R) \tag{17}$$
$$X\frac{dR}{dX} = \frac{1}{2}(PR - Q^2) \tag{18}$$

2. Pour la dernière égalité ($n = 5$), il faut aussi utiliser $1 + 480\Phi_{0,7} = Q^2$.

Démonstration : Montrons juste l'égalité (16) (les deux autres égalités (17) et (18) se démontrent exactement de la même manière). On calcule :

$$X\frac{dP}{dX} = -24X\Phi'_{0,1} \overset{(*)}{=} -24\Phi_{1,2} \overset{(**)}{=} \frac{1}{12}(P - Q^2)$$

Pour l'égalité $(*)$ on utilise la proposition 5.1 et pour $(**)$ on utilise la relation (13). ∎

6.1.2 Série formelle f

Introduisons la série formelle $f := \prod_{n=1}^{\infty}(1 - X^n)$. D'après le cours de combinatoire algébrique (année 2020/2021) on a les relations :

$$f = 1 + \sum_{k\in\mathbb{Z}^*}(-1)^k X^{g_k} \qquad \text{avec } g_k = \frac{k(3k-1)}{2} \in \mathbb{N}^* \tag{19}$$

$$\frac{1}{f} = \sum_{n=0}^{\infty} p(n)X^n \tag{20}$$

6.2 Dernière relation

Pour bien comprendre la dernière égalité nécessaire pour montrer l'une des congruences de Ramanujan, il faut définir la notation "dlog P" où $P \in \mathbb{Q}[[X]]$.

♣ **Définition.** Soit A un anneau commutatif et soit $F = \sum_{n=0}^{\infty} a_n X^n \in A[[X]]$.
On note $\text{val}(F) := \inf\{n \in \mathbb{N}, \quad a_n \neq 0\} \in \mathbb{N} \cup \{\infty\}$. On appelle ce nombre la valuation de F.

♣ **Définition.** Soit $P \in \mathbb{Q}[[X]]$ et $P \neq 0$.
Si $\text{val}(P) = 0$, on note $\text{dlog}(P) := \dfrac{P'}{P}$.
Sinon, on peut noter $X\,\text{dlog}(P) := n + X\,\text{dlog}(\widetilde{P})$ où $P = X^n\widetilde{P}$ avec $n = \text{val}(P)$ et $\text{val}(\widetilde{P}) = 0$. On a alors $P \cdot X\,\text{dlog}(P) = P' \cdot X$.

Proposition 6.1
Soit $P, Q \in \mathbb{Q}[[X]]$ avec $\text{val}(P) = p$ et $\text{val}(Q) = q$. On a les propriétés suivantes :

1. $X\,\text{dlog}(PQ) = X\,\text{dlog}(P) + X\,\text{dlog}(Q)$
2. *Si* $\text{val}(P) = 0$ *alors* $\text{dlog}(P^{-1}) = -\,\text{dlog}(P)$
3. $\forall n \in \mathbb{N}, X\,\text{dlog}(P^n) = n \cdot X\,\text{dlog}(P)$
4. *Si* $\text{val}(P) = \text{val}(Q) = p$ *et si* $X\,\text{dlog}(P) = X\,\text{dlog}(Q)$ *alors il existe* $c \in \mathbb{Q}$ *tel que* $P = cQ$.

Démonstration : Soit $P, Q \in \mathbb{Q}[[X]]$ avec $\text{val}(P) = p$ et $\text{val}(Q) = q$. On note $P = X^p\tilde{P}$ et $Q = X^q\tilde{Q}$ avec $\text{val}(\tilde{P}) = \text{val}(\tilde{Q}) = 0$.

1. On a $X^{p+q}\widetilde{PQ} = PQ = X^p\widetilde{P} \cdot X^q\widetilde{Q} = X^{p+q}\widetilde{P}\widetilde{Q}$. On en déduit que $\widetilde{PQ} = \widetilde{P}\widetilde{Q}$.
   Ainsi, $X\,\text{dlog}(PQ) = p + q + X\,\text{dlog}(\widetilde{PQ}) = p + q + X\left(\dfrac{\widetilde{P}'\widetilde{Q} + \widetilde{P}\widetilde{Q}'}{\widetilde{P}\widetilde{Q}}\right) = X\,\text{dlog}(P) + X\,\text{dlog}(Q)$.
2. D'une part $\text{dlog}(PP^{-1}) = \text{dlog}(1) = 0$. D'autre part, d'après le point précédent, $\text{dlog}(PP^{-1}) = \text{dlog}(P) + \text{dlog}(P^{-1})$. En combinant ces résultats on obtient l'égalité voulue.
3. Par récurrence sur l'entier n. C'est vrai pour $n = 0$ puis on utilise le premier point pour montrer l'hérédité.

4. On commence par traiter le cas où $\mathrm{val}(P) = \mathrm{val}(Q) = 0$. Ainsi, $\mathrm{dlog}(P) = \mathrm{dlog}(Q)$ si et seulement si $\mathrm{dlog}(P) - \mathrm{dlog}(Q) = 0$ si et seulement si $\mathrm{dlog}(P) + \mathrm{dlog}(Q^{-1}) = 0$ (point 2) si et seulement si $\mathrm{dlog}(PQ^{-1}) = 0$ (point 1) si et seulement si $(PQ^{-1})' = 0$ si et seulement s'il existe $c \in \mathbb{Q}$ tel que $P = cQ$.
On se ramène au cas général en écrivant $P = X^p\widetilde{P}$ et $Q = X^p\widetilde{Q}$ où $\mathrm{val}(\widetilde{P}) = \mathrm{val}(\widetilde{Q}) = 0$. Ainsi, $X\,\mathrm{dlog}(P) - X\,\mathrm{dlog}(Q) = X(\mathrm{dlog}(\widetilde{P}) - \mathrm{dlog}(\widetilde{Q})) = 0$ donc $\mathrm{dlog}(\widetilde{P}) - \mathrm{dlog}(\widetilde{Q}) = 0$. D'après le cas particulier, il existe $c \in \mathbb{Q}$ tel que $\widetilde{P} = c\widetilde{Q}$. En multipliant par X^p on obtient le résultat souhaité.

On peut maintenant écrire la dernière relation qui va nous permettre de conclure.

Proposition 6.2
On a l'égalité :

$$Q^3 - R^2 = 1728Xf(X)^{24} \tag{21}$$

Démonstration : • On commence par montrer que $X\,\mathrm{dlog}(Q^3 - R^2) = P$.
On a $\mathrm{val}(Q^3 - R^2) = 1$, on calcule alors :

$$X\,\mathrm{dlog}(Q^3 - R^2) = \frac{X \cdot 3Q'Q^2 - X \cdot 2R'R}{Q^3 - R^2} \overset{(*)}{=} \frac{Q^2(PQ - R) - R(PR - Q^2)}{Q^3 - R^2} = P$$

Pour l'égalité $(*)$ on utilise les relations (17) et (18).
• On montre ensuite que $X\,\mathrm{dlog}(Xf(X)^{24}) = P$.
On a bien $\mathrm{val}(Xf(X)^{24}) = 1$. Posons $f_N(X) := \prod_{n=1}^{N}(1 - X^n)$. En particulier, pour tout $N \in \mathbb{N}$,

$$X\,\mathrm{dlog}(Xf_N(X)^{24}) = 1 - \sum_{n=1}^{N} \frac{24nX^n}{1 - X^n}$$

Soit $k \in \mathbb{N}$, comme $\mathrm{val}\left(\frac{24nX^n}{1-X^n}\right) = n$, alors pour tout $N > k$ le coefficient devant X^k dans $X\,\mathrm{dlog}(Xf_N(X)^{24})$ est le même que dans $X\,\mathrm{dlog}(Xf_k(X)^{24})$. On en déduit que

$$X\,\mathrm{dlog}(Xf(X)^{24}) = 1 - \sum_{n=1}^{\infty} \frac{24nX^n}{1 - X^n} = 1 - 24\Phi_{0,1} = P$$

• Comme $\mathrm{val}(Q^3 - R^2) = 1 = \mathrm{val}(Xf(X)^{24})$, que $X\,\mathrm{dlog}(Q^3 - R^2) = P = X\,\mathrm{dlog}(Xf(X)^{24})$ et que le terme devant X dans $Q^3 - R^2$ est 1728 et est 1 dans $Xf(X)^{24}$. On en déduit que $Q^3 - R^2 = 1728Xf(X)^{24}$ d'après le dernier point de la proposition précédente. ∎

6.3 Conclusion et approfondissement

On a désormais tout ce qu'il faut pour comprendre la partie *Modulus 5* de l'article de Ramanujan publiée en 1921 [7, p.149-150]. On va s'intéresser à l'équation (21) modulo 5.

♣ **Définition.** Soient $A, B \in \mathbb{Z}[[X]]$, on dit que $A \equiv B \pmod 5$ si et seulement s'il existe $J \in \mathbb{Z}[[X]]$ tel que $A = B + 5J$ ou encore (c'est équivalent) si $\widetilde{A} = \widetilde{B}$ où $\widetilde{A}$ et $\widetilde{B}$ sont les séries formelles dans $\mathbb{Z}/5\mathbb{Z}[[X]]$ obtenues en réduisant modulo 5 les coefficients de A et B.

Lemme 6.1 *On a :*

$$Q^3 - R^2 \equiv Q - P^2 \pmod 5$$

Démonstration : On a $Q \equiv 1 + 240\Phi_{0,3} \equiv 1 \pmod 5$ et $R \equiv 1 - 504\Phi_{0,5} \overset{(*)}{\equiv} 1 - 504\sum_{n=1}^{\infty} n^5 \frac{X^n}{1 - X^n} \pmod 5$
pour $(*)$ on utilise la proposition 5.1. De plus, le petit théorème de Fermat affirme que pour tout entier n, $n^5 \equiv n \pmod 5$. Ainsi $R \equiv 1 - 504\sum_{n=1}^{\infty} n\frac{X^n}{1-X^n} \equiv 1 - 504\Phi_{0,1} \equiv 1 - 24\Phi_{0,1} \equiv P \pmod 5$.
Par suite $Q^3 - R^2 \equiv Q \cdot 1^2 - P^2 \equiv Q - P^2 \pmod 5$. ∎

Lemme 6.2 *On a :*

$$f(X)^{25} \equiv f(X^{25}) \pmod 5$$

Démonstration : • Considérons l'ensemble $E := \{F \in \mathbb{Z}/5\mathbb{Z}[[X]], \quad F(X)^5 = F(X^5)\}$. Il contient les X^n pour $n \in \mathbb{N}$ et par le petit théorème de Fermat, E contient les constantes.
De plus si $F, G \in E$ alors $(FG)^5(X) = F(X)^5G(X)^5 = F(X^5)G(X^5) = FG(X^5)$ donc E est stable par $\times$.
Enfin si $F, G \in E$ alors $(F+G)^5 = F^5 + G^5$ donc E est stable par $+$.
Par suite, E contient les polynômes (i.e les séries formelles $F \in \mathbb{Z}/5\mathbb{Z}[[X]]$ nulles à partir d'un certain rang).

• D'après (19), on sait que f peut s'écrire sous la forme d'une série formelle : $f(X) = \sum_{n=0}^{\infty} b_n X^n$. Considérons $F := \overline{f} = \sum_{n=0}^{\infty} a_n X^n$ la classe de f dans $\mathbb{Z}/5\mathbb{Z}[[X]]$ et posons $F_N(X) = \sum_{n=1}^{N} a_n X^n$.
Pour tout $N \in \mathbb{N}, F_N \in E$. D'après ce qui précède : $F_N(X)^5 = F_N(X^5)$.
Écrivons que $F(X) = F_N(X) + R_N(X)$ avec $R_N(X) = \sum_{n=N+1}^{\infty} a_n X^n$ et $\mathrm{val}(R_N) > N$.
Mais alors $F(X)^5 - F(X^5) = \underbrace{F_N(X)^5 - F_N(X^5)}_{=0} + \underbrace{R_N(X)^{25} - R_N(X^{25})}_{\text{de valuation} > 5N}$.
On en déduit que le coefficient devant X^m dans $F(X)^5$ est le même que dans $F(X^5)$ pour tout $m \leq 5N$. C'est vrai pour tout entier naturel N. Par suite, $F(X)^5 = F(X^5)$ donc $F \in E$ et donc $F^5 \in E$. On a donc montré que $F(X)^{25} = \left(F(X)^5\right)^5 = F(X^5)^5 = F(X^{25})$. ∎

On touche au but car les deux derniers lemmes nous permettent de démontrer le théorème annoncé au début du chapitre 5 dont on rappelle l'énoncé :

Théorème 6.1 (Congruence Ramanujan)
Pour tout entier naturel k, on a :

$$p(5k+4) \equiv 0 \pmod 5$$

Démonstration : On part de l'identité (21) :

$$\begin{aligned}
Q^3 - R^2 \equiv 1728Xf(X)^{24} \pmod 5 \text{ donc } Q^3 - R^2 &\equiv 1728X\frac{f(X)^{25}}{f(X)} \pmod 5 \quad \text{car } f \text{ est inversible,}\\
\text{donc } Q - P^2 &\equiv 1728X\frac{f(X^{25})}{f(X)} \pmod 5 \quad \text{cf lemmes précédents,}\\
\text{donc } 288\Phi_{1,2} &\equiv 1728X\frac{f(X^{25})}{f(X)} \pmod 5 \quad \text{d'après (13),}\\
\text{donc } 288\Phi_{1,2} &\equiv 1728Xf(X^{25})\sum_{n=0}^{\infty} p(n)X^n \pmod 5 \quad \text{d'après (20),}\\
\text{donc } \Phi_{1,2} &\equiv Xf(X^{25})\sum_{n=0}^{\infty} p(n)X^n \pmod 5
\end{aligned}$$

En utilisant la remarque suivant la proposition 5.1 on écrit $\Phi_{1,2} = \sum_{n=1}^{\infty} n\sigma(n)X^n$ où $\sigma(n) := \sum_{d|n} d$ est la somme des diviseurs de n. On écrit aussi f sous la forme d'une somme qui est donnée par (19). La dernière congruence s'écrit alors :

$$\sum_{n=1}^{\infty} n\sigma(n)X^n \equiv \left(X + \sum_{k\in\mathbb{Z}^*} (-1)^k X^{25g_k+1}\right)\left(\sum_{n=0}^{\infty} p(n)X^n\right) \pmod 5 \qquad \text{où } g_k = \frac{k(3k-1)}{2} \in \mathbb{N}^*$$

Soit $m \geq 1$.
Dans l'équation précédente le coefficient devant X^{5m} est $5m\sigma(5m) \equiv 0 \pmod 5$ pour le membre de gauche

et est $p(5m-1)-p(5m-26)-p(5m-51)+\cdots+(-1)^k p(5m-1-25g_k)+\cdots$ pour le membre de droite. On en déduit que :

$$p(5m-1) \equiv \sum_{k\in\mathbb{Z}^*} (-1)^{k+1} p(5m-1-25g_k) \pmod 5$$

On conclut que $p(5m-1) \equiv 0 \pmod 5$ par récurrence forte sur m. ∎

Bibliographie

[1] László Tóth, *Menon's identity and arithmetical sums representing functions of several variables*, 2011.

[2] M.Richards, *A remark on the number of cyclic subgroups of a finite group, Amer. Math. Monthly 91*, 1984.

[3] P.Haukkanen et J.Wang, *A generalization of Menon's identity with respect to as set of polynomials, Portugaliae Mathematica 53*, 1996.

[4] V.Sita Ramaiah, *Arithmetical sums in regular convolutions*, 1978.

[5] J.Riou, *Feuille d'exercice n°3 cours de Combinatoire algébrique (Mag306)*, Année universitaire 2020/2021.

[6] S.Ramanujan, *On certain arithmetical functions, Transactions of the Cambridge Philosophical Society XXII, NO.9*, 1916

[7] S.Ramanujan, *Congruence properties of partitions*, 1921