Parité de certains nombres de partitions[1]

Jacques Dixmier et Jean-Louis Nicolas[2]

Abstract. Let us denote by $p(n,r)$ the number of partitions of n in at most r parts. The aim of this article is to study the parity of $p(n,r)$. Setting $u_r^n = 0$ if $p(n-1,r)$ is even and $u_r^n = 1$ if $p(n-1,r)$ is odd, we show that, for r fixed, the sequence $u_r = (u_r^n)_{n\geq 1}$ is periodical and its smallest period ω_r is determined. Various properties of these sequences u_r are considered : symmetry, long range of consecutive equal values,...
Let $d(r)$ be the density of 1's in u_r. The computation of $d(r)$ for small r's drove us to conjecture that $\lim_{r\to\infty} d(r) = 1/2$; but, unfortunately, we have not been able to prove it. Partial results are given, showing that, for some subsets P of the set of positive integers, $\lim_{r\to\infty,\ r\in P} d(r) = 1/2$ holds, and, in some sense, that, for $r \to \infty$, $r \in P$, the sequences u_r tend to be equidistributed.

0 Introduction.

0.1. Si $x \in \mathbb{Z}$, on note $\overline{x}$ sa classe modulo 2. On note $0, 1$ au lieu de $\overline{0}, \overline{1}$ les deux éléments de $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$.

0.2. Soit $p(n)$ le nombre de partitions de n. D'après l'article [9], l'examen des tables numériques laisse supposer que, dans la table des $\overline{p}(n)$, les 0 et les 1 se répartissent à égalité, asymptotiquement ; toutefois, cela n'est pas prouvé. Cf. [8] pour le meilleur résultat connu à ce sujet. On pourra aussi consulter [10] et [11].

0.3. Soit $p(n,r)$ le nombre de partitions de n en au plus r parts, et posons $u_r^n = \overline{p}(n-1,r)$. On a $\overline{p}(n-1) = u_r^n$ pour $r \geq n-1$ (cf. 1.8). L'étude des u_r^n ne nous a malheureusement pas permis d'obtenir des résultats nouveaux concernant les $\overline{p}(n)$. Mais les propriétés des u_r^n sont intéressantes ; elles font l'objet du présent mémoire.

0.4. Les chapitres 1 et 2 sont des préliminaires techniques. Au chapitre 3, nous montrons que les suites $u_r = (u_r^n)_{n\geq 1}$ sont périodiques, et nous déterminons la plus petite période ω_r de u_r (3.8). On a $\omega_r \,|\, \omega_{r+1}$ pour tout r. Nous établissons diverses propriétés (symétries, longues suites de zéros consécutifs) de ces suites u_r. (3.10, 3.11, 3.17, 3.18, 3.20).
On a $\omega_2 = 4$, $\omega_3 = 12$, $\omega_4 = 24$, $\omega_5 = \omega_6 = 240$, $\omega_7 = 1680$, $\omega_8 = 3360$, $\omega_9 = 10080$. Les calculs *à la main* concernant les u_r^n sont donc faisables pour $r \leq 6$, pénibles pour $r = 7, 8$, décourageants pour $r \geq 9$. Les résultats numériques indiqués plus loin ont donc nécessité l'ordinateur.

[1] Manuscript accepté le 22/11/01.
[2] Recherche financée par le CNRS, Institut Girard Desargues, UMR 5028.

0.5. Puisque $\omega_5 = 240$, on a $u_5^{n+240} = u_5^n$. Mais on constate que, plus précisément, on a $u_5^{n+120} = u_5^n + 1$. Nous dirons que u_5 est *antipériodique*. Au chapitre 4, nous déterminons les entiers r tels que u_r soit antipériodique. Ils sont rares et cela pose quelques questions arithmétiques.

0.6. Les chapitres 5 et 6 sont des préliminaires. La suite u_r peut être considérée comme une fonction $\mathbb{Z}/\omega_r \to \{0,1\}$. La décomposition en facteurs premiers de ω_r ne fait intervenir que des nombres premiers $p \leq r$, avec l'exposant 1 si $p > r^{1/2}$. Considérons la restriction $u_{r,p}$ de u_r au facteur direct $\mathbb{Z}/p$ de $\mathbb{Z}/\omega_r$. Aux chapitres 7 et 8, nous déterminons les $u_{r,p}$ pour $r/2 < p \leq r$.

0.7. Dans chaque période ω_r de u_r, considérons la répartition des 0 et des 1 parmi les u_r^n. Soit $d(r)$ la proportion des 1. Au chapitre 11, nous donnons un algorithme de calcul de $d(r)$. En annexe, la table 1 donne, pour $r \leq 32$, la valeur de $1/2 - d(r)$ et celle de la plus petite période ω_r de u_r. La table 2 donne la décomposition en facteurs premiers des périodes ω_r indiquées dans la table 1. Le lemme 9.3 donne une majoration de $|1/2 - d(r)|$ facile à calculer lorsque r est grand. La table 3 donne cette majoration pour $993 \leq r \leq 1002$. Au vu de ces résultats, il ne fait guère de doute que $d(r) \to 1/2$ quand $r \to \infty$. Nous avons seulement pu prouver ce qui suit (9.4, 9.8) :
Soit p un nombre premier tendant vers l'infini. Alors

$$d(p+1) \to \frac{1}{2}, \quad d\left(\frac{3p+1}{2}\right) \to \frac{1}{2}, \quad d\left(\frac{3p+3}{2}\right) \to \frac{1}{2}.$$

Soit $\alpha \in]0.535, 1[$. Pour tout $R \geq 1$, posons $\ell(R) = R^\alpha$. Alors

$$\left(\prod_{R \leq r \leq R+\ell(R)} \left|d(r) - \frac{1}{2}\right|\right)^{1/\ell(R)} \to 0 \quad \text{quand } R \to \infty.$$

0.8. Non seulement les zéros et les uns semblent s'équilibrer parmi les u_r^n (r fixé), mais ils semblent équidistribués. Nous prouvons (10.17) qu'il existe une partie infinie P de $\mathbb{N}$ telle que :
Soient r_0, n_0 des entiers fixés. Pour $r \geq r_0$, soit A_r l'ensemble des $n \in \mathbb{Z}/\omega_r$ tels que $n \equiv n_0 \pmod{\omega_{r_0}}$; soit B_r l'ensemble des $n \in A_r$ tels que $u_r^n = 1$. Alors, Card B_r/Card $A_r \to \frac{1}{2}$ quand $r \to \infty$ en restant dans P. (Il est probable qu'on peut prendre $P = \mathbb{N}$, mais nous ne savons pas le prouver.)

0.9. Dans tout l'article, k désigne le corps $\mathbb{F}_2 = \mathbb{Z}/2$ et $\overline{k}$ une clôture algébrique de k.
Si $P \in k[z]$, on note $\lambda(P)$ le nombre de coefficients de P égaux à 1.
Si f est une fonction complexe définie sur X, $\|f\|_\infty = \sup_{x \in X} |f(x)|$.
Si m et n sont des entiers positifs, nous noterons $m \bmod n$ le reste dans la division euclidienne de m par n. Si a et b sont des entiers, la congruence de a et b modulo n sera notée $a \equiv b \pmod{n}$.

La lettre p désigne toujours un nombre premier (sauf au chapitre 1 où nous sommes forcés de l'utiliser pour des fonctions de partitions), *et il nous arrivera de ne même plus le signaler.*

Table des définitions et des notations.

1 Definition des u_r^n.

1.1. Soient n, r des entiers ≥ 1. On note $p(n,r)$ le nombre de partitions de n en parts au plus égales à r. La série génératrice de $p(n,r)$ vaut donc

$$1 + \sum_{n=1}^{\infty} p(n,r) z^n = \frac{1}{(1-z)(1-z^2)\dots(1-z^r)}.$$

On sait, d'après l'étude du diagramme de Ferrers (cf. [5], chap. 19), que $p(n,r)$ est aussi le nombre de partitions de n en au plus r parts. On pose $p(n,r) = 0$ pour $n < 0$ et $p(0,r) = 1$. On a $p(n,1) = 1$ pour $n \geq 0$.
En utilisant la série génératrice, on obtient la formule (cf. [4]) :

$$p(n,r) = p(n,r-1) + p(n-r,r).$$

Nous allons étudier la parité des $p(n,r)$.

1.2. Pour $n \in \mathbb{Z}$ et $r \geq 1$, posons

$$u_r^n = \overline{p}(n-1,r) \in \mathbb{Z}/2.$$

La série génératrice des u_r^n, pour r fixé, est donc, dans $\mathbb{F}_2$:

$$S_r(z) = \sum_{n=0}^{\infty} u_r^n z^n = \frac{z}{(1+z)(1+z^2)\dots(1+z^r)}.$$

On a

$$u_r^n = 0 \quad \text{pour } n \leq 0. \tag{1}$$

$$u_1^n = 1 \quad \text{pour } n \geq 1. \tag{2}$$

et pour $r \geq 2$,

$$u_r^n = \overline{p}(n-1,r) = \overline{p}(n-1,r-1) + \overline{p}(n-r-1,r)$$

donc,

$$u_r^n = u_r^{n-r} + u_{r-1}^n \quad \text{pour } r \geq 2. \tag{3}$$

Il est clair que la suite double des $u_r^n (n \in \mathbb{Z}, r \geq 1)$ est déterminée par (1), (2), (3). On déduit de (3) :

$$u_r^n = u_{r-1}^n + u_{r-1}^{n-r} + u_{r-1}^{n-2r} + \dots + u_{r-1}^{n-(a-1)r} + u_r^{n-ar} \tag{4}$$

$$u_r^n = u_{r-1}^n + u_{r-1}^{n-r} + u_{r-1}^{n-2r} + \dots \tag{5}$$

1.3. Voici un tableau des premières valeurs des u_r^n (il y a intérêt à partir de $n = 0$, bien que $u_r^0 = 0$).

$n=$	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$r=1$	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
$r=2$	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1	0
$r=3$	0	1	1	0	1	0	1	1	0	0	0	0	0	1	1	0
$r=4$	0	1	1	0	1	1	0	1	1	1	0	1	1	0	1	1
$r=5$	0	1	1	0	1	1	1	0	1	0	1	0	1	1	1	0

$n=$	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
$r=1$	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
$r=2$	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1
$r=3$	1	0	1	1	0	0	0	0	0	1	1	0	1	0	1
$r=4$	0	0	0	0	0	0	0	0	0	1	1	0	1	1	0
$r=5$	0	1	1	1	0	0	1	1	1	1	1	1	0	0	1

1.4. Soit $p(n)$ le nombre de partitions de n. Le nombre de partitions de n en parts au plus égales à r, et ayant une part égale à r, est $p(n-r,r)$. On a

$$p(n) = \sum_r p(n-r,r) = \sum_{r=1}^{n} p(n-r,r)$$

$$\overline{p}(n) = \sum_{r=1}^{n} u_r^{n-r+1}.$$

Mais on va voir qu'il existe des formules plus économiques liant $\overline{p}(n)$ et les coefficients u_r^n.

1.5. Soit $q(n)$ (resp. $q(n,r)$) le nombre de partitions de n en entiers impairs distincts (resp. en r entiers impairs distincts). On pose $q(n,r) = 0$ pour $n < 0$. On a $q(n,r) = 0$ si n et r sont de parités distinctes, $q(n,1) = 1$ pour n impair, $n \geq 1$; il est classique (cf. [4]) que

$$q(n,r) = p\left(\frac{1}{2}n - \frac{1}{2}r^2, r\right).$$

On en déduit les formules :

$$\overline{q}(2m-1,r) = \overline{p}(m - \frac{1}{2}(r^2+1), r) = u_r^{m-\frac{1}{2}(r^2-1)} \quad \text{si } r \text{ est impair}$$

$$\overline{q}(2m,r) = \overline{p}(m - \frac{1}{2}r^2, r) = u_r^{m-\frac{1}{2}r^2+1} \quad \text{si } r \text{ est pair.}$$

D'autre part, $q(n,r) = 0$ pour $n < r^2$ car la somme des r premiers nombres impairs est r^2. Donc

$$q(n) = \sum_r q(n,r) = \sum_{1 \leq r \leq \lfloor \sqrt{n} \rfloor} q(n,r)$$

et par suite

$$\overline{q}(2m-1) = \sum_{1 \leq r \leq \lfloor (1+\sqrt{2m-1})/2 \rfloor} u_{2r-1}^{2m-1-2r^2+2r}$$

$$\overline{q}(2m) = \sum_{1 \leq r \leq \lfloor \sqrt{m/2} \rfloor} u_{2r}^{2m-2r^2+1}.$$

1.6. Il est classique et facile (cf. [5]) que $p(n)$ et $q(n)$ ont la même parité. Dans les deux formules précédentes, on peut donc remplacer $\overline{q}$ par $\overline{p}$, d'où des sommations plus rapides qu'en (1.4). Notons que MacMahon, dans [7], a donné une méthode de calcul de $\overline{p}(n)$ qui utilise l'identité de Jacobi (cette identité est exposée dans [5]).

1.7. A partir de $p(n,1)=1$ (pour $n\geq 0$), la formule donnée en 1.1 :

$$p(n,r)=p(n,r-1)+p(n-r,r)$$

permet de calculer $p(n,r)$ pour $r=2,3,\ldots$ (avec la convention $p(n,r)=0$ pour $n<0$). Par ailleurs, d'après la définition de $p(n,r)$, on a

$$p(n)=p(n,n)=p(n,n+1)=p(n,n+2)=\ldots$$

Ces remarques avaient été utilisées par Euler pour calculer $p(n)$ (cf. [4]).

1.8. De même, les suites u_r "stabilisent" :

$$u_{n-1}^n=u_n^n=u_{n+1}^n=u_{n+2}^n=\ldots \quad (n\geq 2)\ .$$

Notons v_n cette valeur commune. Donc

$$u_r^n=v_n \quad \text{pour } n\leq r+1.$$

De la définition de u_r^n et de 1.7, on conclut

$$v_n=\overline{p}(n-1).$$

2 Quelques fonctions auxiliaires

2.1. Soit $2=p_0<p_1<p_2<\ldots$ la suite des nombres premiers. Pour tout entier $r\geq 1$, on définit les entiers positifs ou nuls $a_0(r)$, $a_1(r)$, $a_2(r),\ldots$ par les conditions

$$p_j^{a_j(r)}\leq r<p_j^{a_j(r)+1}. \tag{6}$$

Autrement dit,

$$a_j(r)=\lfloor \log r/\log p_j\rfloor. \tag{7}$$

On a $a_j(r)=0$ pour $p_j>r$. La suite $(a_0(r),a_1(r),\ldots)$ est décroissante d'après (7).

2.2. Pour tout entier $n>0$, on notera $v_2(n)$ la valuation 2-adique de n. Donc $n=2^{v_2(n)}n'$ avec n' impair. En désignant par x un entier quelconque

$$\begin{aligned} 2^{v_2(n)} &= 1 && \text{pour } n=2x+1,\\ 2^{v_2(n)} &= 2 && \text{pour } n=4x+2,\\ 2^{v_2(n)} &= 4 && \text{pour } n=8x+4,\ldots \end{aligned}$$

On posera :

$$2^{v_2(1)}+2^{v_2(2)}+\ldots+2^{v_2(n)}=c(n).$$

On a $c(1)=1, c(2)=3, c(3)=4, c(4)=8$. D'autres valeurs de $c(n)$ sont données dans la table 1 en annexe.

Pour $n\equiv 0,1,2,3 \pmod 4$, on a $c(n)\equiv 0,1,3,0 \pmod 4$. En effet, on vient de le voir pour $n=1,2,3,4$. Admettons que $c(4i)=4j$ $(i,j\in\mathbb{N})$. Alors $c(4i+1)=c(4i)+1=4j+1\equiv 1 \pmod 4$, $c(4i+2)=c(4i+1)+2=4j+3\equiv 3 \pmod 4$, $c(4i+3)=c(4i+2)+1=4j+4\equiv 0 \pmod 4$, $c(4i+4)=c(4i+3)+2^{v_2(4i+4)}=4j+4+2^{v_2(4i+4)}\equiv 0 \pmod 4$, puisque $v_2(4i+4)\geq 2$.

2.3. Lemme. *Soient n un entier, $n\geq 1$ et $r=2^n$. On a $c(2n)=2c(n)+n$, et pour $r\geq 0$, $c(2^r n)=2^{r-1}(2c(n)+rn)$. En particulier, $c(2^r)=2^{r-1}(r+2)$.*

En séparant les nombres pairs et impairs, on obtient

$$\begin{aligned} c(2n) &= 2^{v_2(2)}+2^{v_2(4)}+\ldots+2^{v_2(2n)}+2^{v_2(1)}+2^{v_2(3)}+\ldots+2^{v_2(2n-1)}\\ &= 2^{1+v_2(1)}+2^{1+v_2(2)}+\ldots+2^{1+v_2(n)}+1+1+\ldots+1\\ &= 2c(n)+n. \end{aligned}$$

La formule $c(2^r n)=2^{r-1}(2c(n)+rn)$ s'obtient alors facilement par récurrence sur r.

2.4. Soient n,s des entiers tels que $s<2^n$. on a $v_2(2^n+s)=v_2(s)$. Il résulte de là que

$$c(2^n+s)=c(2^n)+c(s)=2^{n-1}(n+2)+c(s).$$

On en déduit par récurrence que si un entier r admet la représentation dyadique $2^{n_1}+2^{n_2}+\ldots$ avec $n_1>n_2>\ldots$, alors

$$c(r)=c(2^{n_1})+c(2^{n_2})+\ldots=2^{n_1-1}(n_1+2)+2^{n_2-1}(n_2+2)+\ldots.$$

Notons que, par le lemme 2.3, cela implique, pour $k\geq 1$ et n pair

$$c(2^n k+s)=c(2^n k)+c(s)\equiv c(s) \pmod{2^n}$$

ce qui généralise la propriété décrite en (2.2) pour $n=2$.

2.5. On a

$$c(2^{n+1}-1)=c(2^{n+1})-2^{n+1}=2^n(n+3)-2^{n+1}=2^n(n+1)<2\cdot 2^{n-1}(n+2)$$

donc

$$c(2^{n+1}-1)<2c(2^n).$$

2.6. Si x est un entier, $x\geq 2$, on a

$$c(x+1)\leq 2c(x).$$

En effet, si x et $x+1$ appartiennent à un intervalle $[2^n,2^{n+1}-1]$, cela résulte de (2.5). Sinon, on a $x=2^n-1$, $x+1=2^n$ pour un $n\geq 2$. Alors,

$$\begin{aligned} 2c(x)-c(x+1) &= 2c(2^n-1)-c(2^n)=2(c(2^n)-2^n)-c(2^n)\\ &= c(2^n)-2^{n+1}=2^{n-1}(n+2)-2^{n+1}=2^{n-1}(n-2)\geq 0. \end{aligned}$$

2.7. Soit r un entier, $r > 0$; en désignant par $\log_2$ le logarithme en base 2, on a

$$\frac{1}{4}r(\log_2 r + 1) < c(r) < r(\log_2 r + 3).$$

En effet, posons $n = \lfloor \log_2 r \rfloor$. On a $2^n \leq r < 2^{n+1}$, donc

$$c(2^n) \leq c(r) < c(2^{n+1})$$

c'est-à-dire, d'après 2.3

$$2^{n-1}(n+2) \leq c(r) < 2^n(n+3).$$

Alors

$$\begin{aligned} \frac{1}{4}r(\log_2 r + 1) &< \frac{1}{4}r(n+2) < \frac{1}{4}2^{n+1}(n+2) = 2^{n-1}(n+2) = c(2^n) \\ &\leq c(r) < c(2^{n+1}) = 2^n(n+3) \leq r(\log_2 r + 3). \end{aligned}$$

2.8. On déduit de 2.7 que

$$\log_2 c(r) \sim \log_2 r \quad \text{quand } r \to \infty.$$

2.9. Pour tout entier $r > 0$, on définit l'entier $a(r)$ par

$$2^{a(r)-1} < c(r) \leq 2^{a(r)}.$$

Autrement dit,

$$a(r) = \lceil \log_2 c(r) \rceil.$$

En 2.1, nous avons défini a_0. On a $2^{a_0(r)} \leq r \leq c(r) \leq 2^{a(r)}$ donc $a_0(r) \leq a(r)$. Compte tenu de 2.8,

$$a(r) \sim \log_2 r \quad \text{quand } r \to \infty.$$

2.10. Pour tout entier $r > 0$, on pose

$$\omega_r = 2^{a(r)} \prod_{j \geq 1} p_j^{a_j(r)}.$$

Notons que, d'après la définition des a_j donnée en 2.1, le produit ci-dessus est le ppcm des nombres impairs inférieurs ou égaux à r. Les nombres ω_r vont jouer un rôle essentiel. Leurs valeurs sont listées dans la table 2 en annexe.

2.11. Les nombres $a_i(r)$ introduits en 2.1 ont les propriétés suivantes :
(i) $a_i(r) \geq a_i(r-1)$;
(ii) si r n'est pas une puissance de p_i, $a_i(r) = a_i(r-1)$;
(iii) si $r = p_i^h$ avec $h \geq 1$, on a $a_i(r) = h$, $a_i(r-1) = h-1$.

Les propriétés (i) et (iii) sont évidentes. D'autre part, si $a_i(r-1) < a_i(r)$, on a

$$r - 1 < p_i^{a_i(r-1)+1} \leq p_i^{a_i(r)} \leq r$$

donc $r = p_i^{a_i(r)}$, ce qui prouve (ii). Par ailleurs, les propriétés suivantes sont équivalentes :
(iv) $a(r) > a(r-1)$;
(v) il existe un entier n tel que $c(r-1) \leq 2^n < c(r)$.
En effet, si (iv) est vérifiée, on a $a(r-1) \leq a(r) - 1$, donc

$$c(r-1) \leq 2^{a(r-1)} \leq 2^{a(r)-1} < c(r)$$

donc (v) est vraie avec $n = a(r-1)$. Réciproquement, si $c(r-1) \leq 2^n < c(r)$, on a $a(r-1) \leq n$, $a(r) > n$, donc $a(r) > a(r-1)$.
Nous dirons que r est 2-*critique* si les propriétés (iv) et (v) sont vérifiées. Pour le sujet de cet article, les nombres 2-critiques sont, relativement au nombre premier 2, les analogues des puissances des nombres premiers impairs.
Les nombres 2-critiques inférieurs à 10000 sont

$$2, 4, 5, 8, 16, 24, 40, 65, 128, 256, 448, 769, 1472, 2625, 4865, 8961.$$

Notons que le calcul de $c(r)$ s'effectue très vite en utilisant 2.4.

2.12. Si r est 2-critique et $r \neq 2$, on a $a(r-1) = a(r) - 1$. En effet, si $a(r-1) \leq a(r) - 2$, on a

$$c(r-1) \leq 2^{a(r-1)} \leq 2^{a(r)-2} < 2^{a(r)-1} \leq c(r)$$

donc $c(r) > 2c(r-1)$ et par suite $r-1 = 1$ d'après 2.6. Cela contredit l'hypothèse $r \neq 2$.

2.13. Soit $r \geq 3$. Dans le passage de ω_{r-1} à ω_r, quatre cas sont possibles d'après 2.11 et 2.12 :

1. r n'est pas puissance d'un nombre premier impair et n'est pas 2-critique. Alors $\omega_r = \omega_{r-1}$.
2. $r = p^h$ où p est un nombre premier impair et r n'est pas 2-critique. Alors $\omega_r = p\omega_{r-1}$.
3. r n'est pas puissance d'un nombre premier impair et r est 2-critique. Alors $\omega_r = 2\omega_{r-1}$.
4. $r = p^h$ où p est premier impair et r est 2-critique. Alors $\omega_r = 2p\omega_{r-1}$. Il en est ainsi pour $r = 5$. Cf. 4.9 pour d'autres exemples et des commentaires. Nous ignorons s'il existe une infinité de tels nombres.

2.14. Si $r = \prod p_j^{\alpha_j}$ est la décomposition de r en facteurs premiers, il est clair que $\alpha_j \leq a_j(r)$ pour tout j. En particulier, $\alpha_0 \leq a_0(r) \leq a(r)$. Donc

$r \mid \omega_r$. Si $r \geq 3$ n'est pas une puissance d'un nombre premier impair, on va voir qu'on a même $r \mid \omega_{r-1}$. Si r n'est pas 2-critique, c'est clair puisque $\omega_{r-1} = \omega_r$. Supposons r 2-critique. Alors $\omega_r = 2\omega_{r-1}$. On a $2^{v_2(r)} \leq r < c(r) \leq 2^{a(r)}$ donc $v_2(r) < a(r)$, $v_2(r) \leq a(r) - 1 = a(r-1) = v_2(\omega_{r-1})$ et notre assertion est encore vérifiée.

3 Périodes et symétries des u_r.

3.1. Soit $k = \mathbb{Z}/2$. La série génératrice des u_r^n, pour r fixé, a été donnée en 1.2 :

$$S_r(z) = \sum_{n=0}^{\infty} u_r^n z^n = \frac{z}{(1+z)(1+z^2)\dots(1+z^r)} \in k[[z]] \cap k(z).$$

Nous poserons

$$F_r(z) = (1+z)(1+z^2)\dots(1+z^r).$$

3.2. Disons qu'un entier $\omega \geq 1$ est une période de la suite u_r si $u_r^{n+\omega} = u_r^n$ pour $n \geq 0$. (C'est un abus de langage puisque $u_r^n = 0$ pour $n \leq 0$). Le tableau 1.3 montre que u_1 n'est pas périodique avec cette définition (cf. corollaire 3.10).

Lemme. *Soient r, ω des entiers, $r \geq 2$, $\omega \geq 1$. Les conditions suivantes sont équivalentes :*
(i) ω est une période de u_r ;
(ii) $F_r(z)$ divise $1 + z^\omega$ dans $k[z]$.

(ii) $\Longrightarrow$ (i). Supposons

$$1 + z^\omega = Q(z)F_r(z) = Q(z)(1+z)(1+z^2)\dots(1+z^r)$$

où $Q \in k[z]$. Notons qu'alors

$$\deg Q = \omega - \frac{1}{2}r(r+1) \leq \omega - 3. \tag{8}$$

On a dans $k[[z]]$:

$$S_r(z) = zQ(z)(1+z^\omega)^{-1} = zQ(z)(1 + z^\omega + z^{2\omega} + \dots)$$

donc u_r admet la période ω.

(i) $\Longrightarrow$ (ii) : même raisonnement en sens inverse.

3.3. Soit n un entier, $n > 0$. Posons $v_2(n) = v$ et $n = 2^v n'$. On a dans $k[z]$

$$\begin{aligned} 1 + z^n &= 1 + z^{2^v n'} = (1 + z^{n'})^{2^v} \\ &= (1+z)^{2^v}(1 + z + z^2 + \dots + z^{n'-1})^{2^v} \\ &= (1+z)^{2^v} U(z) \end{aligned}$$

où $U(z) \in k[z]$, $U(1) = 1$ (car n' est impair), donc 1 *est racine d'ordre* $2^{v_2(n)}$ *de* $1 + z^n$. On en déduit que 1 *est racine d'ordre* $c(r)$ *de* $F_r(z)$ (cf. 2.2).

3.4. Soit $\overline{k}$ une clôture algébrique de k. Tout $\rho \in \overline{k} - \{0\}$ est racine i-ème de 1 avec i impair ; (en effet, ρ appartient à une extension finie de k de degré, disons d, et dans cette extension, tout élément non nul est une racine $(2^d - 1)$-ième de l'unité). Si i est le plus petit entier impair tel que $\rho^i = 1$, on dit que ρ est racine primitive i-ème de 1. Supposons qu'il en soit ainsi ; alors

$$\rho^j = 1 \Longleftrightarrow i \mid j.$$

Soit $j = is$ avec s entier. Si s est impair, ρ est racine simple de $1 + z^j$. Plus généralement, soit $s = 2^v s'$ avec $v = v_2(s)$, s' impair. On a

$$1 + z^j = 1 + z^{2^v i s'} = (1 + z^{is'})^{2^v}$$

donc ρ *est racine d'ordre* $2^{v_2(s)}$ *de* $1 + z^{is}$.
Notons que, si q est premier avec i, $\sigma = \rho^q$ est aussi une racine primitive i-ème de 1.

3.5. Soit i un entier impair, $i \geq 3$, et soit $\rho \in \overline{k}$ une racine primitive i-ème de 1. Si $i > r$, ρ n'est pas racine de $F_r(z)$. Si $i \leq r$, posons $\lfloor r/i \rfloor = t$. Alors ρ est racine de $1 + z^i, 1 + z^{2i}, \dots, 1 + z^{ti}$ avec les ordres $2^{v_2(1)}, 2^{v_2(2)}, \dots, 2^{v_2(t)}$, donc ρ *est racine d'ordre* $c(t)$ *de* $F_r(z)$.

3.6. Lemme. *Soient r, ω des entiers strictement positifs, $\omega = \prod_{j \geq 0} p_j^{\alpha_j}$ la décomposition de ω en facteurs premiers. Les conditions suivantes sont équivalentes :*
(i) $F_r(z) \mid 1 + z^\omega$;
(ii) $2^{\alpha_0} \geq c(r)$ et $\alpha_j \geq a_j(r)$ pour $j \geq 1$.

(i)$\Longrightarrow$ (ii). Supposons (i) vérifiée.
D'après 3.3, 1 est racine de $1 + z^\omega$ d'ordre 2^{α_0}, et racine de $F_r(z)$ d'ordre $c(r)$. Donc $2^{\alpha_0} \geq c(r)$.
Fixons $j \geq 1$. Posons $p_j = p$, $a_j(r) = a$, $\alpha_j = \alpha$. Soit $\rho \in \overline{k}$ une racine primitive p^a-ième de 1. Alors $F_r(z)$ s'annule pour $z = \rho$ (car $p^a \leq r$), donc $1 + \rho^\omega = 0$.
On a $\omega = qp^\alpha$ avec q premier à p. Soit $\sigma = \rho^q$. Alors (cf. 3.4) σ est racine primitive p^a-ième de 1. Or

$$0 = 1 + \rho^\omega = 1 + \rho^{qp^\alpha} = 1 + \sigma^{p^\alpha}.$$

Si $\alpha < a$, il y a contradiction. Donc $\alpha \geq a$, c'est-à-dire $\alpha_j \geq a_j(r)$.

(ii)$\Longrightarrow$ (i). Supposons (ii) vérifiée.
D'après 3.3, l'ordre de 1 comme racine de $1 + z^\omega$ majore son ordre comme racine de $F_r(z)$.
Soient maintenant i un entier impair, $i \geq 3$, et $\rho \in \overline{k}$ une racine primitive i-ème de 1.

(a) Si $i > r$, ρ n'est pas racine de $F_r(z)$.

(b) Supposons $i \leq r$. Soit $t = \lfloor r/i \rfloor$. Soit $i = \prod_{j \geq 1} p_j^{\beta_j}$ la décomposition de i en facteurs premiers. Comme $i \leq r$, on a $\beta_j \leq a_j(r)$, donc $\beta_j \leq \alpha_j$ pour $j \geq 1$; donc $i \mid \omega$ et $\omega = is$. D'après 3.4, ρ est racine de $1 + z^\omega$ à l'ordre $2^{v_2(s)} = 2^{v_2(\omega)} = 2^{\alpha_0}$. D'après 3.5, ρ est racine de $F_r(z)$ à l'ordre $c(r)$. Or $c(t) \leq c(r) \leq 2^{\alpha_0}$.
Ainsi, la condition (i) est vérifiée.

3.7. Pour une preuve ultérieure, notons que, ci-dessus, $t = \lfloor r/i \rfloor \leq \lfloor r/3 \rfloor$ donc

$$c(t) \leq c(\lfloor r/3 \rfloor) \leq c(r) - 1.$$

3.8. Proposition. *Pour $r \geq 2$, la suite u_r est périodique. Sa plus petite période est ω_r.*

Cela résulte de 3.2 et 3.6.

3.9. Le polynôme

$$\sum_{n=0}^{\omega_r - 1} u_r^n z^n = z(1 + z^{\omega_r})/F_r(z)$$

sera noté $P_r(z)$ et appelé *le polynôme générateur de u_r*. Posons $\frac{1}{2}r(r+1) = R$. D'après (8), on a

$$\deg P_r = \omega_r - R + 1. \tag{9}$$

3.10. Proposition. *Soit r un entier, $r \geq 1$. Posons $\frac{1}{2}r(r+1) = R$. On a*

$$u_r^n = 0 \quad \textit{pour} \quad \omega_r - R + 2 \leq n \leq \omega_r.$$

D'après 3.9, on a $u_r^n = 0$ pour $\omega_r - R + 2 \leq n \leq \omega_r - 1$. Et $u_r^{\omega_r} = u_r^0 = 0$.

Corollaire. *Pour $r \geq 1$, on a $u_r^{n+\omega_r} = u_r^n$ pour tout $n \geq 2 - \frac{1}{2}r(r+1)$.*

Cela résulte de la proposition 3.10 et de la définition 3.2.

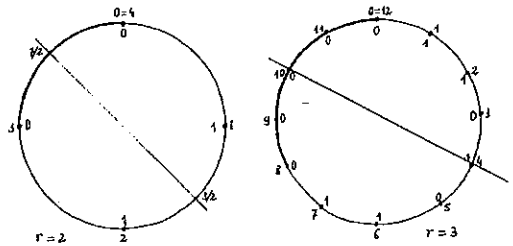
3.11. Proposition (symétrie). *Soient r, R comme en 3.10. On a*

$$u_r^n = u_r^{\omega_r - R + 2 - n} \qquad \textit{pour} \qquad 0 \leq n \leq \omega_r - R + 2. \tag{10}$$

Comme $1 + z_r^\omega$ et $F_r(z)$ sont des polynômes réciproques, il en est de même du polynôme $z^{-1}P_r(z)$, d'où aussitôt (10) (sauf pour $n = 0$) ; mais $u_r^0 = 0$ et $u_r^{\omega_r - R + 2} = 0$ d'après (3.10).

3.12. Remarque. La longue suite de zéros fournie par 3.10 est maximale en ce sens que $u_r^{\omega_r - R + 1} = 1$ (d'après (10)) et $u_r^{\omega_r + 1} = u_r^1 = 1$.

3.13. On considérera souvent la fonction u_r comme définie sur le groupe $\mathbb{Z}/\omega_r$, qui sera parfois identifié à $\{0, 1, 2, \ldots, \omega_r - 1\}$. Pour ne pas alourdir les notations, on confondra parfois les entiers et les classes de congruence. La fonction u_r sur $\mathbb{Z}/\omega_r$ peut aussi être considérée comme un élément de l'algèbre du groupe $k[\mathbb{Z}/\omega_r]$.
Il est bon de visualiser les points de $\mathbb{Z}/\omega_r$ comme ω_r points disposés régulièrement sur un cercle. La répartition des u_r^n fait alors apparaître deux "centres de symétrie" : $\frac{1}{2}\omega_r - \frac{1}{2}R + 1, \omega_r - \frac{1}{2}R + 1$. Comme ω_r est pair (pour $r > 1$), deux cas sont possibles : si $r \equiv 0$ ou $3 \pmod 4$, R est pair et les deux centres de symétrie font partie des ω_r points choisis ; si $r \equiv 1$ ou $2 \pmod 4$, c'est le contraire. Ci-dessous les figures pour $r = 2$ ou $r = 3$ (on a renforcé la portion de cercle correspondant à la suite de zéros de 3.10). On a indiqué à l'intérieur des cercles les valeurs des u_r^n.



3.14. Si $c(r)$ n'est pas une puissance de 2, on a $2^{a(r)} > c(r)$, donc (cf. 3.9, 3.3 et 2.10) $1 + z \mid P_r(z)$. Donc $P_r(1) = 0$, c'est-à-dire

$$\sum_{n=0}^{\omega_r - 1} u_r^n = 0. \tag{11}$$

Par 3.10, cela peut aussi s'écrire, en posant $\frac{1}{2}r(r+1) = R$,

$$\sum_{n=0}^{\omega_r - R + 1} u_r^n = 0. \tag{12}$$

Si $r \equiv 1$ ou $2 \pmod 4$, R est impair et (12) est conséquence triviale de la symétrie (10). Si $r \equiv 0$ ou $3 \pmod 4$, R est pair. Le point fixe de la symétrie $n \mapsto \omega_r - R + 2 - n$ dans $[0, \omega_r - R + 2]$ est l'entier $\frac{1}{2}\omega_r - \frac{1}{2}R + 1$. La relation (12) entraîne compte tenu de (10)

$$u_r^{\frac{1}{2}\omega_r - \frac{1}{2}R + 1} = 0. \tag{13}$$

(Pour $r \leq 10000$, les seules valeurs de r pour lesquelles $c(r)$ est une puissance de 2 sont $1, 3, 4, 15, 64, 255, 447, 768, 1471, 2624, 4864, 8960$).

3.15. Si $c(r)$ n'est ni de la forme 2^n, ni de la forme $2^n - 1$, on a $2^{a(r)} > c(r) + 1$, donc

$$P_r(z) = (1+z)^2 Q(z) = (1+z^2)Q(z)$$

où $Q(z) \in k[z]$. Alors

$$\sum_{0 \leq 2n \leq \omega_r - 1} u_r^{2n} z^{2n} \qquad \text{et} \qquad \sum_{0 \leq 2n+1 \leq \omega_r - 1} u_r^{2n+1} z^{2n+1}$$

sont divisibles par $1+z^2$ (les quotients sont respectivement les parties paires et impaires de Q) ; donc $\sum_{0 \leq 2n \leq \omega_r - 1} u_r^{2n} z^n$ et $\sum_{0 \leq 2n+1 \leq \omega_r - 1} u_r^{2n+1} z^n$ sont divisibles par $1+z$, d'où

$$\sum_{0 \leq 2n \leq \omega_r - 1} u_r^{2n} = 0 \qquad \text{et} \qquad \sum_{0 \leq 2n+1 \leq \omega_r - 1} u_r^{2n+1} = 0.$$

(Pour $r \leq 10000$, les seules valeurs de r pour lesquelles $c(r)$ est de la forme $2^n - 1$ sont $1, 2, 14, 254, 446, 1470$).
On a des énoncés analogues à 3.14 et 3.15 en étudiant la divisibilité de $P_r(z)$ par $1+z^3$, etc.

3.16. Lemme. *Soit r un entier, $r \geq 3$. Soit ω une période de u_{r-1}. Si $u_r^n = 0$ pour $\omega - r + 1 \leq n \leq \omega$, alors ω est une période de u_r.*

Montrons que $u_r^{n+\omega} = u_r^n$ pour $n \geq 0$. Si $n = 0$, on a $u_r^{n+\omega} = u_r^\omega = 0$ par hypothèse, et $u_r^0 = 0$. Supposons $1 \leq n \leq r$. Alors $\omega - r + 1 \leq n + \omega - r \leq \omega$, donc

$$u_r^{n+\omega-r} = 0. \tag{14}$$

Alors

$$\begin{aligned} u_r^{n+\omega} &= u_r^{n+\omega-r} + u_{r-1}^{n+\omega} && \text{d'après (3)} \\ &= u_{r-1}^{n+\omega} && \text{d'après (14)} \\ &= u_{r-1}^n && \text{car } \omega \text{ est période de } u_{r-1} \\ &= u_r^n && \text{d'après (3), car } n - r \leq 0. \end{aligned}$$

Supposons $n > r$ et notre égalité prouvée pour les entiers $\leq n$. Alors $n - r > 0$ donc

$$u_r^{n-r+\omega} = u_r^{n-r} \qquad \text{d'après l'hypothèse de récurrence.} \tag{15}$$

Donc

$$\begin{aligned} u_r^{n+\omega} &= u_r^{n-r+\omega} + u_{r-1}^{n+\omega} && \text{d'après (3)} \\ &= u_r^{n-r} + u_{r-1}^{n+\omega} && \text{d'après (15)} \\ &= u_r^{n-r} + u_{r-1}^n && \text{car } \omega \text{ est période de } u_{r-1} \\ &= u_r^n && \text{d'après (3).} \end{aligned}$$

3.17. Proposition. *Soient r et ω deux entiers, $r \geq 2$, $\omega > 0$. On suppose que $u_r^n = 0$ pour $\omega - \frac{1}{2}r(r+1) + 2 \leq n \leq \omega$. Alors ω est une période de u_r.*

Si $r = 2$, on a $u_2^n = 0$ pour $\omega - 1 \leq n \leq \omega$, donc $4 \mid \omega$ d'après la connaissance de u_2, d'où la proposition dans ce cas. Supposons la proposition établie pour $r - 1$.
Soit n un entier tel que $\omega - \frac{1}{2}r(r-1) + 2 \leq n \leq \omega$. On a

$$n - r \geq \omega - \frac{1}{2}r(r-1) + 2 - r = \omega - \frac{1}{2}r(r+1) + 2$$

donc $u_r^n = u_r^{n-r} = 0$. Par suite, $u_{r-1}^n = 0$ d'après (3). D'après l'hypothèse de récurrence, ω est une période de u_{r-1}. Or on vérifie aisément que $-r + 1 \geq -\frac{1}{2}r(r+1) + 2$. Donc le lemme 3.16 s'applique et entraîne la proposition.

3.18. Proposition. *Soit r un entier, $r \geq 2$. Soient i, s des entiers ≥ 0 tels que $u_r^n = 0$ pour $i \leq n \leq i + s$. Alors $s \leq \frac{1}{2}r(r+1) - 2$.*

Supposons $s > \frac{1}{2}r(r+1) - 2$. Alors $i + s - \frac{1}{2}r(r+1) + 2 > i$. Appliquant la proposition 3.17 avec $\omega = i + s$, on voit que $i + s$ est une période de u_r, donc un multiple de ω_r. Alors $u_r^{i+s-\frac{1}{2}r(r+1)+1} = u_r^{\omega_r - \frac{1}{2}r(r+1)+1} = 1$ (3.12). Or $i + s - \frac{1}{2}r(r+1) + 1 \geq i$, contradiction.

3.19. Appelons *suite principale de zéros* de u_r la suite finie u_r^n,

$$\omega_r - \frac{1}{2}r(r+1) + 2 \leq n \leq \omega_r.$$

Considérons une *suite non principale* de zéros consécutifs de u_r non extraits de la suite principale. Alors, si $r \geq 4$, elle contient au plus $\frac{1}{2}r(r+1) - 9$ éléments. La propriété est vraie pour $r = 4$ (examen direct), et s'en déduit par récurrence par les mêmes raisonnements qu'en 3.16 et 3.18. Ce résultat est certainement loin d'être optimal. Par exemple, pour $r \geq 6$, une suite non principale de zéros contient au plus $\frac{1}{2}r(r+1) - 15$ éléments, car la propriété est vraie pour $r = 6$ (examen direct) donc pour $r \geq 6$ par récurrence.

3.20. Disons qu'une suite finie d'objets $(a_1, a_2, \ldots, a_N)$ est n-périodique si $a_i = a_{i+n}$ pour $1 \leq i \leq i + n \leq N$.

Proposition. *Soient r, i, s, n des entiers $(i, s, n > 0$, $r \geq \frac{n(n-1)}{2} + 2)$. On suppose que la suite $(u_r^i, u_r^{i+1}, u_r^{i+2}, \ldots, u_r^{i+s})$ est n-périodique. Alors $s \leq \frac{1}{2}r(r+1) - 2$.*

Supposons $s > \frac{1}{2}r(r+1) - 2$. En utilisant (3), on voit que la suite

$$(u_{r-1}^{i+r}, u_{r-1}^{i+r+1}, u_{r-1}^{i+r+2}, \ldots, u_{r-1}^{i+s})$$

est n-périodique, et $s - r > \frac{1}{2}(r-1)r - 2$. En outre, si $n \nmid r$, en utilisant encore (3), cette suite est $(0, 0, \dots, 0)$.
L'un des nombres $r, r-1, \dots, r-n+1$, disons $r-t$, est divisible par n. On a $0 \leq t \leq n-1$. En répétant le raisonnement précédent, on voit que la suite

$$(u_{r-t}^{i+tr}, u_{r-t}^{i+tr+1}, u_{r-t}^{i+tr+2}, \dots, u_{r-t}^{i+s})$$

est n-périodique, à condition que $t < r$ et $s > tr$. Or on a

$$r - t - 1 > r - t - 2 \geq \frac{n(n-1)}{2} - t \geq \frac{n(n-1)}{2} - (n-1) \geq 0$$

et

$$\begin{aligned} s - t(r+1) &\geq \frac{1}{2}r(r+1) - 1 - t(r+1) \\ &= \frac{1}{2}(r-t-1)(r-t) + r - 1 - \frac{t(t+1)}{2} \\ &\geq \frac{1}{2}(r-t-1)(r-t) + r - 1 - \frac{n(n-1)}{2} \\ &\geq \frac{1}{2}(r-t-1)(r-t) + 1. \end{aligned}$$

Donc $s - tr \geq 1$. La suite

$$(u_{r-t-1}^{i+t(r+1)}, u_{r-t-1}^{i+t(r+1)+1}, u_{r-t-1}^{i+t(r+1)+2}, \dots, u_{r-t-1}^{i+s})$$

est donc une suite de zéros, et $s - t(r+1) \geq \frac{1}{2}(r-t-1)(r-t) - 1$, ce qui contredit 3.18 puisque $r - t - 1 \geq r - n \geq 2$.
(Nous verrons en 7.7 des exemples non triviaux de suites $(u_r^i, \dots, u_r^{i+s})$ qui sont n-périodiques).

4 Antipériodes des $\mathbf{u_r}$.

4.1. Nous dirons qu'un entier $\alpha \geq 1$ est une *antipériode* de u_r si

$$u_r^{n+\alpha} = u_r^n + 1 \qquad \text{pour } n \geq 0.$$

Soit α la plus petite antipériode de u_r, s'il en existe. On a $2\alpha = h\omega_r$ avec h entier, $h \geq 1$. Supposons $h \geq 2$. Si $h = 2$, on a $\alpha = \omega_r$, contradiction. Si $h \geq 3$, on a $\alpha - \omega_r \geq \frac{3}{2}\omega_r - \omega_r > 0$; or $\alpha - \omega_r$ est une antipériode, contradiction. Donc $h = 1$ et $\alpha = \frac{1}{2}\omega_r$. Ainsi, deux cas sont possibles :

1. Il n'existe pas d'antipériode.
2. La plus petite antipériode est $\frac{1}{2}\omega_r$, auquel cas les antipériodes sont $\frac{1}{2}\omega_r$, $\frac{3}{2}\omega_r, \frac{5}{2}\omega_r, \dots$

4.2. Soient r et n des entiers, avec $r \geq 3$. Les conditions suivantes sont équivalentes :
(i) r est impair et $c(r-1) = 2^n$;
(ii) $c(r) = 2^n + 1$.

Comme $r \geq 3$, on a $c(r) \geq 4$, $c(r-1) \geq 3$, donc $n \geq 2$ dans les deux cas.
Supposons $c(r) = 2^n + 1$. D'après 2.2, $r = 4s + 1$, donc $c(r) = c(r-1) + 1$ et $c(r-1) = 2^n$.
Supposons $r - 1$ pair et $c(r-1) = 2^n$. D'après 2.2, $r - 1 = 4s$, donc $c(r) = c(r-1) + 1 = 2^n + 1$.

4.3. Soit r un entier, $r \geq 3$. Les conditions suivantes sont équivalentes :
(i) Il existe n tel que les propriétés de 4.2 soient vraies.
(ii) r est impair et 2-critique.

(ii)$\Longrightarrow$ (i). Si r est 2-critique, il existe n tel que $c(r-1) \leq 2^n < c(r)$. Si de plus r est impair, on a $c(r) = c(r-1) + 1 = 2^n$.
(i)$\Longrightarrow$ (ii). C'est clair.

4.4. Proposition. *Soit r un entier, $r \geq 3$. Les conditions suivantes sont équivalentes :*
(i) r est impair et 2-critique.
(ii) La suite u_r est antipériodique.
(Cf. 4.9 et 4.10 pour des exemples de tels entiers r).

Soit $\eta = \frac{1}{2}\omega_r$.

(i)$\Longrightarrow$ (ii). Par 4.3 et 4.2, on peut supposer $c(r) = 2^n + 1$. On a (cf. 3.3)

$$(1+z^2)(1+z^3)\dots(1+z^r) = (1+z)^{c(r)-1}V(z)$$

où $V(z) \in k[z]$, $V(1) = 1$. D'autre part, $a(r) = \lceil \log_2(c(r)) \rceil = \lceil \log_2(2^n+1) \rceil = n+1$, donc $v_2(\omega_r) = n+1$, $v_2(\eta) = n$. Ainsi, $1+z$ apparaît avec le même exposant dans les décompositions de $1+z^\eta$ et de $(1+z^2)(1+z^3)\dots(1+z^r)$. Par ailleurs, si $\rho \in \overline{k}$ est une racine primitive i-ème de 1 (i impair, $i \geq 3$) et si $i \leq r$, ρ est racine de $(1+z^2)(1+z^3)\dots(1+z^r)$ à l'ordre $c(t)$ (notations de 3.5), et, d'après 3.7, $c(t) \leq c(\lfloor r/3 \rfloor) \leq c(r) - 1 = 2^n$. Or $2^n = 2^{v_2(\eta)}$ est l'ordre de ρ comme racine de $1+z^\eta$. Il résulte de tout cela que

$$1 + z^\eta = (1+z^2)(1+z^3)\dots(1+z^r)U(z)$$

où $U(z) \in k[z]$, $U(1) = 1$ et $\deg(U) < \eta$. Cette égalité entraîne, en posant $zU(z) = 1 + (1+z)Q(z)$

$$z(1+z^\eta) = (1+z^2)(1+z^3)\dots(1+z^r)(1+(1+z)Q(z))$$

avec $Q(z) \in k[z]$, $\deg(Q) < \eta$. Alors

$$\begin{aligned} P_r(z) &= z\frac{1+z^{\omega_r}}{F_r(z)} = z\frac{(1+z^\eta)^2}{(1+z)(1+z^2)\dots(1+z^r)} \\ &= \frac{1+z^\eta}{1+z}\,\frac{z(1+z^\eta)}{(1+z^2)(1+z^3)\dots(1+z^r)} \\ &= \frac{1+z^\eta}{1+z}\,(1+(1+z)Q(z)) = \frac{1+z^\eta}{1+z} + Q(z) + z^\eta Q(z) \\ &= (Q(z)+1+z+z^2+\dots+z^{\eta-1}) + z^\eta Q(z). \end{aligned}$$

Posons $Q(z) = \alpha_0 + \alpha_1 z + \dots + \alpha_{\eta-1}z^{\eta-1}$. Alors

$$\begin{aligned} P_r(z) &= (\alpha_0+1) + (\alpha_1+1)z + \dots + (\alpha_{\eta-1}+1)z^{\eta-1} \\ &\quad + \alpha_0 z^\eta + \alpha_1 z^{\eta+1} + \dots + \alpha_{\eta-1}z^{2\eta-1} \end{aligned}$$

et l'on voit que $u_r^{n+\eta} = u_r^n + 1$ pour $n \geq 0$.

(ii)$\Longrightarrow$ (i). Supposons u_r antipériodique. Alors, retournant le raisonnement précédent, il existe $Q(z) \in k[z]$ tel que

$$\begin{aligned} P_r(z) &= (Q(z)+1+z+z^2+\dots+z^{\eta-1}) + z^\eta Q(z) \\ &= \frac{1+z^\eta}{1+z}(1+(1+z)Q(z)) \end{aligned}$$

d'où

$$P_r(z) = z\frac{(1+z^\eta)^2}{F_r(z)} = \frac{1+z^\eta}{1+z}(1+(1+z)Q(z))$$

$$1+z^\eta = (1+z^2)(1+z^3)\dots(1+z^r)U(z) \quad \text{où} \quad U(z) \in k[z],\ U(1) = 1.$$

Donc $2^{v_2(\eta)} = c(r) - 1$, $c(r) = 2^{v_2(\eta)} + 1$.

4.5. Une antipériode, combinée avec la symétrie, donne une *antisymétrie*. Expliquons seulement le cas de u_5. On a $\omega_5 = 240$, l'antipériode est 120. Comme $u_5^n = 0$ pour $227 \leq n \leq 240$, on a $u_5^n = 1$ pour $107 \leq n \leq 120$. Ensuite, pour $0 \leq i \leq 107$, on a $u_5^{107-i} + 1 = u_5^{227-i}$ (antipériode), et $u_5^{227-i} = u_5^i$ (symétrie) ; donc

$$u_5^{107-i} = u_5^i + 1.$$

4.6. Proposition. *Soient r, ω deux entiers, $r \geq 3, \omega \geq 1$. On suppose que $u_r^n = 1$ pour $\omega - \frac{1}{2}r(r+1) + 2 \leq n \leq \omega$. Alors ω est une antipériode de u_r. On a $u_r^n = 0$ pour $n = \omega - \frac{1}{2}r(r+1) + 1$ et pour $n = \omega + 1$.*

Si $\omega - \frac{1}{2}r(r-1) + 2 \leq n \leq \omega$, on a $n - r \geq \omega - \frac{1}{2}r(r+1) + 2$, donc $u_{r-1}^n = u_r^n + u_r^{n-r} = 1 + 1 = 0$. D'après 3.17, ω est une période de u_{r-1}. Alors

$u_r^{n+\omega} = u_r^n + 1$ pour tout $n \geq 0$: le raisonnement suit pas à pas celui de 3.16. Ainsi, ω est une antipériode de u_r. Donc 2ω est une période de u_r, et

$$\begin{aligned} u_r^{\omega+1} = u_r^{2\omega+1} + 1 &= u_r^1 + 1 = 1 + 1 = 0 \\ u_r^{\omega-\frac{1}{2}r(r+1)+1} &= u_r^{2\omega-\frac{1}{2}r(r+1)+1} + 1 = 1 + 1 \quad \text{d'après 3.12} \\ &= 0. \end{aligned}$$

4.7. Proposition. *Soit r un entier, $r \geq 3$. Dans tout intervalle d'entiers contenant au moins $\frac{1}{2}r(r+1)$ éléments, u_r prend au moins une fois la valeur 1 et au moins une fois la valeur 0.*

Cela résulte de 3.18 et de 4.6.

4.8. Appelons *suite principale* de 1 une suite finie de 1 de la forme (u_r^n), $\omega - \frac{1}{2}r(r+1) + 2 \leq n \leq \omega$. Alors, pour $r \geq 5$, une suite de 1 consécutifs non extraite d'une suite principale contient au plus $\frac{1}{2}r(r+1) - 9$ éléments : c'est une conséquence facile de 3.19 appliqué à la suite u_{r-1}

4.9. On obtient facilement une table de la fonction $c(r)$ grâce à la remarque suivante : supposons $c(r)$ connu dans l'intervalle $[1, 2^j - 1]$. Alors (cf. 2.3) $c(2^j) = 2^{j-1}(j+2)$, et, (cf. 2.4), pour $1 \leq s \leq 2^j - 1$, $c(2^j + s) = c(2^j) + c(s)$. D'où la valeur de $c(r)$ dans $[1, 2^{j+1} - 1]$.
Cela dit, dans tout intervalle $[2^j, 2^{j+1} - 1]$, il existe au plus un entier n tel que $c(n)$ soit une puissance de 2. Cela résulte de la croissance de $c(r)$ et de 2.5.
Nous avons calculé par ordinateur tous les n tels que $c(n)$ soit une puissance de 2, successivement dans chaque intervalle $[2^j, 2^{j+1} - 1]$, et cela pour $1 \leq j \leq 300$. Les intervalles $[2^j, 2^{j+1} - 1]$ dans lesquels $c(n)$ n'est jamais une puissance de 2 se raréfient quand j augmente : entre 195 et 300, ces valeurs de j sont 199, 200, 201, 217, 225, 226, 249, 254, 256, 298.
En ajoutant 1 aux entiers pairs n tels que $c(n)$ soit une puissance de 2, on obtient, d'après 4.1 et 4.2, les entiers r impairs et 2-critiques qui sont, par 4.4, les entiers r tels que u_r soit antipériodique. Les premiers sont

$$5, 65, 769, 2625, 4865, 8961, 16385, 3023617.$$

En retenant ceux de ces entiers qui sont puissances d'un nombre premier, on obtient 6 entiers vérifiant la propriété 2.13.4 : 5, 769 et les 4 entiers suivants, que nous écrivons en système hexadécimal : 2E2301, 132C35726E2301, 259F35726E2301, 6F50B9FBB9183EA062072E700000000000001. Il se trouve que ces 6 entiers sont premiers. Nous ignorons si ce fait est général.

4.10. *Il existe une infinité d'entiers impairs 2-critiques.*
En effet, soit s un entier, $s \geq 2$ et soit $r = 2^{2^s-2} + 1$. D'après 2.3,

$$c(r-1) = 2^{2^s-3} \cdot 2^s = 2^{2^s-3+s}$$

donc r est impair et 2-critique (cf. 4.3 et 4.2). Pour $s = 2, 3, 4$, on obtient $r = 5, 65, 16385$. D'autres exemples s'obtiennent ainsi. Soit t un entier, $t \geq 2$, $m = \frac{1}{3}(2^{2t+1} - 5)$, $r = 2^m + 2^{m-1} + 1$. (Notons que $2^{2t+1} - 5 \equiv 2(-1)^{2t} - 5 = -3 \equiv 0 \pmod 3$). On a $m \geq \frac{1}{3}(2^5 - 5) = 9$ donc $m - 2 \geq 0$. Cela posé, par 2.4 et 2.3,

$$\begin{aligned} c(r-1) &= c(2^m + 2^{m-1}) = 2^{m-1}(m+2) + 2^{m-2}(m+1) \\ &= 2^{m-2}(3m+5) = 2^{m-2} \cdot 2^{2t+1} = 2^{m+2t-1}. \end{aligned}$$

Pour $t = 2$ et 3, on obtient $r = 769$ et $r = 3 \cdot 2^{40} + 1 = 3298534883329$.

4.11. Si r est un entier *pair* 2-critique, u_r n'est pas antipériodique. Toutefois, on a la propriété suivante (si $r \geq 4$) :
Posons $\eta = \frac{1}{2}\omega_r$. D'après 2.13, on a $\eta = \omega_{r-1}$. Rappelons que $r \mid \omega_{r-1}$ (2.14). L'intervalle $[0, \omega_{r-1}[$ se partage en r classes de congruence modulo r. Si C est une telle classe, soit $\sigma(C) = \sum_{n \in C} u^n_{r-1}$. Alors :
Si $\sigma(C) = 0$, on a $u_r^{n+\eta} = u_r^n$ pour tout $n \in C$.
Si $\sigma(C) = 1$, on a $u_r^{n+\eta} = u_r^n + 1$ pour tout $n \in C$.
En effet, soit $n \in [0, \omega_{r-1}[$. Soit $a = \omega_{r-1}/r$. Alors $\{n+r, n+2r, n+3r, \ldots, n+ar = n+\eta\}$ s'identifie à une des classes C précédentes. On a

$$\begin{aligned} u_r^{n+\eta} &= u_{r-1}^{n+\eta} + u_{r-1}^{n+\eta-r} + u_{r-1}^{n+\eta-2r} + \ldots + u_{r-1}^{n+\eta-(a-1)r} + u_r^n \quad \text{d'après (4)} \\ &= \sigma(C) + u_r^n. \end{aligned}$$

5 Préliminaires sur les algèbres $k[z]/(1+z^p)$.

5.1. On fixe un nombre premier impair p. On note A_p la k-algèbre $k[z]/(1+z^p)$ qui s'identifie à l'algèbre $k[\mathbb{Z}/p]$ du groupe cyclique d'ordre p. Tout élément de A_p admet pour représentant un élément de $k[z]$ de degré $\leq p-1$, et on l'identifiera parfois à ce représentant, ce qui permet de définir $\lambda(F)$ pour tout $F \in A_p$. (Cf. 0.9). On pose $\delta(F) = \lambda(F)/p$.

5.2. Le polynôme cyclotomique $\Phi_p(z) = 1 + z + z^2 + \ldots + z^{p-1} \in k[z]$ sera considéré aussi comme un élément de A_p. On a

$$\Phi_p = z\Phi_p = z^2\Phi_p = \ldots = z^{p-1}\Phi_p.$$

Si $y = \sum \alpha_n z^n \in A_p$, on en déduit que

$$y\Phi_p = (\sum \alpha_n)\Phi_p. \tag{16}$$

En particulier, $\Phi_p^2 = \Phi_p$ car p est impair. On voit que $k\Phi_p = \{0, \Phi_p\}$ est un idéal I_p de A_p.

5.3. Lemme. *Soit $y = \sum \alpha_n z^n \in A_p$. Les conditions suivantes sont équivalentes :*
(i) $y\Phi_p = 0$;
(ii) $\sum \alpha_n = 0$;
(iii) *y est de la forme $(1+z)y'$ où $y' \in A_p$.*

(i) $\Longleftrightarrow$ (ii). Cela résulte de (16).

(ii) $\Longrightarrow$ (iii). C'est vrai même dans $k[z]$ car le reste de la division de $\sum \alpha_n z^n$ par $1+z$ est $\sum \alpha_n$.

(iii) $\Longrightarrow$ (i). Supposons $y = (1+z)y'$. D'après (16), on a $(1+z)\Phi_p = 2\Phi_p = 0$, donc $y\Phi_p = y'(1+z)\Phi_p = 0$.

5.4. Soit J_p l'ensemble des $y \in A_p$ vérifiant les conditions de 5.3. Alors J_p est un idéal de A_p, annulateur de Φ_p, et engendré par $1+z$. Utilisant la condition (ii) de 5.3, on voit que A_p est somme directe de I_p et J_p. Donc l'anneau A_p s'identifie à $I_p \times J_p$, I_p et J_p étant considérés comme des anneaux. Posons

$$\Psi_p(z) = z + z^2 + \ldots + z^{p-1}.$$

On a $\Psi_p \in J_p$ (condition (ii) de 5.3) et $1 = \Phi_p + \Psi_p$, donc Φ_p (resp. Ψ_p) est l'élément unité de l'anneau I_p (resp. J_p).

5.5. Comme $1+z$ engendre l'idéal J_p, on voit que $1+z$ est inversible dans J_p.

5.6. Tout élément a de $(\mathbb{Z}/p)^*$ définit l'automorphisme $\alpha_{a,p} : x \mapsto ax$ de $\mathbb{Z}/p$. Cet automorphisme se prolonge en un automorphisme, noté encore $\alpha_{a,p}$, de $A_p = k[\mathbb{Z}/p]$. On a

$$\alpha_{a,p}(z) = z^a, \quad \alpha_{a,p}(\Phi_p) = \Phi_p, \quad \alpha_{a,p}(J_p) \subset J_p.$$

5.7. Il résulte de 5.5 et 5.6 que $1+z$, $1+z^2$, $1+z^3$, ..., $1+z^{p-1}$ sont des éléments inversibles de J_p.

5.8. On a $J_p = A_p/(\Phi_p)$. Comme $1 + z^p = (1+z)\Phi_p$, on voit que

$$J_p = k[z]/(\Phi_p) = (\mathbb{Z}[z]/2)/(\Phi_p) = (\mathbb{Z}[z]/(\Phi_p))/(2).$$

Posons $E_p = \mathbb{Z}[z]/\Phi_p$. C'est l'anneau des entiers du corps cyclotomique $\mathbb{Q}(e^{2i\pi/p})$, et l'on voit que $J_p = E_p/(2)$. La décomposition de 2 en idéaux premiers de E_p est parfaitement connue, ainsi donc que la structure de l'algèbre J_p. Toutefois, nous aurons besoin seulement de savoir que J_p est réduite (i.e. sans élément nilpotent non nul).
Or, A_p (et donc aussi J_p) est une algèbre réduite : l'élément $F = a_0 + a_1 z + \ldots + a_{p-1}z^{p-1} \in A_p$ a pour carré

$$\begin{aligned} F^2 &= a_0 + a_1 z^2 + a_2 z^4 + \ldots + a_{p-1} z^{2(p-1)} \\ &= a_0 + a_1 z^2 + \ldots + a_{\frac{p-1}{2}} z^{p-1} + a_{\frac{p+1}{2}} z + \ldots + a_{p-1} z^{p-2} \end{aligned}$$

et donc, si $F \neq 0$, on a $F^2 \neq 0$, $F^{2^n} \neq 0$ pour tout $n \geq 0$ et $F^m \neq 0$ pour tout $m \geq 1$.
De façon plus générale, si $f(z) \in k[z]$ est un polynôme premier avec sa dérivée $f'(z)$, l'algèbre $k[z]/f(z)$ est réduite (cf. [2], p. V. 36, prop. 3, et p. V. 34, th. 4).

5.9. Nous noterons $F_{s,p}(z)$ l'image canonique de $F_s(z)$ dans A_p. Cette image étant nulle pour $s \geq p$, on supposera $s \leq p-1$. Avec les conventions de 5.1, on a donc

$$F_{s,p}(z) = (1+z)(1+z^2)\ \ldots\ (1+z^s) \in J_p$$

et d'après 5.7, $F_{s,p}$ est inversible dans J_p. On posera

$$\lambda(F_{s,p}) = \lambda_{s,p} \qquad \delta(F_{s,p}) = \delta_{s,p} = \frac{1}{p}\lambda_{s,p}\,.$$

5.10. Lemme. $F_{p-1,p} = \Psi_p$.

En effet,

$$\begin{aligned}
&(F_{p-1,p}(z))^2 = F_{p-1,p}(z^2) = (1+z^2)(1+z^4)\ \ldots\ (1+z^{2p-2})\\
=\ &[(1+z^2)(1+z^4)\ \ldots\ (1+z^{p-1})][(1+z^{p+1})(1+z^{p+3})\ \ldots\ (1+z^{2p-2})]\\
=\ &[(1+z^2)(1+z^4)\ \ldots\ (1+z^{p-1})][(1+z)(1+z^3)\ \ldots\ (1+z^{p-2})]\\
=\ &F_{p-1,p}(z).
\end{aligned}$$

Ainsi, $F_{p-1,p}$ est un idempotent inversible de l'anneau J_p, donc égal à l'élément unité Ψ_p de J_p.

5.11. On a $1+z^a = z^p + z^a = z^a(1+z^{p-a})$. Donc, pour $1 \leq n \leq p-1$,

$$(1+z)(1+z^2)\ \ldots\ (1+z^n) = z^{n(n+1)/2}(1+z^{p-n})(1+z^{p-n-1})\ \ldots\ (1+z^{p-1}).$$

5.12. Comme $F_{p-1,p}(z) = \Psi_p$ d'après 5.10, on a

$$\begin{aligned}
(1+z)(1+z^2)\ \ldots\ (1+z^{p-n}) &= [(1+z^{p-n+1})(1+z^{p-n+2})\ \ldots\ (1+z^{p-1})]^{-1}\\
&= [z^{-n(n-1)/2}(1+z)(1+z^2)\ \ldots\ (1+z^{n-1})]^{-1} \quad \text{d'après 5.11.}
\end{aligned}$$

Autrement dit,

$$F_{p-n,p}(z) = z^{n(n-1)/2}[F_{n-1,p}(z)]^{-1}. \tag{17}$$

(La formule reste vraie pour $n = 1$, en convenant suivant l'usage que $F_{0,p}(z)$ qui est un produit vide, est l'élément unité Ψ_p de J_p).
En particulier, faisant $n = 2, 3$,

$$F_{p-2,p}(z) = z(1+z)^{-1} \tag{18}$$

$$F_{p-3,p}(z) = z(1+z+z^2+z^3)^{-1}. \tag{19}$$

5.13. Lemme. *L'inverse de $1+z$ dans J_p est donné par les formules suivantes :*
(i) *Si* $p \equiv 1 \pmod 4$, $(1+z)^{-1} = z(1+z^2+z^4+z^6+\ldots+z^{p-3})$
(ii) *Si* $p \equiv 3 \pmod 4$, $(1+z)^{-1} = 1+z^2+z^4+z^6+\ldots+z^{p-1}$.

Notons d'abord que les inverses proposés sont bien des éléments de J_p d'après le critère (ii) de 5.3. Ensuite :

$$\begin{aligned}
z(1+z)(1+z^2+z^4+\ldots+z^{p-3}) &= z(1+z+z^2+\ldots+z^{p-3}+z^{p-2})\\
&= z+z^2+z^3+\ldots+z^{p-1} = \Psi_p
\end{aligned}$$

$$\begin{aligned}
(1+z)(1+z^2+z^4+z^6+\ldots+z^{p-1}) &= 1+z+z^2+\ldots+z^{p-1}+z^p\\
&= z+z^2+z^3+\ldots+z^{p-1} = \Psi_p.
\end{aligned}$$

5.14. Lemme.
(i) *Si* $p \equiv 1 \pmod 4$, $F_{p-2,p}(z) = z^2+z^4+z^6+\ldots+z^{p-1}$.
(ii) *Si* $p \equiv 3 \pmod 4$, $F_{p-2,p}(z) = 1+(z+z^3+z^5+\ldots+z^{p-2})$.

Cela résulte de (18) et de 5.13.

5.15. On a donc $\lambda_{p-2,p} = \dfrac{p-1}{2}$ ou $\dfrac{p+1}{2}$, donc $\left|\delta_{p-2,p} - \dfrac{1}{2}\right| = \dfrac{1}{2p}$.

5.16. Des calculs analogues à ceux de 5.13 montrent que l'inverse de $1+z+z^2+z^3$ dans J_p est donné par les formules suivantes :

$$\begin{aligned}
&\text{Si } p \equiv 1 \pmod 8, \quad (1+z+z^2+z^3)^{-1} = z(1+z^4+z^8+\ldots+z^{p-5}).\\
&\text{Si } p \equiv 3 \pmod 8, \quad (1+z+z^2+z^3)^{-1} = (z+z^2+z^3)\\
&\qquad + (z^5+z^6+z^7)+\ldots+(z^{p-6}+z^{p-5}+z^{p-4})+(z^{p-2}+z^{p-1}).\\
&\text{Si } p \equiv 5 \pmod 8, \quad (1+z+z^2+z^3)^{-1} =\\
&\qquad 1+z((z+z^2+z^3)+(z^5+z^6+z^7)+\ldots+(z^{p-4}+z^{p-3}+z^{p-2})).\\
&\text{Si } p \equiv 7 \pmod 8, \quad (1+z+z^2+z^3)^{-1} = 1+z^4+z^8+\ldots+z^{p-3}.
\end{aligned}$$

Compte tenu de (19), on obtient la valeur explicite de $F_{p-3,p}(z)$, et l'on en déduit que $\delta_{p-3,p} \to \frac{1}{4}$ quand $p \to \infty$ avec $p \equiv 1$ ou $7 \pmod 8$, et $\delta_{p-3,p} \to \frac{3}{4}$ quand $p \to \infty$ avec $p \equiv 3$ ou $5 \pmod 8$.

5.17. Lemme.
(i) *Si* $p \equiv 1$ *ou* $7 \pmod 8$, $F_{(p-1)/2,p}(z) = z^{(p^2-1)/16}\Psi_p$.
(ii) *Si* $p \equiv 3$ *ou* $5 \pmod 8$, $F_{(p-1)/2,p}(z) = z^{(p^2-8p-1)/16}\Psi_p$.

Appliquons (17) avec $n = \frac{p+1}{2}$. Posant $\frac{p^2-1}{8} = q$, il vient :

$$F_{(p-1)/2,p}(z) = z^q F_{(p-1)/2,p}(z)^{-1} = z^{q-p}F_{(p-1)/2,p}(z)^{-1}. \tag{20}$$

Si $p \equiv 1$ ou $7 \pmod 8$, q est pair et (20) donne :

$$\begin{aligned}
(F_{(p-1)/2,p}(z) + z^{q/2}\Psi_p(z))^2 &= F_{(p-1)/2,p}(z)^2 + z^q\Psi_p(z)\\
&= (z^q+z^q)\Psi_p(z) = 0.
\end{aligned}$$

Comme l'algèbre A_p est réduite, on en déduit que $F_{(p-1)/2,p}(z) = z^{q/2}\Psi_p(z)$. Si $p \equiv 3$ ou $5 \pmod 8$, q est impair, donc $q-p$ est pair et (20) donne :

$$(F_{(p-1)/2,p}(z) + z^{(q-p)/2}\Psi_p(z))^2 = 0$$

d'où $F_{(p-1)/2,p}(z) = z^{(q-p)/2}\,\Psi_p(z)$.

5.18. Lemme. *L'inverse de $1+z^{(p-1)/2}$ dans J_p est donné par les formules suivantes :*
(i) Si $p \equiv 1 \pmod 4$, $(1+z^{(p-1)/2})^{-1} = z + z^2 + z^3 + \ldots + z^{(p-1)/2}$.
(ii) Si $p \equiv 3 \pmod 4$, $(1+z^{(p-1)/2})^{-1} = z^{(p+1)/2}(1+z+z^2+z^3+\ldots+z^{(p-1)/2})$ $= z^{(p+1)/2}(1+z+z^2+z^3+\ldots+z^{(p-3)/2}) + 1$.

Les inverses proposés sont bien des éléments de J_p d'après le critère (ii) de 5.3. Ensuite,

$$\begin{aligned}&(1+z^{(p-1)/2})(z+z^2+z^3+\ldots+z^{(p-1)/2})\\ =\ & z+z^2+z^3+\ldots+z^{(p-1)/2}+z^{(p+1)/2}+z^{(p+3)/2}+\cdots+z^{p-1} = \Psi_p\end{aligned}$$

$$\begin{aligned}&(1+z^{(p-1)/2})z^{(p+1)/2}(1+z+z^2+z^3+\ldots+z^{(p-1)/2})\\ =\ & z^{(p+1)/2}(1+z+z^2\ldots+z^{(p-1)/2}+z^{(p-1)/2}+z^{(p+1)/2}+\ldots+z^{p-1})\\ =\ & z^{(p+1)/2}(1+z+z^2+\ldots+z^{(p-3)/2}+z^{(p+1)/2}+\ldots+z^{p-1})\\ =\ & z^{(p+1)/2}+z^{(p+3)/2}+\ldots+z^{p-1}+z+z^2+z^3+\ldots+z^{(p-1)/2} = \Psi_p.\end{aligned}$$

5.19. Lemme. *Ecrivons $F_{(p-1)/2,p}(z) = z^\alpha\Psi_p$ où α est donné par 5.17.*
(i) Si $p \equiv 1 \pmod 4$, $F_{(p-3)/2,p}(z) = z^{\alpha+1}(1+z+z^2+z^3+\ldots+z^{(p-3)/2})$.
(ii) Si $p \equiv 3 \pmod 4$, $F_{(p-3)/2,p}(z) = z^{\alpha+(p+1)/2}(1+z+z^2+z^3+\ldots+z^{(p-1)/2})$.

En effet

$$F_{(p-3)/2,p}(z)(1+z^{(p-1)/2}) = F_{(p-1)/2,p}(z) = z^\alpha\Psi_p$$

d'où

$$F_{(p-3)/2,p}(z) = z^\alpha\Psi_p(1+z^{(p-1)/2})^{-1} = z^\alpha(1+z^{(p-1)/2})^{-1}$$

et il suffit d'appliquer 5.18.

5.20. On a donc $\lambda_{p-3,p} = \dfrac{p-1}{2}$ ou $\dfrac{p+1}{2}$, donc $\left|\delta_{p-3,p} - \dfrac{1}{2}\right| = \dfrac{1}{2p}$.

5.21. Si $F, F' \in A_p$, on écrira désormais $F \sim F'$ s'il existe $n \in \mathbb{Z}$ tel que $F' = z^n F$. On a alors $\lambda(F) = \lambda(F')$, $\delta(F) = \delta(F')$. De plus, $F \sim F'$ et $G \sim G'$ entraînent $FF' \sim GG'$.

5.22. Dans chacun des paragraphes 5.23, 5.24, 5.25, 5.26 on utilisera une fois l'égalité suivante :

$$(1+z^{(p-3)/2})^2 = 1 + z^{p-3} = z^{p-3}(1+z^3).$$

5.23. Lemme. *On suppose $p \equiv 1 \pmod{12}$, de sorte que $6 \mid \frac{p-13}{2}$. Posons*

$$Q(z) = (1+z+z^2)(1+z^6+z^{12}+\ldots+z^{(p-13)/2})(1+z^{(p-3)/2}) \in A_p.$$

(i) $Q(z) \in J_p$ et $\lambda(Q) = \frac{p-1}{2}$.
(ii) $F_{(p-5)/2,p} \sim Q$ et $\lambda_{(p-5)/2,p} = \frac{p-1}{2}$.

On a

$$\begin{aligned}Q(z) \ =\ & (1+z+z^2)+(z^6+z^7+z^8)+\ldots+(z^{(p-13)/2}+z^{(p-11)/2}\\ +\ & z^{(p-9)/2})+(z^{(p-3)/2}+z^{(p-1)/2}+z^{(p+1)/2})\\ +\ & (z^{(p+9)/2}+z^{(p+11)/2}+z^{(p+13)/2})+\ldots+(z^{p-8}+z^{p-7}+z^{p-6})\end{aligned}$$

d'où

$$\lambda(Q) = 3\left(\frac{p-13}{2\cdot 6}+1\right)\cdot 2 = \frac{p-13}{2}+6 = \frac{p-1}{2}$$

donc $\lambda(Q)$ est pair et $Q \in J_p$. On a prouvé (i). Ensuite, d'après 5.22,

$$\begin{aligned}&Q(z)(1+z^{(p-3)/2})(1+z^{(p-1)/2})\\ =\ & (1+z+z^2)(1+z^6+z^{12}+\ldots+z^{(p-13)/2})z^{p-3}(1+z^3)(1+z^{(p-1)/2})\\ =\ & z^{p-3}(1+z+z^2+z^3+z^4+z^5)(1+z^6+z^{12}+\ldots+z^{(p-13)/2})(1+z^{(p-1)/2})\\ =\ & z^{p-3}((1+z+z^2+\ldots+z^{(p-3)/2})+(z^{(p-1)/2}+z^{(p+1)/2}+\ldots+z^{p-2}))\\ \sim\ & 1+z+z^2+\ldots+z^{p-2} \sim \Psi_p.\end{aligned}$$

Or, d'après 5.17,

$$F_{(p-5)/2,p}(1+z^{(p-3)/2})(1+z^{(p-1)/2}) = F_{(p-1)/2,p} \sim \Psi_p$$

donc $F_{(p-5)/2,p} \sim Q$ d'où (ii).

5.24. Lemme. *On suppose $p \equiv 5 \pmod{12}$ et $p \geq 17$, de sorte que $6 \mid \frac{p-17}{2}$. Posons*

$$\begin{aligned}Q(z) = {} & (1+z+z^2)(1+z^6+z^{12}+\ldots+z^{(p-17)/2})(1+z^{(p-3)/2})\\ & +z^{(p-11)/2}+z^{p-6}+z^{p-5}+z^{p-4}.\end{aligned}$$

(i) $Q(z) \in J_p$ et $\lambda(Q) = \frac{p+3}{2}$.
(ii) $F_{(p-5)/2,p} \sim Q$ et $\lambda_{(p-5)/2,p} = \frac{p+3}{2}$.

On a

$$\begin{aligned}Q(z) = {} & (1+z+z^2)+(z^6+z^7+z^8)+\ldots+(z^{(p-17)/2}+z^{(p-15)/2}+z^{(p-13)/2})\\ & +z^{(p-11)/2}\\ & +(z^{(p-3)/2}+z^{(p-1)/2}+z^{(p+1)/2})+(z^{(p+9)/2}+z^{(p+11)/2}+z^{(p+13)/2})\\ & +\ldots+(z^{p-10}+z^{p-9}+z^{p-8})+(z^{p-6}+z^{p-5}+z^{p-4})\end{aligned}$$

d'où

$$\lambda(Q) = 3\left(\frac{p-17}{2\cdot 6}+1\right)\cdot 2 + 4 = \frac{p-17}{2} + 10 = \frac{p+3}{2}$$

d'où (i). Ensuite,

$$\begin{aligned} &Q(z)(1+z^{(p-3)/2})(1+z^{(p-1)/2}) \\ &= (1+z+z^2)(1+z^6+z^{12}+\ldots+z^{(p-17)/2})z^{p-3}(1+z^3)(1+z^{(p-1)/2}) \\ &\quad +(z^{(p-11)/2}+z^{p-6}+z^{p-5}+z^{p-4})(1+z^{(p-3)/2}+z^{(p-1)/2}+z^{p-2}) \\ &= A+B \end{aligned}$$

$$\begin{aligned} A &= z^{p-3}(1+z+z^2+z^3+z^4+z^5)(1+z^6+\ldots+z^{(p-17)/2})(1+z^{(p-1)/2}) \\ &= z^{p-3}((1+z+z^2+\ldots+z^{(p-7)/2})+(z^{(p-1)/2}+z^{(p+1)/2}+\ldots+z^{p-4})) \\ &= (z^{p-3}+z^{p-2}+z^{p-1})+(1+z+\ldots+z^{(p-13)/2}) \\ &\quad +(z^{(p-7)/2}+z^{(p-5)/2}+\ldots+z^{p-7}) \end{aligned}$$

$$\begin{aligned} B &= (z^{(p-11)/2}+z^{p-6}+z^{p-5}+z^{p-4}) \\ &\quad +(z^{p-7}+z^{(p-15)/2}+z^{(p-13)/2}+z^{(p-11)/2}) \\ &\quad +(z^{p-6}+z^{(p-13)/2}+z^{(p-11)/2}+z^{(p-9)/2}) \\ &\quad +(z^{(p-15)/2}+z^{p-8}+z^{p-7}+z^{p-6}) \\ &= z^{(p-11)/2}+z^{(p-9)/2}+z^{p-8}+z^{p-6}+z^{p-5}+z^{p-4} \end{aligned}$$

donc

$$Q(z)(1+z^{(p-3)/2})(1+z^{(p-1)/2}) = (1+z+z^2+\ldots+z^{p-1})+z^{p-8} = z^{p-8}\Psi_p \sim \Psi_p$$

et l'on termine comme en 5.23.

5.25. Lemme. *On suppose $p \equiv 7 \pmod{12}$ et $p \geq 19$, de sorte que $6 \mid \frac{p-19}{2}$. Posons*

$$Q(z) = (1+z+z^2)(1+z^6+z^{12}+\ldots+z^{(p-19)/2})(1+z^{(p-3)/2}) + z^{p-5}+z^{p-4}.$$

(i) $Q(z) \in J_p$ *et* $\lambda(Q) = \frac{p-3}{2}$.
(ii) $F_{(p-5)/2,p} \sim Q$ *et* $\lambda_{(p-5)/2,p} = \frac{p-3}{2}$.

On prouve (i) comme en 5.23 et 5.24. Ensuite,

$$\begin{aligned} &Q(z)(1+z^{(p-3)/2})(1+z^{(p-1)/2}) \\ &= (1+z+z^2)(1+z^6+z^{12}+\ldots+z^{(p-19)/2})z^{p-3}(1+z^3)(1+z^{(p-1)/2}) \\ &\quad +(z^{p-5}+z^{p-4})(1+z^{(p-3)/2}+z^{(p-1)/2}+z^{p-2}) \\ &= A+B \end{aligned}$$

avec

$$\begin{aligned} A &= z^{p-3}(1+z+z^2+z^3+z^4+z^5)(1+z^6+\ldots+z^{(p-19)/2})(1+z^{(p-1)/2}) \\ &= z^{p-3}((1+z+z^2+\ldots+z^{(p-9)/2})+(z^{(p-1)/2}+z^{(p+1)/2}+\ldots+z^{p-5})) \\ &= (z^{p-3}+z^{p-2}+z^{p-1})+(1+z+\ldots+z^{(p-15)/2}) \\ &\quad +(z^{(p-7)/2}+z^{(p-5)/2}+\ldots+z^{p-8}) \end{aligned}$$

$$\begin{aligned} B &= (z^{p-5}+z^{p-4})+(z^{(p-13)/2}+z^{(p-11)/2}) \\ &\quad +(z^{(p-11)/2}+z^{(p-9)/2})+(z^{p-7}+z^{p-6}) \\ &= z^{(p-13)/2}+z^{(p-9)/2}+z^{p-7}+z^{p-6}+z^{p-5}+z^{p-4} \end{aligned}$$

donc

$$Q(z)(1+z^{(p-3)/2})(1+z^{(p-1)/2}) = (1+z+z^2+\ldots+z^{(p-13)/2})+(z^{(p-9)/2}+z^{(p-7)/2}+\ldots+z^{p-1}) \sim \Psi_p$$

et l'on termine comme en 5.23.

5.26. Lemme. *On suppose $p \equiv 11 \pmod{12}$ de sorte que $6 \mid \frac{p-11}{2}$. Posons*

$$Q(z) = (1+z+z^2)(1+z^6+z^{12}+\ldots+z^{(p-11)/2})(1+z^{(p-3)/2}).$$

(i) $Q(z) \in J_p$ *et* $\lambda(Q) = \frac{p+1}{2}$.
(ii) $F_{(p-5)/2,p} \sim Q$ *et* $\lambda_{(p-5)/2,p} = \frac{p+1}{2}$.

On prouve (i) comme en 5.23 et 5.24. Ensuite,

$$\begin{aligned} &Q(z)(1+z^{(p-3)/2})(1+z^{(p-1)/2}) \\ &= (1+z+z^2)(1+z^6+z^{12}+\ldots+z^{(p-11)/2})z^{p-3}(1+z^3)(1+z^{(p-1)/2}) \\ &= z^{p-3}((1+z+z^2+\ldots+z^{(p-1)/2})+(z^{(p-1)/2}+z^{(p+1)/2}+\ldots+z^{p-1})) \\ &= z^{p-3}(1+z+\ldots+z^{(p-3)/2}+z^{(p+1)/2}+z^{(p+3)/2}+\ldots+z^{p-1}) \sim \Psi_p \end{aligned}$$

et l'on termine comme en 5.23.

5.27. D'après 5.23—5.26, on a

$$\lambda_{p-5,p} = \frac{p-3}{2} \quad \text{ou} \quad \frac{p-1}{2} \quad \text{ou} \quad \frac{p+1}{2} \quad \text{ou} \quad \frac{p+3}{2},$$

donc

$$\left|\delta_{p-5,p} - \frac{1}{2}\right| = \frac{1}{2p} \quad \text{ou} \quad \frac{3}{2p}.$$

5.28. Lemme. *Soient $F, G \in A_p$.*
(i) $\lambda(FG) \leq \lambda(F)\lambda(G)$.
(ii) $\lambda(F) + \lambda(\Phi_p + F) = p$.
(iii) Pour $1 \leq s \leq p-1$, on a $\lambda_{s,p} \leq 2\lambda_{s-1,p}$.

L'assertion (i) est claire. Si le coefficient de z^n dans F est 0 (resp. 1), la coefficient de z^n dans Φ_p+F est 1 (resp. 0), d'où (ii). Comme $F_{s,p} = F_{s-1,p}(1+z^s)$, (iii) résulte de (i). Rappelons (cf. 5.12) que $F_{0,p} = \Psi_p$ et donc $\lambda_{0,p} = p-1$.

5.29. Lemme. *Soit $a \in [0,p]$ et $1 \le s \le p-1$. Si $\lambda_{s,p} \ge p-a$, on a*

$$\frac{1}{2}(p-a) \le \lambda_{s-1,p} \le \frac{1}{2}(p+a).$$

D'après 5.28 (iii), $\lambda_{s-1,p} \ge \frac{1}{2}\lambda_{s,p} \ge \frac{1}{2}(p-a)$. D'autre part, $\Phi_p(1+z^s) = 0$, donc $F_{s,p} = (\Phi_p + F_{s-1,p})(1+z^s)$, d'où, en utilisant 5.28 (i) et (ii),

$$p-a \le \lambda_{s,p} \le 2\lambda(\Phi_p + F_{s-1,p}) = 2(p-\lambda_{s-1,p})$$

d'où

$$2\lambda_{s-1,p} \le 2p - p + a = p + a.$$

5.30. Lemme. *Soit $0 \le s \le p-1$. On a $\lambda_{s,p} \ge \sqrt{p-1}$ ou $\lambda_{p-s-1,p} \ge \sqrt{p-1}$.*

On a $F_{p-s-1,p}F_{s,p} \sim \Psi_p$ d'après (17), donc

$$\begin{aligned} p-1 &= \lambda(\Psi_p) = \lambda(F_{p-s-1,p}F_{s,p}) \\ &\le \lambda_{s,p}\lambda_{p-s-1,p} \qquad \text{d'après 5.28 (i)}, \end{aligned}$$

d'où le lemme.

5.31. Lemme. *Soit $s \in \{1,2,\dots,p-1\}$. Il existe $i \in \{s-1, s, p-s-2, p-s-1\}$ tel que $|2\delta_{i,p} - 1| \le 1 - \dfrac{\sqrt{p-1}}{p}$.*

(Remarque : $\dfrac{\sqrt{p-1}}{p} \le \dfrac{1}{2}$ car cela s'écrit $4(p-1) \le p^2$, ou $(p-2)^2 \ge 0$).

A) Supposons $\lambda_{s,p} \ge \sqrt{p-1}$.

- Si $\lambda_{s,p} \le p - \sqrt{p-1}$, on a

$$\frac{\sqrt{p-1}}{p} \le \delta_{s,p} \le 1 - \frac{\sqrt{p-1}}{p}$$

$$\left|\delta_{s,p} - \frac{1}{2}\right| \le \frac{1}{2} - \frac{\sqrt{p-1}}{p} \le \frac{1}{2} - \frac{\sqrt{p-1}}{2p}$$

d'où le lemme.

- Supposons $\lambda_{s,p} > p - \sqrt{p-1}$. D'après 5.29,

$$\frac{1}{2}p - \frac{1}{2}\sqrt{p-1} \le \lambda_{s-1,p} \le \frac{1}{2}p + \frac{1}{2}\sqrt{p-1}$$

$$\frac{1}{2} - \frac{1}{2}\frac{\sqrt{p-1}}{p} \le \delta_{s-1,p} \le \frac{1}{2} + \frac{1}{2}\frac{\sqrt{p-1}}{p}$$

$$2\left|\delta_{s-1,p} - \frac{1}{2}\right| \le \frac{\sqrt{p-1}}{p} \le 1 - \frac{\sqrt{p-1}}{p}$$

(d'après la remarque initiale). D'où le lemme.

B) Supposons $\lambda_{s,p} < \sqrt{p-1}$. D'après 5.30, on a $\lambda_{p-s-1,p} \ge \sqrt{p-1}$. Il suffit alors de changer s en $p-s-1$ dans **A**.

5.32. Lemme. *Soit τ un nombre réel tel que $\dfrac{1}{2} \le \tau \le \dfrac{p}{2} - 2$. On a donc*

$$1 \le \frac{p}{2} - 1 - \tau \le \frac{p}{2} - \frac{3}{2} \qquad \frac{p}{2} - \frac{1}{2} \le \frac{p}{2} - 1 + \tau \le p - 3.$$

Soit I l'ensemble des entiers i tels que

$$\frac{p}{2} - 1 - \tau \le i \le \frac{p}{2} - 1 + \tau.$$

Alors

$$\prod_{i\in I} |2\delta_{i,p} - 1| \le \left(1 - \frac{\sqrt{p-1}}{p}\right)^{\frac{\tau}{2}-\frac{5}{4}}.$$

Notons $s-1$ le plus petit élément de I, de sorte que

$$s - 1 = \left\lceil \frac{p}{2} - 1 - \tau \right\rceil \qquad s = \left\lceil \frac{p}{2} - \tau \right\rceil \le \frac{p}{2} - \tau + 1. \tag{21}$$

On a

$$i \in I \iff p - 2 - i \in I$$

donc $I = \{s-1, s, s+1, \dots, p-s-2, p-s-1\}$. Nous noterons aussi I_0 l'intervalle I. D'après 5.31, il existe $i_0 \in \{s-1, s, p-s-2, p-s-1\}$ tel que $|2\delta_{i_0,p} - 1| \le 1 - \dfrac{\sqrt{p-1}}{p}$. Posons

$$I_1 = I_0 - \{s-1, s, p-s-2, p-s-1\} = \{s+1, s+2, \dots, p-s-4, p-s-3\}.$$

D'après 5.31, il existe $i_1 \in \{s+1, s+2, p-s-4, p-s-3\}$ tel que $|2\delta_{i_1,p} - 1| \le 1 - \dfrac{\sqrt{p-1}}{p}$.

On définit ainsi des intervalles successifs décroissants $I_0, I_1, I_2, \dots$ et des entiers distincts $i_0, i_1, i_2, \dots$ On a

$$I_n = \{s - 1 + 2n, s + 2n, \dots, p - s - 2 - 2n, p - s - 1 - 2n\}.$$

La construction peut continuer tant que $s + 2n < p - s - 2 - 2n$, ce qui équivaut à $4n < p - 2s - 2$ ou $4n \le p - 2s - 3$. Posons donc $\nu = \left\lfloor \dfrac{1}{4}(p - 2s - 3) \right\rfloor$. On a défini des intervalles $I_0, I_1, \dots, I_\nu$, des entiers $i_0, i_1, \dots, i_\nu$, et l'on a donc

$$\prod_{i\in I} |2\delta_{i,p} - 1| \le \left(1 - \frac{\sqrt{p-1}}{p}\right)^{\nu+1}.$$

Or

$$\nu+1 \geq \frac{1}{4}(p-2s-3) \quad \geq \quad \frac{1}{4}p-\frac{1}{2}\left(\frac{p}{2}-\tau+1\right)-\frac{3}{4} \qquad \text{d'après (21)}$$
$$= \frac{\tau}{2}-\frac{5}{4}.$$

5.33. Lemme. *Soient τ et I comme en 5.32. On suppose $p \geq 11$. Alors*

$$\prod_{i\in I} \sup\left(|2\delta_{i,p}-1|, \frac{2}{3}\right) \leq \left(1-\frac{\sqrt{p-1}}{p}\right)^{\frac{\tau}{2}-\frac{5}{4}}.$$

Reprenons pas à pas la démonstration de 5.32. On a $|2\delta_{i_0,p}-1| \leq 1-\dfrac{\sqrt{p-1}}{p}$. Mais

$$p \geq 11 \quad \Longrightarrow \quad 1-\frac{\sqrt{p-1}}{p} > \frac{2}{3}$$

donc

$$\sup\left(|2\delta_{i,p}-1|, \frac{2}{3}\right) \leq 1-\frac{\sqrt{p-1}}{p}.$$

On raisonne de même pour $i_1, i_2, \ldots$, d'où le lemme.

6 Préliminaires sur les décompositions.

6.1. Soient G un groupe commutatif, f une fonction sur G à valeurs dans k. Soient $A_1, A_2, \ldots, A_n$ des sous-groupes de G dont la somme est directe. On dira que f se décompose suivant les A_i si l'on a

$$f\left(\sum_{i=1}^{n} a_i\right) = \sum_{i=1}^{n} f(a_i)$$

quels que soient $a_1 \in A_1, a_2 \in A_2, \ldots$
On en déduit $f(0) = f(0+0+\ldots+0) = nf(0)$, d'où $f(0)=0$ si n est pair.
Une décomposition peut être considérée comme une propriété de périodicité ou d'antipériodicité *partielle*. Prenons le cas de deux sous-groupes A et B. Alors, si $b_0 \in B$ est tel que $f(b_0)=0$, on a

$$f(a+b_0) = f(a)$$

mais seulement pour $a \in A$. Si $f(b_0)=1$, on a de même, pour $a \in A$,

$$f(a+b_0) = f(a)+1.$$

6.2. Exemples. On considère u_3 comme défini sur $\mathbb{Z}/12 = \mathbb{Z}/4 \oplus \mathbb{Z}/3 = \mathbb{Z}3 \oplus \mathbb{Z}4$; et u_4 comme défini sur $\mathbb{Z}/24 = \mathbb{Z}/8 \oplus \mathbb{Z}/3 = \mathbb{Z}3 \oplus \mathbb{Z}8$. Alors u_3 se décompose suivant $\mathbb{Z}3, \mathbb{Z}4$ et u_4 se décompose suivant $\mathbb{Z}3, \mathbb{Z}8$. (Nous prouverons en 7.9 un résultat plus général). Une vérification directe est visualisée par les tableaux suivants :

$\mathbb{Z}/(12)$:

8	11	2	5
4	7	10	1
0	3	6	9

u_3 :

0	0	1	0
1	1	0	1
0	0	1	0

$\mathbb{Z}/(24)$:

16	19	22	1	4	7	10	13
8	11	14	17	20	23	2	5
0	3	6	9	12	15	18	21

u_4 :

0	0	0	1	1	1	0	0
1	1	1	0	0	0	1	1
0	0	0	1	1	1	0	0

Les valeurs des tableaux de droite proviennent de la table 1.3. On vérifie par exemple que $u_4^{17} = 0$ est bien égal à $u_4^9 + u_4^8 = 1+1$, et de même pour les autres cases.

6.3. Désormais, nous n'envisagerons que des groupes *cycliques*, bien que cette restriction soit parfois inutile.
Soit $G = \mathbb{Z}/x$ un groupe cyclique à x éléments. Soit $f \in k[G]$, identifiée à une fonction sur G à valeurs dans k. Nous poserons

$$A(f) = \{g \in G \mid f(g) = 1\} \qquad \lambda(f) = \text{Card } A(f) \qquad \delta(f) = \frac{1}{x}\lambda(f) \in [0,1].$$

Ces notations sont compatibles avec celles de 5.1.

6.4. Lemme.
(i) Soient $f, f' \in k[G]$ tels que $f' = f \circ \alpha$ où α est une permutation de G. On a $\lambda(f) = \lambda(f')$, $\delta(f) = \delta(f')$.
(ii) Soient $f, f' \in k[G]$. On suppose que $f'(g) = f(g)+1$ pour tout $g \in G$. On a $\lambda(f') = x - \lambda(f)$, $\delta(f') - \dfrac{1}{2} = -\left(\delta(f) - \dfrac{1}{2}\right)$.

C'est immédiat.

6.5. Lemme. *Soient x, x' des entiers > 0, $G = \mathbb{Z}/x$, $G' = \mathbb{Z}/x'$, $\Gamma = G \times G'$, $\varphi \in k[\Gamma]$. On suppose que φ se décompose suivant G, G'. Soient $f = \varphi_{|G}$, $f' = \varphi_{|G'}$.*
(i) $2\delta(\varphi) - 1 = -(2\delta(f)-1)(2\delta(f')-1)$.
(ii) $\left|\delta(\varphi) - \dfrac{1}{2}\right| \leq \inf\left(\left|\delta(f) - \dfrac{1}{2}\right|, \left|\delta(f') - \dfrac{1}{2}\right|\right)$.

Soient $A = A(f)$, $B = G - A$, $A' = A(f')$, $B' = G' - A'$, $C = A(\varphi)$. Puisque φ se décompose, C est réunion disjointe de $A \times B'$ et $B \times A'$. Donc

$$\begin{aligned} \lambda(\varphi) &= \lambda(f)(x' - \lambda(f')) + (x - \lambda(f))\lambda(f') \\ &= x'\lambda(f) + x\lambda(f') - 2\lambda(f)\lambda(f') \end{aligned}$$

$$\delta(\varphi) = \frac{\lambda(\varphi)}{xx'} = \frac{\lambda(f)}{x} + \frac{\lambda(f')}{x'} - 2\frac{\lambda(f)}{x}\frac{\lambda(f')}{x'} = \delta(f) + \delta(f') - 2\delta(f)\delta(f')$$

d'où (i). Comme $|2\delta(f)-1| \leq 1$ et $|2\delta(f')-1| \leq 1$, on en déduit (ii).

6.6. Lemme. *Soient $G_1 = \mathbb{Z}/x_1$, $G_2 = \mathbb{Z}/x_2, \ldots$, $G_n = \mathbb{Z}/x_n$ des groupes cycliques, $\Gamma = G_1 \times G_2 \times \cdots \times G_n$, $\varphi \in k[\Gamma]$. On suppose que, pour tout i, φ se décompose suivant $G_i, \prod_{j \neq i} G_j$.*

(i) *φ se décompose suivant $G_1, G_2, \ldots, G_n$.*

(ii) *Soit $f_i = \varphi_{|G_i}$. On a $2\delta(\varphi) - 1 = (-1)^{n-1} \prod_{i=1}^{n} (2\delta(f_i) - 1)$.*

Immédiat par récurrence sur n.

6.7. Soient $x, x', G, G', \Gamma, \varphi$ comme en 6.5, avec de plus $\varphi(0) = 0$. Supposons qu'il existe $g \in k[G]$, $g' \in k[G']$ tels que

$$\varphi(a + a') = g(a) + g'(a') \qquad \text{quels que soient } a \in G,\ a' \in G'.$$

On a $g(0) + g'(0) = \varphi(0) = 0$. Deux cas sont possibles :

1. $g(0) = g'(0) = 0$. Alors $g(a) = g(a) + g'(0) = \varphi(a + 0) = \varphi(a)$, donc $g = \varphi_{|G}$, et de même, $g' = \varphi_{|G'}$. Donc φ se décompose suivant G, G'.

2. $g(0) = g'(0) = 1$. Posons $\widetilde{g}(a) = g(a) + 1$, $\widetilde{g}'(a') = g'(a') + 1$ pour $a \in G$, $a' \in G'$. On a $\widetilde{g}(0) = \widetilde{g}'(0) = 0$, et

$$\varphi(a + a') = g(a) + 1 + g'(a') + 1 = \widetilde{g}(a) + \widetilde{g}'(a').$$

Donc φ se décompose suivant G, G' et $\varphi_{|G} = \widetilde{g}$, $\varphi_{|G'} = \widetilde{g}'$.

7 Décomposition des u_r, première partie.

7.1. Lemme. *Soient p un nombre premier impair, a un entier non multiple de p, $a > 0$. Soit $\rho \in \overline{k}$ une racine primitive i-ème de 1, i impair, $i \neq 1$, i non multiple de p. Alors les ordres de ρ comme racine de $(1+z^a)(1+z^p)$ et $1+z^{ap}$ sont les mêmes.*

Posons $a = 2^x a'$ avec a' impair. Soient α, β, γ les ordres de ρ comme racines de $1+z^p$, $1+z^a$, $1+z^{ap}$. On a $\alpha = 0$. Si i ne divise pas ap, on a $\beta = \gamma = 0$. Supposons que i divise ap, d'où $\gamma = 2^x$. Comme i n'est pas multiple de p, i divise a d'où $\beta = 2^x$.

7.2. Soient r un entier, $r \geq 3$, p un nombre premier impair tel que $r/2 < p \leq r$. On a donc (2.8) $\omega_r = ap$ avec a, p premiers entre eux.

Lemme. *$(1+z)F_r(z)$ divise $(1+z^a)(1+z^p)$.*

Soit $\rho \in \overline{k}$ une racine primitive i-ème de 1, i impair. Soit α (resp. β) son ordre comme racine de $(1+z)F_r(z)$ (resp. $(1+z^a)(1+z^p)$). Montrons que $\alpha \leq \beta$.

1) On suppose $i = 1$. Alors $\rho = 1$. D'après 3.3, $\alpha = 1 + c(r)$. On a $v_2(a) = v_2(\omega_r)$ donc 1 est racine de $1 + z^a$ à l'ordre $2^{v_2(\omega_r)}$. Donc $\beta = 1 + 2^{v_2(\omega_r)}$. Or $c(r) \leq 2^{v_2(\omega_r)}$ (2.9 et 2.10), donc $\alpha \leq \beta$. Supposons désormais $i > 1$.
2) Si $i > r$, on a $\alpha = 0 \leq \beta$. Supposons désormais $i \leq r$.
3) Si i est multiple de p, alors $i = p$ (car $2p > r$). Il en résulte que $\alpha = 1$ (car $2i = 2p > r$). D'autre part $\beta = 1$.
4) Enfin, supposons $1 < i \leq r$ et i non multiple de p. On sait que $F_r(z) \mid 1 + z^{\omega_r}$ (3.6), c'est-à-dire $F_r(z) \mid 1 + z^{ap}$. Donc α est majoré par l'ordre de ρ dans $1 + z^{ap}$, c'est-à-dire par β d'après 7.1.

7.3. Soient $r \geq 3$, p premier impair, $r/2 < p \leq r$. On a $\omega_r = ap$ avec a, p premiers entre eux. Dans le groupe $\mathbb{Z}/\omega_r$, a engendre le sous-groupe $\mathbb{Z}a = \{0, a, 2a, \ldots, (p-1)a\}$, qu'on peut identifier à $\mathbb{Z}/p$ par $ia \mapsto i \bmod p$. Et p engendre le sous-groupe $\mathbb{Z}p = \{0, p, 2p, \ldots, (a-1)p\}$, qu'on peut identifier à $\mathbb{Z}/a$ par $ip \mapsto i \bmod a$. Le groupe produit $\mathbb{Z}a \times \mathbb{Z}p$ s'identifie à $\mathbb{Z}/\omega_r$ par $(ma, np) \mapsto ma + np \bmod \omega_r$.
Nous noterons $t \in \{1, 2, \ldots, p-1\}$ et $t' \in \{1, 2, \ldots, a-1\}$ les entiers tels que

$$t'p = 1 + ta. \tag{22}$$

(Il suffit de prendre pour t' l'inverse de p modulo a, puis son représentant dans $\{1, 2, \ldots, a-1\}$).

7.4. Proposition. *On conserve les notations de 7.3. Alors u_r se décompose suivant $\mathbb{Z}/p = \mathbb{Z}a$ et $\mathbb{Z}/a = \mathbb{Z}p$.*

Comme $F_r(z) = (1+z)(1+z^2)\ldots(1+z^r)$, Φ_p divise F_r à l'ordre 1. Posons $F_r(z) = A(z)\Phi_p(z)$. Les polynômes A et Φ_p sont premiers entre eux. Il existe donc $B(z), C(z) \in k[z]$ tels que

$$\frac{z}{F_r(z)} = \frac{B(z)}{A(z)} + \frac{C(z)}{\Phi_p(z)}, \qquad \deg B < \deg A, \quad \deg C < p - 1. \tag{23}$$

D'après 7.2, $A(z)\Phi_p(z)$ divise $(1+z^a)\Phi_p(z)$, donc $A(z)$ divise $1 + z^a$. Il existe donc des polynômes $D(z)$, $E(z) = (1+z)C(z)$ tels que

$$\begin{aligned} \frac{z}{F_r(z)} &= \frac{D(z)}{1+z^a} + \frac{E(z)}{1+z^p} \\ &= \sum_{n \geq 0} \alpha_n z^n + \sum_{n \geq 0} \beta_n z^n \end{aligned}$$

où la suite (α_n) (resp. (β_n)) admet la période a (resp. p). On a (cf. 3.1)

$$u_r^n = \alpha_n + \beta_n. \tag{24}$$

Avec les notations de 7.3,

$$\begin{aligned} n &= -nta + nt'p \equiv n(p-t)a + nt'p \pmod{\omega_r} \\ n &\equiv nt'p \pmod{a} \\ n &\equiv n(p-t)a \pmod{p} \end{aligned}$$

donc (24) s'écrit

$$u_r^{n(p-t)a+(nt')p} = \alpha_{(nt')p} + \beta_{n(p-t)a}.$$

Comme $u_r^0 = 0$, la proposition résulte alors de 6.7.

7.5. Proposition (symétrie partielle). *On conserve les notations de 7.3. Soit* $R' = -\frac{1}{2}r(r+1)+2$. *Posons* $w(n) = u_r^{na}$ $(n = 0, 1, \dots, p-1)$. *Alors*

$$w(n) = w(-R't - n) \qquad \text{pour tout } n.$$

On a $1 = t'p - ta$, et $u_r^m = u_r^{R'-m}$ pour tout m (3.11). Donc, quels que soient $e, f \in \mathbb{Z}$,

$$u_r^{ea+fp} = u_r^{R'(t'p-ta)-ea-fp}$$

c'est-à-dire, d'après 7.4,

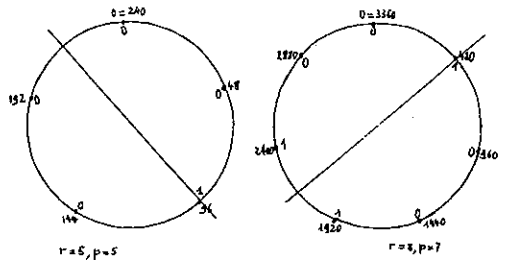
$$u_r^{ea} + u_r^{fp} = u_r^{(-R't-e)a} + u_r^{(R't'-f)p}. \tag{25}$$

Donc $u_r^{ea} + u_r^{(-R't-e)a}$ est indépendant de e. L'application involutive $ea \mapsto (-R't-e)a$ de $\mathbb{Z}a = \mathbb{Z}/p$ sur $\mathbb{Z}a = \mathbb{Z}/p$ a un point fixe e_0 puisque Card($\mathbb{Z}a$)=p est impair. Alors

$$u_r^{e_0 a} + u_r^{(-R't-e_0)a} = 2u_r^{e_0 a} = 0.$$

Donc $u_r^{ea} + u_r^{(-R't-e)a} = 0$ pour tout e, d'où la proposition.

7.6. Cette proposition se visualise comme en 3.13. On dispose régulièrement p points sur un cercle. Comme p est impair, l'un des centres de symétrie fait partie des points choisis, l'autre non. On a représenté les exemples $r = 5$, $p = 5$ et $r = 8$, $p = 7$. On a indiqué à l'intérieur des cercles les valeurs de u_r^n.



7.7. Proposition. *On conserve les notations de 7.3 et 7.5. Soit* S *un nombre vérifiant* $S \geq 0$ *et* $S \equiv R'$ (mod a). *Alors la suite*

$$(u_r^S, u_r^{S+1}, \dots, u_r^{S+\frac{1}{2}r(r+1)-2})$$

est p-périodique.

Posons $u(n) = u_r^n$, $v(n) = u_r^{np}$, $w(n) = u_r^{na}$. Alors $v(n)$ ne dépend que de n mod a, $w(n)$ ne dépend que de n mod p. La formule (25) s'écrit :

$$v(f) + w(e) = v(R't' - f) + w(-R't - e)$$

d'où, compte tenu de 7.5, $v(f) = v(R't' - f)$. Comme $S \equiv R'$ (mod a), cela peut aussi s'écrire :

$$v(f) = v(St' - f). \tag{26}$$

On a $u(n) = u(nt'p - nta) = u(nt'p) + u(-nta)$, c'est-à-dire

$$u(n) = v(nt') + w(-nt). \tag{27}$$

Changeons n en $S - n$:

$$\begin{aligned} u(S-n) &= v((S-n)t') + w(-(S-n)t) \\ &= v(nt') + w((-S-n)t) \qquad \text{d'après (26).} \end{aligned} \tag{28}$$

Ajoutons membre à membre (27) et (28) :

$$u(n) + u(S-n) = w(-nt) + w((-S-n)t).$$

Le membre de droite ne dépend que de n mod p, donc

$$u(n) + u(S-n) = u(n+p) + u(S-n-p). \tag{29}$$

Si maintenant n est tel que

$$S \leq n \leq n+p \leq S + \frac{1}{2}r(r+1) - 2,$$

on a

$$-\frac{1}{2}r(r+1) + 2 \leq S - n - p \leq S - n \leq 0$$

donc $u(S-n) = u(S-n-p) = 0$ (d'après 3.10) et (29) donne

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

7.8. La proposition 7.7 ne nous apprend rien si $S = \omega_r + R'$ (d'après 3.10, les nombres

$$u_r^S, u_r^{S+1}, \dots, u_r^{S+\frac{1}{2}r(r+1)-2}$$

sont alors tous nuls). Mais voici un autre exemple. Prenons $r = p = 5$. Alors $a = 48$, $R' = -13$. Prenons par exemple $S = 35$. La suite $u_5^{35}, u_5^{36}, \dots, u_5^{48}$ est la suivante :

0 1 0 0 1 0 1 0 0 1 0 1 0 0

On observe bien le phénomène de 5-périodicité.

7.9. Proposition. *Soit $2 = p_0 < p_1 < p_2 < \dots$ la suite des nombres premiers. Soit r un entier, $r \geq 3$. Définissons i et j par*

$$p_i \leq \frac{1}{2}r < p_{i+1} \qquad\qquad p_j \leq r < p_{j+1}.$$

Soit

$$\omega_r = p_0^{h_0} p_1^{h_1} \dots p_i^{h_i} p_{i+1} p_{i+2} \dots p_j$$

la décomposition de ω_r en facteurs premiers. Alors u_r se décompose suivant $\mathbb{Z}/p_0^{h_0}p_1^{h_1}\dots p_i^{h_i}$, $\mathbb{Z}/p_{i+1}, \mathbb{Z}/p_{i+2}, \dots, \mathbb{Z}/p_j$.

Cela résulte de 7.4 et 6.6.

7.10. Exemples. On a $\omega_5 = 16 \cdot 3 \cdot 5$. D'après 7.9, u_5 se décompose suivant $\mathbb{Z}/16, \mathbb{Z}/3, \mathbb{Z}/5$. Pour définir u_5, il suffit alors de connaître les u_5^n pour $n \in \mathbb{Z}\cdot 15$, $n \in \mathbb{Z}\cdot 80$, $n \in \mathbb{Z}\cdot 48$.

Suite	$u_5^{i\cdot 15}$,	$0 \leq i < 16$:	0 0 1 0 1 1 0 0 1 1 0 1 0 0 1 1
Suite	$u_5^{i\cdot 80}$,	$0 \leq i < 3$:	0 0 1
Suite	$u_5^{i\cdot 48}$,	$0 \leq i < 5$:	0 0 1 0 0

On a $\omega_6 = 16\cdot 3\cdot 5$. D'après 7.9, u_6 se décompose suivant $\mathbb{Z}/16 \oplus \mathbb{Z}/3$, $\mathbb{Z}/5$. On a $\mathbb{Z}/16 = \mathbb{Z}\cdot 15$, $\mathbb{Z}/3 = \mathbb{Z}\cdot 80$. Or,

$$u_6^{30} = 1 \qquad u_6^{160} = 0 \qquad u_6^{160+30} = 0$$

donc, *on n'a pas* décomposition suivant $\mathbb{Z}/16$, $\mathbb{Z}/3$. Toutefois, on peut montrer que u_6 se décompose suivant $\mathbb{Z}/4 = \mathbb{Z}\cdot 60$, $\mathbb{Z}/3 = \mathbb{Z}\cdot 80$.

7.11. On conserve les notations de 7.3. *On notera $u_{r,p}$ la restriction de u_r à $\mathbb{Z}/p$ $(= \mathbb{Z}a)$.* Le but du chapitre suivant est de déterminer $u_{r,p}$ explicitement.

8 Décomposition des u_r, deuxième partie.

Dans tout ce chapitre, on supposera $r \geq 3$, p premier et $r/2 < p \leq r$.

8.1. Lemme. *On reprend les notations de 7.4. Soit $\sigma \in \{0, 1, \dots, p-1\}$ tel que $\sigma \equiv -\frac{1}{2}(2p-r-1)r - 1 \pmod p$. Dans l'algèbre J_p du chap. 5, on a*

$$E(z) = z^{-\sigma} F_{2p-r-1,p}(z).$$

On multiplie les deux membres de (23) par $F_r(z) = A(z)\Phi_p(z)$. Comme

$$F_r(z)/\Phi_p(z) = (1+z)(1+z^2)\dots(1+z^{p-1})(1+z)(1+z^{p+1})(1+z^{p+2})\dots(1+z^r),$$

on obtient

$$z = B(z)\Phi_p(z) + C(z)(1+z)^2(1+z^2)\dots(1+z^{p-1})(1+z^{p+1})\dots(1+z^r)$$

donc

$$z(1+z) = B(z)(1+z^p) + E(z)(1+z)^2(1+z^2)\dots(1+z^{p-1})(1+z^{p+1})\dots(1+z^r).$$

Réduisant modulo $1+z^p$, on obtient, dans l'algèbre A_p du chap. 5,

$$\begin{aligned} z(1+z) &= E(z)(1+z)F_{p-1,p}(z)(1+z)(1+z^2)\dots(1+z^{r-p}) \qquad (30)\\ &= E(z)(1+z)F_{p-1,p}(z)F_{r-p,p}(z). \end{aligned}$$

On a $z(1+z) \in J_p$, $E(z) \in J_p$ (car $E(z) = (1+z)C(z)$), $F_{p-1,p} = \Psi_p$ d'après 5.10. On déduit de (30)

$$E(z) = z(F_{r-p,p}(z))^{-1}$$

donc, d'après (17) où l'on fait $n = r-p+1$,

$$\begin{aligned} E(z) &= z \cdot z^{-n(n-1)/2} F_{2p-r-1,p}(z)\\ &= z^{\frac{1}{2}(2p-r-1)r+1} F_{2p-r-1,p}(z) \end{aligned}$$

d'où le lemme.

8.2. Utilisons toujours les notations de 7.4, et posons

$$F_{2p-r-1,p}(z) = \sum_{i=0}^{p-1} \gamma_i z^i. \qquad (31)$$

On a $\alpha_0 + \beta_0 = u_r^0 = 0$. D'autre part, β_0 est le terme constant de $E(z)$. D'après 8.1, on a $\beta_0 = \gamma_\sigma$. Donc
Si $\gamma_\sigma = 0$, on a $\alpha_0 = \beta_0 = 0$.
Si $\gamma_\sigma = 1$, on a $\alpha_0 = \beta_0 = 1$.

8.3. Proposition. *Avec les notations de 7.4, 8.1, 8.2, on a, pour tout n multiple de a*

$$u_r^n = \gamma_{(n+\sigma) \bmod p} \qquad \text{si } \gamma_\sigma = 0$$
$$u_r^n = 1 + \gamma_{(n+\sigma) \bmod p} \qquad \text{si } \gamma_\sigma = 1$$

Supposons $\gamma_\sigma = 0$, donc $\alpha_0 = \beta_0 = 0$. Alors $\alpha_n = 0$ puisque $a \mid n$. Soit $n' \in \{0, 1, \dots, p-1\}$ tel que $n' \equiv n \pmod p$. Alors, d'après (24),

$$u_r^n = \alpha_n + \beta_n = \beta_n$$

et β_n est le coefficient de $z^{n'}$ dans $E(z)$, c'est-à-dire, d'après 8.1, $\gamma_{(n'+\sigma) \bmod p} = \gamma_{(n+\sigma) \bmod p}$.
Supposons $\gamma_\sigma = 1$, donc $\alpha_0 = \beta_0 = 1$. Alors $\alpha_n = 1$ donc $u_r^n = 1 + \beta_n = 1 + \gamma_{(n+\sigma) \bmod p}$.

8.4. Exemple : r = 2p − 1.

On a $\sigma \equiv -1 \pmod p$, donc $\sigma = p-1$, et (cf. 5.12)

$$F_{2p-r-1,p} = F_{0,p} = \Psi_p,$$

donc $\gamma_\sigma = 1$. Alors, pour n multiple de a,

$$u_r^n = 1 + \gamma_{(n-1) \bmod p}.$$

Donc $u_r^n = 1$ *si* $n \equiv 1 \pmod p$, $u_r^n = 0$ *sinon.*

Cas particulier : $r = 5$, $p = 3$. Alors $\omega_5 = 240$, $a = 80$, donc

$$u_5^0 = 0, \qquad u_5^{80} = 0, \qquad u_5^{160} = 1$$

car $80 \equiv 2 \pmod 3$ et $160 \equiv 1 \pmod 3$.

8.5. Exemple : r = 2p − 2.

On a $\sigma \equiv -\frac{1}{2}(2p-2) - 1 = -p \equiv 0 \pmod p$, donc $\sigma = 0$, et

$$F_{2p-r-1,p} = F_{1,p} = 1 + z$$

donc $\gamma_\sigma = 1$. Alors, pour n multiple de a,

$$u_r^n = 1 + \gamma_{n \bmod p}.$$

Donc $u_r^n = 0$ *si* $n \equiv 0$ *ou* $1 \pmod p$, $u_r^n = 1$ *sinon.*

Cas particulier : $r = 8$, $p = 5$. Alors $\omega_8 = 32 \cdot 3 \cdot 5 \cdot 7$, $a = 672$, donc

$$u_8^0 = 0, \qquad u_8^{672} = 1, \qquad u_8^{1344} = 1, \qquad u_8^{2016} = 0, \qquad u_8^{2688} = 1.$$

8.6. Exemple : r = p.

On a $\sigma \equiv -\frac{1}{2}(p-1)p - 1 \equiv -1 \pmod p$, donc $\sigma = p-1$, et (cf. 5.10)

$$F_{2p-r-1,p} = F_{p-1,p} = \Psi_p$$

donc $\gamma_\sigma = 1$. Alors, pour n multiple de a,

$$u_r^n = 1 + \gamma_{(n-1) \bmod p}.$$

Donc $u_r^n = 1$ *si* $n \equiv 1 \pmod p$, $u_r^n = 0$ *sinon.*

Cas particulier : $r = p = 7$. Alors $\omega_7 = 16 \cdot 3 \cdot 5 \cdot 7$, $a = 240 \equiv 2 \pmod 7$,

$$u_7^0 = 0, \quad u_7^{240} = 0, \quad u_7^{480} = 0, \quad u_7^{720} = 0, \quad u_7^{960} = 1, \quad u_7^{1200} = 0, \quad u_7^{1440} = 0.$$

8.7. Exemple : r = p + 1.

On a $\sigma \equiv -\frac{1}{2}(p-2)(p+1) - 1 = \frac{p+1}{2}p + p + 1 - 1 \equiv 0 \pmod p$, donc $\sigma = 0$, et

$$F_{2p-r-1,p} = F_{p-2,p}.$$

Utilisons 5.14. Supposons d'abord $p \equiv 1 \pmod 4$. Alors, $F_{p-2,p}(z) = z^2 + z^4 + z^6 + \ldots + z^{p-1}$, donc $\gamma_\sigma = 0$. Pour n multiple de a,

$$\begin{aligned} u_r^n &= 0 \quad \text{si } n \equiv 0,\ 1,\ 3,\ 5,\ \ldots,\ p-2 \pmod p \\ &= 1 \quad \text{si } n \equiv 2,\ 4,\ 6,\ \ldots,\ p-1 \pmod p. \end{aligned}$$

Supposons $p \equiv 3 \pmod 4$. Alors, $F_{p-2,p}(z) = 1 + (z + z^3 + z^5 + \ldots + z^{p-2})$, donc $\gamma_\sigma = 1$. Pour n multiple de a,

$$\begin{aligned} u_r^n &= 0 \quad \text{si } n \equiv 0,\ 1,\ 3,\ 5,\ \ldots,\ p-2 \pmod p \\ &= 1 \quad \text{si } n \equiv 2,\ 4,\ 6,\ \ldots,\ p-1 \pmod p. \end{aligned}$$

Le résultat est le même dans les deux cas.

8.8. Lemme. *On a* $|2\delta(u_{r,p}) - 1| = |2\delta_{2p-r-1,p} - 1|$.

Cela résulte de 8.3 et 6.4.

9 Comportement asymptotique de d(r).

9.1. Rappelons (cf. 0.7) que $d(r) = \delta(u_r)$, où l'on considère u_r comme une fonction $\mathbb{Z}/\omega_r \longrightarrow \{0,1\}$.

9.2. On pose $\varepsilon_r = \prod_{r/2<p\le r} |2\delta_{2p-r-1,p} - 1|$.

9.3. Lemme. $|2d(r) - 1| \le \varepsilon_r$.

Cela résulte de 6.6, 7.4 et 8.8.

9.4. Proposition. *Soit* $(p_0, p_1, p_2, \ldots)$ *la suite croissante des nombres premiers.*
(i) $d(p_n + 1) \to \frac{1}{2}$ *quand* $n \to \infty$.
(ii) $d\left(\frac{1}{2}(3p_n + 1)\right) \to \frac{1}{2}$ *quand* $n \to \infty$.
(iii) $d\left(\frac{1}{2}(3p_n + 3)\right) \to \frac{1}{2}$ *quand* $n \to \infty$.

Soit p un nombre premier impair.
(i) Posons $r = p + 1$. On a $2p - r - 1 = p - 2$. D'après 5.15, $\left|\delta_{p-2,p} - \frac{1}{2}\right| = \frac{1}{2p}$, donc $|2d(r) - 1| \le \frac{1}{p}$ d'après 9.3. Cela prouve (i).
(ii) Posons $r = \frac{1}{2}(3p + 1)$. On a $2p - r - 1 = \frac{1}{2}(p - 3)$. D'après 5.20, $\left|\delta_{(p-3)/2,p} - \frac{1}{2}\right| = \frac{1}{2p}$, donc $|2d(r) - 1| \le \frac{1}{p}$ d'après 9.3. Cela prouve (ii).

(iii) Posons $r = \frac{1}{2}(3p+3)$. On a $2p-r-1 = \frac{1}{2}(p-5)$. D'après 5.27, $\left|\delta_{(p-5)/2,p} - \frac{1}{2}\right| = \frac{1}{2p}$ ou $\frac{3}{2p}$, donc $|2d(r)-1| \le \frac{3}{p}$ d'après 9.3. Cela prouve (iii).

9.5. Il est clair que si u_r est antipériodique, on a $d(r) = \frac{1}{2}$. En particulier d'après 4.10,

$$d\left(2^{2^s-2}+1\right) = \frac{1}{2} \qquad \text{pour tout entier } s > 0.$$

9.6. Lemme. *Soient ℓ, R des entiers tels que $\ell \ge 4$, $R > 2\ell$. On a*

$$\prod_{R\le r\le R+\ell} \varepsilon_r \le \prod_{(4R+\ell)/6\le p\le(4R+3\ell)/6} \left(1-\frac{\sqrt{p-1}}{p}\right)^{\frac{2\ell-25}{20}}.$$

Soit A l'ensemble des (r,p) tels que $R \le r \le R+\ell$, $r/2 < p \le r$, p premier. On a

$$\prod_{R\le r\le R+\ell} \varepsilon_r = \prod_{(r,p)\in A} |2\delta_{2p-r-1,p} - 1|.$$

Soit B l'ensemble des (r,p) tels que

$$R \le r \le R+\ell, \qquad \frac{2}{3}R+\frac{1}{6}\ell \le p \le \frac{2}{3}R+\frac{1}{2}\ell, \qquad p \text{ premier.} \tag{32}$$

Notons que

$$\left(\frac{2}{3}R+\frac{1}{6}\ell\right) - \left(\frac{1}{2}R+\frac{1}{2}\ell\right) = \frac{1}{6}R-\frac{1}{3}\ell > 0. \tag{33}$$

Si $(r,p) \in B$, on a, d'après (32), (33) et la condition $R > 2\ell$,

$$\frac{1}{2}r \le \frac{1}{2}R+\frac{1}{2}\ell < \frac{2}{3}R+\frac{1}{6}\ell \le p \le \frac{2}{3}R+\frac{1}{2}\ell < \frac{2}{3}R+\frac{1}{4}R < R \le r$$

donc $(r,p) \in A$. Ainsi $B \subset A$ et par suite

$$\prod_{R\le r\le R+\ell} \varepsilon_r \le \prod_{(r,p)\in B} |2\delta_{2p-r-1,p} - 1|. \tag{34}$$

Fixons p dans $[\frac{2}{3}R+\frac{1}{6}\ell, \frac{2}{3}R+\frac{1}{2}\ell]$. Quand r varie de R à $R+\ell$, $2p-r-1$ varie de $2p-R-\ell-1$ à $2p-R-1$. Or

$$p \le \frac{2}{3}R+\frac{1}{2}\ell \Rightarrow p \le \frac{2}{3}R+\frac{8}{15}\ell \Rightarrow \frac{3p}{2} \le R+\frac{4}{5}\ell \Rightarrow 2p-R-\ell-1 \le \frac{p}{2}-\frac{\ell}{5}-1$$

$$p \ge \frac{2}{3}R+\frac{1}{6}\ell \Rightarrow p \ge \frac{2}{3}R+\frac{2}{15}\ell \Rightarrow \frac{3p}{2} \ge R+\frac{1}{5}\ell \Rightarrow 2p-R-1 \ge \frac{p}{2}+\frac{\ell}{5}-1$$

donc

$$\prod_{R\le r\le R+\ell,\ p \text{ fixé}} |2\delta_{2p-r-1,p} - 1| \le \prod_{\frac{1}{2}p-\frac{1}{5}\ell-1\le i\le\frac{1}{2}p+\frac{1}{5}\ell-1} |2\delta_{i,p} - 1|. \tag{35}$$

Posons $\tau = \frac{1}{5}\ell$. On a

$$p \ge \frac{2}{3}R+\frac{1}{6}\ell \ge \frac{4}{3}\ell+\frac{1}{6}\ell = \frac{3}{2}\ell \ \ge\ \frac{2}{5}\ell+4 \qquad (\text{car } \ell \ge 4)$$
$$= \ 2\tau+4$$

donc $\tau \le \frac{p}{2}-2$. D'autre part, $\tau \ge \frac{1}{2}$. Donc 5.32 s'applique et donne

$$\prod_{\frac{1}{2}p-\frac{1}{5}\ell-1\le i\le\frac{1}{2}p+\frac{1}{5}\ell-1} |2\delta_{i,p} - 1| \le \left(1-\frac{\sqrt{p-1}}{p}\right)^{\frac{\ell}{10}-\frac{5}{4}}. \tag{36}$$

Les relations (34), (35) et (36) entraînent

$$\prod_{R\le r\le R+\ell} \varepsilon_r \le \prod_{\frac{2}{3}R+\frac{1}{6}\ell\le p\le\frac{2}{3}R+\frac{1}{2}\ell} \left(1-\frac{\sqrt{p-1}}{p}\right)^{\frac{\ell}{10}-\frac{5}{4}}.$$

9.7. Lemme. *Soit α un nombre fixé, $0.535 < \alpha < 1$. Pour tout $R > 1$, posons $\ell(R) = R^\alpha$. On a*

$$\left(\prod_{R\le r\le R+\ell(R)} \varepsilon_r\right)^{1/\ell(R)} \to 0 \qquad \textit{quand } R \to \infty.$$

Pour R assez grand, on a, d'après 9.6,

$$\left(\prod_{R\le r\le R+\ell(R)} \varepsilon_r\right)^{1/\ell(R)} \le \prod_{(4R+\ell(R))/6\le p\le(4R+3\ell(R))/6} \left(1-\frac{\sqrt{p-1}}{p}\right)^{\frac{2\ell(R)-25}{20\ell(R)}}$$

donc

$$\log\left(\prod_{R\le r\le R+\ell(R)} \varepsilon_r\right)^{1/\ell(R)} \le -\frac{2\ell(R)-25}{20\ell(R)} \sum_{(4R+\ell(R))/6\le p\le(4R+3\ell(R))/6} \frac{\sqrt{p-1}}{p}$$

$$\le -\frac{2\ell(R)-25}{20\ell(R)} \sum_{(4R+\ell(R))/6\le p\le(4R+3\ell(R))/6} \frac{1}{2\sqrt{p}}$$

$$\le -\frac{2\ell(R)-25}{20\ell(R)} \frac{1}{2\sqrt{(4R+3\ell(R))/6}} \left(\pi\left(\frac{4R+3\ell(R)}{6}\right) - \pi\left(\frac{4R+\ell(R)}{6}\right)\right)$$

où $\pi(x)$ désigne le nombre de nombres premiers au plus égaux à x. Nous utiliserons le résultat suivant de [1] : pour x assez grand et $x^{0.535} \leq y \leq x$, on a

$$\pi(x) - \pi(x-y) > \frac{y}{20 \log x}.$$

Or, pour R assez grand, $\frac{4R+3\ell(R)}{6} < R$ et

$$\frac{1}{6}(4R+3\ell(R)) - \frac{1}{6}(4R+\ell(R)) = \frac{1}{3}\ell(R) = \frac{1}{3}R^{\alpha} \geq R^{0.535}$$

d'où

$$\pi\left(\frac{4R+3\ell(R)}{6}\right) - \pi\left(\frac{4R+\ell(R)}{6}\right) > \frac{\ell(R)}{60 \log R} = \frac{R^{\alpha}}{60 \log R}.$$

Donc

$$\log\left(\prod_{R\leq r\leq R+\ell(R)} \varepsilon_r\right)^{1/\ell(R)} \leq -C\frac{1}{\sqrt{R}}\frac{R^{\alpha}}{\log R}$$

où C est une constante > 0. Cela prouve le lemme.

9.8. Proposition. *Soit $\alpha \in]0.535, 1[$. Pour tout $R > 1$, posons $\ell(R) = R^{\alpha}$. On a*

$$\left(\prod_{R\leq r\leq R+\ell(R)} |2d(r)-1|\right)^{1/\ell(R)} \to 0 \qquad \textit{quand } R \to \infty.$$

Cela résulte de 9.3 et 9.7.

10 Equirépartition des u_r^n.

10.1. Soient $G = \mathbb{Z}/x$ un groupe cyclique à x éléments, f une fonction sur G à valeurs dans $\{0,1\}$. *Dans ce chapitre, il s'agit des nombres complexes* $0, 1$, *non des classes modulo* 2. Les définitions de $A(f), \lambda(f), \delta(f)$ sont inchangées. Munissons G de sa mesure de Haar normalisée, pour laquelle chaque élément de G a pour mesure $1/x$. Alors $\lambda(f)$ est l'intégrale de f, $\delta(f)$ est sa moyenne.

10.2. Soit $\widetilde{G}$ le groupe dual de G, qui est cyclique d'ordre x. Nous identifierons $\widetilde{G}$ au groupe des racines x-ièmes de 1 dans $\mathbb{C}$. Nous identifierons parfois G à $\{0, 1, \ldots, x-1\}$. Si $\rho \in \widetilde{G}$, le caractère χ_ρ de G défini par ρ est la fonction $g \mapsto \rho^g$. La transformée de Fourier $\mathcal{F}f$ de f est la fonction complexe sur $\widetilde{G}$ définie par

$$(\mathcal{F}f)(\rho) = \frac{1}{x}\sum_{g=0}^{x-1} \rho^g f(g).$$

En particulier,

$$(\mathcal{F}f)(1) = \delta(f).$$

Nous noterons $i_{\widetilde{G}}$ la fonction caractéristique de l'élément neutre dans $\widetilde{G}$. On a donc $i_{\widetilde{G}}(1) = 1$ et pour $\rho \in \widetilde{G}$, $\rho \neq 1$, $i_{\widetilde{G}}(\rho) = 0$.
Rappelons que la norme $\| \|_\infty$ d'une fonction complexe est la borne supérieure de son module.

10.3. Lemme. *Soit $f : G \to \{0,1\}$ une fonction. On a*

$$\|2\mathcal{F}f - i_{\widetilde{G}}\|_\infty \leq 1.$$

D'abord, $\left|\left(2\mathcal{F}f - i_{\widetilde{G}}\right)(1)\right| = |2\delta(f) - 1| \leq 1$. Ensuite, soit $\rho \in \widetilde{G}$, $\rho \neq 1$. Alors

$$\left(2\mathcal{F}f - i_{\widetilde{G}}\right)(\rho) = 2\mathcal{F}f(\rho) = \frac{2}{x}\sum_{g=0}^{x-1} \rho^g f(g) = \frac{2}{x}\sum_{g\in A(f)} \rho^g.$$

Or, puisque $\rho \neq 1$,

$$\sum_{g\in A(f)} \rho^g + \sum_{g\in G-A(f)} \rho^g = \sum_{g\in G} \rho^g = 0 \tag{37}$$

donc

$$\left|\frac{1}{x}\sum_{g\in A(f)} \rho^g\right| = \left|\frac{1}{x}\sum_{g\in G-A(f)} \rho^g\right| \leq \inf\left(\frac{\lambda(f)}{x}, \frac{x-\lambda(f)}{x}\right).$$

L'un des nombres $\frac{\lambda(f)}{x}$, $\frac{x-\lambda(f)}{x}$ est $\leq \frac{1}{2}$, donc $|2\mathcal{F}f(\rho)| \leq 1$.

10.4. Lemme. *Soient x, x' des entiers > 0, $G = \mathbb{Z}/x$, $G' = \mathbb{Z}/x'$, f (resp. f') une fonction sur G (resp. G') à valeurs dans $\{0,1\}$. Soit $\varphi : G \times G' \to \{0,1\}$, définie par*

$$\varphi(g,g') = 0 \quad si \quad f(g) = f'(g') = 0 \quad ou \quad f(g) = f'(g') = 1$$
$$\varphi(g,g') = 1 \quad si \quad f(g) = 0,\ f'(g') = 1 \quad ou \quad f(g) = 1,\ f'(g') = 0.$$

Soit $\varepsilon, \varepsilon'$ tels que

$$\|2\mathcal{F}f - i_{\widetilde{G}}\|_\infty \leq \varepsilon \qquad \|2\mathcal{F}f' - i_{\widetilde{G}'}\|_\infty \leq \varepsilon'.$$

Alors

$$\|2\mathcal{F}\varphi - i_{\widetilde{G}\times\widetilde{G}'}\|_\infty \leq \varepsilon\varepsilon'.$$

Soient $A = A(f)$, $A' = A(f')$, $a = \lambda(f)$, $a' = \lambda(f')$. Par hypothèse,

$$\varepsilon \geq \left|2\mathcal{F}f(1) - i_{\widetilde{G}}(1)\right| = \left|2\frac{a}{x} - 1\right| \tag{38}$$

$$\varepsilon' \geq \left|2\mathcal{F}f'(1) - i_{\widetilde{G}'}(1)\right| = \left|2\frac{a'}{x'} - 1\right| \tag{39}$$

$$\varepsilon \geq |2\mathcal{F}f(\rho)| = \left|\frac{2}{x}\sum_{g\in A}\rho^g\right| = \left|\frac{2}{x}\sum_{g\in G-A}\rho^g\right| \qquad \text{si } \rho \neq 1 \tag{40}$$

$$\varepsilon' \geq |2\mathcal{F}f'(\rho')| = \left|\frac{2}{x'}\sum_{g'\in A'}\rho'^{g'}\right| = \left|\frac{2}{x'}\sum_{g'\in G'-A'}\rho'^{g'}\right| \qquad \text{si } \rho' \neq 1. \tag{41}$$

Soit $(\rho,\rho')\in G\times G'$. On a

$$\begin{aligned}
&2\mathcal{F}\varphi(\rho,\rho')\\
&= \frac{1}{xx'}\sum_{g\in G,\,g'\in G'}\rho^g\rho'^{g'}\varphi(g,g')\\
&= \frac{2}{xx'}\left(\sum_{g\in A,\,g'\in G'-A'}\rho^g\rho'^{g'}+\sum_{g\in G-A,\,g'\in A'}\rho^g\rho'^{g'}\right)\\
&= \frac{2}{xx'}\left(\left(\sum_{g\in A}\rho^g\right)\left(\sum_{g'\in G'-A'}\rho'^{g'}\right)+\left(\sum_{g\in G-A}\rho^g\right)\left(\sum_{g'\in A'}\rho'^{g'}\right)\right)
\end{aligned} \tag{42}$$

Cas 1 : $\rho\neq 1$, $\rho'\neq 1$. En majorant par (40) et (41) les modules des quatre sommes de (42), on obtient

$$\left|\left(2\mathcal{F}\varphi - i_{\widetilde{G}\times\widetilde{G}'}\right)(\rho,\rho')\right| = |2\mathcal{F}\varphi(\rho,\rho')| \leq \frac{2}{xx'}\left(\frac{x\varepsilon}{2}\frac{x'\varepsilon'}{2}+\frac{x\varepsilon}{2}\frac{x'\varepsilon'}{2}\right) = \varepsilon\varepsilon'.$$

Cas 2 : $\rho\neq 1$, $\rho'=1$. La relation (42) entraîne

$$\begin{aligned}
|2\mathcal{F}\varphi(\rho,1)| &= \tfrac{2}{xx'}\left|(x'-a')\textstyle\sum_{g\in A}\rho^g + a'\sum_{g\in G-A}\rho^g\right| \\
&= \tfrac{2}{xx'}\left|(x'-2a')\textstyle\sum_{g\in A}\rho^g\right| && \text{d'après (37)}\\
&\leq \tfrac{1}{x'}(x'-2a')\varepsilon && \text{d'après (40)}\\
&\leq \varepsilon\varepsilon' && \text{d'après (39).}
\end{aligned}$$

Cas 3 : $\rho=1$, $\rho'\neq 1$. Même raisonnement.

Cas 4 : $\rho=\rho'=1$. La relation (42) entraîne

$$\begin{aligned}
|2\mathcal{F}\varphi(1,1)-1| &= \left|\frac{2}{xx'}(a(x'-a')+(x-a)a')-1\right| \\
&= \left|-\left(\frac{2a-x}{x}\right)\left(\frac{2a'-x'}{x'}\right)\right| \leq \varepsilon\varepsilon' \quad \text{d'après (38) et (39).}
\end{aligned}$$

10.5. Lemme. *Soient n un entier, $n\geq 2$, $R\subset\mathbb{C}$ l'ensemble des racines n-ièmes de 1, P une partie de R. Posons $\sigma_P=\sum_{\rho\in P}\rho$, $\nu_P=|\sigma_P|$, $\xi(n)=\max_{P\subset R}\nu_P$. Alors*

$$\text{si } n \text{ est pair}, \quad \xi(n)=\frac{1}{\sin\frac{\pi}{n}}; \qquad \text{si } n \text{ est impair}, \quad \xi(n)=\frac{1}{2\sin\frac{\pi}{2n}}.$$

Ce résultat est cetainement connu, mais nous n'avons pas trouvé de réfèrences. Soit P tel que $\nu_P=|\sigma_P|$ soit maximal, autrement dit tel que $\nu_P=\xi(n)$. Comme $\nu_P=\nu_{R-P}$, on peut choisir P tel que Card $(P)\leq n/2$. Soit Δ la droite du plan complexe passant par l'origine et perpendiculaire à σ_P. Cette droite partage le plan complexe en deux demi-plans : Π_1, demi-plan ouvert contenant σ_P, et Π_2, demi-plan fermé contenant $-\sigma_P$ et Δ. Notons que, si $v\in\Pi_1\cup\Delta$ et $v\neq 0$, on a $|\sigma_P+v|>|\sigma_P|=\nu_P$.
Aucun élément de P n'est dans Π_2 ; en effet, si ρ appartenait à $P\cap\Pi_2$, on aurait $-\rho\in\Pi_1\cup\Delta$ et

$$|\sigma_{P-\{\rho\}}| = |\sigma_P+(-\rho)| > |\sigma_P|.$$

De même, tout élément ρ de R situé dans Π_1 appartient à P (sinon, en rajoutant ρ à P, on augmenterait ν_P).
En conséquence, P est l'ensemble des éléments de R situés dans un demi-plan ouvert limité par une droite passant par l'origine. Si n est pair, un tel demi-plan contient $\frac{n}{2}$ ou $\frac{n}{2}-1$ éléments consécutifs de R. Comme

$$\left|1+e^{\frac{2i\pi}{n}}+e^{\frac{4i\pi}{n}}+\ldots+e^{\frac{\left(\frac{n}{2}-1\right)2i\pi}{n}}\right| = \left|\frac{2}{1-e^{\frac{2i\pi}{n}}}\right| = \frac{1}{\sin\frac{\pi}{n}}$$

et que

$$\left|1+e^{\frac{2i\pi}{n}}+e^{\frac{4i\pi}{n}}+\ldots+e^{\frac{\left(\frac{n}{2}-2\right)2i\pi}{n}}\right| = \left|\frac{1+e^{-\frac{2i\pi}{n}}}{1-e^{\frac{2i\pi}{n}}}\right| = \frac{\cos\frac{\pi}{n}}{\sin\frac{\pi}{n}} < \frac{1}{\sin\frac{\pi}{n}},$$

on conclut que $\nu_P=\xi(n)=\frac{1}{\sin\frac{\pi}{n}}$.
Lorsque n est impair, un demi-plan limité par une droite passant par l'origine contient $\frac{n+1}{2}$ ou $\frac{n-1}{2}$ éléments consécutifs de R. Comme Card$(P)\leq n/2$, on a Card$(P)=\frac{n-1}{2}$, et

$$\nu_P = \left|1+e^{\frac{2i\pi}{n}}+e^{\frac{4i\pi}{n}}+\ldots+e^{\frac{\left(\frac{n-3}{2}\right)2i\pi}{n}}\right| = \left|\frac{1+e^{-\frac{i\pi}{n}}}{1-e^{\frac{2i\pi}{n}}}\right| = \frac{\cos\frac{\pi}{2n}}{\sin\frac{\pi}{n}} = \frac{1}{2\sin\frac{\pi}{2n}}.$$

Corollaire. *Soit $n\geq 3$ un entier impair. Avec les notations du lemme 10.5, on a, pour tout $P\subset R$*

$$\nu_P \leq \xi(n) \leq \frac{n}{3}.$$

Le lemme 10.5 donne

$$\nu_P \leq \xi(n) = \frac{n}{\pi}\left(\frac{\pi/2n}{\sin(\pi/2n)}\right) \leq \frac{n}{\pi}\left(\frac{\pi/6}{\sin(\pi/6)}\right) = \frac{n}{3}$$

car la fonction $t\mapsto \sin t/t$ est décroissante dans l'intervalle $[0,\pi/6]$.

10.6. Lemme. *Soit $n \geq 3$ un entier impair. Soit $\rho \neq 1$ une racine n-ième de 1 dans $\mathbb{C}$. Soient $0 \leq a < b < c < \cdots < \ell \leq n-1$ des entiers. On a*

$$\frac{1}{n}\left|\rho^a + \rho^b + \rho^c + \ldots + \rho^\ell\right| \leq \frac{1}{3}.$$

Soit $m \in \{1, 2, \ldots, n-1\}$ tel que $\rho = e^{2i\pi m/n}$. Soit d le pgcd de m et n de sorte que $m = dt$, $n = du$ avec t premier avec u. On a $\rho = e^{2i\pi t/u}$ et ρ est une racine primitive u-ième de 1. La somme $\rho^a + \rho^b + \ldots + \rho^\ell$ est une somme de racines u-ièmes de 1, avec répétitions possibles ; on a

$$\rho^\alpha = \rho^\beta \iff \alpha \equiv \beta \pmod{u}.$$

Chaque classe modulo u contient exactement d éléments de l'ensemble $\{0, 1, 2, \ldots, n-1\}$. Dans la somme $\rho^a + \rho^b + \ldots + \rho^\ell$, chaque racine u-ième est donc répétée au plus d fois. Donc, avec les notations de 10.5,

$$\left|\rho^a + \rho^b + \rho^c + \ldots + \rho^\ell\right| \leq d\xi(u).$$

Comme n est impair, u est impair. Comme $\rho \neq 1$, on a $u \neq 1$ donc $u \geq 3$. Alors $\xi(u) \leq \frac{1}{3}u$ d'après le corollaire 10.5. Donc

$$\left|\rho^a + \rho^b + \rho^c + \ldots + \rho^\ell\right| \leq \frac{1}{3}du = \frac{n}{3}.$$

10.7. Lemme. *On a*

$$\|2\mathcal{F}u_r - i_{(\mathbb{Z}/\omega_r)^\sim}\|_\infty \leq \prod_{r/2<p\leq r} \sup\left(|2\delta_{2p-r-1} - 1|, \frac{2}{3}\right).$$

En effet,

$$\left|\left(2\mathcal{F}u_{r,p} - i_{(\mathbb{Z}/p)^\sim}\right)(1)\right| = |2\delta(u_{r,p}) - 1| = |2\delta_{2p-r-1} - 1|$$

d'après 8.8. Et, si $\rho \neq 1$,

$$\left|\left(2\mathcal{F}u_{r,p} - i_{(\mathbb{Z}/p)^\sim}\right)(\rho)\right| = |2\mathcal{F}u_{r,p}(\rho)| = \frac{2}{p}\left|\sum_{j\in X}\rho^j\right| \text{ où } X \subset \{0, 1, \ldots, p-1\}$$

$$\leq \frac{2}{3} \qquad \text{d'après 10.6 .}$$

Donc

$$\|2\mathcal{F}u_{r,p} - i_{(\mathbb{Z}/p)^\sim}\|_\infty \leq \sup\left(|2\delta_{2p-r-1} - 1|, \frac{2}{3}\right).$$

Alors le lemme résulte de 10.4 (appliqué par récurrence au cas d'un produit d'un nombre fini de groupes).

10.8. On posera :

$$\varepsilon'_r = \prod_{r/2<p\leq r} \sup\left(|2\delta_{2p-r-1} - 1|, \frac{2}{3}\right).$$

10.9. Lemme. *Soient ℓ, R des entiers tels que $\ell \geq 6$, $R > 2\ell$. On a*

$$\prod_{R\leq r\leq R+\ell} \varepsilon'_r \leq \prod_{(4R+\ell)/6\leq p\leq(4R+3\ell)/6} \left(1 - \frac{\sqrt{p-1}}{p}\right)^{\frac{2\ell-25}{20}}.$$

Il suffit de recopier la preuve de 9.6. Là où on utilisait le lemme 5.32, on applique 5.33. C'est possible car $R \geq 13$ donc $p \geq (4R+\ell)/6 \geq (52+6)/6 > 9$, donc $p \geq 11$.

10.10. Lemme. *Soit α un nombre fixé, $0.535 < \alpha < 1$. Pour tout $R > 1$, posons $\ell(R) = R^\alpha$. On a*

$$\left(\prod_{R\leq r\leq R+\ell(R)} \varepsilon'_r\right)^{1/\ell(R)} \to 0 \qquad \textit{quand } R \to \infty.$$

Même preuve qu'en 9.7, en utilisant 10.9 au lieu de 9.6.

10.11. Proposition. *Soit α un nombre fixé, $0.535 < \alpha < 1$. Pour tout $R > 1$, posons $\ell(R) = R^\alpha$. On a*

$$\left(\prod_{R\leq r\leq R+\ell(R)} \|2\mathcal{F}u_r - i_{(\mathbb{Z}/\omega_r)^\sim}\|_\infty\right)^{1/\ell(R)} \to 0 \qquad \textit{quand } R \to \infty.$$

Cela résulte de 10.7, 10.8 et 10.10.

10.12. Proposition. *Il existe une partie infinie P de $\mathbb{N}$ telle que*

$$\|2\mathcal{F}u_r - i_{(\mathbb{Z}/\omega_r)^\sim}\|_\infty \to 0 \qquad \textit{quand } r \to \infty, \quad r \in P.$$

En effet, si l'on avait $\liminf_{r\to\infty} \|2\mathcal{F}u_r - i_{(\mathbb{Z}/\omega_r)^\sim}\|_\infty > 0$, cela contredirait 10.11.

10.13. Soit $\widehat{\mathbb{Z}}$ le complété de $\mathbb{Z}$ pour la topologie dans laquelle les idéaux différents de $\{0\}$ de $\mathbb{Z}$ forment un système fondamental de voisinages de 0.
Ce groupe compact commutatif est un sous-groupe du groupe des adèles de $\mathbb{Q}$. Il possède une mesure de Haar μ de masse totale 1, d'où un espace hilbertien $L^2(\mu)$ avec norme $\|\ \|_2$ et produit scalaire $<,>$.

Comme $\omega_{r-1} \mid \omega_r$, et que tout entier divise ω_r pour r assez grand, on a

$$\widehat{\mathbb{Z}} = \varprojlim (\mathbb{Z}/\omega_r)$$

la limite étant prise relativement aux homomorphismes canoniques :

$$\pi_{r',r} : \mathbb{Z}/\omega_{r'} \longrightarrow \mathbb{Z}/\omega_r \qquad (r' \geq r).$$

Nous noterons π_r l'homomorphisme canonique $\widehat{\mathbb{Z}} \longrightarrow \mathbb{Z}/\omega_r$. La mesure $\pi_r(\mu)$ est la mesure qui attribue la masse $1/\omega_r$ à chaque point de Z/ω_r.
Soit $R \subset \mathbb{C}$ le groupe des racines de l'unité. Soit ρ une racine (ω_r)-ième de 1. Alors ρ définit le caractère χ_ρ de $\mathbb{Z}/\omega_r$, tel que $\chi_\rho(x) = \rho^x$. Si $r' \geq r$, et si $x' \in \mathbb{Z}/\omega_{r'}$ est tel que $\pi_{r',r}(x') = x$, on a $x' \equiv x \pmod{\omega_r}$, donc $\rho^x = \rho^{x'}$. Donc il existe un caractère ψ_ρ de $\widehat{\mathbb{Z}}$ tel que $\psi_\rho(z) = \chi_\rho(\pi_r(z))$ pour tout z. Tout caractère de $\widehat{\mathbb{Z}}$ s'obtient de cette manière, et l'on peut identifier le groupe dual de $\widehat{\mathbb{Z}}$ au groupe R muni de la topologie discrète. La famille $(\psi_\rho)_{\rho \in R}$ est une base orthonormale de $L^2(\mu)$ (propriété générale des groupes compacts commutatifs). *La fonction relevée de u_r à $\widehat{\mathbb{Z}}$, c'est-à-dire $u_r \circ \pi_r$, sera notée $\widehat{u}_r$.*

10.14. Rappel sur les espaces hilbertiens.
Soit $\mathcal{H}$ un espace hilbertien, et $x_1, x_2, \ldots \in \mathcal{H}$.
a) La suite (x_i) tend faiblement vers x si $< x_i, y > \to < x, y >$ pour tout $y \in \mathcal{H}$. Cela entraîne que $\sup \|x_i\| < +\infty$. (Cf. par exemple [6], p. 21).
b) Soit T une partie totale de $\mathcal{H}$, par exemple une base orthonormale. Si $\sup \|x_i\| < +\infty$, et si $< x_i, y > \to < x, y >$ pour tout $y \in T$, alors (x_i) tend faiblement vers x. (Très facile).

10.15. Proposition. *Dans $L^2(\mu)$, la suite $\widehat{u}_r$ tend faiblement vers la constante $\frac{1}{2}$ si $r \to \infty$, $r \in P$ (notation de 10.12).*

a) Comme les valeurs de $\widehat{u}_r$ appartiennent à $\{0, 1\}$, on a $\|u_r\|_2 \leq 1$.
b) Considérons le caractère unité ψ_1 de $\widehat{\mathbb{Z}}$, correspondant à l'élément 1 de R (cf. 10.13). On a

$$< \widehat{u}_r, \psi_1 >= \int_{\widehat{\mathbb{Z}}} \widehat{u}_r \psi_1 \, d\mu = \int_{\mathbb{Z}/\omega_r} u_r \cdot 1 \, d\pi_r(\mu) = \frac{1}{\omega_r} \sum_{0 \leq n < \omega_r} u_r^n.$$

D'après 10.12, ce nombre tend vers $\frac{1}{2}$, c'est-à-dire vers $< \frac{1}{2}, \psi_1 >$.
c) Considérons le caractère ψ_ρ de $\widehat{\mathbb{Z}}$ correspondant à l'élément ρ de $R - \{1\}$. On a, pour r assez grand (plus précisément, quand ρ est une racine (ω_r)-ième de 1),

$$< \widehat{u}_r, \psi_\rho >= \int_{\widehat{\mathbb{Z}}} \widehat{u}_r \psi_\rho \, d\mu = \int_{\mathbb{Z}/\omega_r} u_r \cdot \chi_\rho \, d\pi_r(\mu) = (\mathcal{F} u_r)(\rho).$$

D'après 10.12, ce nombre tend vers 0, c'est-à-dire vers $< \chi_\rho, \frac{1}{2} >=< \psi_\rho, \frac{1}{2} >$.
La proposition résulte de a), b), c).

10.16. Corollaire. *La suite $\widehat{u}_r$ tend vers la constante $\frac{1}{2}$ au sens des distributions sur $\widehat{\mathbb{Z}}$, si $r \in P$.*

En effet, les fonctions indéfiniment dérivables sur $\widehat{\mathbb{Z}}$ sont des éléments de $L^2(\mu)$. (Le corollaire est d'ailleurs, compte tenu du fait que $\|u_r\|_2 \leq 1$, équivalent à la proposition 10.15, puisque les fonctions indéfiniment dérivables forment une partie dense de $L^2(\mu)$).

10.17. Proposition. *Soient r_0, n_0 des entiers fixés ($r_0 > 0$). Pour $r \geq r_0$, soit A_r l'ensemble des $n \in \mathbb{Z}/\omega_r$ tels que $n \equiv n_0 \pmod{\omega_{r_0}}$. Soit B_r l'ensemble des $n \in A_r$ tels que $u_r^n = 1$. Alors, quand $r \to \infty$ en restant dans P (notation de 10.12), on a*

$$\text{Card } B_r / \text{Card } A_r \quad \to \quad \frac{1}{2}.$$

(Pour $r_0 = 1$, on a $A_r = \mathbb{Z}/\omega_r$ et Card B_r/Card $A_r = d(r)$).
On a $A_{r_0} = \{n_0\}$ et, pour $r \geq r_0$,

$$A_r = \pi_{r,r_0}^{-1}(A_{r_0}), \qquad \text{donc Card } A_r = \omega_r/\omega_{r_0}.$$

Soit a_r la fonction caractéristique de A_r dans $\mathbb{Z}/\omega_r$.
Soit A l'ensemble des $z \in \widehat{\mathbb{Z}}$ tels que $\pi_{r_0}(z) \equiv n_0 \pmod{\omega_{r_0}}$. Sa fonction caractéristique a est un élément de $L^2(\mu)$. On a

$$< \widehat{u}_r, a > \quad \to \quad < \frac{1}{2}, a > \qquad \text{si } r \to \infty, r \in P \tag{43}$$

d'après 10.15. Or

$$< \frac{1}{2}, a >= \int_{\widehat{\mathbb{Z}}} \frac{1}{2} \cdot a \, d\mu = \int_{\mathbb{Z}/\omega_{r_0}} \frac{1}{2} \cdot a_{r_0} \, d\pi_{r_0}(\mu) = \frac{1}{2\omega_{r_0}} > 0,$$

$$< \widehat{u}_r, a >= \int_{\widehat{\mathbb{Z}}} \widehat{u}_r \cdot a \, d\mu = \int_{\mathbb{Z}/\omega_r} u_r \cdot a_r \, d\pi_r(\mu) = (\text{Card } B_r)/\omega_r,$$

donc

$$< \widehat{u}_r, a > / < \frac{1}{2}, a >= 2\,(\text{Card } B_r)\frac{\omega_{r_0}}{\omega_r} = 2\,\frac{\text{Card } B_r}{\text{Card } A_r}.$$

La proposition résulte alors de (43).

10.18. Remarque. La suite $\widehat{u}_r(z)$ diverge pour presque tout $z \in \widehat{\mathbb{Z}}$. En effet, soit $X \subset \widehat{\mathbb{Z}}$ l'ensemble des $z \in \widehat{\mathbb{Z}}$ tels que $\widehat{u}_r(z)$ ait une limite quand $r \to \infty$. Cet ensemble est μ-mesurable. Supposons $\mu(X) > 0$. D'après le théorème d'Egoroff ([3], p. 175, th. 2), il existe une partie mesurable A de X telle que $\mu(A) > 0$ et que $(\widehat{u}_r)_{|A}$ converge uniformément. Donc A est la réunion disjointe de deux ensembles mesurables A_0, A_1 tels que, pour $r \geq r_0$, on ait $\widehat{u}_r(z) = 0$ pour tout $z \in A_0$, $\widehat{u}_r(z) = 1$ pour tout $z \in A_1$. L'un au moins des nombres $\mu(A_0)$, $\mu(A_1)$ est strictement positif. Si $\mu(A_0) > 0$, la fonction caractéristique φ de A_0 dans $\widehat{\mathbb{Z}}$ est un élément non nul de $L^2(\mu)$, et $< \widehat{u}_r, \varphi >= 0$ pour $r \geq r_0$, alors que $< \frac{1}{2}, \varphi >= \frac{1}{2}\mu(A_0) > 0$, contradiction. Raisonnement analogue si $\mu(A_1) > 0$.

10.19. Pour $z \in \mathbb{Z} \subset \widehat{\mathbb{Z}}$, la suite $\widehat{u}_r(z)$ a une limite et même mieux :

Si $z > 0$, on a $\widehat{u}_r(z) = \overline{p}(z-1)$ pour r assez grand ;
si $z \leq 0$, on a $\widehat{u}_r(z) = 0$ pour r assez grand.

La première assertion résulte de 1.7 et 1.8. Supposons $z \leq 0$. Pour r assez grand, on a $-\frac{1}{2}r(r+1)+2 \leq z \leq 0$, donc z est congru modulo ω_r à un nombre de $[\omega_r - \frac{1}{2}r(r+1)+2, \omega_r]$, d'où $u_r(z) = 0$.

11 Méthode de calcul de d(r).

11.1. Soit t un entier, $t \geq 1$. Nous noterons $\Phi_t(z) \in k[z]$ le polynôme cyclotomique d'indice t ; on a donc, pour $n \geq 1$

$$1 + z^n = \prod_{t \mid n} \Phi_t(z).$$

Lorsque n est pair, on écrit $n = 2^{v_2(n)}n'$ avec n' impair, et l'on a

$$1 + z^n = (1+z^{n'})^{2^{v_2(n)}} = \prod_{t \mid n'} (\Phi_t(z))^{2^{v_2(n)}}.$$

Il s'ensuit, avec les notations du chapitre 2

$$\begin{aligned} F_r(z) &= \prod_{n=1}^{r}(1+z^n) = \prod_{n=1}^{r} \prod_{\substack{t \mid n \\ t \text{ impair}}} (\Phi_t(z))^{2^{v_2(n)}} \\ &= \prod_{\substack{t=1 \\ t \text{ impair}}}^{r} \prod_{j=1}^{\lfloor r/t \rfloor} (\Phi_t(z))^{2^{v_2(jt)}} = \prod_{\substack{t=1 \\ t \text{ impair}}}^{r} (\Phi_t(z))^{c(\lfloor r/t \rfloor)} \end{aligned}$$

car $v_2(jt) = v_2(j)$.

11.2. Soit t et t' deux nombres impairs distincts. Alors $\Phi_t(z)$ et $\Phi_{t'}(z)$ sont premiers entre eux dans $k[z]$. En effet, si $\rho \in \overline{k}$ était une racine commune à $\Phi_t(z)$ et $\Phi_{t'}(z)$, ce serait une racine primitive t-ième et t'-ième de l'unité ; on aurait donc $t \mid t'$, $t' \mid t$ et $t = t'$.

11.3. En raison de 11.1 et 11.2, on a la décomposition en éléments simples

$$f(z) = \frac{1}{F_r(z)} = \sum_{\substack{t=1 \\ t \text{ impair}}}^{r} f_t(z), \qquad f_t(z) = \frac{C_t(z)}{(\Phi_t(z))^{c(\lfloor r/t \rfloor)}} \tag{44}$$

avec $C_t(z) \in k[z]$ et $\deg C_t < c(\lfloor r/t \rfloor)\varphi(t)$ où φ est l'indicateur d'Euler. En utilisant la fonction a définie en 2.9, on a

$$f_t(z) = \frac{E_t(z)}{(1+z^t)^{2^{a(\lfloor r/t \rfloor)}}} = \frac{E_t(z)}{1+z^{t2^{a(\lfloor r/t \rfloor)}}} \tag{45}$$

avec

$$E_t(z) = \frac{(1+z^t)^{2^{a(\lfloor r/t \rfloor)}}}{(\Phi_t(z))^{c(\lfloor r/t \rfloor)}} C_t(z). \tag{46}$$

Notons que $\deg(E_t) < t2^{a(\lfloor r/t \rfloor)}$.

11.4. Calcul de C_t et E_t. Le polynôme C_t est l'inverse modulo $(\Phi_t(z))^{c(\lfloor r/t \rfloor)}$ du polynôme $\dfrac{F_r(z)}{(\Phi_t(z))^{c(\lfloor r/t \rfloor)}}$. Ce calcul sera exécuté en MAPLE avec la fonction `Gcdex` qui programme l'algorithme d'Euclide étendu. Ensuite, E_t est calculé par la formule (46). Notons que MAPLE calcule les polynômes cyclotomiques.

11.5. Soit $M \geq 1$ un nombre entier. On dira qu'une série formelle $f(z) = a_0 + a_1 z + a_2 z^2 + \ldots$ est périodique de période M si la suite de ses coefficients (a_n) est périodique de période M.
Si les coefficients a_n valent 0 ou 1, on posera

$$\delta(f) = \frac{1}{M}\lambda\left(a_0 + a_1 z + a_2 z^2 + \ldots + a_{M-1}z^{M-1}\right) = \frac{1}{M}\sum_{i=0}^{M-1} a_i. \tag{47}$$

C'est la valeur moyenne des coefficients de f.
Il est clair que la définition ci-dessus ne dépend pas de la période M de f choisie. Dans tout ce chapitre, pour chacune des séries considérées, nous allons déterminer une période (afin de calculer la densité δ) mais on ne se souciera pas de préciser si c'est la plus petite période.
Exemples : la fraction f_t définie par (45) a pour période $t2^{a(\lfloor r/t \rfloor)}$ et $\delta(f_t) = \dfrac{\lambda(E_t)}{t2^{a(\lfloor r/t \rfloor)}}$. Pour $r \geq 2$, soit f défini par

$$f(z) = \frac{1}{F_r(z)} = \sum_{n=0}^{\infty} u_r^{n+1} z^n.$$

D'après 3.8, et 3.10, f est périodique de période ω_r, et

$$\delta(f) = \delta(u_r) = d(r). \tag{48}$$

11.6. Proposition. *Soient deux entiers $M \geq 1$ et $N \geq 1$ premiers entre eux. Soit deux séries formelles $f, g \in k[[z]]$ de périodes respectives M et N. Alors la série $f+g$ est périodique de période MN et*

(i) $\delta(f+g) = \delta(f) + \delta(g) - 2\delta(f)\delta(g) = \dfrac{1}{2} - 2\left(\delta(f) - \dfrac{1}{2}\right)\left(\delta(g) - \dfrac{1}{2}\right)$.

(ii) $\left|\delta(f+g) - \dfrac{1}{2}\right| \leq \inf\left(\left|\delta(f) - \dfrac{1}{2}\right|, \left|\delta(g) - \dfrac{1}{2}\right|\right)$.

Posons $f(z) = a_0 + a_1 z + a_2 z^2 + \ldots$, $g(z) = b_0 + b_1 z + b_2 z^2 + \ldots$ On a $\varphi(z) = f(z) + g(z) = c_0 + c_1 z + c_2 z^2 + \ldots$ avec $c_n = a_n + b_n$. Clairement, les coefficients de φ sont périodiques de période MN.

On a (cf. 7.3) $\mathbb{Z}N \oplus \mathbb{Z}M = \mathbb{Z}/MN$ et tout élément $n \in \mathbb{Z}/MN$ s'écrit $n = (xN + yM) \bmod MN$, avec $0 \leq x \leq M-1$ et $0 \leq y \leq N-1$. On a donc

$$c_n = a_n + b_n = a_{(xN)} + b_{(yM)}$$

et cela montre que l'application $n \mapsto c_n$ de $\mathbb{Z}/MN \to \{0,1\}$ se décompose suivant $\mathbb{Z}/M$ et $\mathbb{Z}/N$. On applique alors le lemme 6.5.

11.7. Vecteur densité. Soit $f(z) = a_0 + a_1 z + a_2 z^2 + \ldots \in \mathbb{R}[[z]]$ une série formelle de période M à coefficients 0 ou 1. Soit $\nu \geq 1$ un entier. On pose $d = \operatorname{pgcd}(M, \nu)$, $M = dm$. Pour chaque j, $0 \leq j \leq \nu - 1$, la série

$$f_j(z) = \sum_{n=0}^{\infty} a_{j+n\nu} z^n$$

est périodique de période $m = M/d$. Pour f et ν donnés, on définit le vecteur densité :

$$\overrightarrow{\Delta}_\nu(f) = (\Delta_0, \Delta_1, \ldots, \Delta_{\nu-1}), \quad \text{avec } \Delta_j = \delta(f_j) = \frac{1}{\widehat{m}} \sum_{n=0}^{\widehat{m}-1} a_{j+n\nu}, \tag{49}$$

où $\widehat{m}$ est un multiple quelconque de m. Nous allons donner ci-dessous quelques règles pour calculer $\overrightarrow{\Delta}_\nu(f)$.

a) On a

$$\overrightarrow{\Delta}_M(f) = (a_0, a_1, \ldots, a_{M-1}).$$

b) *Réduction.* On conserve les notations de (49) ; soit ν' un diviseur de ν et $s = \nu/\nu'$. Alors on a

$$\overrightarrow{\Delta}_{\nu'}(f) = (\Delta'_0, \Delta'_1, \ldots, \Delta'_{\nu'-1}), \quad \text{avec } \Delta'_j = \frac{1}{s} \sum_{n=0}^{s-1} \Delta_{j+n\nu'}.$$

En appliquant (49) avec $\widehat{m} = sM$, il vient

$$\begin{aligned} \Delta'_j &= \frac{1}{sM} \sum_{i=0}^{sM-1} a_{j+i\nu'} = \frac{1}{s} \sum_{n=0}^{s-1} \left(\frac{1}{M} \sum_{\ell=0}^{M-1} a_{j+(n+s\ell)\nu'} \right) \\ &= \frac{1}{s} \sum_{n=0}^{s-1} \left(\frac{1}{M} \sum_{\ell=0}^{M-1} a_{(j+n\nu')+\ell\nu} \right) = \frac{1}{s} \sum_{n=0}^{s-1} \Delta_{j+n\nu'}. \end{aligned}$$

Cas particulier : $\nu' = 1$. On obtient par (47)

$$\delta(f) = \overrightarrow{\Delta}_1(f) = \frac{1}{\nu} \sum_{n=0}^{\nu-1} \Delta_n. \tag{50}$$

c) *Extension.* On conserve les notations de (49), mais cette fois, $\nu' = s\nu$ est un multiple de ν. On pose $d = \operatorname{pgcd}(M, \nu)$, $M = dm$, et l'on suppose que s est premier avec $m = M/d$. Alors on a

$$\overrightarrow{\Delta}_{s\nu}(f) = \Big(\underbrace{\Delta_0, \Delta_1, \ldots, \Delta_{\nu-1}}, \underbrace{\Delta_0, \Delta_1, \ldots, \Delta_{\nu-1}}, \ \cdots, \ \underbrace{\Delta_0, \Delta_1, \ldots, \Delta_{\nu-1}}_{s \text{ fois}} \Big).$$

Posons $\overrightarrow{\Delta}_{s\nu}(f) = (\Delta'_0, \Delta'_1, \ldots, \Delta'_{\nu'-1})$. Par (49) (avec $\widehat{m} = m$), on a, pour j vérifiant $0 \leq j \leq \nu' - 1$:

$$\Delta'_j = \frac{1}{m} \left(a_j + a_{j+s\nu} + a_{j+2s\nu} + \ldots + a_{j+(m-1)s\nu} \right).$$

Dans $\mathbb{Z}/M$, le sous-groupe cyclique engendré par ν est d'ordre $m = M/d$, et, comme $(s, m) = 1$, ce sous-groupe est aussi engendré par $s\nu$. Donc,

$$\Delta'_j = \frac{1}{m} \left(a_j + a_{j+\nu} + a_{j+2\nu} + \ldots + a_{j+(m-1)\nu} \right) = \Delta_{j \bmod \nu}.$$

d) *Redimensionnement.* On suppose que l'on connaît $\overrightarrow{\Delta}_\nu(f)$. Soit $\nu' \geq 1$ un autre entier. Alors, si

$$d' = (\nu', M) \quad \text{divise} \quad \nu, \tag{51}$$

on peut calculer $\overrightarrow{\Delta}_{\nu'}(f)$.
En effet, comme $d' \mid \nu$, on calcule $\overrightarrow{\Delta}_{d'}(f)$ par réduction. Ensuite, $\nu' = d's$, $M = d'm'$ avec $(s, m') = (s, M/d') = 1$, et l'on calcule $\overrightarrow{\Delta}_{\nu'}(f)$ à partir de $\overrightarrow{\Delta}_{d'}(f)$ par extension.
e) *Composition.* Si $\overrightarrow{\Delta}_\nu = (\Delta_0, \Delta_1, \ldots, \Delta_{\nu-1})$ et $\overrightarrow{\Delta}'_\nu = (\Delta'_0, \Delta'_1, \ldots, \Delta'_{\nu-1})$ sont deux vecteurs densité de même longueur, on les composera par la loi suivante :

$$\overrightarrow{\Delta}''_\nu = \overrightarrow{\Delta}_\nu * \overrightarrow{\Delta}'_\nu = (\Delta''_0, \Delta''_1, \ldots, \Delta''_{\nu-1})$$

avec, pour tout j, $0 \leq j \leq \nu - 1$,

$$\Delta''_j = \Delta_j * \Delta'_j = \Delta_j + \Delta'_j - 2\Delta_j\Delta'_j.$$

Cette définition trouvera son sens dans le paragraphe suivant.

11.8. Proposition. *Soit $f, g \in k[[z]]$ deux séries formelles périodiques de périodes respectives M et N. On pose $D = (M, N)$. Alors, la série $f + g$ a pour période $\dfrac{MN}{D}$ et l'on a, pour tout ν multiple de D,*

$$\overrightarrow{\Delta}_\nu(f + g) = \overrightarrow{\Delta}_\nu(f) * \overrightarrow{\Delta}_\nu(g)$$

où la composition $*$ est définie en 11.7 e).

Soit j vérifiant $0 \le j \le \nu - 1$. Avec les notations de 11.6, la série $f_j(z) = \sum_{n\ge 0} a_{j+n\nu} z^n$ est périodique de période M/D (puisque $D \mid \nu$) et, de même, $g_j(z) = \sum_{n\ge 0} b_{j+n\nu} z^n$ a pour période N/D. Comme M/D et N/D sont premiers entre eux, la proposition 11.6 (i) donne :

$$\delta(f_j + g_j) = \delta(f_j) * \delta(g_j).$$

11.9. L'algorithme d'addition. Soit $f, g \in k[[z]]$ deux séries formelles périodiques de périodes respectives M et N, et $D = (M, N)$. Soit m_1 et m_2 deux entiers positifs non nuls. On suppose que l'on connait $\overrightarrow{\Delta}_{m_1}(f)$ et $\overrightarrow{\Delta}_{m_2}(g)$. Soit $m \ge 1$ un entier. Alors, si les conditions suivantes sont remplies

$$\begin{array}{ll} (i) & (m, M) \text{ divise } m_1\,; \\ (ii) & (m, N) \text{ divise } m_2\,; \\ (iii) & D \text{ divise } m \end{array} \qquad (52)$$

on peut calculer $\overrightarrow{\Delta}_m(f+g)$ de la façon suivante : on calcule $\overrightarrow{\Delta}_m(f)$ par redimensionnement, car la condition (51) est satisfaite par (52, (i)). Il en est de même pour $\overrightarrow{\Delta}_m(g)$ en raison de (52, (ii)). Enfin, on évalue $\overrightarrow{\Delta}_m(f+g) = \overrightarrow{\Delta}_m(f) * \overrightarrow{\Delta}_m(g)$ par la proposition 11.8.

11.10. L'algorithme r/2. Pour les petites valeurs de r, on peut calculer les coefficients de $f(z) = 1/F_r(z)$ jusqu'à l'indice $\omega_r - 1$, calculer $\delta(f)$ par (47) et, par (48), on a $d(r) = \delta(f)$. Mais ω_r grandit très vite avec r, et la méthode est inutilisable pour $r > 18$.
Une méthode plus efficace consiste à utiliser les nombres premiers de l'intervalle $]r/2, r]$, comme nous l'avons fait de façon théorique au chapitre 8. Pour chacun de ces nombres premiers p, on calcule la fonction f_p (cf. 11.3 et 11.4), de période p. Ensuite on calcule par différence la fraction rationnelle

$$f' = f - \sum_{r/2<p\le r} f_p$$

dont la période est $\omega'_r = \dfrac{\omega_r}{\prod_{r/2<p\le r} p}$. Puis, on évalue $\delta(f')$ en calculant ses coefficients jusqu'à l'indice $\omega'_r - 1$. Enfin, pour calculer $d(r) = \delta(f) = \delta\left(f' + \sum_{r/2<p\le r} f_p\right)$, on applique la proposition 11.6, car les périodes de f' et des f_p sont premières entre elles deux à deux. Pour $r \ge 27$, $\omega'_r \ge 86486400$, et cette méthode n'est plus utilisable.

11.11. Introduisons quelques définitions et notations. Nous désignerons par $P^+(n)$ le plus grand facteur premier de l'entier n. Nous noterons p^+ (resp. p^-) le nombre premier suivant (resp. précédant) p. Enfin, pour x, y réels positifs, on définit

$$L(x,y) = \prod_{3\le p\le x} p^{w_p(y)}, \quad \text{avec} \quad w_p(y) = \left\lfloor \frac{\log y}{\log p} \right\rfloor. \qquad (53)$$

Remarquons que l'on a $p^{w_p(y)} \le y < p^{w_p(y)+1}$ et que $L(x,y)$ est le ppcm des nombres impairs $t \le y$ tels que $P^+(t) \le x$.
Pour chaque t impair satisfaisant $1 \le t \le r$, on calcule la fonction f_t décrite en 11.3. Ensuite, on détermine pour p premier, $3 \le p \le r$,

$$f'_p = \sum_{\substack{1\le t \text{ impair} \le r \\ P^+(t)=p}} f_t \qquad (54)$$

qui est, d'après (45), périodique de période

$$N_p = 2^{a(\lfloor r/p \rfloor)} \operatorname{ppcm}_{\substack{1\le t \text{ impair} \le r \\ P^+(t)=p}} t = 2^{a(\lfloor r/p \rfloor)} p L\left(p, \frac{r}{p}\right) \qquad (55)$$

et donc s'écrit

$$f'_p(z) = \frac{E'_p(z)}{1 + z^{N_p}}. \qquad (56)$$

Les polynômes E'_p se calculent facilement à partir des polynômes E_t (cf. (45)). De (44) et (54), il suit

$$f := f_1 + \sum_{3\le p\le r} f'_p. \qquad (57)$$

Nous noterons

$$S_p = f_1 + \sum_{3\le q \text{ premier} \le p} f'_q \qquad (58)$$

et nous appellerons M_p la période de S_{p^-} ; (55) entraîne

$$M_p = \operatorname{ppcm}\left(2^{a(r)}, N_3, N_5, \ldots, N_{p^-}\right) = 2^{a(r)} L(p^-, r). \qquad (59)$$

On pose ensuite

$$D_p = (M_p, N_p) = 2^{a(\lfloor r/p \rfloor)} L\left(p^-, \frac{r}{p}\right) \qquad \text{(d'après (59) et (55))} \qquad (60)$$

et

$$\nu_p = 2^{a(\lfloor r/p \rfloor)} L\left(p^-, \frac{r}{p}\right) p^{\left(\left\lfloor \frac{\log r/p^+}{\log p} \right\rfloor\right)}. \qquad (61)$$

Le choix de ν_p lui assure les trois propriétés suivantes :

$$\begin{array}{ll} (i) & \nu_p \text{ est un multiple de } D_p\,; \\ (ii) & \nu_p \text{ est un diviseur de } N_p\,; \\ (iii) & (M_p, \nu_p) \text{ divise } \nu_{p^-} \text{ pour tout } p \ge 5. \end{array} \qquad (62)$$

Les conditions (i) et (ii) résultent de (61), (60) et (55). Par (59) et (61), on a

$$(M_p, \nu_p) = 2^{a(\lfloor r/p \rfloor)} L\left(p^-, \frac{r}{p}\right) = 2^{a(\lfloor r/p \rfloor)} L\left(p^{--}, \frac{r}{p}\right) (p^-)^{\left(\lfloor \frac{\log r/p}{\log p^-} \rfloor\right)},$$

$$\nu_{p^-} = 2^{a(\lfloor r/p^- \rfloor)} L\left(p^{--}, \frac{r}{p^-}\right) (p^-)^{\left(\lfloor \frac{\log r/p}{\log p^-} \rfloor\right)}$$

et la croissance des fonctions $y \mapsto a(y)$ et $y \mapsto L(x,y)$ démontre (iii).

11.12. L'algorithme "tous p". On conserve les notations de 11.9 et 11.11. On applique l'algorithme d'addition 11.9 à la somme $S_3 = f_1 + f_3'$ afin de calculer $\overrightarrow{\Delta}_{\nu_3}(S_3)$. On pose $m = \nu_3$, $m_1 = M = 2^{a(r)}$ (qui est la période de f_1), $m_2 = N_3$ (qui est la période de f_3') et les conditions (52, (i)) et (52, (ii)) sont satisfaites. On a $D = (m_1, m_2) = D_3$, et la condition (52, (iii)) résulte de (62, (i)). On détermine $\overrightarrow{\Delta}_{m_1}(f_1) = \overrightarrow{\Delta}_M(f_1)$ par 11.7 a) où les coefficients a_i sont ceux du polynôme E_1 (cf. 11.3 et 11.4). On calcule $\overrightarrow{\Delta}_{m_2}(f_3') = \overrightarrow{\Delta}_{N_3}(f_3')$ par 11.7 a) où, cette fois, les coefficients a_i sont ceux du polynôme E_3' défini en (56). L'algorithme d'addition 11.9 nous permet alors d'évaluer $\overrightarrow{\Delta}_m(S_3) = \overrightarrow{\Delta}_{\nu_3}(S_3)$. Ensuite, pour chaque nombre premier $p \geq 5$, on applique l'algorithme d'addition 11.9 à $S_p = S_{p^-} + f_p'$ avec $M = M_p$, $m_1 = \nu_{p^-}$, $N = N_p$, $m_2 = N = N_p$ et $m = \nu_p$. La condition (52, (i)) résulte de (62, (iii)) ; (52, (ii)) est évidente et (52, (iii)) résulte de (62, (i)). Par récurrence, on connaît le vecteur densité $\overrightarrow{\Delta}_{m_1}(S_{p^-}) = \overrightarrow{\Delta}_{\nu_{p^-}}(S_{p^-})$. Comme pour $p = 3$, on calcule $\overrightarrow{\Delta}_{m_2}(f_p') = \overrightarrow{\Delta}_{N_p}(f_p')$ par 11.7 a) où les coefficients a_i sont ceux du polynôme E_p' défini en (56). L'algorithme d'addition 11.9 nous permet alors d'évaluer $\overrightarrow{\Delta}_m(S_p) = \overrightarrow{\Delta}_{\nu_p}(S_p)$. Lorsque p est le plus grand nombre premier inférieur ou égal à r, par (57) et (58), on a $f = S_p$, et en utilisant (50), on obtient $\delta(f)$ par réduction de $\overrightarrow{\Delta}_{\nu_p}(S_p)$. En fait, il n'y a rien à réduire, car, d'après le postulat de Bertrand, il y a toujours un nombre premier impair q vérifiant $r/2 < q \leq r$ pour $r \geq 3$; et pour un tel nombre q, (61) donne $\nu_q = 1$. On a donc, pour $r \geq 3$, $\nu_p = 1$. Finalement, $d(r) = \delta(f)$ par (48).

11.13. La partie la plus longue de l'algorithme 11.12 est le calcul de f_p' défini par (54). On peut éviter ce calcul en évaluant directement $\overrightarrow{\Delta}_{\nu_p}(f_p')$.
On commence par écrire $f_p' = f_p'' + f_p'''$ en séparant, dans (54), les termes f_t suivant que p^2 divise t ou pas. Les période respectives de f_p'' et f_p''' sont

$$N_p'' = 2^{a(\lfloor r/p^2 \rfloor)} p^2 L(p, r/p^2) \quad \text{et} \quad N_p''' = 2^{a(\lfloor r/p \rfloor)} p L(p^-, r/p).$$

Puis, on se propose d'évaluer $\overrightarrow{\Delta}_{N_p'''}(f_p''')$ et $\overrightarrow{\Delta}_{N_p''}(f_p'')$.
Pour calculer $\overrightarrow{\Delta}_{N_p'''}(f_p''')$, on ordonne les t impairs, $t \leq r$, qui sont multiples de p et qui satisfont $P^+(t/p) < p$, en une suite $p, v_1 p, v_2 p, \ldots, v_s p$ avec $P^+(v_i) \leq P^+(v_{i+1})$, et $v_i < v_{i+1}$ lorsque $P^+(v_i) = P^+(v_{i+1})$. D'après la définition de f_p''', on a

$$f_p''' = f_p + \sum_{i=1}^{s} f_{v_i p}.$$

Pour $1 \leq j \leq s$, on pose

$$\Sigma_j = f_p + \sum_{i=1}^{j} f_{v_i p}$$

et l'on calcule, à l'aide de 11.9, $\overrightarrow{\Delta}_{\nu_j'}(\Sigma_j)$ avec

$$\nu_j' = 2^{a(\lfloor r/p \rfloor)} p L(q, r/p) \qquad \text{et} \qquad q = P^+(v_j).$$

Pour calculer $\overrightarrow{\Delta}_{N_p''}(f_p'')$, on ordonne les t impairs, $t \leq r$, qui sont multiples de p^2 et qui satisfont $P^+(t/p^2) \leq p$ en une suite $p^2, w_1 p^2, w_2 p^2, \ldots, w_{s'} p^2$ avec $P^+(w_i) \leq P^+(w_{i+1})$, et $w_i < w_{i+1}$ lorsque $P^+(w_i) = P^+(w_{i+1})$. D'après la définition de f_p'', on a

$$f_p'' = f_{p^2} + \sum_{i=1}^{s'} f_{w_i p^2}.$$

Pour $1 \leq j \leq s'$, on pose

$$\Sigma_j' = f_{p^2} + \sum_{i=1}^{j} f_{w_i p^2}$$

et l'on calcule $\overrightarrow{\Delta}_{\nu_j''}(\Sigma_j')$ avec

$$\nu_j'' = 2^{a(\lfloor r/p^2 \rfloor)} p^2 L(q, r/p^2) \qquad \text{et} \qquad q = P^+(w_j).$$

Enfin, en observant que $\nu_s' = N_p'''$ et que $\nu_{s'}'' = N_p''$ (noter pour cela que pour $x \geq y$, on a $L(x,y) = L(y,y)$) on calcule $\overrightarrow{\Delta}_{\overline{\nu}_p}(f_p')$ à partir de $\overrightarrow{\Delta}_{N_p''}(f_p'')$ et de $\overrightarrow{\Delta}_{N_p'''}(f_p''')$ avec $\overline{\nu}_p = \text{pgcd}(N_p'', N_p''') = \text{ppcm}(p, \nu_p)$, et donc, par réduction, on en déduit $\overrightarrow{\Delta}_{\nu_p}(f_p')$.
On pourra vérifier (comme on l'avait fait en 11.12 pour ν_p) que les valeurs choisies pour ν_j', ν_j'' et $\overline{\nu}_p$ impliquent, pour chaque application de l'algorithme d'addition 11.9, que les conditions (52) sont satisfaites. En fait, cette vérification théorique n'est pas indispensable, car elle est faite dans l'implémentation et un message d'erreur est affiché si l'une des trois conditions (52) n'est pas vérifiée.

11.14. L'algorithme 11.12–11.13 consiste d'abord à trouver pour la somme (44) (qui comporte $\lfloor \frac{r+1}{2} \rfloor$ termes) une permutation de ses termes suivie d'un parenthésage. Ensuite, pour chacune des $\lfloor \frac{r-1}{2} \rfloor$ additions partielles $g_1 + g_2$, il faut choisir le nombre ν pour lequel on veut déterminer le vecteur densité $\overrightarrow{\Delta}_\nu(g_1 + g_2)$. Ce choix doit respecter les conditions (52).
Ainsi, par exemple, pour $r = 27$, L'algorithme 11.12–11.13 range les termes f_t de la somme (44) dans l'ordre suivant des valeurs de t : $1, 3, 9, 27, 5, 15, 25, 7, 21, 11, 13, 17, 19, 23$. Le début du parenthésage est

$$\Big(\big(1, (3, (9, 27))\big), ((5, 15), 25)\Big), \ldots$$

Puis, l'algorithme calcule successivement

$$\overrightarrow{\Delta}_{108}(f_9+f_{27}),\quad \overrightarrow{\Delta}_{96}(f_3+(f_9+f_{27})),\quad \overrightarrow{\Delta}_{96}\Big(f_1+(f_3+(f_9+f_{27}))\Big),$$

$$\overrightarrow{\Delta}_{240}(f_5+f_{15}),\quad \overrightarrow{\Delta}_{240}((f_5+f_{15})+f_{25}),$$

$$\overrightarrow{\Delta}_{48}\Big(\Big(f_1+(f_3+(f_9+f_{27}))\Big)+((f_5+f_{15})+f_{25})\Big),\dots$$

Le choix de la dimension des différents vecteurs densité (ν_p, ν'_j, ν''_j et $\overline{\nu}_p$) est, en principe, optimal (relativement à leur maximum) pour l'ordre des opérations que nous proposons et qui est rappelé ci-dessus dans l'exemple $r = 27$. Nous ne savons pas montrer qu'il est aussi optimal quels que soient la permutation et le parenthésage utilisés

11.15. L'algorithme 11.12–11.13 a été programmé en MAPLE, et il a permis le calcul de $d(r)$ jusqu'a $r = 220$[3]. Nous remercions vivement B. Salvy pour plusieurs remarques qui ont considérablement diminué le temps d'exécution. Pour $200 \le r \le 220$, le calcul de chaque valeur de $d(r)$ prend environ une demi-heure et la taille maximum des vecteurs densité utilisés est 2882880. Le nombre $r = 221 = 13 \times 17$ semble une barrière, car on doit déterminer $\overrightarrow{\Delta}_{N''_{17}}(f''_{17})$ avec $N''_{17} = 32\times9\times5\times7\times11\times13\times17 = 24504480$. Pour illustrer concrètement la remarque finale de 11.14, est-il possible de calculer $d(221)$ en utilisant uniquement des vecteurs densité de dimension inférieure à 20 millions ?

[3]On peut consulter la table de $d(r)$ sur le site http ://euler.univ-lyon1.fr/home/nicolas

TABLE 1[4]

r	$c(r)$	ω_r	$1/2 - d(r)$	$0.5 - d(r)$
1	1	1	$-1/2$	-0.5
2	3	4	0	0
3	4	12	1/12	0.083
4	8	24	1/24	0.042
5	9	240	0	0
6	11	240	1/60	0.017
7	12	1680	5/56	0.089
8	20	3360	0	0
9	21	10080	1/56	0.018
10	23	10080	0	0
11	24	110880	1/616	$(1.6)10^{-3}$
12	28	110880	1/660	$(1.5)10^{-3}$
13	29	1441440	$-5/1092$	$-(4.6)10^{-3}$
14	31	1441440	$-1/80080$	$-(1.2)10^{-5}$
15	32	1441440	133/68640	$(1.9)10^{-3}$
16	48	2882880	63/22880	$(2.8)10^{-3}$
17	49	49008960	5/272272	$(1.8)10^{-5}$
18	51	49008960	3/1361360	$(2.2)10^{-6}$
19	52	931170240	27/55328	$(4.9)10^{-4}$
20	56	931170240	89/13302432	$(6.7)10^{-6}$
21	57	931170240	$-9/146965$	$-(6.1)10^{-5}$
22	59	931170240	$-1/23279256$	$-(4.3)10^{-8}$
23	60	21416915520	$-945/8498776$	$-(1.1)10^{-4}$
24	68	42833831040	27/3979360	$(6.8)10^{-6}$
25	69	214169155200	11/489440	$(2.2)10^{-5}$
26	71	214169155200	0	0
27	72	642507465600	5917/1189828640	$(5.0)10^{-6}$
28	76	642507465600	$-1/1999712$	$-(5.0)10^{-7}$
29	77	18632716502400	$-9/3450503056$	$-(2.6)10^{-9}$
30	79	18632716502400	$-7/1478787024$	$-(4.7)10^{-9}$
31	80	577614211574400	$-63/32932757$	$-(1.9)10^{-6}$
32	112	577614211574400	83/148106208096	$(5.6)10^{-10}$

[4]$c(r)$ et ω_r sont définis au chapitre 2. L'algorithme de calcul de $d(r)$ est expliqué au chapitre 11.

TABLE 2

$r =$	ω_r	facteurs premiers de ω_r
1	1 =	
2	4 =	2^2
3	12 =	$2^2\ 3$
4	24 =	$2^3\ 3$
5, 6	240 =	$2^4\ 3\ 5$
7	1680 =	$2^4\ 3\ 5\ 7$
8	3360 =	$2^5\ 3\ 5\ 7$
9, 10	10080 =	$2^5\ 3^2\ 5\ 7$
11, 12	110880 =	$2^5\ 3^2\ 5\ 7\ 11$
13 à 15	1441440 =	$2^5\ 3^2\ 5\ 7\ 11\ 13$
16	2882880 =	$2^6\ 3^2\ 5\ 7\ 11\ 13$
17, 18	49008960 =	$2^6\ 3^2\ 5\ 7\ 11\ 13\ 17$
19 à 22	931170240 =	$2^6\ 3^2\ 5\ 7\ 11\ 13\ 17\ 19$
23	21416915520 =	$2^6\ 3^2\ 5\ 7\ 11\ 13\ 17\ 19\ 23$
24	42833831040 =	$2^7\ 3^2\ 5\ 7\ 11\ 13\ 17\ 19\ 23$
25, 26	214169155200 =	$2^7\ 3^2\ 5^2\ 7\ 11\ 13\ 17\ 19\ 23$
27, 28	642507465600 =	$2^7\ 3^3\ 5^2\ 7\ 11\ 13\ 17\ 19\ 23$
29, 30	18632716502400 =	$2^7\ 3^3\ 5^2\ 7\ 11\ 13\ 17\ 19\ 23\ 29$
31, 32	577614211574400 =	$2^7\ 3^3\ 5^2\ 7\ 11\ 13\ 17\ 19\ 23\ 29\ 31$

TABLE 3 : Majoration de $|0.5 - d(r)|$ (cf. 9.3)

$r =$	993	994	995	996	997
$\lvert 0.5 - d(r)\rvert \leq$	$(2.7)10^{-104}$	$(1.5)10^{-111}$	$(3.9)10^{-109}$	$(2.5)10^{-106}$	$(1.2)10^{-112}$
$r =$	998	999	1000	1001	1002
$\lvert 0.5 - d(r)\rvert \leq$	$(1.7)10^{-108}$	$(7.9)10^{-104}$	$(1.5)10^{-106}$	$(1.5)10^{-108}$	$(3.9)10^{-107}$

Références

[1] R.C. Baker and G. Harman, The difference between consecutive primes, Proc. London Math. Soc. **72**, 1996), 261-280.

[2] N. Bourbaki, Algèbre, chap. 4 à 7, Masson, Paris, 1981.

[3] N. Bourbaki, Intégration, chap. 1 à 4, Hermann, Paris, 1965.

[4] H. Gupta, C.E. Gwyther and J.C.P. Miller, Table of partitions, Cambridge University Press, 1962.

[5] G.H. Hardy and E.M. Wright, An Introduction to the Theory of Numbers, 5th edition, Oxford, at the Clarendon Press, 1979.

[6] L.H. Loomis, An introduction to abstract harmonic analysis, Van Nostrand, Totonto, 1953.

[7] P.A. MacMahon, Note on the parity of the number which enumerates the partitions of a number, Proc. Cambridge, Philos. Soc., **20**, 1920–1921, 281-283.

[8] J.-L. Nicolas, I.Z. Ruzsa and A. Sárközy, On the parity of additive representation functions, appendice de J.-P. Serre, J. Number Theory, **73**, 1998, 292-317.

[9] T.R. Parkin and D. Shanks, On the distribution of parity in the partition function, Math. Comp., **21**, 1967, 466-480.

[10] K. Ono, Parity of the partition function in arithmetic progressions, J. Reine Angew. Math. **472** (1996), 1-15.

[11] K. Ono, Distribution of the partition function modulo m, Ann. of Math. **151** (2000), 293-307.

Jacques Dixmier
11 bis rue du Val de Grâce
F-75005 Paris, France

Jean-Louis Nicolas
Institut Girard Desargues, UMR 5028,
Bâtiment Doyen Jean Braconnier,
Université Claude Bernard (Lyon 1),
21 Avenue Claude Bernard,
F-69622 Villeurbanne, France
e-mail : jlnicola@in2p3.fr