ACTA ARITHMETICA
137.1 (2009)

Palindromes dans les progressions arithmétiques

par

Sylvain Col (Nancy)

La recherche sur les palindromes a commencé il y a plus de vingt siècles : les auteurs grecs et latins se divertissaient déjà en composant des phrases palindromiques. Le plus célèbre exemple est très certainement :

νιψον ανομηματα μη μοναν οψιν
(lave tes péchés et non seulement ton visage),

maxime qui orne les fonts baptismaux grecs ainsi que de nombreuses églises de Cambridge jusqu'à Constantinople. Dans toutes les langues et tous les alphabets des auteurs ont joué avec cette contrainte. En anglais, le palindrome

A man, a plan, a canal : Panama.

est tout aussi connu. Des auteurs comme G. Perec ont composé des textes et poèmes palindromiques. Le lecteur intéressé en trouvera plusieurs sur le site *http://www.fatrazie.com*. Et maintenant,

Engage le jeu, que je le gagne !

1. Énoncé des résultats. Dans toute cette partie, $g \geq 2$ est un entier fixé : c'est la base utilisée pour écrire les nombres. Nous notons $\|x\|$ la distance de x aux entiers. Si $\mathscr{A}$ est un ensemble de nombres, nous notons $\mathscr{A}^* := \mathscr{A} \setminus \{0\}$ les éléments non nuls de $\mathscr{A}$. Sauf mention explicite du contraire, toutes les constantes $c_1, c_2, \ldots$ et les constantes implicites de Vinogradov peuvent dépendre de g. Nous désignons par $\log_k x$ la $k^{\text{ème}}$ composée du logarithme,

$$\log_k x := \log(\log_{k-1} x) \quad \text{et} \quad \log_1 x := \log x.$$

Nous appelons *écriture de n dans la base g* l'unique suite presque nulle $(n_j)_j$ d'entiers $0 \leq n_j \leq g-1$ telle que n s'écrit

$$n = \sum_j n_j g^j.$$

2000 *Mathematics Subject Classification*: 11A63, 11K36, 11L07, 11N36.
Key words and phrases: palindrome.

DOI: 10.4064/aa137-1-1

Nous disons que n *possède* N *chiffres en base* g si $N-1$ est le plus grand indice j pour lequel $n_j \neq 0$. Nous notons $\mathscr{P}_N$ les palindromes ayant exactement N chiffres en base g : ce sont les entiers de N chiffres dont l'écriture en base g possède la symétrie par rapport à $(N-1)/2$, i.e.

$$n \in \mathscr{P}_N \;\Leftrightarrow\; n = \sum_{j<N} n_j g^j,\ n_{N-1} \neq 0 \text{ et } n_j = n_{N-1-j}.$$

Nous désignons respectivement par $\mathscr{P}^0$ et $\mathscr{P}^1$ les palindromes ayant un nombre respectivement pair et impair de chiffres et par $\mathscr{P}$ l'ensemble de tous les palindromes, de sorte que

$$\mathscr{P} = \mathscr{P}^0 \sqcup \mathscr{P}^1 \quad \text{avec} \quad \mathscr{P}^\delta = \bigsqcup_{M\geq 0} \mathscr{P}_{2M+\delta}, \tag{1.1}$$

toutes ces unions étant disjointes (nous avons convenu que 0 est l'unique palindrome de 0 chiffre).

Pour des raisons techniques, il est souvent plus simple de ne pas avoir la condition $n_{N-1} \neq 0$. Nous dirons alors que l'entier n est un *pseudopalindrome de taille* N si n possède au plus N chiffres et si son écriture en base g possède la symétrie par rapport à $(N-1)/2$. Nous notons $\mathscr{Q}_N$ l'ensemble des pseudopalindromes de taille N, i.e.

$$n \in \mathscr{Q}_N \;\Leftrightarrow\; n = \sum_{j<N} n_j g^j,\ n_j = n_{N-1-j}.$$

Comme pour les palindromes, nous notons respectivement $\mathscr{Q}$, $\mathscr{Q}^0$ et $\mathscr{Q}^1$ la famille des pseudopalindromes de toute taille, de taille paire et de taille impaire. Remarquons que 0 est un pseudopalindrome de toute taille (car son écriture possède toutes les symétries) et qu'un palindrome différent de 0 est exactement un pseudopalindrome ne se terminant pas par 0 :

$$\mathscr{Q}^* = \bigsqcup_{N\geq 0} g^N \mathscr{P}^* \quad \text{et} \quad \mathscr{P}^* = \mathscr{Q} \setminus g\mathscr{Q}.$$

Il est donc aisé d'obtenir des résultats sur les palindromes à partir de résultats sur les pseudopalindromes et réciproquement.

Nous notons

$$\Phi_N(k) := g^{N-k} + g^k, \tag{1.2}$$

ce qui permet d'écrire

$$n \in \mathscr{Q}_{2M} \;\Leftrightarrow\; n = \sum_{j<M} n_j \Phi_{2M-1}(j), \qquad 0 \leq n_j < g,$$

$$n \in \mathscr{Q}_{2M+1} \;\Leftrightarrow\; n = \sum_{j<M} n_j \Phi_{2M}(j) + n_M g^M,\ 0 \leq n_j < g.$$

Enfin, pour tout ensemble d'entiers $\mathscr{A}$, nous posons

$$\mathscr{A}(x) := \{n \in \mathscr{A} : n < x\},$$
$$\mathscr{A}(x,a,q) := \{n \in \mathscr{A}(x) : n \equiv a \bmod q\}.$$

Le but de cet article est d'évaluer le cardinal de $\mathscr{P}(x,a,q)$. Nous l'estimons uniformément dans le théorème 1 et en moyenne dans le théorème 2 par rapport à q. À notre connaissance, il existe actuellement un seul résultat de ce type dans la littérature : le corollaire 4.5 de W. D. Banks, D. N. Hart et M. Sakata [BHS04] donne la majoration suivante :

THÉORÈME A. *Il existe une constante $c > 0$ ne dépendant que de g telle qu'uniformément pour les entiers q premiers avec $g^3 - g$ et $x > 0$, nous avons la majoration*

$$\max_{a\in\mathbb{Z}} \left| \#\mathscr{P}(x,a,q) - \frac{\#\mathscr{P}(x)}{q} \right| \ll_g \#\mathscr{P}(x) q \exp\left(-\frac{c\log x}{q^2}\right).$$

Si $(q, g^3-g) = 1$ et si q n'est pas trop grand, i.e. essentiellement pour

$$q < \left(\frac{c\log x}{\log_2 x}\right)^{1/2} \quad \text{et} \quad (q, g^3-g) = 1, \tag{1.3}$$

le théorème A fournit un équivalent du cardinal de $\mathscr{P}(x,a,q)$. Sous la condition (1.3), les palindromes inférieurs à x sont uniformément distribués dans les progressions arithmétiques de module q. Le théorème A impose cependant de choisir q beaucoup trop petit pour avoir des applications arithmétiques de bonne qualité. Dans le théorème suivant, nous prolongeons le domaine de validité de q :

THÉORÈME 1. *Il existe des constantes $c, \widetilde{c} > 0$ ne dépendant que de g telles qu'uniformément pour les entiers q vérifiant*

$$q \le \exp\left(\frac{c\log x}{\log_2 x}\right) \quad \textit{et} \quad (q, g^3-g) = 1, \tag{1.4}$$

nous avons la majoration

$$\max_{a\in\mathbb{Z}} \left| \#\mathscr{P}(x,a,q) - \frac{\#\mathscr{P}(x)}{q} \right| \ll_g \frac{\#\mathscr{P}(x)}{q} \exp\left(-\frac{\widetilde{c}\log x}{\log q}\right).$$

Il faut remarquer que notre démonstration ne reprend pas les idées de [BHS04] : leur démonstration utilise des outils plus élaborés puisqu'elle repose sur des majorations de sommes de Kloosterman. La notre présente l'avantage d'être élémentaire : les seules propriétés des pseudopalindromes que nous utiliserons réellement sont deux identités très simples :

$$g\Phi_{N-1}(k) = \Phi_{N+1}(k+1), \tag{1.5}$$
$$g\Phi_N(k+1) - \Phi_N(k) = (g^2-1)g^k. \tag{1.6}$$

L'identité (1.5) nous servira pour exprimer les moyennes de palindromes comme un produit, et l'identité (1.6) pour supprimer la symétrie qui caractérise les palindromes : le membre de gauche de (1.6) représente une combinaison linéaire de pseudopalindromes où le paramètre N est important, alors que le membre de droite représente simplement un entier divisible par g^2-1 où le paramètre N n'intervient plus ! Nous démontrerons dans le paragraphe 5.7 que cette identité (1.6) est optimale dans la mesure où toute autre identité permettant une telle simplification fait aussi intervenir un facteur g^2-1.

La technique développée ici s'adapte à l'étude de toute famille d'entiers définie par des propriétés simples de géométrie sur les chiffres en utilisant des identités analogues à (1.5) et (1.6). Par exemple, toute famille d'entiers obtenue par translation ou symétrie centrale ou symétrie axiale ou... de blocs de chiffres et concaténation de telles applications. De plus, la technique que nous mettons en œuvre est totalement compatible avec celle utilisée pour l'étude des nombres ellipséphiques (i.e. les entiers dont l'écriture n'utilise que certains chiffres). À ces familles d'entiers, nous pouvons donc imposer l'absence de certains chiffres dans leur écriture.

Le théorème 1 est l'analogue du théorème de Siegel–Walfisz concernant la répartition des nombres premiers dans les progressions arithmétiques. Il reste cependant insuffisant pour de nombreuses applications car il ne permet pas de choisir q de la taille d'une puissance de x. Nous démontrons alors l'analogue du théorème de Bombieri–Vinogradov pour la famille des palindromes : en moyenne, les palindromes restent bien distribués dans les progressions arithmétiques pour des diviseurs de l'ordre d'une certaine puissance de x.

THÉORÈME 2. *Il existe $\beta>0$ ne dépendant au plus que de g tel que pour tout A et $\varepsilon>0$, nous avons la majoration*

$$\sum_{\substack{q<x^{\beta-\varepsilon}\\(q,g^3-g)=1}} \sup_{y\le x}\max_{a\in\mathbb{Z}}\left|\#\mathscr{P}(y,a,q)-\frac{\#\mathscr{P}(y)}{q}\right| \ll_{g,A,\varepsilon} \frac{\#\mathscr{P}(x)}{\log^A x}. \tag{1.7}$$

Nous pouvons choisir l'exposant $\beta-\varepsilon=\beta_g$ avec $\varepsilon>0$ et

g	2	3	4	5	6	7	8	9	10
β_g	$\frac{1}{30}$	$\frac{1}{94}$	$\frac{1}{74}$	$\frac{1}{122}$	$\frac{1}{114}$	$\frac{1}{158}$	$\frac{1}{150}$	$\frac{1}{194}$	$\frac{1}{186}$

Si g est assez grand, nous pouvons prendre

$$\beta\sim\frac{1}{6\pi g}.$$

Un nombre $\beta>0$ vérifiant la propriété (1.7) pour tous les A et $\varepsilon>0$ est appelé un *exposant de répartition* pour la famille des palindromes.

Remarque 1. Les sommes d'exponentielles de pseudopalindromes sont des fonctions extrêmement oscillantes puisque

$$\Phi_N(j) = g^{N-j} + g^j$$

réunit ensemble les indices de très bas et de très haut degré. Pour éviter que les dérivées de ces fonctions ne soient trop importantes, nous sommes obligés d'utiliser une voie détournée : plutôt que d'étudier directement les moyennes d'exponentielles de pseudopalindromes, nous montrons dans le lemme 2 que nous pouvons supprimer le caractère symétrique en combinant astucieusement un indice avec son successeur à l'aide de l'identité (1.6). Cette simplification a évidemment un coût et c'est la raison pour laquelle les exposants β_g obtenus dans le théorème 2 sont petits par rapport à $1/2$.

En utilisant des techniques de crible, nous déduirons du théorème 2 le

Théorème 3. *Soient $\beta > 0$ un exposant de distribution pour les palindromes et $\varepsilon > 0$. Uniformément pour tous x et z assez grands, si $z < x^{\beta/2-\varepsilon}$, nous avons l'estimation*

$$\#\{n \in \mathscr{P}(x) : P^-(n) \geq z\} \asymp_{g,\varepsilon} \frac{\#\mathscr{P}(x)}{\log z}. \tag{1.8}$$

Remarque 2. Il peut paraître décevant d'obtenir un ordre de grandeur et non pas un équivalent du membre de gauche de (1.8), comme nous pourrions nous y attendre. Un équivalent du type du membre de droite est impossible, car tout palindrome possédant un nombre pair de chiffres est divisible par $g+1$. Ainsi, entre g^{2N-1} et g^{2N}, tous les palindromes ont un nombre pair de chiffres donc ne peuvent pas être premiers, et donc

$$\frac{\#\mathscr{P}(g^{2N-1})}{\log g^{2N-1}} = \frac{g^{N-1}(g-1)}{(2N-1)\log g} \not\asymp \frac{g^N(g-1)}{2N\log g} = \frac{\#\mathscr{P}(g^{2N})}{\log g^{2N}}.$$

Nous pourrions tout de même espérer une estimation ressemblant à

$$\#\{n \in \mathscr{P}(x) : P^-(n) \geq z\} \sim c_g \frac{\log x}{\log z} \frac{\#\mathscr{P}^1(x)}{\log z},$$

mais cela est encore impossible à cause des facteurs premiers de g. En particulier, la formule conjecturée par [BHS04] sur le nombre de palindromes premiers, à savoir l'existence d'une constante $c_g > 0$ telle que

$$\#\{n \in \mathscr{P}(x) : n \text{ premier}\} \sim c_g \frac{\#\mathscr{P}(x)}{\log x}$$

est clairement fausse (sauf si g est un nombre premier en remplaçant $\mathscr{P}$ par $\mathscr{P}^1$ dans le membre de droite).

Nous déduirons du théorème 3 deux applications. La première est une majoration du bon ordre de grandeur du nombre de palindromes premiers :

Corollaire 1. *Uniformément pour tout x, nous avons*

$$\#\{n \in \mathscr{P}(x) : n \text{ premier}\} \ll_g \frac{\#\mathscr{P}(x)}{\log x}.$$

La seconde est une minoration du bon ordre de grandeur à des puissances de $\log_2 x = \log\log x$ près, du nombre de palindromes presque premiers :

Corollaire 2. *Il existe une constante $k_g > 0$ ne dépendant que de g telle que*

$$\#\{n \in \mathscr{P}(x) : \Omega(n) \le k_g\} \gg_g \frac{\#\mathscr{P}(x)}{\log x}.$$

Par exemple, nous pouvons choisir $k_2 = 60$, $k_{10} = 372$ et si g est assez grand, $k_g \sim 24\pi g$.

2. Majoration d'une moyenne de pseudopalindromes. Nous posons

$$U(x) := \frac{1}{g}\sum_{d<g} \mathrm{e}(dx) \quad \text{et} \quad G_N(x) := \frac{1}{\#\mathscr{Q}_N}\sum_{n\in\mathscr{Q}_N} \mathrm{e}(nx), \tag{2.1}$$

où nous avons noté traditionnellement $\mathrm{e}(z) := e^{2i\pi z}$. Remarquons que $U(x)$ s'exprime aisément à l'aide de G_N puisque $U(x) = G_1(x)$. Le lemme suivant montre que $G_N(x)$ s'exprime également à partir de U.

Lemme 1. *Soient N un entier et $\delta = 0$ ou 1 de même parité que N. Pour tout x réel, nous avons*

$$G_N(x) = G_\delta(g^{(N-1)/2}x) \prod_{k<(N+1)/2} U(\Phi_{N-1}(k)x), \tag{2.2}$$

où $G_0(y) = 1$ et $G_1(y) = U(y)$ sont des fonctions bornées par 1.

Démonstration. Écrivons $N = 2M + \delta$ et montrons par récurrence sur M la factorisation

$$G_N(x) = G_\delta(g^M x) \prod_{k<M+1} U(\Phi_{N-1}(k)x), \tag{2.2$'$}$$

qui est équivalente à (2.2). Si $M = 0$, alors $G_N(x) = G_\delta(x) = G_\delta(g^M x)$ et le résultat est vrai. Supposons donc la factorisation vraie pour $M \ge 0$ et prouvons-la pour $M+1$. En isolant le premier chiffre, nous avons la partition

$$\mathscr{Q}_{N+2} = \bigsqcup_{n_0<g} (n_0\Phi_{N+1}(0) + g\mathscr{Q}_N).$$

Donc

$$G_{N+2}(x) = \frac{1}{\#\mathscr{Q}_{N+2}}\sum_{n\in\mathscr{Q}_{N+2}} \mathrm{e}(nx) = \frac{1}{g\#\mathscr{Q}_N}\sum_{n_0<g}\sum_{n\in\mathscr{Q}_N} \mathrm{e}((n_0\Phi_{N+1}(0)+gn)x),$$

ce qui s'écrit en utilisant la définition de U,

$$G_{N+2}(x) = U(\Phi_{N+1}(0)x)G_N(gx). \tag{2.3}$$

Si nous utilisons l'hypothèse de récurrence pour évaluer le membre de droite de (2.3), nous en déduisons

$$G_{N+2}(x) = U(\Phi_{N+1}(0)x)G_\delta(g^{M+1}x) \prod_{k<M+1} U(g\Phi_{N-1}(k)x).$$

En utilisant l'identité (1.5), nous trouvons finalement

$$G_{N+2}(x) = U(\Phi_{N+1}(0)x)G_\delta(g^{M+1}x) \prod_{0<k<M+2} U(\Phi_{N+1}(k)x),$$

ce qui est exactement la factorisation (2.2′) pour $M+1$. ∎

Le lemme 1 exprime la moyenne $G_N(x)$ sous la forme d'un produit de fonctions bornées par 1. Si nous montrons que chacune de ces fonctions s'approche rarement de 1, nous en déduirons une bonne majoration pour $|G_N(x)|$. C'est l'objectif du lemme 2 : exprimer sous une forme plus simple les facteurs du produit.

Soit $0 < c_3 < 4$ une constante (pouvant dépendre de g). Nous définissons, pour tous réels $\mu > 0$ et x,

$$\mathcal{U}(x) := 1 - c_3\|x\|^2 \quad \text{et} \quad \mathcal{G}_\mu(x) := \prod_{k<\mu} \mathcal{U}(g^k x). \tag{2.4}$$

Nous n'indiquons pas la dépendance de ces fonctions par rapport à c_3 car cette constante est fixée dans toute la suite avec le lemme suivant.

Lemme 2. *Notons*

$$c_3 := \begin{cases} 1 & \text{si } g \text{ est pair}, \\ 1 - 1/g - 1/g^2 + 1/g^3 & \text{si } g \text{ est impair}. \end{cases} \tag{2.5}$$

Pour tous k et x, nous avons alors

$$|U(\Phi_N(k)x)U^2(\Phi_N(k+1)x)| \le \mathcal{U}((g^2-1)g^k x). \tag{2.6}$$

En particulier,

$$|G_N(r)| \le |\mathcal{G}_{(N-1)/2}((g^2-1)r)|^{1/3}. \tag{2.7}$$

Démonstration. Traitons en détail le cas g pair. En développant avec le binôme de Newton, nous avons

$$U(x)^2 = \frac{1}{g^2} \sum_{d<2g-1} a_h \mathrm{e}(hx) \quad \text{où} \quad a_h := \min\{h+1, 2g-1-h\}.$$

Nous marions les exponentielles dont les exposants h sont de même reste modulo g :

$$|U(x)^2| \leq \frac{1}{g^2} \sum_{d<g} |(d+1)\,\mathrm{e}(dx) + (g-d-1)\,\mathrm{e}((d+g)x)|.$$

Nous avons ainsi fait apparaître des termes $|1+\mathrm{e}(gx)|$. Nous allons les dénombrer :

$$\begin{aligned}|(d+1)\,\mathrm{e}(dx) + (g-d-1)\,\mathrm{e}((d+g)x)| \leq \min(d+1, g-d-1)|1+\mathrm{e}(gx)| \\ + \max(d+1, g-d-1) - \min(d+1, g-d-1).\end{aligned}$$

En distinguant suivant la taille de $d+1$ et de $g-d-1$, nous obtenons

$$\begin{aligned}&|(d+1)\,\mathrm{e}(dx) + (g-d-1)\,\mathrm{e}((d+g)x)| \\ &\qquad \leq \begin{cases} (d+1)|1+\mathrm{e}(gx)| + g - 2(d+1) & \text{si } d < g/2-1, \\ \frac{1}{2}g|1+\mathrm{e}(gx)| & \text{si } d = g/2-1, \\ (g-d-1)|1+\mathrm{e}(gx)| + 2(d+1) - g & \text{si } d > g/2-1, \end{cases}\end{aligned}$$

et finalement

$$\begin{aligned}|U(x)^2| &\leq \frac{2}{g^2} \sum_{d<g/2-1} (d+1)|1+\mathrm{e}(gx)| + \frac{1}{2g}\,|1+\mathrm{e}(gx)| + A \\ &\leq \left(\frac{2}{g^2}\,\frac{\frac{g}{2}\left(\frac{g}{2}-1\right)}{2} + \frac{1}{2g}\right)|1+\mathrm{e}(gx)| + A\end{aligned}$$

où A correspond aux termes majorés trivialement :

$$A = \frac{1}{g^2}\Big(g^2 - 4 \sum_{d<g/2-1} (d+1) - g\Big).$$

Ainsi,

$$|U(x)^2| \leq \tfrac{1}{4}|1+\mathrm{e}(gx)| + \tfrac{1}{2}. \tag{2.8}$$

La base g étant paire, nous pouvons regrouper chaque élément pair de $\{0, \dots, g-2\}$ avec son successeur. Ainsi,

$$|U(x)| \leq \frac{1}{g}\,\frac{g}{2}\,|1+\mathrm{e}(x)| = \tfrac{1}{2}|1+\mathrm{e}(x)| \tag{2.9}$$

et en ne conservant du produit que la moitié des exponentielles (celles qui ont le même exposant), nous en déduisons l'estimation

$$\begin{aligned}|\overline{U(\Phi_N(k)x)}U^2(\Phi_N(k+1)x)| &\leq \tfrac{1}{8}|1+\mathrm{e}(-\Phi_N(k)x)|\,|1+\mathrm{e}(g\Phi_N(k+1)x)| + \tfrac{1}{2} \\ &\leq \tfrac{1}{8}|1+\mathrm{e}(-\Phi_N(k)x + g\Phi_N(k+1))| + \tfrac{3}{4} \\ &\leq \tfrac{1}{8}|1+\mathrm{e}((g^2-1)g^k x)| + \tfrac{3}{4}\end{aligned}$$

en utilisant l'identité (1.6). Nous utilisons maintenant la majoration classique

$$|1+\mathrm{e}(y)| \le 2(1-4\|y\|^2) \tag{2.10}$$

que nous pouvons prouver en utilisant la concavité de $z \mapsto \sin(\pi z/2)$ entre 0 et $1/2$ et l'écriture

$$|1+\mathrm{e}(y)| = 2\cos(\pi y) = 2-4\sin^2(\pi y/2).$$

Nous avons alors

$$\begin{aligned} |U(\Phi_N(k)x)U^2(\Phi_N(k+1)x)| &\le \tfrac{1}{8}|1+\mathrm{e}((g^2-1)g^k x)| + \tfrac{3}{4} \\ &\le \tfrac{1}{4}(1-4\|(g^2-1)g^k x\|^2) + \tfrac{3}{4} \\ &\le 1-\|(g^2-1)g^k x\|^2, \end{aligned}$$

ce qui termine la preuve de la première majoration lorsque g est pair.

Si g est impair, la démarche est identique : quelques points de détail seulement changent (principalement le fait qu'il reste un terme célibataire que nous majorons donc par 1). Nous indiquons les deux résultats intermédiaires :

$$|U(x)^2| \le \frac{1-1/g^2}{4}\,|1+\mathrm{e}(gx)| + 1 - \frac{1-1/g^2}{4}, \tag{2.8$'$}$$

$$|U(x)| \le \frac{1-1/g}{2}\,|1+\mathrm{e}(x)| + 1 - \frac{1-1/g}{2}, \tag{2.9$'$}$$

d'où nous déduisons la majoration du lemme de la même façon que précédemment.

En regroupant $U(\Phi_N(k)r)$ avec $U(\Phi_N(k+1)r)^2$ dans l'expression de G_N donnée par le lemme 1, nous obtenons

$$|G_N(r)| \le \prod_{k<(N-1)/2} |U(\Phi_N(k)r)U(\Phi_N(k+1)r)^2|^{1/3} \le |\mathcal{G}_{(N-1)/2}(r)|^{1/3},$$

ce qui finit la preuve du lemme. ∎

Lemme 3. *Pour tout ensemble sans répétition $\mathfrak{R}$ de points de $]0,1[$ globalement invariant modulo 1 par les multiplications par g et par g^2-1 :*

$$g\mathfrak{R} = \mathfrak{R} \bmod 1 \quad \textit{et} \quad (g^2-1)\mathfrak{R} = \mathfrak{R} \bmod 1,$$

pour tout entier $m \ge 1$ et pour tout N, nous avons

$$\sum_{r\in\mathfrak{R}} |G_N(r)| \le \sum_{r\in\mathfrak{R}} |\mathcal{G}_\mu(r)|^\alpha, \tag{2.11}$$

où nous avons posé $\mu := (N-1)/2m$, $\alpha := m/3$ et où c_3 est la constante du lemme 2.

Démonstration. Soit r un réel fixé. Le lemme 2 et l'inégalité arithmético-géométrique donnent la majoration

$$\begin{aligned}|G_N(r)| &\le |\mathcal{G}_{(N-1)/2}((g^2-1)r)|^{1/3}\\ &\le \frac{1}{m}\sum_{h<m}\prod_{h(N-1)/2m\le k<(h+1)(N-1)/2m}|\mathcal{U}(g^k(g^2-1)r)|^{m/3}.\end{aligned}$$

En sommant sur les $r\in\mathfrak{R}$, nous avons donc

$$\begin{aligned}\sum_{r\in\mathfrak{R}}|G_N(r)| &\le \frac{1}{m}\sum_{h<m}\sum_{r\in\mathfrak{R}}\prod_{h(N-1)/2m\le k<h(N-1)/2m+\mu}|\mathcal{U}(g^k(g^2-1)r)|^{\alpha}\\ &\le \frac{1}{m}\sum_{h<m}\sum_{r\in\mathfrak{R}}\prod_{j<\mu}|\mathcal{U}(g^j(g^2-1)r)|^{\alpha}\end{aligned}$$

puisque la multiplication par une puissance de g laisse $\mathfrak{R}$ invariant modulo 1. Par définition de $\mathcal{G}_\mu$, nous avons donc

$$\sum_{r\in\mathfrak{R}}|G_N(r)|\le\sum_{r\in\mathfrak{R}}|\mathcal{G}_\mu((g^2-1)r)|^{\alpha}, \tag{2.12}$$

ce qui implique immédiatement la majoration (2.11) puisque $\mathfrak{R}$ est invariant modulo 1 par la multiplication par g^2-1. ∎

Les deux prochains chapitres sont consacrés à l'obtention de majorations pour

$$\sum_{r\in\mathfrak{R}}|\mathcal{G}_\mu(r)|^{\alpha}, \tag{2.13}$$

suivant la taille de μ, α et de propriétés spécifiques de $\mathfrak{R}$.

3. Théorèmes 1 et 2 dans le cas des pseudopalindromes de taille N. Pour démontrer le théorème 1, nous allons choisir α très grand dans (2.13) puisque ce paramètre va tendre vers l'infini avec μ. Il nous faut donc une majoration de (2.13) uniforme en α. Il existe à notre connaissance deux techniques permettant d'obtenir ce type de résultat : celle développée par C. Mauduit et A. Sárközy dans [MS97] pour l'étude des entiers dont la somme des chiffres est fixée et celle développée par S. Konyagin dans [Kon01] pour l'étude des entiers ellipséphiques. Nous utilisons ici cette seconde méthode qui permet d'obtenir une bonne majoration pour les très grands diviseurs.

3.1. *Lemme de S. Konyagin.* Soit $\delta>0$. Un ensemble $\mathfrak{R}$ est dit *δ bien espacé* si pour tous choix de $r\neq r'$ dans $\mathfrak{R}$, nous avons $|r-r'|\ge\delta$. Nous énonçons sous une forme générale un résultat obtenu par S. Konyagin lors d'une étape de la démonstration du théorème 1 de [Kon01] sur l'estimation

du cardinal des nombres ellipséphiques dans les progressions arithmétiques : il a étudié le cas particulier où $\mathfrak{R} = \{a/q : 1 \le a \le q-1\}$, pour q fixé.

LEMME 4 (Konyagin). *Soit $\mathfrak{R}$ un ensemble δ bien espacé de points de $[\delta/2, 1-\delta/2]$ tel que si une fraction est dans $\mathfrak{R}$, son dénominateur irréductible est premier avec $2g$. Soit M un entier tel que $\delta g^M > 1$. Il existe alors une application injective*

$$\mathfrak{R} \to (\mathbb{Z} \cap]-(g+1)/2, (g+1)/2[)^M, \qquad r \mapsto (\Delta_j)_{j<M},$$

telle que $\|g^j r\| \le 1/2g$ si et seulement si $\Delta_j = 0$. De plus, si $r \in \mathfrak{R}$, alors (Δ_j) n'est pas identiquement nulle.

Démonstration. Notons

$$\mathfrak{N} := \{(n_0, \dots, n_M) \in \mathbb{Z}^{M+1} : 0 \le n_j \le g^j \ \forall j,\ 0 < n_M < g^M\}.$$

Montrons que les deux applications suivantes sont bien définies et injectives :

$$\mathfrak{R} \to \mathfrak{N} \to \mathbb{Z}^M \setminus \{0\}, \qquad r \mapsto (n_j)_{j<M+1} \mapsto (\Delta_j)_{j<M},$$

où $\Delta_j := n_{j+1} - g n_j$ et n_j est le plus proche entier de $g^j r$.

L'hypothèse faite sur $\mathfrak{R}$ assure que le nombre $g^j r$ n'est jamais un demi-entier si $r \in \mathfrak{R}$. La suite (n_j) est donc bien définie. Montrons qu'elle appartient à $\mathfrak{N}$: nous avons $0 < g^j r < g^j$ puisque $0 < r < 1$ et donc $0 \le n_j \le g^j$ pour tout j. Comme nous avons l'encadrement plus précis

$$\delta/2 \le r \le 1 - \delta/2 \quad \text{et} \quad \delta g^M > 1,$$

nous en déduisons $1/2 < g^M r < g^M - 1/2$. En utilisant maintenant que n_M est un entier, nous avons $1 \le n_j \le g^M - 1$, ce qui démontre que $(n_j) \in \mathfrak{N}$.

Soient $r \ne r'$ deux points différents de $\mathfrak{R}$. Alors

$$1 < g^M \delta \le |g^M r - g^M r'|,$$

ce qui assure que $n_M \ne n'_M$. La première application est bien injective.

Clairement la suite (Δ_j) est bien définie. La seule propriété à prouver est qu'elle n'est pas identiquement nulle. Raisonnons par l'absurde et supposons que $\Delta_j = 0$ pour tout j. Alors $0 = \Delta_j = n_{j+1} - n_j$ pour tout j, ce qui implique que $n_M = g^M n_0$. Mais $n_0 = 0$ ou 1 par définition de $\mathfrak{N}$. Donc $n_M = 0$ ou g^M ce qui est incompatible avec la définition de $\mathfrak{N}$.

Pour montrer l'injectivité de la seconde application, il suffit de montrer que n_0 se détermine de façon unique à partir de (Δ_j). La suite (n_j) sera alors complètement déterminée puisque $n_{j+1} = g n_j + \Delta_j$. Notons Δ_i le premier terme non nul de la suite (Δ_j) dont nous venons de prouver l'existence. Comme précédemment, nous avons

$$n_{i+1} = g^{i+1} n_0 + \Delta_i \tag{3.1}$$

puisque (n_j) est une suite géométrique de raison g tant que $j \le i$. Mais par définition de $\mathfrak{N}$, nous savons que $0 \le n_i \le g^i$. L'équation (3.1) impose

donc $n_0 = 0$ si $\Delta_i > 0$ et $n_0 = 1$ si $\Delta_i < 0$. La valeur de n_0 est donc bien déterminée par la suite (Δ_j), ce qui prouve l'injectivité.

Pour terminer la preuve du lemme, il reste à prouver que si $r \in \mathfrak{R}$, alors

(1) $|\Delta_j| < (g+1)/2$ pour tout j,
(2) $\|g^j r\| \leq 1/2g$ si et seulement si $\Delta_j = 0$.

Pour cela, notons $\varepsilon_j := g^j r - n_j$ l'erreur commise en remplaçant $g^j r$ par son approximation entière n_j. L'entier Δ_j admet une nouvelle expression :

$$\Delta_j = -\varepsilon_{j+1} + g\varepsilon_j.$$

La majoration du premier point se déduit immédiatement de cette nouvelle expression de Δ_j puisque $g^j r$ n'est jamais un demi-entier. L'équivalence du second point est tout aussi simple puisque $\|g^j r\| = |\varepsilon_j| = (1/g)|\Delta_j + \varepsilon_{g+1}|$ et Δ_j est un entier. ∎

Corollaire 3 (Konyagin). *Il existe une constante $c_2 > 0$ ne dépendant que de g telle que pour tout $\mathfrak{R}$ ensemble δ bien espacé de points de l'intervalle $[\delta/2, 1-\delta/2]$ vérifiant l'hypothèse du lemme 4, pour tout réel $\alpha > 0$ et tout entier $M \geq 1$ tel que $1/\delta < g^M$, nous avons*

$$\sum_{r\in\mathfrak{R}} |\mathcal{G}_M(r)|^\alpha \leq \left(1 + c_2\left(1 - \frac{c_3}{4g^2}\right)^\alpha\right)^M - 1.$$

Par exemple, nous pouvons choisir $c_2 := g$. Dans le cas où g est impair, nous pouvons choisir $c_2 := g - 1$.

Démonstration. Le lemme 4 permet de réaliser une partition de $\mathfrak{R}$ suivant le nombre de fois où $\|g^j r\|$ est "petit" : pour tout entier k, nous notons $\mathfrak{R}(k)$ l'ensemble des points $r \in \mathfrak{R}$ pour lesquels

$$\#\{j < M : \|g^j r\| > 1/2g\} = k,$$

de sorte que

$$\sum_{r\in\mathfrak{R}} |\mathcal{G}_M(r)|^\alpha = \sum_{r\in\mathfrak{R}} \prod_{j<M} (1 - c_3\|g^j r\|^2)^\alpha \leq \sum_{k\geq 0} \#\mathfrak{R}(k)\left(1 - \frac{c_3}{4g^2}\right)^{\alpha k}.$$

Mais $\#\mathfrak{R}(0) = 0$, puisque le lemme 4 assure que la suite (Δ_j) n'est pas identiquement nulle. L'application injective du lemme 4 permet de majorer $\#\mathfrak{R}(k)$ par le nombre de M-uplets à valeurs dans $\{-c_2/2, \ldots, c_2/2\}$ avec exactement $M - k$ composantes nulles : il y a $\binom{M}{M-k}$ choix pour les $M - k$ zéros de la suite et c_2 choix pour chacun des k autres nombres. Donc

$$\sum_{r\in\mathfrak{R}} |\mathcal{G}_M(r)|^\alpha \le \sum_{k\ge 1} \binom{M}{M-k} c_2^k \Big(1-\frac{c_3}{4g^2}\Big)^{\alpha k}$$
$$\le \Big(1+c_2\Big(1-\frac{c_3}{4g^2}\Big)^\alpha\Big)^M - 1,$$

ce qui termine la preuve. ∎

3.2. *Preuve du théorème 1 pour $\mathscr{Q}_N$.* Soit $\mathfrak{R}$ un ensemble de fractions de $]0,1[$. Nous disons que $\mathfrak{R}$ *vérifie l'hypothèse* (H_δ) si $\mathfrak{R}$ est δ bien espacé, si $\mathfrak{R}$ est invariant modulo 1 par les multiplications par g et par g^2-1 et si les dénominateurs irréductibles de $\mathfrak{R}$ sont tous premiers avec $2g$:

$$(\mathrm{H}_\delta)\qquad \begin{cases} r\ne r'\in\mathfrak{R} \;\Rightarrow\; |r-r'|\ge\delta, \\ g\mathfrak{R}=\mathfrak{R} \bmod 1 \quad\text{et}\quad (g^2-1)\mathfrak{R}=\mathfrak{R}\bmod 1, \\ l/q\in\mathfrak{R} \text{ et } (l,q)=1 \;\Rightarrow\; (q,2g)=1. \end{cases}$$

Lemme 5. *Il existe une constante $c_4>0$ ne dépendant que de g telle qu'uniformément pour tout $\delta>0$, tout ensemble $\mathfrak{R}$ de fractions de $[\delta/2,1-\delta/2]$ vérifiant l'hypothèse (H_δ) et tout entier N assez grand pour que*

$$\frac{N-1}{4}\ge\frac{\log(1/\delta)}{\log g} \quad et \quad c_4N\ge\log(1/\delta)\log_2(1/\delta), \tag{3.2}$$

nous avons la majoration

$$\sum_{r\in\mathfrak{R}} |G_N(r)| \ll_g \log(g/\delta)e^{-c_4N/\log(1/\delta)}.$$

Par exemple, si c_3 est une constante admissible pour le lemme 2, nous pouvons choisir $c_4:=(\log g)c_3/24g^2$.

Remarque 3. Dès que $1/\delta$ est assez grand par rapport à g, ce qui est toujours le cas en pratique, la seconde condition de (3.2) implique la première.

Démonstration. Nous choisissons l'entier m tel que

$$\frac{N-1}{2}\frac{\log g}{\log(1/\delta)}-1\le m<\frac{N-1}{2}\frac{\log g}{\log(1/\delta)}.$$

Nous avons bien $m\ge 1$ grâce à la première condition de notre hypothèse (3.2). Le lemme 3 permet alors d'écrire, en notant $\mu:=(N-1)/2m$,

$$\sum_{r\in\mathfrak{R}} |G_N(r)| \le \sum_{r\in\mathfrak{R}} |\mathcal{G}_\mu(r)|^{m/3}. \tag{3.3}$$

Remarquons que le majorant de la définition de m implique

$$g^\mu = g^{(N-1)/2m} > g^{\log(1/\delta)/\log g} = \frac{1}{\delta}.$$

Si nous notons $M := \lceil \mu \rceil$, nous aurons donc $1/\delta < g^M$ et nous pouvons utiliser le corollaire 3 pour majorer le membre de droite de (3.3). Ainsi,

$$\sum_{r\in\mathfrak{R}} |G_N(r)| \le \left(1 + c_2\left(1 - \frac{c_3}{4g^2}\right)^{m/3}\right)^M - 1 \le (1 + c_2 e^{-\frac{c_3}{4g^2}\frac{m}{3}})^M - 1$$
$$\le \exp(c_2(\mu+1)e^{-c_3 m/12g^2}) - 1.$$

Donc

$$\sum_{r\in\mathfrak{R}} |G_N(r)| \le \exp\left(c_2\left(\frac{N-1}{2m}+1\right)e^{-c_3 m/12g^2}\right) - 1. \tag{3.4}$$

Le minorant de la définition de m donne

$$\frac{\log g}{\log(1/\delta)}\,\frac{N-1}{2m} \le 1 + \frac{1}{m} \le 2.$$

Donc

$$\frac{N-1}{2m} + 1 \ll_g \log(1/\delta).$$

Le membre de droite de (3.4) étant décroissant avec m, nous avons pour deux constantes $c_4 > 0$ et $c_5 > 0$ ne dépendant que de g,

$$\sum_{r\in\mathfrak{R}} |G_N(r)| \le \exp(c_5 \log(1/\delta) e^{-c_4 N/\log(1/\delta)}) - 1 \le e^{c_5}\log(1/\delta) e^{-c_4 N/\log(1/\delta)},$$

puisque la convexité de l'exponentielle assure que $e^{ax} - 1 \le (e^a - 1)x$ lorsque $x \in [0,1]$. La seconde condition de notre hypothèse (3.2) garantit que nous sommes effectivement dans l'intervalle $[0,1]$. ∎

Lemme 6. *Il existe des constantes $c, \widetilde{c} > 0$ ne dépendant que de g telles qu'uniformément pour N assez grand (en terme de g) et q un entier vérifiant*

$$q \le \exp\left(\frac{cN}{\log N}\right) \quad et \quad (q, g^3 - g) = 1,$$

nous avons la majoration

$$\max_{a\in\mathbb{Z}} \left| \#\mathscr{Q}_N(g^N, a, q) - \frac{\#\mathscr{Q}_N}{q} \right| \ll_g \frac{\#\mathscr{Q}_N}{q} \exp\left(-\frac{\widetilde{c}N}{\log q}\right).$$

Si c_4 désigne une constante admissible pour le lemme 5, nous pouvons prendre tous les $c, \widetilde{c} > 0$ tels que

$$c + \widetilde{c} \le c_4.$$

Démonstration. Pour estimer le nombre de pseudopalindromes divisibles par q, nous introduisons des sommes d'exponentielles :

$$\begin{aligned}\#\mathscr{Q}_N(g^N,a,q) &= \sum_{n\in\mathscr{Q}_N}\frac{1}{q}\sum_{l<q}\mathrm{e}\Big(l\,\frac{n-a}{q}\Big) = \frac{1}{q}\sum_{l<q}\mathrm{e}\Big(-\frac{al}{q}\Big)\sum_{n\in\mathscr{Q}_N}\mathrm{e}\Big(\frac{nl}{q}\Big)\\ &= \frac{\#\mathscr{Q}_N}{q}\sum_{l<q}\mathrm{e}\Big(-\frac{al}{q}\Big)G_N\Big(\frac{l}{q}\Big).\end{aligned}$$

Nous isolons le terme $l=0$ qui fournit la partie principale :

$$\#\mathscr{Q}_N(g^N,a,q) = \frac{\#\mathscr{Q}_N}{q} + \frac{\#\mathscr{Q}_N}{q}\sum_{0<l<q}\mathrm{e}\Big(-\frac{al}{q}\Big)G_N\Big(\frac{l}{q}\Big).$$

Avec une inégalité triangulaire, nous obtenons donc

$$\Big|\#\mathscr{Q}_N(g^N,a,q) - \frac{\#\mathscr{Q}_N}{q}\Big| \le \frac{\#\mathscr{Q}_N}{q}\sum_{0<l<q}\Big|G_N\Big(\frac{l}{q}\Big)\Big|. \tag{3.5}$$

Notons $\mathfrak{R} := \{l/q : 0<l<q\}$. Comme nous avons fait l'hypothèse que $(q, g^3-g)=1$, nous avons $(q,g)=1$ et $(q,g^2-1)=1$, donc les multiplications par g et par g^2-1 sont des bijections dans $(\mathbb{Z}/q\mathbb{Z})\setminus\{0\}$. Ainsi $\mathfrak{R}$ est un ensemble de fractions de $[\delta/2, 1-\delta/2]$ vérifiant l'hypothèse (H_δ) avec $\delta := 1/q$. De plus

$$\begin{aligned}\log(1/\delta)\log_2(1/\delta) = \log q\log_2 q &\le \frac{cN}{\log N}\Big(\log\frac{cN}{\log N}\Big)\\ &\le cN(1+o(1)).\end{aligned}$$

Comme $c<c_4$, les hypothèses du lemme 5 sont donc vérifiées lorsque N est assez grand par rapport à g, ce qui permet de majorer :

$$\Big|\#\mathscr{Q}_N(g^N,a,q) - \frac{\#\mathscr{Q}_N}{q}\Big| \ll_g \frac{\#\mathscr{Q}_N}{q}\log(q)\exp\Big(-\frac{c_4N}{\log q}\Big).$$

Mais

$$\log(q)\exp\Big(-\frac{cN}{\log q}\Big) \le \frac{cN}{\log N}\exp(-\log N) = \frac{c}{\log N} \ll_g 1,$$

et puisque nous avons imposé $c+\widetilde{c}\le c_4$, nous avons donc

$$\log(q)\exp\Big(-\frac{c_4N}{\log q}\Big) \ll_g \exp\Big(-\frac{\widetilde{c}N}{\log q}\Big),$$

ce qui termine la preuve du lemme. ∎

4. Lemmes préliminaires à la démonstration du théorème 2

4.1. *Majoration des moyennes de $\mathcal{G}_N$.* Pour un réel $\alpha \geq 1$, nous définissons $\mathcal{K}_\alpha$ par

$$\mathcal{K}_\alpha := \limsup_{\mu\to\infty} \| \, |\mathcal{G}_\mu|^\alpha \|_1^{1/\mu}. \tag{4.1}$$

Lemme 7. *Définissons*

$$\mathcal{M}_\alpha := \max_{u\in[0,1]} \frac{1}{g} \sum_{0\leq h<g} \left| \mathcal{U}\Big(\frac{u+h}{g}\Big)\right|^\alpha. \tag{4.2}$$

Alors $\mathcal{K}_\alpha \leq \mathcal{M}_\alpha$ pour tout $\alpha \geq 1$.

Démonstration. Prenons un entier $N \geq 1$ et calculons l'intégrale de $\mathcal{G}_N^{2l}$ en découpant le segment $[0,1]$ en g sous-segments de longueur $1/g$:

$$\begin{aligned}
\| \, |\mathcal{G}_N|^\alpha \|_1 &= \sum_{0\leq h<g} \int_{h/g}^{(h+1)/g} \prod_{k<N} |\mathcal{U}(g^k s)|^\alpha \, ds \\
&= \sum_{0\leq h<g} \int_{h/g}^{(h+1)/g} |\mathcal{U}(s)|^\alpha \prod_{k<N-1} |\mathcal{U}(g^k g s)|^\alpha \, ds \\
&= \frac{1}{g} \sum_{0\leq h<g} \int_0^1 \left|\mathcal{U}\Big(\frac{u+h}{g}\Big)\right|^\alpha \prod_{k<N-1} |\mathcal{U}(g^k(u+h))|^\alpha \, du \\
&= \frac{1}{g} \sum_{0\leq h<g} \int_0^1 \left|\mathcal{U}\Big(\frac{u+h}{g}\Big)\right|^\alpha |\mathcal{G}_{N-1}(u)|^\alpha \, du
\end{aligned} \tag{4.3}$$

puisque $\mathcal{G}_{N-1}$ est une fonction 1-périodique. La définition de $\mathcal{M}_\alpha$ implique

$$\|\mathcal{G}_N^\alpha\|_1 \leq \mathcal{M}_\alpha \|\mathcal{G}_{N-1}^\alpha\|_1 \leq \cdots \leq \mathcal{M}_\alpha^N.$$

Ainsi, $\limsup_{N\to\infty} \| \, |\mathcal{G}_N|^\alpha \|_1^{1/N} \leq \mathcal{M}_\alpha$. Comme

$$\| \, |\mathcal{G}_\mu|^\alpha \|_1^{1/\mu} = (\| \, |\mathcal{G}_{\lceil\mu\rceil}|^\alpha \|_1^{1/\lceil\mu\rceil})^{\lceil\mu\rceil/\mu},$$

nous obtenons $\mathcal{K}_\alpha \leq \mathcal{M}_\alpha$ en prenant la limite supérieure à gauche et à droite de cette égalité. ∎

Nous redonnons avec les notations propres à cet articles la majoration de $\mathcal{M}$ obtenue dans l'article [Colre, lemme 15].

Lemme 8. *Soit B tel que pour tout $x \in \mathbb{R}$,*

$$\|\mathscr{U}(x)\| \leq 1 - B\|x\|^2.$$

Alors pour tout réel $\alpha \geq 1$,

$$\mathcal{M}_\alpha < \frac{1}{g} \sum_{-g/2 \leq h \leq g/2} \left(1 - \frac{B}{g^2}\, h^2\right) < \frac{1}{g} + \sqrt{\frac{\pi}{\alpha c_3}}. \tag{4.4}$$

Plus g est grand, plus la majoration $\mathcal{K}_\alpha \leq \mathcal{M}_\alpha$ donnée par le lemme 7 est précise. Lorsque g est très petit, nous obtiendrons une majoration plus fine en effectuant plus d'itérations dans le processus de moyenne. Définissons par récurrence sur k les fonctions

$$P_0(u) := 1 \quad \text{et} \quad P_{k+1}(u) := \frac{1}{g} \sum_{0 \leq h < g} \left|\mathcal{U}\left(\frac{u+h}{g}\right)\right|^\alpha P_k\left(\frac{u+h}{g}\right). \tag{4.5}$$

Des fonctions P_k de ce type ont déjà été introduites et étudiées par [FM96] et [DM01].

Lemme 9. *Pour tout réel* $\alpha \geq 1$ *et tout entier* k, *nous avons*

$$\mathcal{K}_\alpha \leq \mathcal{M}_\alpha^k \quad \text{où} \quad \mathcal{M}_\alpha^k := (\max_{u \in [0,1]} \widetilde{P}_k(u))^{1/k}. \tag{4.6}$$

Démonstration. Nous repartons de la majoration (4.3) :

$$\| \, |\mathcal{G}_N|^\alpha \|_1 = \int_0^1 \frac{1}{g} \sum_{0 \leq h < g} \left|\mathcal{U}\left(\frac{u+h}{g}\right)\right|^\alpha |\mathcal{G}_{N-1}(u)|^\alpha \, du.$$

La définition de $P_1(u)$ donne donc

$$\| \, |\mathcal{G}_N|^\alpha \|_1 = \int_0^1 P_1(u) |\mathcal{G}_{N-1}(u)|^\alpha \, du.$$

En utilisant le même argument de découpage de l'intégrale puis de changement de variable, nous avons pour tout entier $k \leq N$,

$$\| \, |\mathcal{G}_N|^\alpha \|_1 = \int_0^1 P_k(u) |\mathcal{G}_{N-k}(u)|^\alpha \, du,$$

ce qui implique immédiatement la majoration $\mathcal{K}_\alpha \leq \mathcal{M}_\alpha^k$. ∎

Lemme 10. *Si* $c_3 < 4$ *et* $\alpha \geq 1$, *alors uniformément pour* N *assez grand*, *nous avons*

$$\|(\mathcal{G}_N^\alpha)'\|_1 \leq \frac{4c_3\alpha}{4 - c_3} \frac{g^N - 1}{g - 1} \|\mathcal{G}_N^\alpha\|_1 \ll_{g,\alpha,c_3} g^N \|\mathcal{G}_N^\alpha\|_1.$$

Démonstration. Supposons $\alpha > 1$. Nous écrivons alors l'égalité vérifiée presque partout

$$(\mathcal{G}_N^\alpha)' = \alpha \mathcal{G}_\alpha' \mathcal{G}_N^{\alpha-1}$$

et nous appliquons l'inégalité de Hölder avec les exposants α et $\alpha/(\alpha-1)$. Ainsi,

$$\|(\mathcal{G}_N^\alpha)'\|_1 \le \alpha \|\mathcal{G}_N^\alpha\|_1^{1-1/\alpha} \|\mathcal{G}_N'\|_\alpha. \tag{4.7}$$

Mais si $g^k x$ n'est pas un demi-entier (donc pour presque tout x),

$$|\mathcal{G}_N'(x)| \le |\mathcal{G}_N(x)| \sum_{k<N} 2c_3 g^k \frac{\|g^k x\|}{1 - c_3 \|g^k x\|^2},$$

ce qui implique que pour presque tout x,

$$|\mathcal{G}_N'(x)| \le \frac{c_3}{1 - c_3/4} \frac{g^N - 1}{g - 1} |\mathcal{G}_N(x)|. \tag{4.8}$$

Nous reportons cette majoration dans (4.7) et le lemme est démontré. Si $\alpha = 1$, le lemme se déduit directement de la majoration (4.8). ∎

4.2. *Lemme de C. Mauduit et A. Sárközy.* C. Mauduit et A. Sárközy dans [MS97, lemme 2] ont prouvé le lemme suivant. Nous donnons ici une preuve simplifiée et légèrement améliorée de leur résultat, preuve obtenue en choisissant de façon optimale les différents paramètres à notre disposition au cours de la démonstration.

Lemme 11 (Mauduit–Sárközy). *Soient $r = l/q$ une fraction irréductible et $\mu > 0$. S'il existe un nombre premier p tel que $p \mid q$ et $p \nmid g$, alors*

$$\sum_{k<\mu} \|g^k r\|^2 > \frac{\log g}{(g+1)^2} \frac{\mu}{\log(gq)} - \frac{1}{(g+1)^2}. \tag{4.9}$$

En particulier, si q est premier avec $g(g-1)$, pour tout $\beta \in \mathbb{R}$, nous avons

$$\sum_{k<\mu} \|\beta + g^k r\|^2 > \frac{\log g}{4(g+1)^2} \frac{\mu}{\log(gq)} - \frac{1}{2(g+1)^2}. \tag{4.9$'$}$$

Remarque 4. La condition restante sur l'existence d'un p divisant m mais pas g est évidemment nécessaire, sans quoi le membre de gauche est une fonction bornée de μ alors que le membre de droite tend vers l'infini.

Démonstration. Notons $d := \lceil \log q / \log g \rceil$ et réalisons la division euclidienne de μ par d. Il existe un entier $n \ge 0$ tel que

$$nd \le \mu < (n+1)d.$$

Alors

$$\sum_{k<\mu} \|g^k r\|^2 \ge \sum_{k<n} \sum_{j<d} \|g^{j+kd} r\|^2. \tag{4.10}$$

Fixons l'entier k et montrons que nous pouvons toujours trouver un indice $j = j_k < d$ pour lequel

$$\|g^{j+kd}r\| \geq \frac{1}{g+1}.$$

Notre hypothèse sur l'existence d'un nombre premier p divisant q mais pas g implique que $q \nmid g^{kd}$ donc que $g^{kd}r \notin \mathbb{Z}$. Comme $g/(g+1) > 1/2$, il existe un entier t tel que

$$0 < R := |g^{kd}r - t| < \frac{g}{g+1}.$$

Choisissons alors l'entier $j = j_k$ tel que

$$g^j R < \frac{g}{g+1} \leq g^{j+1}R. \tag{4.11}$$

Donc

$$\frac{1}{g+1} = \frac{1}{g}\,\frac{g}{g+1} \leq \frac{1}{g}\,g^{j+1}R = g^jR < \frac{g}{g+1} = 1 - \frac{1}{g+1},$$

ce qui nous assure que pour ce choix de j_k,

$$\|g^{j_k+kd}r\| = \|g^{j_k}R\| \geq \frac{1}{g+1}. \tag{4.12}$$

Mais $1/R \leq q$ puisque R est une fraction non triviale de dénominateur au plus q. La minoration de (4.11) assure donc

$$j_k < \frac{\log \frac{gq}{g+1}}{\log g} < \frac{\log q}{\log g} \leq d.$$

En reportant la minoration (4.12) dans (4.10), nous trouvons que

$$\sum_{k<\mu} \|g^k r\|^2 \geq \sum_{k<n} \|g^{j_k}g^{kd}r\|^2 \geq \frac{n}{(g+1)^2}.$$

Mais par définition de n et de d, nous avons

$$n > \frac{\mu}{d} - 1 \geq \frac{\mu \log g}{\log(gq)} - 1,$$

ce qui implique la minoration (4.9).

Pour en déduire (4.9′), nous regroupons chaque terme de la somme avec son successeur :

$$\begin{aligned}\sum_{k<\mu} \|\beta + g^k r\|^2 &\geq \frac{1}{2} \sum_{k<\mu-1} (\|\beta + g^k r\|^2 + \|\beta + g^{k+1} r\|^2) \\ &\geq \frac{1}{4} \sum_{k<\mu-1} \|g^k(g-1)r\|^2\end{aligned}$$

en utilisant la minoration $\|x\|^2 + \|y\|^2 \geq \frac{1}{2}\|x-y\|^2$ valable pour tous réels x et y. Comme nous avons supposé q premier avec $g(g-1)$, nous pouvons

appliquer (4.9) à la fraction $(g-1)r$. Ainsi,

$$\sum_{k<\mu} \|\beta + g^k r\|^2 > \frac{\log g}{4(g+1)^2}\,\frac{\mu-1}{\log gq} - \frac{1}{4(g+1)^2},$$

ce qui implique immédiatement (4.9′). ∎

Corollaire 4. *Il existe une constante $c_6 > 0$ ne dépendant que de g telle que pour toute fraction r de dénominateur irréductible q premier avec g et tout $\mu > 0$, nous avons*

$$|\mathcal{G}_\mu(r)| < 2\exp\Big(-\frac{c_6\mu}{\log gq}\Big). \tag{4.13}$$

Par exemple, $c_6 := (\log g)c_3/(g+1)^2$ convient.

Démonstration. Nous reportons directement la majoration du lemme 11 dans la définition de $\mathcal{G}_\mu$:

$$\begin{aligned}|\mathcal{G}_\mu(r)| &= \exp\Big(\sum_{k<\mu} \log(1 - c_3\|g^k r\|^2)\Big) \le \exp\Big(\sum_{k<\mu} -c_3\|g^k r\|^2\Big)\\ &\le \exp\Big(-\frac{c_6\mu}{\log gq} + \frac{1}{(g+1)^2}\Big),\end{aligned}$$

ce qui termine la preuve puisque $\exp((g+1)^{-2}) \le \exp(1/(2+1)^2) < 2$. ∎

4.3. *Preuve du théorème 2 pour $\mathscr{Q}_N$.* À l'inverse de la démonstration du théorème 1 où nous avions choisi α très grand dans (2.13) puisque α tendait vers l'infini avec μ, nous essayons ici de trouver le plus petit α possible, car l'exposant de distribution que nous obtiendrons sera décroissant avec α. En particulier, α doit absolument rester borné quand μ est grand et nos majorations peuvent donc dépendre du paramètre α.

Nous posons, pour tous réels $\mu > 0$ et $\alpha \ge 1$,

$$\mathscr{S}_\mu^\alpha(Q) := \sum_{\substack{q<Q\\(q,g)=1}} \sum_{(l,q)=1} |\mathcal{G}_\mu(l/q)|^\alpha. \tag{4.14}$$

En utilisant une méthode similaire à celle de la démonstration du lemme 2 de l'article de S. Konyagin [Kon01], nous pourrions montrer que pour un choix convenable des paramètres $c, \widetilde{c} > 0$ et $\alpha \ge 1$ ne dépendant que de g, nous avons

$$\mathscr{S}_\mu^\alpha(Q) \ll_g Q\exp\Big(-\frac{\widetilde{c}}{2}\sqrt{\mu}\Big) \quad \text{dès que} \quad \exp(\widetilde{c}\sqrt{\mu}) < Q < g^{c\mu},$$

qui est le type de majoration nécessaire pour démontrer le théorème 2. Nous allons utiliser une autre méthode pour majorer $\mathscr{S}_\mu^\alpha(Q)$ qui fournira une majoration du même type mais valable pour une constante c nettement plus grande.

LEMME 12. *Soient $\alpha \geq 1$ et $c_7 > 0$ fixés. Uniformément pour $\mu > 0$ et $Q \leq (1/g)\exp(c_7\sqrt{\mu})$, nous avons*

$$\mathscr{S}_\mu^\alpha(Q) \ll_{g,\alpha} \exp\Big(-\Big(\frac{\alpha c_6}{c_7} - 2c_7\Big)\sqrt{\mu}\Big), \tag{4.15}$$

où c_6 désigne une constante admissible pour le corollaire 4.

Démonstration. Puisque nous sommons sur des entiers premiers avec g, nous pouvons utiliser la majoration du corollaire 4 qui fournit

$$\begin{aligned}\mathscr{S}_\mu^\alpha(Q) &\leq \sum_{q<Q}\sum_{(l,q)=1} 2^\alpha \exp\Big(-\frac{\alpha c_6\mu}{\log gq}\Big) \leq \sum_{q<Q}\sum_{(l,q)=1} 2^\alpha \exp\Big(-\frac{\alpha c_6\mu}{\log gQ}\Big)\\ &\leq 2^\alpha \sum_{q<Q} \varphi(q)\exp\Big(-\frac{\alpha c_6\mu}{\log gQ}\Big)\end{aligned}$$

où $\varphi(q)$ désigne la fonction d'Euler. Comme $\varphi(q) \leq q-1$, nous avons

$$\mathscr{S}_\mu^\alpha(Q) \leq 2^{\alpha-1}Q^2\exp\Big(-\frac{\alpha c_6\mu}{\log gQ}\Big) \leq \frac{2^{\alpha-1}}{g^2}\exp\Big(\Big(2c_7 - \frac{\alpha c_6}{c_7}\Big)\sqrt{\mu}\Big),$$

ce qui termine la preuve de cette majoration. ∎

LEMME 13. *Soient $\alpha \geq 1$ et $\varepsilon > 0$ fixés. Uniformément pour $\mu > 0$ et Q assez grands, nous avons*

$$\mathscr{S}_\mu^\alpha(Q) \ll_{g,\alpha,\varepsilon} Q^2(\mathcal{K}_\alpha + \varepsilon)^\mu + Q^{2+2\log(\mathcal{K}_\alpha+\varepsilon)/\log g}. \tag{4.16}$$

Démonstration. Comme $\mathcal{G}_\mu$ est un produit de fonctions bornées par 1, on observe que l'application $\nu \mapsto \mathscr{S}_\nu^\alpha(Q)$ est décroissante. Pour tout $\nu \leq \mu$, nous avons donc

$$\mathscr{S}_\mu^\alpha(Q) \leq \mathscr{S}_\nu^\alpha(Q) = \sum_{r\in\mathfrak{R}} |\mathcal{G}_\nu(r)|^\alpha, \tag{4.17}$$

avec $\mathfrak{R} := \{l/q : (l,q) = 1,\ q < Q,\ (q,g) = 1\}$ qui est une famille $\delta = Q^{-2}$ bien espacée de points de $[\delta/2, 1-\delta/2]$. Nous majorons cette some en utilisant le lemme de Sobolev–Gallagher énoncé dans [Mon71] que nous rappelons ici :

LEMME 14 (Sobolev–Gallagher). *Soient $\delta > 0$, $\mathfrak{R}$ un ensemble δ bien espacé de points de $[\delta/2, 1-\delta/2]$ et f une fonction admettant une dérivée continue sur $[0,1]$. Alors*

$$\sum_{x\in\mathfrak{R}} |f(x)| \leq \delta^{-1}\|f\|_1 + \tfrac{1}{2}\|f'\|_1.$$

Ainsi (4.17) devient

$$\mathscr{S}_\mu^\alpha \leq Q^2\|\mathcal{G}_\nu^\alpha\|_1 + \|(\mathcal{G}_\nu^\alpha)'\|_1 \ll_{\alpha,g} (Q^2 + g^\nu)\|\mathcal{G}_\nu^\alpha\|_1$$

en utilisant le lemme 10 pour majorer la dérivée. Si ν est assez grand, la définition de $\mathcal{K}_\alpha$ implique que

$$\mathscr{S}_\mu^\alpha(Q) \ll_{g,\alpha,\varepsilon} (Q^2 + g^\nu)(\mathcal{K}_\alpha + \varepsilon)^\nu.$$

Nous optimisons notre paramètre $\nu \le \mu$ en choisissant

$$\nu := \min\left\{\mu, 2\,\frac{\log Q}{\log g}\right\}, \tag{4.18}$$

qui est effectivement assez grand par rapport à g, α et ε dès que Q et μ le sont, ce qui est une hypothèse du lemme. Nous obtenons ainsi

$$\mathscr{S}_\mu^\alpha \ll_{g,\alpha,\varepsilon} Q^2(\mathcal{K}_\alpha + \varepsilon)^\mu + Q^2(\mathcal{K}_\alpha + \varepsilon)^{2\log Q/\log g},$$

ce qui termine la preuve du lemme. ∎

Lemme 15. *Soit $\alpha \ge 1$ vérifiant*

$$\mathcal{K}_\alpha < g^{-1/2}. \tag{4.19}$$

Pour tout $\varepsilon > 0$, il existe une constante $c_8 > 0$ ne dépendant que de g, de α et de ε telle qu'uniformément pour $\mu > 0$ et Q assez grands, nous avons

$$\sum_{\substack{q<Q\\(q,g)=1}} \sum_{0<l<q} |\mathcal{G}_\mu(l/q)|^\alpha \ll_{g,\alpha,\varepsilon} Qe^{-c_8\sqrt{\mu}} + Q^2(\mathcal{K}_\alpha + \varepsilon)^\mu. \tag{4.20}$$

Démonstration. Remarquons que pour tout $\varepsilon > 0$ assez petit, nous avons

$$2 + 2\,\frac{\log(\mathcal{K}_\alpha + \varepsilon)}{\log g} \le 1 - \varepsilon. \tag{4.21}$$

En effet, la condition (4.21) varie continûment avec ε et notre hypothèse (4.19) assure que c'est une inégalité stricte lorsque $\varepsilon = 0$. Sans perte de généralité, nous pouvons supposer que $\varepsilon > 0$ réalise la condition (4.21).

Dans la somme du lemme, nous rendons les fractions irréductibles en isolant leur plus grand facteur commun d. Donc

$$\begin{aligned}\sum_{\substack{q<Q\\(q,g)=1}} \sum_{0<l<q} |\mathcal{G}_\mu(l/q)|^\alpha &\le \sum_{d<Q} \sum_{\substack{q<Q/d\\(q,g)=1}} \sum_{(l,q)=1} |\mathcal{G}_\mu(l/q)|^\alpha \\ &\le \Big(\sum_{d<D} + \sum_{D\le d<Q}\Big)\mathscr{S}_\mu^\alpha(Q/d),\end{aligned}$$

où D est un paramètre à notre disposition.

Soit c_6 une constante admissible pour le corollaire 4. Nous choisissons

$$c_7 := \sqrt{\frac{\alpha c_6}{2+\varepsilon}} \quad \text{et} \quad c_8 := \varepsilon c_7 \tag{4.22}$$

qui ne dépendent donc que de g, de α et de ε. Nous prenons enfin

$$D := gQ\exp(-c_7\sqrt{\mu}). \tag{4.23}$$

Lorsque $d \geq D$, alors Q/d est *petit* et nous utilisons le lemme 12 pour estimer $\mathscr{S}_\mu^\alpha(Q/d)$. Lorsque $d < D$, alors Q/d est *grand* et nous estimons $\mathscr{S}_\mu^\alpha(Q/d)$ à l'aide du lemme 13. Ainsi,

$$\sum_{\substack{q<Q\\(q,g)=1}} \sum_{0<l<q} |\mathcal{G}_\mu(l/q)|^\alpha \ll_{g,\alpha} \sum_{d<D} (Q/d)^{2+2\log(\mathcal{K}_\alpha+\varepsilon)/\log g} + \sum_{d<D} (Q/d)^2(\mathcal{K}_\alpha+\varepsilon)^\mu + \sum_{D\leq d<Q} e^{-(\alpha c_6/c_7-2c_7)\sqrt{\mu}}.$$

Notre condition (4.21) sur le choix de $\varepsilon > 0$ fournit donc

$$\sum_{\substack{q<Q\\(q,g)=1}} \sum_{0<l<q} |\mathcal{G}_\mu(l/q)|^\alpha \ll_{g,\alpha} \sum_{d<D} (Q/d)^{1-\varepsilon} + \sum_{d\geq 1} (Q/d)^2(\mathcal{K}_\alpha+\varepsilon)^\mu + \sum_{d<Q} e^{-(\alpha c_6/c_7-2c_7)\sqrt{\mu}}$$

et en calculant la somme de ces séries, nous obtenons

$$\sum_{\substack{q<Q\\(q,g)=1}} \sum_{0<l<q} |\mathcal{G}_\mu(l/q)|^\alpha \ll_{g,\alpha} Q(Q/D)^{-\varepsilon} + Q^2(\mathcal{K}_\alpha+\varepsilon)^\mu + Qe^{-(\alpha c_6/c_7-2c_7)\sqrt{\mu}} \ll_{g,\alpha} Qe^{-\varepsilon c_7\sqrt{\mu}} + Q^2(\mathcal{K}_\alpha+\varepsilon)^\mu + Qe^{-(\alpha c_6/c_7-2c_7)\sqrt{\mu}},$$

ce qui démontre le lemme puisque $c_8 := \varepsilon c_7 = \alpha c_6/c_7 - 2c_7$ grâce à notre choix du paramètre c_7. ∎

Lemme 16. *Soit $m \geq 3$ un entier tel que*

$$\mathcal{K}_{m/3} < g^{-1/2}. \tag{4.24}$$

Notons β l'exposant défini par

$$\beta := -\frac{\log \mathcal{K}_{m/3}}{2m\log g} > \frac{1}{4m}. \tag{4.25}$$

Pour tout $\varepsilon > 0$, il existe une constante $c_9 > 0$ ne dépendant que de g, de m et de ε telle qu'uniformément pour N et $Q \leq g^{(\beta-\varepsilon)N}$ assez grands, nous avons

$$\sum_{\substack{Q/2\leq q<Q\\(q,g^3-g)=1}} \max_{a\in\mathbb{Z}} \left| \#\mathscr{Q}_N(g^N,a,q) - \frac{\#\mathscr{Q}_N}{q} \right| \ll_{g,m,\varepsilon} \#\mathscr{Q}_N e^{-c_9\sqrt{N}}.$$

Démonstration. L'équation (3.5) que nous avons déjà utilisée pour démontrer le lemme 6 permet d'écrire

$$\sum_{\substack{Q/2\le q<Q\\(q,g^3-g)=1}} \max_{a\in\mathbb{Z}} \left|\#\mathscr{Z}_N(g^N,a,q)-\frac{\#\mathscr{Z}_N}{q}\right| \le \#\mathscr{Z}_N \sum_{\substack{Q/2\le q<Q\\(q,g^3-g)=1}} \frac{1}{q}\sum_{0<l<q}|G_N(l/q)| \le \frac{2\#\mathscr{Z}_N}{Q}\sum_{\substack{q<Q\\(q,g^3-g)=1}}\sum_{0<l<q}|G_N(l/q)|.$$

Pour chaque q, nous utilisons le lemme 3 avec l'ensemble

$$\mathfrak{R} := \{l/q : 0<l<q\},$$

qui est invariant modulo 1 par les multiplications par g et par g^2-1 puisque q est premier avec $g^3-g=g(g^2-1)$. Donc

$$\sum_{\substack{Q/2\le q<Q\\(q,g^3-g)=1}} \max_{a\in\mathbb{Z}} \left|\#\mathscr{Z}_N(g^N,a,q)-\frac{\#\mathscr{Z}_N}{q}\right| \le \frac{2\#\mathscr{Z}_N}{Q}\sum_{\substack{q<Q\\(q,g^3-g)=1}}\sum_{0<l<q}|\mathcal{G}_\mu(l/q)|^\alpha$$

en ayant noté $\alpha := m/3$ et $\mu := (N-1)/2m$. Nous avons $\alpha \ge 1$ puisque $m\ge 2$ et notre hypothèse (4.24) permet donc d'appliquer la majoration du lemme 15.

Si $\varepsilon>0$ est assez petit, la définition de β permet d'écrire

$$\beta-\varepsilon+\frac{\log(\mathcal{K}_{m/3}+\varepsilon^2)}{2m\log g} = -\varepsilon+O_{g,m}(\varepsilon^2)<0. \tag{4.26}$$

Sans perte de généralité, nous pouvons supposer que $\varepsilon>0$ est assez petit pour vérifier (4.26).

Le lemme 15 permet donc de trouver une constante $c_8>0$ telle que

$$\sum_{\substack{Q/2\le q<Q\\(q,g^3-g)=1}} \max_{a\in\mathbb{Z}} \left|\#\mathscr{Z}_N(g^N,a,q)-\frac{\#\mathscr{Z}_N}{q}\right| \ll_{g,m,\varepsilon} \#\mathscr{Z}_N(e^{-c_8\sqrt{\mu}}+Q(\mathcal{K}_\alpha+\varepsilon^2)^\mu),$$

ce qui démontre la majoration du lemme avec

$$c_9 := c_8 m^{-1/2} \tag{4.27}$$

puisque

$$Q(\mathcal{K}_\alpha+\varepsilon^2)^\mu \ll_g g^{(\beta-\varepsilon+\frac{\log(\mathcal{K}_\alpha+\varepsilon^2)}{2m\log g})N}$$

et l'exposant est strictement négatif grâce à notre hypothèse (4.26). ∎

COROLLAIRE 5. *Soient c_3 une constante admissible pour le lemme 2 et*

$$\alpha := \frac{\pi g}{c_3(1-g^{-1/2})^2}. \tag{4.28}$$

Alors tout entier m supérieur à 3α vérifie l'hypothèse (4.24). En particulier, lorsque g tend vers l'infini, un exposant de distribution admissible pour le théorème 2 est

$$\beta = \frac{1+o(1)}{12\pi g}.$$

Démonstration. L'application $\alpha \mapsto \mathcal{K}_\alpha$ étant clairement décroissante, il suffit de montrer que le réel α défini par (4.28) vérifie l'hypothèse (4.19) pour en déduire que tout entier $m \geq 2\alpha$ vérifie (4.24) (comme $c_3 < 4$ et $g \geq 2$, nous avons bien $\alpha \geq 1$). Ceci est immédiat en utilisant les lemmes 7 et 8 et le corollaire est donc démontré. ∎

Dans la partie 6, nous améliorerons les résultats obtenus de ce chapitre.

5. Preuve des théorèmes

5.1. *Cardinal de $\mathscr{Q}_N(x)$ et de $\mathscr{Q}_N(x,a,q)$*

LEMME 17. *Soit N un entier. Pour tout pseudopalindrome x de taille N s'écrivant*

$$x = \sum_{k<N} x_k g^k \quad \textit{avec} \quad x_{N-1-k} = x_k,$$

nous avons (avec la convention $\mathscr{Q}_{-1} = \{0\}$)

$$\#\mathscr{Q}_N(x) = \sum_{k<(N+1)/2} x_k \#\mathscr{Q}_{N-2k} \tag{5.1}$$

et pour tout entier q premier avec g nous avons la majoration

$$\max_{a\in\mathbb{Z}} \left| \#\mathscr{Q}_N(x,a,q) - \frac{\#\mathscr{Q}_N(x)}{q} \right| \leq \sum_{k<(N+1)/2} x_k \#\mathscr{Q}_{N-2k}\mathscr{R}_{N-2k}(q) \tag{5.2}$$

en ayant noté

$$\mathscr{R}_N(q) := \frac{1}{q} \sum_{0<l<q} |G_N(l/q)|.$$

Démonstration. Décomposons $N = 2M + \delta$ avec $\delta = 0$ ou 1 de même parité que N et traitons en détail le cas légèrement plus technique correspondant à $\delta = 1$. Pour tout $0 \leq k \leq M$, nous notons

$$X_k := \sum_{j<k} x_j \Phi_{N-1}(j),$$

$$\widetilde{X}_k := x_M g^{M-k} + \sum_{k\leq j<M} x_j \Phi_{N-1-2k}(j-k),$$

de sorte que $x = X_k + g^k \widetilde{X}_k$ pour tout k ; X_k est le *bord* du pseudopalindrome x obtenu en remplaçant par des 0 les chiffres centraux et $\widetilde{X}_k$ est le *milieu* du pseudopalindrome x. Avec ces notations, montrons la partition

$$\mathscr{Q}_N(x) = \bigsqcup_{k<M+\delta} (X_k + g^k \mathscr{Q}_{N-2k}(x_k g^{N-1-2k})), \tag{5.3}$$

l'union étant disjointe.

Soit n un pseudopalindrome de N chiffres que nous décomposons en

$$n := n_{N-1}\Phi_{N-1}(0) + g\widetilde{n},$$

$\widetilde{n}$ étant un pseudopalindrome à $N-2$ chiffres. Alors n est inférieur à $x = \widetilde{X}_0$ si et seulement si

$$\begin{cases} n_0 = x_0 \text{ et } \widetilde{n} \text{ est inférieur à } \frac{1}{g}(\widetilde{X}_0 - x_0\Phi_{N-1}(0)) = \widetilde{X}_1 \\ \text{ou} \\ n_0 < x_0 \text{ et } \widetilde{n} \text{ est quelconque} \end{cases}$$

si et seulement si

$$[n_0 = x_0 \text{ et } \widetilde{n} \in \mathscr{Q}_{N-2}(\widetilde{X}_1)] \quad \text{ou} \quad n \in \mathscr{Q}_N(x_0 g^{N-1})$$

si et seulement si

$$n \in X_1 + g\mathscr{Q}_{N-2}(\widetilde{X}_1) \quad \text{ou} \quad n \in X_0 + g^0 \mathscr{Q}_N(x_0 g^{N-1}).$$

Nous suivons la même méthode pour décomposer $\mathscr{Q}_{N-2}(\widetilde{X}_1)$. Par récurrence décroissante, nous obtenons exactement la formule (5.3) à la $(M+\delta)^{\text{ème}}$ étape.

En calculant le cardinal de la décomposition (5.3), nous trouvons

$$\#\mathscr{Q}_N(x) = \sum_{k<M+\delta} \#\mathscr{Q}_{N-2k}(x_k g^{N-1-2k}) = \sum_{k<M+\delta} x_k \#\mathscr{Q}_{N-2k-2},$$

ce qui prouve la formule (5.1).

Pour évaluer le nombre de pseudopalindromes divisibles par q, nous introduisons des somme d'exponentielles, exactement comme nous l'avons déjà fait dans les démonstrations des lemmes 6 et 16 :

$$\begin{aligned} \#\mathscr{Q}_N(x,a,q) &= \sum_{n\in\mathscr{Q}_N(x)} \frac{1}{q} \sum_{l<q} \mathrm{e}\left(l\,\frac{n-a}{q}\right) \\ &= \frac{1}{q} \sum_{l<q} \mathrm{e}\left(-\frac{al}{q}\right) \sum_{n\in\mathscr{Q}_N(x)} \mathrm{e}\left(\frac{nl}{q}\right). \end{aligned} \tag{5.4}$$

Nous isolons le terme $l = 0$ qui fournit la partie principale :

$$\#\mathscr{Q}_N(x,a,q) = \frac{\#\mathscr{Q}_N(x)}{q} + \frac{1}{q} \sum_{0<l<q} \mathrm{e}\left(-\frac{al}{q}\right) \sum_{n\in\mathscr{Q}_N(x)} \mathrm{e}\left(\frac{nl}{q}\right).$$

La décomposition (5.3) permet donc d'écrire, pour tout entier a,

$$\begin{aligned}(5.5)\qquad &\left|\#\mathscr{Q}_N(x,a,q)-\frac{\#\mathscr{Q}_N(x)}{q}\right| \\ &\le \frac{1}{q}\sum_{0<l<q}\sum_{k<M+\delta}\left|\sum_{n\in\mathscr{Q}_N(x_k g^{N-1-2k})}\mathrm{e}\left((X_k+g^k n)\,\frac{l}{q}\right)\right| \\ &\le \frac{1}{q}\sum_{0<l<q}\sum_{k<M+\delta}x_k\left|\sum_{n\in\mathscr{Q}_{N-2k}}\mathrm{e}\left(g^k n\,\frac{l}{q}\right)\right| \\ &\le \sum_{k<M+\delta}\frac{1}{q}\sum_{0<l<q}x_k\#\mathscr{Q}_{N-2k}\left|G_{N-2k}\left(\frac{g^k l}{q}\right)\right|\end{aligned}$$

par définition de G_{N-2k}. Par hypothèse, q est premier avec g, donc la multiplication par g^k est une bijection de $(\mathbb{Z}/q\mathbb{Z})\setminus\{0\}$. Le changement de variable $\widetilde{l}=g^k l$ fournit donc

$$\left|\#\mathscr{Q}_N(x,a,q)-\frac{\#\mathscr{Q}_N(x)}{q}\right|\le\sum_{k<M+\delta}x_k\#\mathscr{Q}_{N-2k}\,\frac{1}{q}\sum_{0<\widetilde{l}<q}|G_{N-2k}(\widetilde{l}/q)|$$

ce qui termine la preuve du lemme. ∎

Corollaire 6. *Soit N un entier. Pour tout nombre réel x, pour tout $\widetilde{N}\le\frac{1}{2}N$ et pour tout ensemble d'entiers $\mathcal{Q}$ dont chaque élément est premier avec g, nous avons*

$$\begin{aligned}(5.6)\qquad &\sum_{q\in\mathcal{Q}}\sup_{y\le x}\max_{a\in\mathbb{Z}}\left|\#\mathscr{Q}_N(y,a,q)-\frac{\#\mathscr{Q}_N(y)}{q}\right| \\ &\ll_g \#\mathscr{Q}_N(x)g^{-\widetilde{N}}\#\mathcal{Q}+\#\mathscr{Q}_N(x)\sup_{\substack{N-2\widetilde{N}\le M\le N\\ M\equiv N \bmod 2}}\mathscr{R}_M(\mathcal{Q})\end{aligned}$$

en ayant noté

$$\mathscr{R}_N(\mathcal{Q}):=\sum_{q\in\mathscr{Q}}\frac{1}{q}\sum_{0<l<q}|G_N(l/q)|.$$

Démonstration. Soit $y\le x$. Quitte à remplacer y par le plus petit pseudopalindrome supérieur à y, nous pouvons supposer que y est un pseudopalindrome. Distinguons la méthode utilisée suivant la taille de y.

Si $y\ge g^N$, alors $\mathscr{Q}_N(y,a,q)=\mathscr{Q}_N(g^N,a,q)$ puisque g^N-1 est le plus grand pseudopalindrome de N chiffres.

Si $y<g^N$, nous notons k l'entier minimal tel que y possède au moins $N-2k$ chiffres. Alors $\mathscr{Q}_N(y)=g^k\mathscr{Q}_{N-2k}(y/g^{2k})$. Les éléments de $\mathcal{Q}$ étant premiers avec g, nous avons

$$\#\mathscr{Q}_N(y,a,q)=\#\mathscr{Q}_{N-2k}(y/g^{2k},a',q),$$

a' étant défini par $g^k a' \equiv a \bmod q$. Le résultat se déduit donc de l'estimation obtenue pour $N - 2k$.

Pour chaque entier $q \in \mathcal{Q}$, nous pouvons donc utiliser la majoration du lemme 17. D'où, pour tout $y \leq x$,

$$\max_{a\in\mathbb{Z}} \left| \#\mathscr{Q}_N(y,a,q) - \frac{\#\mathscr{Q}_N(y)}{q} \right| \ll_g \sum_{k<(N+1)/2} \#\mathscr{Q}_N g^{-k} \mathscr{R}_{N-2k}(q).$$

En sommant sur les entiers q de $\mathcal{Q}$, nous obtenons

$$\sum_{q\in\mathcal{Q}} \sup_{y\leq x} \max_{a\in\mathbb{Z}} \left| \#\mathscr{Q}_N(y,a,q) - \frac{\#\mathscr{Q}_N(y)}{q} \right| \ll_g \sum_{k<(N+1)/2} \#\mathscr{Q}_N g^{-k} \mathscr{R}_{N-2k}(\mathcal{Q}).$$

Lorsque $k \geq \widetilde{N}$, nous utilisons la majoration triviale $|\mathscr{R}_{N-2k}| \leq \#\mathcal{Q}$. Ainsi,

$$\begin{aligned}\sum_{q\in\mathscr{Q}} \sup_{y\leq x} \max_{a\in\mathbb{Z}} &\left| \#\mathscr{Q}_N(x,a,q) - \frac{\#\mathscr{Q}_N(x)}{q} \right| \\ &\ll_g \#\mathscr{Q}_N \sum_{k>\widetilde{N}} g^{-k} \#\mathcal{Q} + \#\mathscr{Q}_N \sum_{k\leq\widetilde{N}} g^{-k} \sup_{\substack{N-2\widetilde{N}\leq M\leq N \\ M\equiv N \bmod 2}} \mathscr{R}_M(\mathcal{Q}).\end{aligned}$$

Mais x possède N chiffres par hypothèse, ce qui implique $\#\mathscr{Q}_N \leq g\#\mathscr{Q}_N(x)$ et termine la démonstration. ∎

5.2. *Termes d'erreurs de $\mathscr{P}(x,a,q)$ et $\mathscr{Q}(x,a,q)$*

Lemme 18. *Si q est un entier premier avec g, alors pour tout x nous avons la majoration*

$$\sup_{y\leq x} \max_{a\in\mathbb{Z}} \left| \#\mathscr{P}(y,a,q) - \frac{\#\mathscr{P}(y)}{q} \right| \leq 2 \sup_{y\leq x} \max_{a\in\mathbb{Z}} \left| \#\mathscr{Q}(y,a,q) - \frac{\#\mathscr{Q}(y)}{q} \right|.$$

Démonstration. Un palindrome étant un pseudopalindrome ne se finissant pas par 0, nous avons

$$\mathscr{P} = \mathscr{Q} \setminus g\mathscr{Q}. \tag{5.7}$$

Donc

$$\#\mathscr{P}(y) = \#\mathscr{Q}(y) - \#\mathscr{Q}(y/g)$$

et en notant a' un entier tel que $ga' \equiv a \bmod q$,

$$\#\mathscr{P}(y,a,q) = \#\mathscr{Q}(y,a,q) - \#\mathscr{Q}(y/g,a',q).$$

Si $y \leq x$, nous avons donc

$$\begin{aligned}\left|\#\mathscr{P}(y,a,q) - \frac{\#\mathscr{P}(y)}{q}\right| &\\ \leq \left|\#\mathscr{Q}(y,a,q) - \frac{\#\mathscr{Q}(y)}{q}\right| &+ \left|\#\mathscr{Q}(y/g,a',q) - \frac{\#\mathscr{Q}(y/g)}{q}\right| \\ \leq 2\sup_{z\leq x}\max_{b\in\mathbb{Z}} &\left|\#\mathscr{Q}(z,b,q) - \frac{\#\mathscr{Q}(z)}{q}\right|.\end{aligned}$$

En prenant la borne supérieure en a puis en y, nous trouvons exactement la majoration du lemme. ∎

5.3. *Preuve du théorème 1.* Il suffit de réunir les résultats du corollaire 6 et du lemme 6 puisque

$$\mathscr{Q}(x) = \bigsqcup_{M\leq N} \mathscr{Q}_M(x) \quad \text{où} \quad N > \frac{\log x}{\log g}.$$

Cela démontre donc le théorème 1 pour $\mathscr{Q}$. Le lemme 18 finit la démonstration.

5.4. *Preuve du théorème 2.* Il suffit de réunir les résultats du corollaire 6 et du lemme 16 puisque

$$\mathscr{Q}(x) = \bigsqcup_{M\leq N} \mathscr{Q}_M(x) \quad \text{où} \quad N > \frac{\log x}{\log g}.$$

Cela démontre donc la première partie du théorème 2 pour $\mathscr{Q}$. Le lemme 18 finit la démonstration de (1.7), c'est-à-dire l'existence d'un exposant β. En utilisant les lemmes 7 et 8, nous vérifions que l'entier $m := 1/4\beta_g$ vérifie l'hypothèse (4.24) du lemme 16 où β_g est donné par

g	2	3	4	5	6	7	8	9	10
β_g	$\frac{1}{68}$	$\frac{1}{180}$	$\frac{1}{144}$	$\frac{1}{236}$	$\frac{1}{220}$	$\frac{1}{308}$	$\frac{1}{288}$	$\frac{1}{380}$	$\frac{1}{368}$

Donc β_g est un exposant de distribution. L'exposant $\beta \sim 1/6\pi g$ et les autres exposants β_g du théorème 2 seront obtenu dans le corollaire 7.

Pour prouver que la fraction β_g donnée par le tableau convient, il suffit donc juste de vérifier que si nous posons $m := 1/4\beta_g$, alors $m \geq 3$ est un entier qui réalise la condition (4.24). Faisons-le par exemple en détail pour $g = 10$. Pour cela, nous utilisons les lemmes 7 et 8 pour majorer $\mathcal{K}_{m/3}$. Ainsi,

$$\mathcal{K}_{m/3} \leq \mathcal{M}_{m/3} \leq \frac{1}{g}\sum_{-g/2\leq h\leq g/2}\left(1-\frac{h^2}{g^2}\right)^{m/3} < 0.31622 < 10^{-1/2}.$$

Nous pouvons donc choisir

$$\beta := -\frac{\log \mathcal{K}_{m/3}}{2m \log g} > -\frac{\log 0.31622}{2 \cdot 46 \log 10} > 0.0027174,$$

ce qui démontre le corollaire pour $g = 10$.

Si g est quelconque, nous utilisons directement la majoration du lemme 8 pour majorer $\mathcal{K}_{m/3}$. Nous devons donc trouver un entier $m \geq 3$ tel que

$$\frac{1}{g} + \sqrt{\frac{3\pi}{mc_3}} \leq \sqrt{\frac{1}{g}}, \quad \text{i.e.} \quad m \geq \frac{3\pi g}{c_3} (1 - g^{-1/2})^{-2},$$

et nous pouvons alors choisir l'exposant $\beta = 1/4m$. Le choix du plus petit entier supérieur à $\frac{3\pi g}{c_3}(1 - g^{-1/2})^{-2}$ pour m termine donc la preuve.

5.5. *Préparation au crible.* Nous établissons dans ce paragraphe une variante du théorème 2 plus adaptée aux méthodes de cribles : le lemme 22. Nous avons besoin d'étudier la répartition des palindromes ayant des facteurs en commun avec

$$g^3 - g = (g-1)g(g+1).$$

Comme nous le verrons, les diviseurs impairs de $g^2 - 1$ ne sont pas un vrai problème (quitte à distinguer l'étude de $\mathscr{P}^0$ et celle de $\mathscr{P}^1$), mais il en va tout autrement des diviseurs de $2g$: par exemple, si $q_g \mid g$, quand le premier chiffre x_0 de x n'est pas un multiple de q_g, il n'y a aucun pseudopalindrome divisible par q_g ayant x_0 pour premier chiffre.

Plutôt que d'étudier de nombreux cas différents, nous simplifions le résultat en remplaçant l'étude des palindromes par celle de $\widetilde{\mathscr{P}}$, défini dans le lemme 20.

Lemme 19. *Supposons g impair. Tout élément de $\mathscr{P}^0$ est pair. Tout élément de $\mathscr{P}^1$ est de même parité que son chiffre médian.*

Démonstration. Montrons que $\Phi_N(j)$ est pair pour tout $j \leq N$:

$$\Phi_N(j) \equiv 1^j + 1^{N-j} \equiv 0 \bmod 2.$$

Le lemme s'en déduit immédiatement. ∎

Lemme 20. *Posons*

$$\widetilde{\mathscr{P}^0} := \{n \in \mathscr{P}^0 : (n, g) = 1\}, \qquad \widetilde{\mathscr{P}^1} := \{n \in \mathscr{P}^1 : (n, 2g) = 1\},$$
$$\widetilde{\mathscr{P}} := \mathscr{P}^0 \cup \mathscr{P}^1.$$

Alors

$$\#\widetilde{\mathscr{P}^0}(x) \gg_g \#\mathscr{P}(x) \quad \textit{et} \quad \#\widetilde{\mathscr{P}^1}(x) \gg_g \#\mathscr{P}(x).$$

Démonstration. En utilisant la décomposition (1.1), il suffit de prouver qu'uniformément sur N, nous avons

$$\#\widetilde{\mathscr{P}}_N \gg_g \frac{\phi(g)}{g}\,\#\mathscr{P}_N, \tag{5.8}$$

en ayant noté $\widetilde{\mathscr{P}}_N$ les éléments de $\widetilde{\mathscr{P}}$ dont l'écriture dans la base g possède exactement N chiffres.

Supposons N pair. Soit $n \in \mathscr{P}_N$ que nous décomposons en

$$n = n_0\Phi_{N-1}(0) + g\widetilde{n} \quad \text{avec } \widetilde{n} \in \mathscr{Q}_{N-2}.$$

Alors

$$(n, g) = 1 \;\Leftrightarrow\; (n_0, g) = 1.$$

Il existe donc exactement $\phi(g)$ choix possibles pour n_0 et les autres chiffres de n peuvent être choisis arbitrairement, ce qui prouve (5.8).

Supposons N impair et notons $M := (N-1)/2$. Soit $n \in \mathscr{P}_N$ que nous décomposons en

$$n = n_0\Phi_{N-1}(0) + g\widetilde{n} + n_M g^M,$$

où $\widetilde{n}$ est un élément de $\mathscr{Q}_{N-2}$ dont le chiffre médian est 0. En utilisant le lemme 19, nous avons alors

$$(n, 2g) = 1 \;\Leftrightarrow\; (n_0, g) = 1 \text{ et } (n_M, 2) = 1.$$

Il existe donc exactement $\phi(g)$ choix possibles pour n_0, $\lceil (g-1)/2 \rceil$ choix pour n_M et les autres chiffres de n peuvent être choisis arbitrairement, ce qui prouve (5.8). ∎

Lemme 21. *Soit $r = l/q$ une fraction irréductible telle que q possède un facteur commun $q_1 \geq 3$ avec $g-1$. Pour tout entier $j \leq N$,*

$$\|\Phi_N(j)r\| \geq 1/q.$$

Soit $r = l/q$ une fraction irréductible telle que q possède un facteur commun $q_1 \geq 3$ avec $g+1$. Si N est pair, pour tout entier $j \leq N$,

$$\|\Phi_N(j)r\| \geq 1/q.$$

Démonstration. Pour la première minoration, réduisons $\Phi_N(j)$ modulo $g-1$:

$$\Phi_N(j) \equiv 1^j + 1^{N-j} \equiv 2 \bmod g-1.$$

Comme $q_1 \mid g-1$, nous avons donc

$$\Phi_N(j) \equiv 2 \bmod q_1.$$

L'hypothèse $q_1 \geq 3$ assure donc $\Phi_N(j) \neq 0 \bmod q_1$. Mais $q_1 \mid q$, donc $\Phi_N(j)r \notin \mathbb{Z}$ puisque $r = l/q$ est irréductible. La fraction $\Phi_N(j)r \notin \mathbb{Z}$ étant de dénominateur au plus q, nous avons bien $\|\Phi_N(j)r\| \geq 1/q$.

Pour la seconde minoration, nous procédons exactement de la même façon après avoir remarqué que

$$\begin{aligned}\Phi_N(j) &\equiv (-1)^j + (-1)^{N-j} \bmod g+1\\ &\equiv (-1)^j(1+(-1)^N) \bmod g+1\\ &\equiv (-1)^j 2 \bmod g+1\end{aligned}$$

puisque N est pair. ∎

LEMME 22. *Il existe deux fonctions multiplicatives ϱ_0 et ϱ_1 telles que*

$$\varrho_0(p) = \begin{cases} 1 & si\ (p, g(g+1)) = 1,\\ 0 & si\ p \mid g,\\ p & si\ p \mid g+1,\end{cases} \qquad \varrho_1(p) = \begin{cases} 1 & si\ (p, 2g) = 1,\\ 0 & si\ p \mid 2g,\end{cases}$$

et si β est l'exposant obtenu dans la preuve du théorème 2, alors

$$\sum_{\substack{q<x^{\beta-\varepsilon}\\ \mu^2(q)=1}} \left| \#\widetilde{\mathscr{P}}^k(x,0,q) - \frac{\varrho_k(q)}{q}\,\#\widetilde{\mathscr{P}}^k(x)\right| \ll_{g,\beta,\varepsilon,A} \frac{\#\widetilde{\mathscr{P}}^k(x)}{\log^A x}. \tag{5.9}$$

Démonstration. Traitons le cas particulier légèrement plus technique où g est impair (si g est pair, le module 2 est exclu directement puisque nous avons remplacé l'étude de $\mathscr{P}$ par celle de $\widetilde{\mathscr{P}}$) et où $k = 0$ (si $k = 1$, nous traitons les diviseurs de $g+1$ exactement comme nous traitons ici ceux de $g-1$). Si q est un entier premier avec g et sans facteur carré, nous définissons q_0 et q' par

$$q := q_0 q', \quad q_0 \mid g^2-1, \quad (g^2-1, q') = 1, \tag{5.10}$$

ces conditions déterminant q_0 et q' de façon unique. Nous décomposons ensuite q_0 en

$$q_0 := q_{g-1}q_{g+1}, \quad q_{g-1} \mid g-1, \quad q_{g+1} \mid g+1, \quad (q_{g-1}, 2) = 1, \tag{5.11}$$

ces conditions déterminant q_{g-1} et q_{g+1} de façon unique.

Tout d'abord, nous montrons que nous pouvons nous restreindre à l'étude des pseudopalindromes en adaptant la preuve du lemme 18. Comme

$$\widetilde{\mathscr{P}}_N = \bigsqcup_{(d,g)=1} (d\Phi_{N-1}(0) + g\mathscr{Q}_{N-2}),$$

pour tout $y \in \widetilde{\mathscr{P}}_N$ que nous décomposons en $y = y_0\Phi_{N-1}(0) + g\widetilde{y}$ avec $\widetilde{y} \in \mathscr{Q}_{N-2}$,

$$\#\widetilde{\mathscr{P}}_N(y) = \sum_{\substack{(d,g)=1\\ d<y_0}} \#\mathscr{Q}_{N-2} + \#\mathscr{Q}_{N-2}(\widetilde{y})$$

et, en notant g' un inverse de g modulo q,

$$\#\widetilde{\mathscr{P}}_N(y,a,q) = \sum_{\substack{(d,g)=1\\ d<y_0}} \#\mathscr{Q}_{N-2}(\infty, a - d\Phi_{N-1}(0)g', q) + \#\mathscr{Q}_{N-2}(\widetilde{y}, a - y_0\Phi_{N-1}(0)g', q).$$

Comme dans la preuve du lemme 18, nous en déduisons

$$\sup_{y\le x}\max_{a\in\mathbb{Z}}\left|\#\widetilde{\mathscr{P}}_N(y,a,q) - \frac{\varrho_0(q)}{q}\,\#\widetilde{\mathscr{P}}_N(y)\right| \le \phi(g)\sup_{z\le x}\max_{b\in\mathbb{Z}}\left|\#\mathscr{Q}_{N-2}(z,b,q) - \frac{\varrho_0(q)}{q}\,\#\mathscr{Q}_{N-2}(z)\right|. \tag{5.12}$$

Nous adaptons la preuve du lemme 17 en intégrant dans le terme général tous les diviseurs de $g+1$ puisque les lemmes 21 et 19 nous assurent qu'ils sont tous divisibles par q_{g+1} : le théorème chinois permet de remplacer l'équation (5.4) par

$$\#\mathscr{Q}_N(x,0,q) = \frac{1}{q}\sum_{l_{g+1}<q_{g+1}}\sum_{l<q_{g-1}q'}\sum_{n\in\mathscr{Q}_N(x)} \mathrm{e}\left(\frac{nl_{g+1}}{q_{g+1}} + \frac{nl}{q_{g-1}q'}\right) = \frac{q_{g+1}}{q}\sum_{l<q_{g-1}q'}\sum_{n\in\mathscr{Q}_N(x)} \mathrm{e}\left(\frac{nl}{q_{g-1}q'}\right).$$

En reprenant la démonstration du lemme 17, nous obtenons alors

$$\left|\#\mathscr{Q}_N(x,0,q) - \frac{\varrho_0(q)}{q}\,\#\mathscr{Q}_N(x)\right| \le \sum_{j<(N+1)/2} x_j \#\mathscr{Q}_{N-2j}\mathscr{R}_{N-2j}(q_{g-1}q') \tag{5.13}$$

avec les mêmes notations que dans le lemme 17 :

$$\mathscr{R}_N(d) := \frac{1}{d}\sum_{0<l<d}|G_N(l/d)|.$$

Il nous suffit donc de montrer que les majorations obtenues pour $\mathscr{R}_N(q)$ lorsque q est un entier premier avec g^3-g, restent valables lorsque nous supposons seulement que q est premier avec g^2+g et sans facteur carré. Comme $(q_{g-1}, q') = 1$, le théorème chinois permet d'écrire

$$\mathscr{R}_N(q) := \frac{1}{q}\sum_{0<l_{g-1}<q_{g-1}}\left|G_N\left(\frac{l_{g-1}}{q_{g-1}}\right)\right| + \frac{1}{q}\sum_{l_{g-1}<q_{g-1}}\sum_{0<l'<q'}\left|G_N\left(\frac{l_{g-1}}{q_{g-1}} + \frac{l'}{q'}\right)\right| =: \mathscr{S}_{g-1} + \mathscr{S}',$$

disons.

Commençons par majorer $\mathscr{S}'$, le terme correspondant à $l' \neq 0$. Nous utilisons le lemme 2, ce qui permet de faire disparaître la fraction l_{g-1}/q_{g-1} puisque $q_0 \mid g^2-1$:

$$\left|G_N\left(\frac{l_{g-1}}{q_{g-1}}+\frac{l'}{q'}\right)\right| \leq \left|\mathcal{G}_{(N-1)/2}\left((g^2-1)\left(\frac{l_{g-1}}{q_{g-1}}+\frac{l'}{q'}\right)\right)\right|^{1/3}$$
$$\leq \left|\mathcal{G}_{(N-1)/2}\left((g^2-1)\,\frac{l'}{q'}\right)\right|^{1/3}.$$

Le changement de variable $l=(g^2-1)l'$ laisse invariant modulo q' l'ensemble $\{0<l'<q'\}$ puisque $(g^2-1,q')=1$. Donc

$$\mathscr{S}' \leq \frac{q_{g-1}}{q}\sum_{0<l'<q'}\left|\mathcal{G}_{(N-1)/2}\left((g^2-1)\,\frac{l'}{q'}\right)\right|^{1/3}$$
$$=\frac{1}{q'}\sum_{0<l'<q'}\left|\mathcal{G}_{(N-1)/2}\left(\frac{l'}{q'}\right)\right|^{1/3}.$$

Nous pouvons utiliser maintenant les majorations du lemme 15 et terminer la majoration de $\mathscr{S}'$ comme nous avons prouvé le théorème 2.

Comme q_{g-1} est impair, nous pouvons utiliser le lemme 21 pour évaluer $\mathscr{S}_{g-1}$. La factorisation (2.2) fournit, pour $0<l_{g-1}<q_{g-1}$,

$$\left|G_N\left(\frac{l_{g-1}}{q_{g-1}}\right)\right| \ll_g \left(1-\frac{1}{q_{g-1}}\right)^N,$$

ce qui est suffisant pour terminer la preuve du lemme. ∎

5.6. *Preuve du théorème 3.* Commençons par nous souvenir que tout élément de $\mathscr{P}^0$ est divisible par $g+1$ donc n'aura aucune chance de vérifier le résultat du théorème. Nous allons donc travailler uniquement avec les éléments de $\mathscr{P}^1$ et en réalité seulement avec ceux de $\widetilde{\mathscr{P}^1}$ puisque les éléments de $\mathscr{P}^1 \setminus \widetilde{\mathscr{P}^1}$ sont exactement ceux possédant un facteur commun avec $2g$, donc en particulier, un petit facteur premier.

Soit $\varepsilon>0$ fixé. Si z est assez grand (par exemple dès que $z>g+1$), alors

$$\#\{n\in\mathscr{P}(x) : P^-(n)\geq z\} = \#\{n\in\mathscr{P}^1(x) : P^-(n)\geq z\}$$
$$= \#\{n\in\widetilde{\mathscr{P}^1}(x) : P^-(n)\geq z\}.$$

Nous appliquons le crible linéaire tel qu'énoncé dans le théorème de [Iwa80] avec la famille $\mathscr{A} := \widetilde{\mathscr{P}^1}$, $X := \#\widetilde{\mathscr{P}^1}$, $s := 2+\varepsilon$. Ainsi, si z est assez grand,

$$\#\{n \in \mathscr{P}^1(x) : P^-(n) \geq z\}$$
$$\geq \#\widetilde{\mathscr{P}^1} \prod_{p<z} \left(1 - \frac{\varrho_1(p)}{p}\right) f(2+\varepsilon)(1 + O(\log^{-1/3} z))$$
$$- \sum_{\substack{q<z^{2+\varepsilon} \\ \mu^2(q)=1}} \left| \#\widetilde{\mathscr{P}^1}(x,0,q) - \frac{\varrho_1(q)}{q} \#\widetilde{\mathscr{P}^1}(x) \right|.$$

Le lemme 20 permet de remplacer dans le membre de gauche le facteur $\#\widetilde{\mathscr{P}^1}(x)$ par $\#\mathscr{P}^1(x)$, la formule de Mertens permet de minorer le produit restant par $O_g(\log^{-1} z)$ et le lemme 22 de montrer que le terme d'erreur est négligeable puisque que

$$z^{2+\varepsilon} < x^{(2+\varepsilon)(\beta/2-\varepsilon)} < x^{\beta-\varepsilon},$$

ce qui montre que

$$\#\{n \in \mathscr{P}(x) : P^-(n) \geq z\} \asymp \frac{\#\mathscr{P}^1(x)}{\log z} \asymp \frac{\#\mathscr{P}(x)}{\log z}. \tag{5.14}$$

Le théorème 3 est donc prouvé.

5.7. *Optimalité de l'identité (1.6).* Nous pouvons nous demander s'il ne serait pas possible d'utiliser une autre identité que (1.6) dans laquelle les facteurs de $g-1$ ne sont pas artificiellement exclus. Nous allons démontrer que c'est effectivement impossible.

Soit $(P_j)_{j\leq J}$ une famille de polynômes telle qu'il existe un polynôme P vérifiant l'identité

$$\sum_{j\leq J} P_j(g)\Phi_N(k+j) = P(g)g^k.$$

En identifiant à gauche et à droite de l'égalité les coefficients dépendant de N et ceux n'en dépendant pas, nous devons donc avoir

$$\sum_{j\leq J} g^{J-j} P_j(g) = 0 \quad \text{et} \quad \sum_{j\leq J} g^j P_j(g) = P(g).$$

En calculant $P_J(g)$ à l'aide de la relation linéaire, nous avons

$$g^J P_J(g) = -\sum_{j<J} g^{2J-j} P_j(g).$$

En reportant cette estimation dans la seconde égalité, nous trouvons

$$\sum_{j<J} (g^j - g^{2J-j}) P_j(g) = P(g). \tag{5.15}$$

Le membre de gauche de (5.15) s'annulant pour $g=1$ et $g=-1$, le polynôme $P(g)$ est divisible par g^2-1. La relation (1.6) est donc optimale.

5.8. *Palindromes premiers et presque premiers : preuve des corollaires 1 et 2.* Pour le corollaire 1, nous utilisons le théorème 3 avec (par exemple)

$$z := x^{\beta/3}.$$

Si $n < x$ est un nombre premier, alors n vérifie l'une des deux propriétés

$$n < z \quad \text{ou} \quad P^-(n) \geq z.$$

Nous donc avons la majoration

$$\#\{n \in \mathscr{P}(x) : n \text{ premier}\} \leq z + \#\{n \in \mathscr{P}(x) : P^-(n) \geq z\} \ll_g z + \frac{\#\mathscr{P}(x)}{\log z}.$$

z est absorbé par le second terme puisque $\beta/3 < 1/2$, donc

$$\#\{n \in \mathscr{P}(x) : n \text{ premier}\} \ll_g \frac{\#\mathscr{P}(x)}{\log x},$$

ce qui termine la preuve du corollaire 1.

Pour le corollaire 2, il suffit de remarquer que les conditions $n < x$ et $P^-(n) \geq z$ impliquent la majoration $\Omega(n) < \log x/\log z$.

6. Amélioration de l'exposant de distribution : moyennes quadratiques de pseudopalindromes. Dans cette partie, nous améliorons l'exposant β trouvé dans la partie 5 en remarquant que le milieu d'un palindrome reste un palindrome. Nous introduisons un paramètre $0 < \eta < 1$ et nous notons alors $B(x)$ le produit des facteurs du bord de $G_N(x)$,

$$B(x) := \prod_{k<(1-\eta)N} U(\Phi_{N-1}(k)x), \tag{6.1}$$

et $C(x)$ le produit des facteurs centraux de $G_N(x)$,

$$C(x) := \prod_{(1-\eta)N\leq k\leq N/2} U(\Phi_{N-1}(k)x). \tag{6.2}$$

Lemme 23. *Soit c_3 une constante admissible pour le lemme 2. Pour tout entier m et tout réel $\eta \in [0,1]$, il existe un entier K tel que pour tout réel x,*

$$|G_N(x)| \leq |G_{\eta N}(g^K x)| \cdot |\mathcal{G}_{((1-\eta)N-1)/2}((g^2-1)x)|^{1/3}.$$

En particulier, si $\mathfrak{R}$ est un ensemble de points de $[0,1[$ sans répétition et stable par les multiplications par g^2-1 et g, alors

$$\sum_{r\in\mathfrak{R}} |G_N(r)| \leq \Big(\sum_{r\in\mathfrak{R}} |G_{\eta N}(r)|^2 \sum_{r\in\mathfrak{R}} |\mathcal{G}_\mu(r)|^{2m/3}\Big)^{1/2},$$

avec $\mu := ((1-\eta)N-1)/2m$.

Démonstration. Nous utilisons la factorisation (2.2) pour obtenir

$$|G_N(x)| \leq |C(x)|\,|B(x)|.$$

Nous majorons le terme du bord $B(x)$ de la même façon que dans le lemme 2. Ainsi

$$|B(x)| \leq |\mathcal{G}_{((1-\eta)N-1)/2}((g^2-1)x)|^{1/3}.$$

Pour le facteurs $C(x)$, nous pouvons suivre la démarche inverse de la démonstration du lemme 1 et nous reconnaissons donc que

$$C(x) = G_{\eta N}(g^K x),$$

K étant le plus grand entier inférieur à $(1-\eta)N/2$, ce qui termine la démonstration de la majoration de G_N.

Pour prouver le second point, nous commençons par utiliser l'inéglité de Cauchy–Schwarz

$$\sum_{r\in\mathfrak{R}} |G_N(r)| \leq \Big(\sum_{r\in\mathfrak{R}} |G_{\eta N}(g^K r)|^2 \sum_{r\in\mathfrak{R}} |\mathcal{G}_{((1-\eta)N-1)/2}((g^2-1)r)|^{2/3}\Big)^{1/2}.$$

Dans la première somme nous effectuons le changement de variable $r' = g^K r$. Nous majorons la seconde somme en suivant exactement la même démarche que dans la preuve du lemme 3. ∎

LEMME 24. *Soit α un entier pair. Uniformément pour tout μ assez grand et pour tout ensemble $\mathfrak{R}$ de points de $[\delta/2, 1-\delta/2]$ qui est δ bien espacé et stable modulo* 1 *par la multiplication par g, nous avons*

$$\sum_{r\in\mathfrak{R}} |G_\mu(r)|^\alpha \ll_{g,\alpha,\varepsilon} \delta^{-1}(K_\alpha+\varepsilon)^\mu + \delta^{-1-\log(K_\alpha+\varepsilon)/\log g}.$$

Pour $\alpha = 2$, nous avons la majoration

$$\sum_{r\in\mathfrak{R}} |G_\mu(r)|^2 \ll_g \delta^{-1} g^{-\mu/2} + \delta^{-1/2}.$$

Démonstration. Soit $\nu \leq \mu$ tel que $\lceil\nu\rceil$ et $\lceil\mu\rceil$ sont de même parité. Pour $K = \lfloor(\mu-\nu)/2\rfloor$ et pour tout réel x, nous avons

$$|G_\mu(x)| \leq \prod_{k<\mu/2} U(\Phi_{\mu-1}(k)x) \leq \prod_{K\leq k<\mu/2} U(\Phi_{\mu-1}(k)x) \leq |G_\nu(g^K x)|.$$

La multiplication par g laissant $\mathfrak{R}$ invariant, nous en déduisons la majoration

$$\sum_{r\in\mathfrak{R}} |G_\mu(r)|^\alpha \leq \sum_{r\in\mathfrak{R}} |G_\nu(r)|^\alpha. \tag{6.3}$$

Nous majorons cette somme exactement comme nous l'avons fait dans le lemme 13. Le lemme 14 de Sobolev–Gallagher fournit donc la majoration

$$\sum_{r\in\mathfrak{R}} |G_\mu(r)|^\alpha \leq \delta^{-1}\|G_\nu^\alpha\|_1 + \|(G_\nu^\alpha)'\|_1.$$

La même technique que celle déjà développée dans la preuve du lemme 13 donne alors

$$\sum_{r\in\mathfrak{R}} |G_\mu(r)|^\alpha \ll_{g,\alpha,\varepsilon} (\delta^{-1}+g^\nu)(K_\alpha+\varepsilon)^\nu,$$

par définition de K_α (la dérivée se majorant bien ainsi car α est un entier pair). Nous optimisons notre paramètre ν en choisissant

$$\nu := \min\left\{\mu, -\frac{\log\delta}{\log g}\right\} \quad \text{ou} \quad \min\left\{\mu, -\frac{\log\delta}{\log g}\right\} - 1$$

pour avoir $\lceil\nu\rceil$ et $\lceil\mu\rceil$ de même parité. Ainsi,

$$\sum_{r\in\mathfrak{R}} |G_\mu(r)|^\alpha \ll_{g,\alpha,\varepsilon} \delta^{-1}(K_\alpha+\varepsilon)^\mu + \delta^{-1}(K_\alpha+\varepsilon)^{-\log\delta/\log g},$$

ce qui termine la preuve de la première majoration. Le cas $\alpha = 2$ s'en déduit immédiatement puisqu'il est clair que

$$\|G_\mu^2\|_1 \ll_g g^{-\mu/2} \quad \text{et} \quad \|(G_\mu^2)'\|_1 \ll_g g^{\mu/2}.$$

La majoration est donc vraie pour $\varepsilon = 0$ avec $K_2 = g^{-1/2}$. ∎

Lemme 25. *Soient $m \geq 2$ un entier et $\varepsilon > 0$. Uniformément pour tout N assez grand et pour tout ensemble $\mathfrak{R}$ de points de $[\delta/2, 1-\delta/2]$ vérifiant l'hypothèse* (H_δ), *nous avons la majoration*

$$\sum_{r\in\mathfrak{R}} |G_N(r)| \ll_{g,m,\varepsilon} (\delta^{-1/2}g^{-N/(8m+4)} + \delta^{-1/4})\delta^{-1/2}(\mathcal{K}_\alpha+\varepsilon)^{N/(4m+2)}, \tag{6.4}$$

en ayant noté $\alpha := 2m/3$.

Démonstration. En réunissant les majorations des lemmes 23 et 24, nous obtenons, pour tout choix de $\eta \in [0,1]$ et tout entier $m \geq 2$,

$$\sum_{r\in\mathfrak{R}} |G_N(r)| \ll_{g,m,\varepsilon} (\delta^{-1/2}g^{-\eta N/4} + \delta^{-1/4})(\delta^{-1/2}(\mathcal{K}_\alpha+\varepsilon)^{\mu/2} + \delta^{-1/2-\frac{\log(\mathcal{K}_\alpha+\varepsilon)}{2\log g}})$$

en ayant noté

$$\alpha := \frac{2m}{3} \quad \text{et} \quad \mu := \frac{1-\eta}{2m}N. \tag{6.5}$$

Comme $m \geq 2$, nous avons bien $\alpha \geq 1$ et la majoration est donc licite. Nous optimisons notre paramètre η en choisissant

$$\eta := \frac{1}{2m+1} \quad \text{de sorte que} \quad \mu = \eta N. \tag{6.6}$$

Donc

$$\sum_{r\in\mathfrak{R}} |G_N(r)| \ll_{g,m,\varepsilon} (\delta^{-1/2}g^{-\eta N/4} + \delta^{-1/4})\delta^{-1/2}(\mathcal{K}_\alpha+\varepsilon)^{\mu/2},$$

ce qui démontre la majoration annoncée. ∎

LEMME 26. *Soient $m \geq 2$ un entier et $\varepsilon > 0$. Il existe une constante $c_8 > 0$ telle qu'uniformément pour Q et N assez grand, nous avons la majoration*

$$\sum_{\substack{q<Q\\(q,g^3-g)=1}} \sum_{0<l<q} |G_N(l/q)| \ll_{g,m,\varepsilon} Q^2 g^{-N/(8m+4)} (\mathcal{K}_\alpha + \varepsilon)^{N/(4m+2)} + Q^{3/2} (\mathcal{K}_\alpha + \varepsilon)^{N/(4m+2)} + Q e^{-c_8\sqrt{N}}, \tag{6.7}$$

en ayant noté $\alpha := 2m/3$.

Démonstration. Nous suivons la même démonstration que celle du lemme 15. Nous commençons par rendre les fractions irréductibles en isolant leur facteur commun d. Ainsi, pour le même choix du paramètre

$$D := gQ \exp(-c_7\sqrt{N})$$

que dans le lemme 15, nous avons la majoration

$$\sum_{\substack{q<Q\\(q,g^3-g)=1}} \sum_{0<l<q} |G_N(l/q)| \leq \sum_{d<D} \sum_{r\in\mathfrak{R}} |G_N(r)| + \sum_{D\leq d<Q} \sum_{r\in\mathfrak{R}} |G_N(r)|$$

pour l'ensemble

$$\mathfrak{R} := \{l/q : q < Q/q,\ (l,q) = 1,\ (q, g^3 - g) = 1\},$$

qui vérifie l'hypothèse (H_δ) pour $\delta = (Q/d)^{-2}$. Lorsque $d \geq D$, nous utilisons la même majoration que dans le lemme 15. Lorsque $d < D$, nous utilisons la majoration du lemme 25. Ainsi,

$$\sum_{\substack{q<Q\\(q,g^3-g)=1}} \sum_{0<l<q} |G_N(l/q)| \ll_{g,m,\varepsilon} \sum_{d<D} (Q/d)^2 g^{-N/(8m+4)} (\mathcal{K}_\alpha + \varepsilon)^{N/(4m+2)} + \sum_{d<D} (Q/d)^{3/2} (\mathcal{K}_\alpha + \varepsilon)^{N/(4m+2)} + \sum_{D\leq d<Q} e^{-c_8\sqrt{N}}.$$

En évaluant ces séries, nous avons donc

$$\sum_{\substack{q<Q\\(q,g^3-g)=1}} \sum_{0<l<q} |G_N(l/q)| \ll_{g,m,\varepsilon} Q^2 g^{-N/(8m+4)} (\mathcal{K}_\alpha + \varepsilon)^{N/(4m+2)} + Q^{3/2} (\mathcal{K}_\alpha + \varepsilon)^{N/(4m+2)} + Q e^{-c_8\sqrt{N}},$$

ce qui termine la preuve. ∎

COROLLAIRE 7. *Si $m \geq 2$ est un entier tel que*

$$\mathcal{K}_{2m/3} < g^{-1/2}, \tag{6.8}$$

alors

$$\beta := \left(\frac{1}{2} - \frac{\log \mathcal{K}_{2m/3}}{\log g}\right) \frac{1}{4m+2} > \frac{1}{4m+2}$$

est un exposant de distribution admissible pour $\mathscr{P}$. Pour toute base g, il existe donc un exposant de distribution admissible $\beta > \beta_g$, où β_g est donné par le tableau

g	2	3	4	5	6	7	8	9	10
β_g	$\frac{1}{38}$	$\frac{1}{98}$	$\frac{1}{74}$	$\frac{1}{122}$	$\frac{1}{114}$	$\frac{1}{158}$	$\frac{1}{150}$	$\frac{1}{194}$	$\frac{1}{186}$

et lorsque g est assez grand,

$$\beta = \frac{1 + o(1)}{6\pi g}.$$

Démonstration. L'exposant β se déduit du lemme 26 exactement comme nous avons trouvé le premier exposant de distribution. ∎

Corollaire 8. *Pour $g = 2$, il existe un exposant de distribution*

$$\beta > 0.03356 > \frac{1}{30}.$$

Pour $g = 3$, il existe un exposant de distribution

$$\beta > 0.01065 > \frac{1}{94}.$$

Démonstration. Pour $g = 2$, nous choisissons $m = 7$ dans le corollaire 7 puis nous majorons $\mathcal{K}_\alpha$ grâce au lemme 9. Pour $g = 3$, nous choisissons $m = 23$. En notant $\alpha := 2m/3$, nous avons,

$$\begin{aligned} \text{pour } g = 2 : &\quad \mathcal{K}_\alpha \le \mathcal{M}_\alpha^5 < 0.703763 < 2^{-1/2}, \\ \text{pour } g = 3 : &\quad \mathcal{K}_\alpha \le \mathcal{M}_\alpha^2 < 0.576562 < 3^{-1/2}, \end{aligned}$$

donc l'hypothèse du corollaire 7 est vérifiée, ce qui termine la preuve. ∎

Remarque 5. Pour $g = 2$, nous avons choisi $k = 5$ pour la majoration $\mathcal{K}_\alpha \le \mathcal{M}_\alpha^k$ du lemme 9, car c'est le plus petit entier permettant de choisir $m = 7$ dans le corollaire 7. Le nombre de termes à sommer dans la définition de $\mathcal{M}_\alpha^k$ étant proportionnel à g^k, les calculs dépassent très vite les capacités des machines actuelles, même s'ils sont réalisables en valeur exacte ($\mathcal{M}_\alpha^k$ ne fait intervenir que des nombres algébriques de degré au plus k). Il est à noter qu'il est impossible d'utiliser la valeur $m = 6$ dans le corollaire 7 même pour des entiers k beaucoup plus grands.

Références

[BHS04] W. D. Banks, D. N. Hart and M. Sakata, *Almost all palindromes are composite*, Math. Res. Lett. 11 (2004), 853–868.

[Colre] S. Col, *Diviseurs des nombres ellipséphiques*, Period. Math. Hungar., à paraître.

[DM01] C. Dartyge et C. Mauduit, *Ensembles de densité nulle contenant des entiers possédant au plus deux facteurs premiers*, J. Number Theory 91 (2001), 230–255.

[FM96] E. Fouvry et C. Mauduit, *Méthodes de crible et fonctions sommes des chiffres*, Acta Arith. 77 (1996), 339–351.

[Iwa80] H. Iwaniec, *Rosser's sieve*, ibid. 36 (1980), 171–202.

[Kon01] S. Konyagin, *Arithmetic properties of integers with missing digits: distribution in residue classes*, Period. Math. Hungar. 42 (2001), 145–162.

[MS97] C. Mauduit and A. Sárközy, *On the arithmetic structure of the integers whose sum of digits is fixed*, Acta Arith. 81 (1997), 145–173.

[Mon71] H. L. Montgomery, *Topics in Multiplicative Number Theory*, Lecture Notes in Math. 227, Springer, 1971.

Institut Élie Cartan Nancy (Mathématiques)
Université Henri Poincaré Nancy 1
B.P. 239
F-54506 Vandœuvre-lès-Nancy Cedex, France

Reçu le 15.6.2006 (5209)