ACTA ARITHMETICA
170.2 (2015)

Fonctions digitales le long des nombres premiers

par

Bruno Martin (Calais), Christian Mauduit (Marseille)
et Joël Rivat (Marseille)

1. Introduction. Dans tout cet article, q désigne un nombre entier supérieur ou égal à 2. Rappelons que tout entier strictement positif n admet un unique développement q-adique de la forme

$$n = \sum_{j=0}^{\nu} n_j q^j, \quad 0 \le n_j \le q-1,\ n_\nu \ge 1. \tag{1}$$

Pour $n = 0$, on convient de poser $\nu = 0$ et $n_0 = 0$. Conformément à l'usage, on désigne pour tout $0 \le k \le q-1$ par $|\cdot|_k$ la fonction comptant le nombre d'apparitions du chiffre k dans le développement en base q, soit

$$|n|_k = \#\{0 \le j \le \nu \mid n_j = k\}.$$

Dans la suite, nous notons $\mathcal{P}$ l'ensemble des nombres premiers et, pour tout nombre réel x, $\mathrm{e}(x) = \exp(2i\pi x)$, $\|x\|$ la distance de x à l'entier relatif le plus proche, $\pi(x)$ le nombre de nombres premiers inférieurs ou égaux à x, et pour tout $(a, m) \in \mathbb{Z} \times \mathbb{N}^*$, $\pi(x; a, m)$ le nombre de nombres premiers inférieurs ou égaux à x congrus à a modulo m. Enfin nous désignons par Λ la fonction de von Mangoldt définie pour tout nombre entier positif n par

$$\Lambda(n) = \begin{cases} \log p & \text{si } n = p^\ell \text{ avec } p \text{ premier et } \ell \ge 1, \\ 0 & \text{sinon,} \end{cases}$$

et par φ la fonction indicatrice d'Euler.

Afin de détecter les congruences nous utiliserons la relation d'orthogonalité classique : pour $m \in \mathbb{N}^*$ et $(a, b) \in \mathbb{Z}^2$, on a

$$\frac{1}{m} \sum_{j=0}^{m-1} \mathrm{e}\left(\frac{j(a-b)}{m}\right) = \begin{cases} 1 & \text{si } a \equiv b \bmod m, \\ 0 & \text{sinon.} \end{cases} \tag{2}$$

2010 *Mathematics Subject Classification*: 11A63, 11B85, 11N05.
Key words and phrases: prime numbers, exponential sums, digital functions.

DOI: 10.4064/aa170-2-5

Si f est une fonction à valeurs complexes et g une fonction à valeurs réelles strictement positives, la notation $f \ll g$ signifie que le rapport $|f|/g$ est borné.

Toutes les constantes, implicites ou explicites, intervenant dans cet article peuvent dépendre de la base de numération q.

1.1. Fonctions q-additives et fonctions digitales. La notion de *fonction q-additive* a été introduite indépendamment par Bellman et Shapiro [2] et Gelfond [12]. Il s'agit des fonctions $f : \mathbb{N} \to \mathbb{R}$ qui vérifient, pour tout $(a, b, j) \in \mathbb{N}^3$ tel que $0 \le b < q^j$,

$$f(aq^j + b) = f(aq^j) + f(b).$$

Une fonction q-additive vérifie donc nécessairement $f(0) = 0$. Lorsque l'on a de plus $f(aq^j) = f(a)$ pour tout $(a, j) \in \mathbb{N}^2$ on dit que la fonction f est *fortement q-additive*. Si f est fortement q-additive alors on a, pour tout nombre entier positif n vérifiant (1),

$$f\Big(\sum_{0\le j\le \nu} n_j q^j\Big) = \sum_{0\le j\le \nu} f(n_j) = \sum_{1\le k<q} f(k)|n|_k, \tag{3}$$

de sorte que f est complètement déterminée par ses valeurs $f(k)$ pour $1 \le k < q$. Réciproquement, toute fonction de la forme $f(n) = \sum_{1\le k<q} \alpha_k |n|_k$ est fortement q-additive. Par contre on remarquera que la fonction $|\cdot|_0$ n'est pas fortement q-additive.

Notation 1. On note $\mathcal{F}$ l'ensemble des fonctions $f : \mathbb{N} \to \mathbb{R}$ définies pour tout nombre entier positif n par

$$f(n) = \sum_{0\le k<q} \alpha_k |n|_k, \tag{4}$$

avec $(\alpha_0, \alpha_1, \ldots, \alpha_{q-1}) \in \mathbb{R}^q$.

Drmota et Mauduit ont étudié dans [9] certaines propriétés statistiques de ces fonctions, appelées *fonctions digitales*, et l'objet de ce travail est de montrer comment les résultats obtenus dans [17] permettent d'étudier les propriétés statistiques de la restriction de ces fonctions à l'ensemble des nombres premiers.

1.2. Recherche de nombres premiers dans une suite automatique. Les théorèmes 3 et 5 présentés dans le paragraphe 6 concernent la recherche de nombres premiers dans une suite reconnaissable par un q-automate fini (voir [10, chapitre 5] pour cette notion). En effet il est facile de vérifier que lorsque g est une fonction digitale à valeurs entières alors, pour tous nombres entiers $a \in \mathbb{Z}$ et $m \ge 2$, la suite formée des nombres entiers n tels que $g(n) \equiv a \bmod m$ est reconnaissable par un q-automate fini. Lorsque g est la fonction somme des chiffres, ce problème a été entièrement

résolu par Mauduit et Rivat dans [19], répondant ainsi à une question due à Gelfond [12]. Ils ont donné dans [20] une méthode assez générale permettant de traiter le cas des automates de Rudin–Shapiro généralisés, et Drmota a montré dans [8] que cette méthode permet de traiter le cas d'une famille assez large d'automates finis (automates inversibles).

La recherche de nombres premiers dans une suite reconnaissable par un q-automate fini quelconque est un problème en général extrêmement difficile. Par exemple les suites $(2^n+1)_{n\in\mathbb{N}}$ et $(2^n-1)_{n\in\mathbb{N}}$ sont chacune reconnaissable par un 2-automate fini et les problèmes associés correspondent respectivement à la recherche de nombres premiers de Fermat et de Mersenne. Lorsque $\mathbf{u}$ est une suite reconnaissable par un q-automate fini irréductible (c'est-à-dire dont le graphe est fortement connexe) il résulte d'une remarque de Fouvry et Mauduit [11] que la suite $\mathbf{u}$ contient une infinité de nombres presque premiers. Mais le problème de la recherche de nombres presque premiers dans une suite automatique quelconque est lui aussi largement ouvert (voir [4], [5] et [3] pour le cas particulier des nombres ellipséphiques).

2. Résultats. Dans [17], nous avons étudié les sommes d'exponentielles le long des nombres premiers associées aux fonctions digitales. Nous reformulons les théorèmes 1 et 2 de [17] sous la forme suivante ([1]).

THÉORÈME A. *Il existe $c_0>0$ tel que l'on a, uniformément pour tout q-uplet $(\alpha_0,\dots,\alpha_{q-1})\in\mathbb{R}^q$, $f=\sum_{0\le k<q}\alpha_k|\cdot|_k$, et pour tous $x\ge 2$, $\beta\in\mathbb{R}$,*

$$\sum_{n\le x}\Lambda(n)\,\mathrm{e}(f(n)+\beta n)\ll(\log x)^4 x^{1-c_0\|(q-1)(\alpha_1-\alpha_0)\|^2} \tag{5}$$

et

$$\sum_{n\le x}\Lambda(n)\,\mathrm{e}(f(n)+\beta n)\ll(\log x)^4 x^{1-c_0\sigma_q(f)}, \tag{6}$$

où

$$\sigma_q(f)=\min_{t\in\mathbb{R}}\sum_{0\le j<i<q}\|\alpha_i-\alpha_j-(i-j)t\|^2.$$

Signalons que la constante c_0, qui dépend de q, peut être explicitée en reprenant les démonstrations des théorèmes 1 et 2 de [17].

Dans cet article, nous étudions la répartition sur $\mathcal{P}$ des fonctions digitales à valeurs entières, c'est-à-dire des fonctions $g:\mathbb{N}\to\mathbb{Z}$ de la forme

$$g(n)=\sum_{0\le k<q}a_k|n|_k,$$

() ([1]) Le théorème 1 de [17] n'est énoncé que pour des fonctions digitales appartenant à une certaine sous-classe $\mathcal{F}_0$ de $\mathcal{F}$. Un examen de la preuve de ce théorème permet de constater que cette restriction n'est pas nécessaire.

avec $(a_0, \dots, a_{q-1}) \in \mathbb{Z}^q$. Il est difficile de fournir des énoncés tout à la fois directement utilisables et valables en toute généralité pour de telles fonctions. Aussi allons-nous concentrer notre étude sur la classe $\mathcal{F}^+$ des fonctions digitales à valeurs entières vérifiant les conditions

$$a_0 = 0 \quad \text{et} \quad \operatorname{pgcd}(a_1, \dots, a_{q-1}) = 1. \tag{7}$$

(Nous convenons maintenant et dans la suite que le pgcd d'un seul nombre entier a est égal à $|a|$.) Ce faisant nous ne restreignons pas la généralité car il est toujours possible de déduire le comportement d'une fonction digitale à valeurs entières de celui d'une fonction de $\mathcal{F}^+$. Nous illustrerons ce propos dans le paragraphe 6.4 et discuterons certains exemples dans le cas de l'étude de la répartition des valeurs de $(g(p))_{p\in\mathcal{P}}$ dans les progressions arithmétiques.

Soit $g = \sum_{1\le k<q} a_k|\cdot|_k \in \mathcal{F}^+$, $(\alpha, \beta) \in \mathbb{R}^2$. Dans ce cas particulier, le théorème A fournit une majoration non triviale de

$$\sum_{n\le x} \Lambda(n) e(\alpha g(n) + \beta n)$$

si et seulement si

$$\sigma_q(\alpha g) + \|(q-1)a_1\alpha\|^2 > 0. \tag{C}$$

Le lemme 1 de [17] montre que la condition (C) est équivalente à la condition

> *les nombres* $0, \alpha a_1, \dots, \alpha a_{q-1}$ *ne constituent pas une progression arithmétique modulo* 1 *dont la raison est un multiple entier de* $1/(q-1)$.

Ces deux conditions équivalentes sont peu maniables et notre premier objectif dans ce travail est d'obtenir une condition équivalente qui l'est davantage. À cet effet nous introduisons la quantité suivante.

Définition 1. Si $g \in \mathcal{F}^+$, on appelle *entier caractéristique de* g le nombre

$$d_g = \operatorname{pgcd}(a_2 - 2a_1, \dots, a_{q-1} - (q-1)a_1, q-1). \tag{8}$$

En particulier pour tout $k \in \{1, \dots, n\}$,

$$a_k \equiv k a_1 \bmod d_g, \tag{9}$$

ce qui par q-additivité de g entraîne que pour tout $n \in \mathbb{N}$,

$$g(n) \equiv g(1)n \bmod d_g.$$

Remarquons que, d'après la condition (7), on a

$$\operatorname{pgcd}(g(1), d_g) = \operatorname{pgcd}(a_1, d_g) = 1. \tag{10}$$

Lemme 1. *Pour* $g = \sum_{1\le k<q} a_k|\cdot|_k \in \mathcal{F}^+$ *et* $\alpha \in \mathbb{R}$, *on a l'équivalence*

$$\text{(C)} \ \Leftrightarrow \ d_g\alpha \notin \mathbb{Z}. \tag{11}$$

Pour $g \in \mathcal{F}_+$, nous introduisons la quantité

$$\kappa_g = d_g^2\Big(((q-1)a_1)^2 + \sum_{2\le k<q} (a_k - ka_1)^2\Big)^{-1}. \tag{12}$$

Remarquons que κ_g est strictement positive puisque g est non nulle. Nous définissons également la constante

$$c_1 = \frac{1}{(q-1)((q-1)^2+1)} \min\left(\frac{c_0}{2}, \frac{1}{2}\left(\frac{1}{4} + \frac{q(q-1)}{8}\right)^{-1}\right) > 0. \tag{13}$$

Dans le paragraphe 4 nous démontrons le théorème suivant, dont l'intérêt est de fournir une majoration dont l'exposant de x est complètement explicite en fonction de α, ce qui nous permettra d'obtenir plusieurs applications arithmétiques.

THÉORÈME 1. *Pour $g \in \mathcal{F}^+$, $(\alpha, \beta) \in \mathbb{R}^2$, $x \ge 2$, on a*

$$\sum_{p\le x} \mathrm{e}(\alpha g(p) + \beta p) \ll (\log x)^3 x^{1-c_1\kappa_g \|d_g\alpha\|^2}, \tag{14}$$

où la constante implicite ne dépend que de q.

REMARQUE 1. Le lemme 1 garantit que le théorème 1 résume à lui seul l'information qualitative contenue dans les deux estimations du théorème A.

2.1. Propriétés statistiques de suites arithmétiques. De nombreux travaux concernent l'étude des propriétés statistiques des suites de nombres entiers $\mathbf{u} = (u_n)_{n\in\mathbb{N}}$ définie par un algorithme « simple » (cf. [23]). En particulier l'étude précise des sommes d'exponentielles associées à ces suites permet d'étudier la répartition modulo 1 de la suite $(u_n\alpha)_{n\in\mathbb{N}}$ lorsque $\alpha \in \mathbb{R}\setminus\mathbb{Q}$ ainsi que la répartition dans les progressions arithmétiques de la suite $\mathbf{u}$ (voir par exemple [18] pour le cas des suites reconnaissables par un q-automate fini). Dans ce travail nous nous intéressons à l'étude beaucoup plus délicate des propriétés statistiques des suites extraites le long des nombres premiers d'une telle suite $\mathbf{u}$. Lorsque $u_n = n$ la répartition dans les progressions arithmétiques de la suite $(p)_{p\in\mathcal{P}}$ a été étudiée par Hadamard et de la Vallée Poussin dans [13] et [7], et la répartition modulo 1 de la suite $(\alpha p)_{p\in\mathcal{P}}$ pour $\alpha \in \mathbb{R}\setminus\mathbb{Q}$ par Vinogradov dans [24] (voir également [1, théorème 9.12] et [15, théorème 21.3]) :

THÉORÈME B (Hadamard et de la Vallée Poussin). *Si $(a,m) \in \mathbb{Z}\times\mathbb{N}^*$ vérifie $(a,m) = 1$, alors*

$$\pi(x; a, m) \sim \frac{1}{\varphi(m)} \cdot \frac{x}{\log x}.$$

THÉORÈME C (Vinogradov). *Si $\alpha \in \mathbb{R}\setminus\mathbb{Q}$ alors la suite $(\alpha p)_{p\in\mathcal{P}}$ est équirépartie modulo* 1.

Dans le paragraphe 5 nous étudions l'équipartition modulo 1 de la suite $(\alpha g(p))_{p\in\mathcal{P}}$ et nous généralisons le théorème 2 de [19].

L'objet du paragraphe 6.1 est d'étudier, pour $b \in \mathbb{Z}$, $m \in \mathbb{N}^*$, $g \in \mathcal{F}^+$, le comportement asymptotique de la quantité $\operatorname{card}\{p \le x \mid g(p) \equiv b \bmod m\}$ lorsque $x \to \infty$, et donc de généraliser le théorème 3 de [19]. Dans les paragraphes 6.2 et 6.3 nous généralisons les théorèmes B et C au cas de la suite $\mathbf{u}$ constituée des nombres entiers n tels que $g(n) \equiv b \bmod m$, où $g \in \mathcal{F}^+$. Dans le paragraphe 6.4 nous expliquons comment l'étude de la répartition d'une fonction digitale à valeurs entières quelconque dans les progressions arithmétiques se ramène au cas des fonctions de $\mathcal{F}^+$.

2.2. Problème de Goldbach ternaire. Vinogradov a démontré le théorème suivant, qui implique que tout entier impair assez grand est la somme de trois nombres premiers (voir [24] ou [6, chapitre 26]).

Théorème D (Vinogradov). *Pour tout réel $A > 0$ et tout entier $N \ge 2$, on a*

$$R(N) := \sum_{\substack{n_1,n_2,n_3\\ n_1+n_2+n_3=N}} \Lambda(n_1)\Lambda(n_2)\Lambda(n_3) = \frac{1}{2}\mathfrak{S}(N)N^2 + O_A\left(\frac{N^2}{(\log N)^A}\right)$$

avec

$$\mathfrak{S}(N) = \prod_{p\mid N}\left(1-\frac{1}{(p-1)^2}\right)\prod_{p\nmid N}\left(1-\frac{1}{(p-1)^3}\right).$$

Lorsque N est un entier impair, on a $\mathfrak{S}(N) \gg 1$, de sorte que $R(N) \gg N^2$ pour tout entier N impair suffisamment grand.

L'objet du paragraphe 7 est de généraliser le théorème D en imposant des conditions digitales aux entiers n_1, n_2 et n_3.

3. Preuve du lemme 1. Posons $d = d_g$ et supposons tout d'abord que $d\alpha$ est un nombre entier. En multipliant la relation (9) par α, nous obtenons directement que $0, \alpha a_1, \dots, \alpha a_{q-1}$ constituent une suite arithmétique modulo 1 de raison $a_1\alpha$. Comme $d\alpha \in \mathbb{Z}$ et $d \mid q-1$, nous avons $(q-1)a_1\alpha \in \mathbb{Z}$.

Supposons réciproquement qu'il existe $\ell \in \mathbb{Z}$ tel que pour tout $k \in \{1, \dots, q-1\}$,

$$\alpha a_k = k\frac{\ell}{q-1} \bmod 1.$$

Cela entraîne que $\alpha \in \mathbb{Q}$. Posons $\alpha = r/s$ avec $\operatorname{pgcd}(r,s) = 1$. On a donc pour tout $k \in \{1, \dots, q-1\}$,

$$\frac{r}{s}a_k = k\frac{\ell}{q-1} \bmod 1. \tag{15}$$

En multipliant (15) par s, on obtient $s \mid (q-1)ra_k$, et il résulte du lemme de Gauss que pour tout $k \in \{1, \dots, n\}$,

$$s \mid a_k(q-1). \tag{16}$$

La condition $\operatorname{pgcd}(a_1, \dots, a_k) = 1$ entraîne, d'après le théorème de Bézout, l'existence d'un uplet $(u_1, \dots, u_{q-1}) \in \mathbb{Z}^{q-1}$ tel que

$$a_1u_1 + \cdots + a_{q-1}u_{q-1} = 1, \tag{17}$$

Nous déduisons directement de (17) et (16) que s divise $q-1$. La relation (15) prise pour $k = 1$ montre que $(q-1)/s$ divise ℓ. Il existe donc $t \in \mathbb{Z}$ tel que $\ell = t(q-1)/s$. En insérant cette identité dans (15) et en multipliant par s, nous obtenons

$$ra_k \equiv kt \bmod s.$$

Et comme $\operatorname{pgcd}(r, s) = 1$, il suit

$$a_k \equiv kt' \bmod s,$$

avec $t' \in \mathbb{Z}$. Nous en déduisons que pour tout $k \in \{1, \dots, q-1\}$,

$$a_k \equiv ka_1 \bmod s.$$

En conséquence s divise $a_k - ka_1$ pour tout $k \in \{1, \dots, q-1\}$. Comme de plus s divise $q-1$, s divise d. Finalement $d\alpha = dr/s$ appartient à $\mathbb{Z}$.

Remarque 2. Le lemme 5 établi dans le paragraphe 4 fournit directement une autre démonstration de l'implication $d_g\alpha \notin \mathbb{Z} \Rightarrow$ (C) du lemme 1.

4. Preuve du théorème 1. La proposition suivante est une conséquence rapide du théorème A.

Proposition 1. *Pour* $g = \sum_{1 \le k < q} a_k |\cdot|_k$ *avec* $(a_1, \dots, a_{q-1}) \in \mathbb{Z}^{q-1}$, $(\alpha, \beta) \in \mathbb{R}^2$, $x \ge 2$, *on a*

$$\sum_{p \le x} \mathrm{e}(\alpha g(p) + \beta p) \ll (\log x)^3 x^{1 - c_2 \tau_q(\alpha, g)} \tag{18}$$

avec

$$\tau_q(\alpha, g) = \sigma_q(\alpha g) + \|(q-1)a_1\alpha\|^2, \tag{19}$$

et

$$c_2 = \min\left(\frac{c_0}{2}, \frac{1}{2}\left(\frac{1}{4} + \frac{q(q-1)}{8}\right)^{-1}\right).$$

La constante implicite dans (18) *ne dépend que de* q.

Démonstration. On applique le théorème A pour $f = \alpha g$, ce qui donne pour $(\alpha, \beta) \in \mathbb{R}^2$,

$$\sum_{n\le x} \Lambda(n)\,\mathrm{e}(\alpha g(n) + \beta n) \ll (\log x)^4 x^{1-c_0\|(q-1)a_1\alpha\|^2},$$
$$\sum_{n\le x} \Lambda(n)\,\mathrm{e}(\alpha g(n) + \beta n) \ll (\log x)^4 x^{1-c_0\sigma_q(\alpha g)}.$$

Nous déduisons de ces deux majorations que

$$\begin{aligned}\sum_{n\le x} \Lambda(n)\,\mathrm{e}(\alpha g(n) + \beta n) &\ll (\log x)^4 x^{1-c_0(\sigma_q(\alpha g)+\|(q-1)a_1\alpha\|^2)/2}\\ &\ll (\log x)^4 x^{1-c_2(\sigma_q(\alpha g)+\|(q-1)a_1\alpha\|^2)}.\end{aligned}$$

Notons que

$$c_2\big(\sigma_q(\alpha g) + \|(q-1)a_1\alpha\|^2\big) \le 1/2,$$

puisque $\|(q-1)a_1\alpha\|^2 \le 1/4$ et $\sigma_q(\alpha g) \le q(q-1)/8$. Maintenant une intégration par parties standard fournit la majoration

$$\begin{aligned}\sum_{p\le x} \mathrm{e}(\alpha g(p) + \beta p) &\ll \frac{1}{\log x}\max_{t\le x}\Big|\sum_{n\le t} \Lambda(n)\,\mathrm{e}(\alpha g(n) + \beta n)\Big| + \sqrt{x}\\ &\ll (\log x)^3 x^{1-c_2(\sigma_q(\alpha g)+\|(q-1)a_1\alpha\|^2)} + \sqrt{x}\\ &\ll (\log x)^3 x^{1-c_2(\sigma_q(\alpha g)+\|(q-1)a_1\alpha\|^2)},\end{aligned}$$

ce qui correspond au résultat souhaité. ∎

La suite de cette section consiste à montrer que pour $g \in \mathcal{F}^+$,

$$\tau_q(\alpha, g) \ge \frac{1}{(q-1)((q-1)^2+1)}\kappa_g\|d_g\alpha\|^2. \tag{20}$$

Compte tenu de (18), cela fournira directement le théorème 1.

Nous aurons besoin d'un raffinement du lemme de Bézout.

Lemme 2. *Pour $n \in \mathbb{N}$, $n \ge 2$ et $(b_1, \dots, b_n) \in \mathbb{Z}^n$, il existe $(k_1, \dots, k_n) \in \mathbb{Z}^n$ tel que*

$$\begin{cases} k_1b_1 + \cdots + k_nb_n = \mathrm{pgcd}(b_1, \dots, b_n),\\ k_1^2 + \cdots + k_n^2 \le \dfrac{|b_1|^2 + \cdots + |b_n|^2}{\mathrm{pgcd}(b_1, \dots, b_n)^2}.\end{cases}$$

Démonstration. Ce résultat est certainement classique mais en l'absence de référence nous en donnons une preuve directe. On peut supposer que $\mathrm{pgcd}(b_1, \dots, b_n) = 1$ et $1 \le b_1 \le \cdots \le b_n$. Le théorème de Bézout fournit l'existence de $(k_1, \dots, k_n) \in \mathbb{Z}^n$ tel que $k_1b_1 + \cdots + k_nb_n = 1$. Dans la suite de cette démonstration nous notons $\langle \cdot \,|\, \cdot \rangle$ le produit scalaire canonique de $\mathbb{R}^n$, $\|\cdot\|_2$ la norme euclidienne associée et $(\mathbf{e}_j)_{1\le j\le n}$ les vecteurs de la base canonique de $\mathbb{R}^n$. Pour $1 \le j \le n-1$ posons $\mathbf{u}_j = b_{j+1}\mathbf{e}_j - b_j\mathbf{e}_{j+1}$. Notons P le

projeté orthogonal de l'origine O de $\mathbb{R}^n$ sur l'hyperplan affine H passant par $M_0 = (k_1, \dots, k_n)$ et de direction $V = \{(x_1, \dots, x_n) \in \mathbb{R}^n \mid b_1x_1 + \cdots + b_nx_n = 0\} = \mathrm{Vect}\,(\mathbf{u}_j)_{1\le j\le n-1}$. Il existe $(\ell_1, \dots, \ell_{n-1}) \in \mathbb{Z}^{n-1}$ et $(\varepsilon_1, \dots, \varepsilon_{n-1}) \in [-1/2, 1/2]^{n-1}$ tels que

$$\overrightarrow{M_0P} = (\ell_1 + \varepsilon_1)\mathbf{u}_1 + \cdots + (\ell_{n-1} + \varepsilon_{n-1})\mathbf{u}_{n-1}.$$

Le point M défini par $\overrightarrow{M_0M} = \ell_1\mathbf{u}_1 + \cdots + \ell_{n-1}\mathbf{u}_{n-1}$ a des coordonnées $(m_1, \dots, m_n) \in \mathbb{Z}^n$ vérifiant $m_1b_1 + \cdots + m_nb_n = 1$. On a $\|\overrightarrow{MP}\|_2^2 = \sum_{j=1}^{n-1} \varepsilon_j^2\|\mathbf{u}_j\|_2^2 + 2\sum_{j=1}^{n-2} \varepsilon_j\varepsilon_{j+1}\langle \mathbf{u}_j \mid \mathbf{u}_{j+1}\rangle$ donc

$$\|\overrightarrow{MP}\|_2^2 \le \frac{1}{4}\sum_{j=1}^{n-1}(b_j^2 + b_{j+1}^2) + \frac{1}{4}\sum_{j=1}^{n-2} 2b_jb_{j+2} \le \sum_{j=1}^{n} b_j^2 - \frac{1}{4}(b_1^2 + b_n^2)$$

(car $2b_jb_{j+2} \le b_j^2 + b_{j+2}^2$). Comme $\|\overrightarrow{OM}\|_2^2 = \|\overrightarrow{OP}\|_2^2 + \|\overrightarrow{MP}\|_2^2$, on obtient

$$\sum_{j=1}^{n} m_j^2 \le \Big(\sum_{j=1}^{n} b_j^2\Big)^{-1} + \sum_{j=1}^{n} b_j^2 - \frac{1}{4}(b_1^2 + b_n^2) \le \sum_{j=1}^{n} b_j^2,$$

la dernière inégalité résultant du fait que $\sum_{j=1}^{n} b_j^2 \ge 2$ et $b_1^2 + b_n^2 \ge 2$. ∎

Rappelons que la fonction $x \mapsto \|x\|$, qui à tout nombre réel x associe la distance de x à l'entier relatif le plus proche, vérifie pour tout $(u, v) \in \mathbb{R}^2$,

$$\|u + v\| \le \|u\| + \|v\|, \tag{21}$$

et que l'on peut en déduire par récurrence que pour tous $u \in \mathbb{R}$ et $k \in \mathbb{Z}$,

$$\|ku\| \le |k|\,\|u\|. \tag{22}$$

Nous aurons également besoin des inégalités suivantes.

Lemme 3.

(i) *Pour $n \in \mathbb{N}^*$, $(k_1, \dots, k_n) \in \mathbb{Z}^n$, et $(u_1, \dots, u_n) \in \mathbb{R}^n$, on a*

$$\Big\|\sum_{j=1}^{n} k_ju_j\Big\|^2 \le \Big(\sum_{j=1}^{n} k_j^2\Big)\Big(\sum_{j=1}^{n} \|u_j\|^2\Big). \tag{23}$$

(ii) *Pour $n \in \mathbb{N}$, $n \ge 2$, $(b_1, \dots, b_n) \in \mathbb{Z}^n \setminus \{(0, \dots, 0)\}$, et $\alpha \in \mathbb{R}$, on a*

$$\sum_{k=1}^{n} \|b_k\alpha\|^2 \ge \Big(\sum_{j=1}^{n} b_j^2\Big)^{-1} \mathrm{pgcd}(b_1, \dots, b_n)^2\|\mathrm{pgcd}(b_1, \dots, b_n)\alpha\|^2. \tag{24}$$

Démonstration. (i) Les inégalités (21) et (22) permettent d'écrire

$$\Big\|\sum_{j=1}^{n} k_ju_j\Big\| \le \sum_{j=1}^{n} |k_j|\,\|u_j\|,$$

et l'inégalité de Cauchy–Schwarz donne (23).

(ii) D'après le lemme 2, il existe $(k_1, \dots, k_n) \in \mathbb{Z}^n$ tel que

$$k_1 b_1 + \cdots + k_n b_n = \operatorname{pgcd}(b_1, \dots, b_n).$$

et

$$\sum_{j=1}^{n} k_j^2 \le \frac{1}{\operatorname{pgcd}(b_1, \dots, b_n)^2} \sum_{j=1}^{n} b_j^2. \tag{25}$$

L'inégalité (23) avec $u_j = \alpha b_j$ et l'inégalité (25) conduisent bien à (24). ∎

Nous donnons à présent une minoration de la quantité $\sigma_q(f)$.

LEMME 4. *Pour* $(\alpha_0, \dots, \alpha_{q-1}) \in \mathbb{R}^q$, $f = \sum_{0 \le k < q} \alpha_k |\cdot|_k$, *on a*

$$\sigma_q(f) \ge \frac{1}{(q-1)((q-1)^2+1)} \sum_{2 \le k < q} \|\alpha_k - \alpha_0 - k(\alpha_1 - \alpha_0)\|^2.$$

Démonstration. Si $q = 2$, la minoration est triviale. On peut donc supposer $q \ge 3$. Soit t_0 un nombre réel pour lequel

$$\sigma_q(f) = \sum_{0 \le j < i < q} \|\alpha_i - \alpha_j - (i-j)t_0\|^2.$$

On a par conséquent

$$\begin{aligned}\sigma_q(f) &\ge \sum_{2 \le k < q} \|\alpha_k - \alpha_0 - kt_0\|^2 + \|\alpha_1 - \alpha_0 - t_0\|^2 \\ &\ge \frac{1}{q-1} \sum_{2 \le k < q} (\|\alpha_k - \alpha_0 - kt_0\|^2 + \|\alpha_1 - \alpha_0 - t_0\|^2).\end{aligned}$$

En employant, pour chaque valeur de $k \in \{2, \dots, q-1\}$, l'inégalité (23) avec $n = 2$, $u_1 = \alpha_k - \alpha_0 - kt_0$, $u_2 = \alpha_1 - \alpha_0 - t_0$, $k_1 = 1$, $k_2 = -k$, on aboutit à

$$\sigma_q(f) \ge \frac{1}{q-1} \sum_{2 \le k < q} \frac{\|\alpha_k - \alpha_0 - k(\alpha_1 - \alpha_0)\|^2}{k^2+1},$$

ce qui permet directement de conclure. ∎

Nous sommes maintenant en mesure d'établir l'inégalité (20).

LEMME 5. *Pour* $g \in \mathcal{F}^+$, $\alpha \in \mathbb{R}$ *on a*

$$\sigma_q(\alpha g) + \|(q-1)a_1\alpha\|^2 \ge \frac{1}{(q-1)((q-1)^2+1)} \kappa_g \|d_g \alpha\|^2, \tag{26}$$

où d_g *et* κ_g *sont définis respectivement en* (8) *et* (12).

Démonstration. Posons $c_3 = ((q-1)((q-1)^2+1))^{-1}$. Si $q = 2$, alors $c_3 = 1/2$, et la condition (7) entraîne $a_1 = 1$, $d_g = 1$ et $\kappa_g = 1$. L'inégalité (26) est donc bien satisfaite.

Supposons à présent $q \ge 3$ et posons $D = \operatorname{pgcd}(a_2 - 2a_1, \dots, a_{q-1} - (q-1)a_1)$. Compte tenu de l'hypothèse (7), les entiers a_1 et D ne peuvent

être simultanément nuls. De plus leur pgcd divise tous les entiers a_k pour $k \in \{1, \dots, q-1\}$, qui sont premiers entre eux. On a donc $\operatorname{pgcd}(a_1, D) = 1$. D'après le lemme 4,

$$\sigma_q(\alpha g) \geq c_3 \sum_{2 \leq k < q} \|(a_k - k a_1)\alpha\|^2.$$

On a donc, puisque $c_3 < 1$,

$$\|(q-1)a_1\alpha\|^2 + \sigma_q(\alpha g) \geq c_3\Big(\|(q-1)a_1\alpha\|^2 + \sum_{2 \leq k < q} \|(a_k - k a_1)\alpha\|^2\Big).$$

L'inégalité (24) appliquée avec $b_1 = a_1(q-1)$ et $b_k = a_k - k a_1$ pour $2 \leq k < q$, ainsi que l'associativité du pgcd, donnent bien l'inégalité souhaitée puisque $\operatorname{pgcd}(D, a_1(q-1)) = \operatorname{pgcd}(D, q-1) = d_g$. ∎

Le théorème 1 se déduit de la proposition 1 et du lemme 5.

5. Équirépartition modulo 1 de la suite $(\alpha g(p))_{p \in \mathcal{P}}$. Rappelons qu'une suite $(u_n)_{n \in \mathbb{N}}$ de nombres réels est *équirépartie modulo* 1 si pour tout intervalle I inclus dans $[0,1]$, on a

$$\lim_{x \to \infty} \frac{1}{x} \sum_{n \leq x} \mathbb{1}_{\{u_n\} \in I} = |I|, \tag{27}$$

où $|I|$ désigne la longueur de l'intervalle I. Selon le critère de Weyl (cf. par exemple [16, théorème 2.1]), ceci est équivalent à dire que pour tout entier h non nul,

$$\sum_{n \leq x} \mathrm{e}(h u_n) = o(x) \quad (x \to \infty).$$

Le résultat suivant généralise le théorème 2 de [19] concernant l'équirépartition modulo 1 de la suite $(\alpha s_q(p))_{p \in \mathcal{P}}$. Dans cette situation, il n'est pas nécessaire de se restreindre à $g \in \mathcal{F}^+$.

THÉORÈME 2. *Soit $g = \sum_{0 \leq k < q} a_k |\cdot|_k$ avec $a_k \in \mathbb{Z}$ pour tout $0 \leq k < q$, et $\alpha \in \mathbb{R}$. Si la suite $a_0, \dots, a_{q-1}$ est constante alors la suite $(\alpha g(p))_{p \in \mathcal{P}}$ n'est pas équirépartie modulo* 1. *Dans le cas contraire la suite $(\alpha g(p))_{p \in \mathcal{P}}$ est équirépartie modulo* 1 *si et seulement si $\alpha \in \mathbb{R} \setminus \mathbb{Q}$.*

Démonstration. Supposons tout d'abord que $a_0 = a_1 = \cdots = a_{q-1}$. Étant donné $\alpha \in \mathbb{R}$, supposons par l'absurde que la suite $(\alpha g(p))_{p \in \mathcal{P}}$ est équirépartie modulo 1 : d'après le critère de Weyl, on a

$$\frac{1}{\pi(x)} \sum_{p < x} \mathrm{e}(\alpha g(p)) = o(1) \quad (x \to \infty),$$

et donc, pour $j \in \mathbb{N}^*$,

$$\sum_{q^{j-1} \le p < q^j} \mathrm{e}(\alpha g(p)) = o(\pi(q^j)) \quad (j \to \infty).$$

Par ailleurs,

$$\begin{aligned}\sum_{q^{j-1} \le p < q^j} \mathrm{e}(\alpha g(p)) &= \sum_{q^{j-1} \le p < q^j} \mathrm{e}\left(\alpha a_0 \left\lfloor \frac{\log p}{\log q} \right\rfloor\right) \\ &= e(\alpha a_0 j)(\pi(q^j) - \pi(q^{j-1})) + O(1).\end{aligned}$$

Comme $e(\alpha a_0 j) \neq 0$, on obtient ainsi

$$\frac{\pi(q^j) - \pi(q^{j-1})}{\pi(q^j)} = o(1) \quad (j \to \infty),$$

une contradiction puisque le théorème des nombres premiers fournit

$$\lim_{j\to\infty} \frac{\pi(q^j) - \pi(q^{j-1})}{\pi(q^j)} = 1 - \frac{1}{q}.$$

Traitons à présent le cas où la suite $a_0, \dots, a_{q-1}$ n'est pas constante. Si α est rationnel, alors la suite $(\alpha g(p))_{p\in\mathcal{P}}$ ne comporte qu'un nombre fini de termes modulo 1 et n'est donc pas équirépartie modulo 1. Étant donnés $\alpha \in \mathbb{R} \setminus \mathbb{Q}$ et $h \in \mathbb{Z}^*$, supposons par l'absurde que $h\alpha a_0, \dots, h\alpha a_{q-1}$ est une progression arithmétique modulo 1 de raison $\ell/(q-1)$ avec $\ell \in \mathbb{Z}$. Si j est tel que $a_j \neq a_0$, comme

$$h\alpha(a_j - a_0) = \frac{j\ell}{q-1} \bmod 1,$$

on aboutit à $h\alpha \in \mathbb{Q}$, ce qui est absurde. Donc $(h\alpha a_0, \dots, h\alpha a_{q-1})$ n'est pas une progression arithmétique modulo 1 dont la raison est un multiple entier de $1/(q-1)$. Par conséquent la quantité $\tau_q(\alpha h, g)$ définie en (19) est strictement positive. En employant la proposition 1, on obtient directement

$$\sum_{p\le x} \mathrm{e}(\alpha h g(p)) = o(\pi(x)) \quad (h \in \mathbb{Z}^*,\ x \to \infty).$$

La conclusion résulte alors du critère de Weyl. ∎

6. Propriétés statistiques de la suite des nombres premiers p tels que $g(p) \equiv b \bmod m$. Soit $g \in \mathcal{F}^+$ et $m \ge 2$ un nombre entier. Nous allons voir que la répartition de $(g(p))_{p\in\mathcal{P}}$ dans les progressions arithmétiques modulo m dépend de l'entier

$$r_{m,g} = \mathrm{pgcd}(d_g, m). \tag{28}$$

Comme $r_{m,g} \mid d_g$, on a pour tout $n \in \mathbb{Z}$,

$$g(n) \equiv g(1)n \bmod r_{m,g}. \tag{29}$$

Par ailleurs observons que $r_{m,g} = 1$ dès que $\operatorname{pgcd}(m, q-1) = 1$. De plus, d'après la relation (10), nous avons

$$\operatorname{pgcd}(g(1), r_{m,g}) = 1. \tag{30}$$

Dans ce qui suit, nous posons

$$J_1 = \{0 \le j \le m-1 \mid j \equiv 0 \bmod m/r_{m,g}\}, \quad J_2 = \{0, 1, \dots, m-1\} \setminus J_1. \tag{31}$$

Rappelons les définitions de κ_g et c_1 respectivement en (12) et (13).

LEMME 6. *Pour $m \ge 2$, $g \in \mathcal{F}^+$, $r = r_{m,g}$, $\beta \in \mathbb{R}$, $x \ge 2$, on a*

$$\max_{j \in J_2} \left| \sum_{p \le x} \mathrm{e}\left(\frac{j}{m} g(p) + \beta p\right) \right| \ll (\log x)^3 x^{1 - c_1 \kappa_g r^2/m^2}.$$

La constante implicite ne dépend que de q.

Démonstration. Soit $j \in J_2$. Notons $d = d_g$. D'après le théorème 1, on a

$$\sum_{p \le x} \mathrm{e}\left(\frac{j}{m} g(p) + \beta p\right) \ll (\log x)^3 x^{1 - c_1 \kappa_g \|dj/m\|^2}.$$

Posons $m' = m/\operatorname{pgcd}(m, d) = m/r$ et $d' = d/\operatorname{pgcd}(m, d)$. Comme $\operatorname{pgcd}(m', d') = 1$, la condition $m' \nmid j$ entraîne que

$$\|dj/m\| = \|d'j/m'\| \ge 1/m',$$

ce qui donne bien la majoration souhaitée. ∎

6.1. Répartition dans les progressions arithmétiques de $(g(p))_{p \in \mathcal{P}}$ pour $g \in \mathcal{F}^+$. Le résultat suivant généralise le théorème 3 de [19]. Nous emploierons la notation suivante : lorsque k est un nombre entier supérieur ou égal à 2 et a un nombre entier inversible modulo k, on note $i_k(a)$ l'unique entier $b \in \{1, \dots, k-1\}$ tel que $ab \equiv 1 \bmod k$.

THÉORÈME 3. *Pour $m \ge 2$, $g \in \mathcal{F}^+$, $r = r_{m,g}$, $s = i_r(g(1))$, $b \in \mathbb{Z}$, $x \ge 2$, on a*

$$\begin{aligned} &\operatorname{card}\{p \le x \mid g(p) \equiv b \bmod m\} \\ &\quad = \begin{cases} 0 \text{ ou } 1 & \text{si } \operatorname{pgcd}(b, r) > 1, \\ \dfrac{r}{m} \pi(x; bs, r) + O((\log x)^3 x^{1 - c_1 \kappa_g r^2/m^2}) & \text{sinon,} \end{cases} \end{aligned} \tag{32}$$

et la constante implicite ne dépend que de q.

Démonstration. D'après les relations (29) et (30), on a les inclusions d'ensembles

$$\begin{aligned}(33)\qquad \{p\le x \mid g(p)\equiv b \bmod m\} &\subseteq \{p\le x \mid g(p)\equiv b \bmod r\}\\ &\subseteq \{p\le x \mid g(1)p\equiv b \bmod r\}\\ &\subseteq \{p\le x \mid p\equiv bs \bmod r\}\\ &\subseteq \{p\le x \mid p\equiv 0 \bmod \operatorname{pgcd}(b,r)\},\end{aligned}$$

ce qui implique que l'ensemble $\{p\le x \mid g(p)\equiv b \bmod m\}$ contient au plus un élément dès que $\operatorname{pgcd}(b,r)>1$.

Supposons à présent que $\operatorname{pgcd}(b,r)=1$. Alors

$$\operatorname{card}\{p\le x \mid g(p)\equiv b \bmod m\} = S_1+S_2$$

avec

$$S_1=\frac{1}{m}\sum_{j\in J_1}\sum_{p\le x}\mathrm{e}\Big(\frac{j}{m}(g(p)-b)\Big) \quad\text{et}\quad S_2=\frac{1}{m}\sum_{j\in J_2}\sum_{p\le x}\mathrm{e}\Big(\frac{j}{m}(g(p)-b)\Big).$$

D'après le lemme 6, on a

$$S_2 \ll (\log x)^3 x^{1-c_1\kappa_g r^2/m^2}.$$

Tout entier $j\in J_1$ est de la forme $j=um/r$ avec $0\le u<r$, d'où

$$S_1=\frac{1}{m}\sum_{p\le x}\sum_{0\le u<r}\mathrm{e}\Big(\frac{u}{r}(g(p)-b)\Big).$$

D'après les relations (29) et (2), on obtient

$$S_1=\frac{1}{m}\sum_{p\le x}\sum_{0\le u<r}\mathrm{e}\Big(\frac{u}{r}(g(1)p-b)\Big)=\frac{r}{m}\sum_{\substack{p\le x\\ g(1)p\equiv b \bmod r}}1=\frac{r}{m}\pi(x;bs,r),$$

et la preuve est achevée. ∎

6.2. Théorème de Vinogradov avec condition digitale. Soit $g\in\mathcal{F}^+$. Au vu du théorème 3, la suite des nombres premiers satisfaisant à une relation du type $g(p)\equiv b \bmod m$ ne comporte un nombre infini de termes que si $\operatorname{pgcd}(b,r)=1$, avec $r=r_{m,g}$.

Théorème 4. *Soient $m\ge 2$, $g\in\mathcal{F}^+$, $r=r_{m,g}$, $b\in\mathbb{Z}$ tels que* $\operatorname{pgcd}(b,r)=1$, *et $\alpha\in\mathbb{R}$. La suite $u=(p\alpha)_{p\in\mathcal{P},\, g(p)\equiv b \bmod m}$ est équirépartie modulo* 1 *si et seulement si α est un nombre irrationnel.*

Démonstration. Si α est un nombre rationnel, la suite u ne prend qu'un nombre fini de valeurs modulo 1 et n'est donc pas équirépartie modulo 1. Supposons réciproquement que α est irrationnel. D'après le critère de Weyl,

il suffit de prouver que pour tout $h \in \mathbb{Z}^*$,

$$\frac{1}{\operatorname{card}\{p \le x \mid g(p) \equiv b \bmod m\}} \sum_{\substack{p \le x \\ g(p) \equiv b \bmod m}} \mathrm{e}(h\alpha p) = o(1) \quad (x \to \infty). \tag{34}$$

La condition $\operatorname{pgcd}(b, r) = 1$ entraîne, en vertu du théorème 3 et du théorème B,

$$\operatorname{card}\{p \le x \mid g(p) \equiv b \bmod m\} \gg_{m,g} \pi(x). \tag{35}$$

Par ailleurs,

$$\Big| \sum_{\substack{p \le x \\ g(p) \equiv b \bmod m}} \mathrm{e}(h\alpha p) \Big| = \Big| \frac{1}{m} \sum_{j=0}^{m-1} \sum_{p \le x} \mathrm{e}\Big(\frac{j}{m}(g(p) - b) + h\alpha p \Big) \Big|$$

$$\le \frac{1}{m} \sum_{j \in J_1} \Big| \sum_{p \le x} \mathrm{e}\Big(\frac{j}{m} g(p) + h\alpha p \Big) \Big| + \frac{1}{m} \sum_{j \in J_2} \Big| \sum_{p \le x} \mathrm{e}\Big(\frac{j}{m} g(p) + h\alpha p \Big) \Big|.$$

D'après le lemme 6,

$$\frac{1}{m} \sum_{j \in J_2} \Big| \sum_{p \le x} \mathrm{e}\Big(\frac{j}{m} g(p) + h\alpha p \Big) \Big| \ll (\log x)^3 x^{1 - c_1 \kappa_g r^2/m^2}.$$

Par ailleurs, si $j \in J_1$ alors $j = um/r$ avec $0 \le u < r$ et d'après (29) on a

$$\sum_{p \le x} \mathrm{e}\Big(\frac{j}{m} g(p) + h\alpha p \Big) = \sum_{p \le x} \mathrm{e}\Big(\frac{u}{r} g(p) + h\alpha p \Big) = \sum_{p \le x} \mathrm{e}\Big(\frac{u}{r} g(1) p + h\alpha p \Big)$$

$$= \sum_{p \le x} \mathrm{e}\Big(p\Big(\frac{ug(1)}{r} + h\alpha \Big) \Big).$$

Comme α est un nombre irrationnel, le nombre $ug(1)/d + h\alpha$ l'est également. Donc d'après le critère de Weyl et le théorème C, on a

$$\sum_{p \le x} \mathrm{e}\Big(p\Big(\frac{ug(1)}{r} + h\alpha \Big) \Big) = o(\pi(x)) \quad (x \to \infty), \tag{36}$$

et par suite,

$$\frac{1}{m} \sum_{j \in J_1} \Big| \sum_{p \le x} \mathrm{e}\Big(\frac{j}{m} g(p) + h\alpha p \Big) \Big| = o(\pi(x)) \quad (x \to \infty). \tag{37}$$

Finalement,

$$\frac{1}{m} \sum_{0 \le j < m} \Big| \sum_{p \le x} \mathrm{e}\Big(\frac{j}{m} g(p) + h\alpha p \Big) \Big| = o(\pi(x)) \quad (x \to \infty), \tag{38}$$

et compte tenu de (35), nous obtenons bien la relation (34). ∎

6.3. Théorème d'Hadamard–de la Vallée Poussin avec condition digitale. Nous aurons l'usage du théorème des restes chinois sous la forme

LEMME 7. *Pour tous* $(a_1, a_2) \in \mathbb{Z}^2$, $(n_1, n_2) \in (\mathbb{Z}^*)^2$, *le système d'équations*

$$\begin{cases} x \equiv a_1 \bmod n_1, \\ x \equiv a_2 \bmod n_2 \end{cases}$$

admet une solution si et seulement si $a_1 \equiv a_2 \bmod \operatorname{pgcd}(n_1, n_2)$. *Dans ce cas, la solution est unique modulo* $\operatorname{ppcm}(n_1, n_2)$.

Démonstration. Voir par exemple [22], ou [21, théorème 2.9]. ∎

THÉORÈME 5. *Pour* $m \geq 2$, $g \in \mathcal{F}^+$, $r = r_{m,g}$, $s = i_r(g(1))$, $k \geq 2$, $(\ell, b) \in \mathbb{Z}^2$, $x \geq 2$, *on a*

$$\begin{aligned} (39) \qquad &\operatorname{card}\{p \leq x \mid p \equiv \ell \bmod k,\ g(p) \equiv b \bmod m\} \\ &= \begin{cases} 0 & \text{si } \ell \not\equiv bs \bmod \operatorname{pgcd}(k, r), \\ \dfrac{r}{m}\pi(x; v, \operatorname{ppcm}(k, r)) + O((\log x)^3 x^{1-c_1\kappa_g r^2/m^2}) & \text{sinon,} \end{cases} \end{aligned}$$

où v *est une solution du système*

$$\begin{cases} v \equiv \ell \bmod k, \\ v \equiv bs \bmod r, \end{cases}$$

et la constante implicite ne dépend que de q. *En particulier, lorsque* $r = 1$, *on a*

$$\begin{aligned} &\operatorname{card}\{p \leq x \mid p \equiv \ell \bmod k,\ g(p) \equiv b \bmod m\} \\ &\qquad = \frac{\pi(x; \ell, k)}{m} + O((\log x)^3 x^{1-c_1\kappa_g r^2/m^2}). \end{aligned}$$

Démonstration. Notons tout d'abord que d'après (29) et (30),

$$\begin{aligned} &\{p \leq x \mid p \equiv \ell \bmod k,\ g(p) \equiv b \bmod m\} \\ &\qquad \subseteq \{p \leq x \mid p \equiv \ell \bmod k,\ g(p) \equiv b \bmod r\} \\ &\qquad \subseteq \{p \leq x \mid p \equiv \ell \bmod k,\ g(1)p \equiv b \bmod r\} \\ &\qquad \subseteq \{p \leq x \mid p \equiv \ell \bmod k,\ p \equiv bs \bmod r\}, \end{aligned}$$

ce qui, d'après le lemme 7, règle le cas $\ell \not\equiv bs \bmod \operatorname{pgcd}(k, r)$. Supposons à présent que $\ell \equiv bs \bmod \operatorname{pgcd}(k, r)$. Nous avons

$$\begin{aligned} &\operatorname{card}\{p \leq x \mid p \equiv \ell \bmod k,\ g(p) \equiv b \bmod m\} \\ &\qquad = \frac{1}{m} \sum_{0 \leq j < m} \sum_{\substack{p \leq x \\ p \equiv \ell \bmod k}} \mathrm{e}\left(\frac{j}{m}(g(p) - b)\right) = S_1 + O(S_2) \end{aligned}$$

avec

$$S_1 = \frac{1}{m}\sum_{j\in J_1}\sum_{\substack{p\le x\\ p\equiv \ell \bmod k}} \mathrm{e}\Big(\frac{j}{m}(g(p)-b)\Big), \qquad S_2 = \frac{1}{m}\sum_{j\in J_2}\Big|\sum_{\substack{p\le x\\ p\equiv \ell \bmod k}} \mathrm{e}\Big(\frac{j}{m}g(p)\Big)\Big|.$$

Lorsque $j \in J_2$, d'après le lemme 6 on a

$$\Big|\sum_{\substack{p\le x\\ p\equiv \ell \bmod k}} \mathrm{e}\Big(\frac{j}{m}g(p)\Big)\Big| \le \frac{1}{k}\sum_{0\le n<k}\Big|\sum_{p\le x}\mathrm{e}\Big(\frac{j}{m}g(p)+\frac{n}{k}p\Big)\Big| \ll (\log x)^3 x^{1-c_1\kappa_g r^2/m^2},$$

et par suite,

$$S_2 \ll (\log x)^3 x^{1-c_1\kappa_g r^2/m^2}.$$

Par ailleurs,

$$S_1 = \frac{1}{m}\sum_{\substack{p\le x\\ p\equiv \ell \bmod k}}\sum_{0\le u<r}\mathrm{e}\Big(\frac{u}{r}(g(1)p-b)\Big) = \frac{r}{m}\sum_{\substack{p\le x\\ p\equiv \ell \bmod k\\ g(1)p\equiv b \bmod r}} 1 = \frac{r}{m}\sum_{\substack{p\le x\\ p\equiv \ell \bmod k\\ p\equiv bs \bmod r}} 1,$$

ce qui, compte tenu du lemme 7 et de la définition de v, fournit bien le résultat escompté. ∎

6.4. Répartition d'une fonction digitale dans les progressions arithmétiques. Dans ce paragraphe nous montrons comment étudier la répartition de $(g(p))_{p\in\mathcal{P}}$ dans les progressions arithmétiques lorsque g est une fonction digitale à valeurs entières quelconque. Nous allons voir qu'il est toujours possible de se ramener au cas où $g \in \mathcal{F}^+$ et donc d'employer le théorème 3.

En effet si g est non nulle et fortement q-additive donc de la forme

$$g = \sum_{1\le k<q} a_k|\cdot|_k,$$

on peut introduire δ, le plus grand diviseur commun des entiers $a_1,\dots,a_{q-1}$, puis la fonction $\widetilde{g}$ définie par $g = \delta\widetilde{g}$. Les coefficients $\widetilde{g}(1) = \widetilde{a}_1,\dots,\widetilde{g}(q-1) = \widetilde{a}_{q-1}$ sont premiers dans leur ensemble, et donc $\widetilde{g} \in \mathcal{F}^+$. Par ailleurs, la relation de congruence $g(p) \equiv b \bmod m$ est équivalente à une relation du type $\widetilde{g}(p) \equiv \widetilde{b} \bmod \widetilde{m}$ avec $\widetilde{m}, \widetilde{b} \in \mathbb{Z}$.

Plus généralement, si g est une fonction de la forme

$$g = \sum_{0\le k<q} a_k|\cdot|_k,$$

on peut introduire la fonction g_0 fortement q-additive définie par

$$g_0 = \sum_{1\le k<q} (a_k - a_0)|\cdot|_k,$$

et on a alors

$$g(n) = a_0(|n|_0 + \cdots + |n|_{q-1}) + g_0(n) = a_0(\lfloor \log_q n \rfloor + 1) + g_0(n).$$

En se ramenant au cas précédent, on peut évaluer le nombre de nombres premiers p d'un intervalle de la forme $[q^{j-1}, q^j[$ satisfaisant à $g(p) \equiv b \bmod m$. En effet, avec ces notations,

$$\begin{aligned}(40)\qquad &\operatorname{card}\{q^{j-1} \le p < q^j \mid g(p) \equiv b \bmod m\} \\ &\qquad = \operatorname{card}\{q^{j-1} \le p < q^j \mid g_0(p) \equiv b - a_0 j \bmod m\}.\end{aligned}$$

Suivant les valeurs de j, la quantité (40) peut valoir 0, 1 ou alors approximativement $C(\pi(q^j) - \pi(q^{j-1}))$ où C est une constante strictement positive qui ne dépend ni de j, ni de b, de sorte qu'il existe des cas pour lesquels la limite

$$\lim_{x\to\infty} \frac{1}{\pi(x)} \operatorname{card}\{p \le x \mid g(p) \equiv b \bmod m\}$$

existe, et d'autres pour lesquels elle n'existe pas. À titre d'illustration, nous présentons trois exemples.

(1) Lorsque $q \ge 2$, $m \in \mathbb{N}^*$, et $g(n) = |n|_0$, pour $j \in \mathbb{N}^*$, $b \in \mathbb{Z}$, $q^{j-1} \le x < q^j$ on a

$$\begin{aligned}&\{q^{j-1} \le p < x \mid g(p) \equiv b \bmod m\} \\ &\qquad = \Big\{q^{j-1} \le p < x \Big| \sum_{k=1}^{q-1} |p|_k \equiv j - b \bmod m\Big\}.\end{aligned}$$

Comme l'entier caractéristique d de la fonction $g_0 : n \mapsto |n|_1 + \cdots + |n|_{q-1}$ vaut toujours 1 quelle que soit la base q, on a $r = r_{m,g_0} = 1$ et le théorème 3 fournit l'estimation

$$\begin{aligned}&\operatorname{card}\{q^{j-1} \le p < x \mid g(p) \equiv b \bmod m\} \\ &\qquad = \frac{\pi(x) - \pi(q^{j-1})}{m} + O((\log x)^3 x^{1-c_1\kappa_{g_0}/m^2}),\end{aligned}$$

et cela entraîne que pour tous $q \ge 2$, $m \ge 2$ et $b \in \mathbb{Z}$,

$$\lim_{x\to\infty} \frac{1}{\pi(x)} \{p \le x \mid |p|_0 \equiv b \bmod m\} = \frac{1}{m}.$$

(2) Lorsque $q = 3$, $m = 4$, $g(n) = 2|n|_0 + 3|n|_1 + 2|n|_2$, pour $j \in \mathbb{N}^*$ et $q^{j-1} \le x < q^j$ on a

$$\{q^{j-1} \le p < x \mid g(p) \equiv 1 \bmod 4\} = \{q^{j-1} \le p < x \mid |p|_1 \equiv 1 - 2j \bmod 4\}.$$

L'entier caractéristique de la fonction $g_0 : n \mapsto |n|_1$ en base 3 vaut $d = 2$, et donc $r_{4,g_0} = 2$. Alors en appliquant le théorème 3, pour tout $j \in \mathbb{N}^*$ nous

obtenons

$$\operatorname{card}\{q^{j-1} \le p < x \mid g(p) \equiv 1 \bmod 4\} \\ = \frac{\pi(x) - \pi(q^{j-1})}{2} + O((\log x)^3 x^{1-c_1\kappa_{g_0}/4})$$

et ainsi

$$\lim_{x\to\infty} \frac{1}{\pi(x)} \operatorname{card}\{p \le x \mid 2|p|_0 + 3|p|_1 + 2|p|_2 \equiv 1 \bmod 4\} = \frac{1}{2}.$$

(3) Toujours avec $q = 3$, $m = 4$, pour $g(n) = |n|_0 + 2|n|_1 + |n|_2$, $j \in \mathbb{N}^*$, $q^{j-1} \le x < q^j$ on a maintenant

$$\{q^{j-1} \le p < x \mid g(p) \equiv 1 \bmod 4\} = \{q^{j-1} \le p < x \mid |p|_1 \equiv 1 - j \bmod 4\}.$$

On retrouve la fonction $g_0 : n \mapsto |n|_1$ de l'exemple précédent, et le théorème 3 fournit

$$\operatorname{card}\{q^{j-1} \le p < x \mid g(p) \equiv 1 \bmod 4\} \\ = \begin{cases} 0 \text{ ou } 1 & \text{si } j \text{ est impair,} \\ \dfrac{\pi(x) - \pi(q^{j-1})}{2} + O((\log x)^3 x^{1-c_1\kappa_{g_0}/4}) & \text{sinon,} \end{cases}$$

de sorte que la quantité

$$\frac{1}{\pi(x)} \operatorname{card}\{p \le x \mid |p|_0 + 2|p|_1 + |p|_2 \equiv 1 \bmod 4\}$$

n'a pas de limite lorsque $x \to \infty$.

7. Problème de Goldbach ternaire avec conditions digitales. Dans ce qui suit, nous considérons pour $i \in \{1, 2, 3\}$ une base de numération entière $q_i \ge 2$ ainsi qu'une fonction g_i fortement q-additive non nulle, donc de la forme

$$g_i(n) = \sum_{1\le k<q_i} a_{ik}|n|_k^i \quad (a_{ik} \in \mathbb{Z} \text{ pour } i \in \{1, 2, 3\},\ 1 \le k < q_i), \tag{41}$$

où $|n|_k^i$ désigne le nombre d'occurrences du chiffre k dans le développement en base q_i de n. On suppose également que pour chaque $i \in \{1, 2, 3\}$, $\operatorname{pgcd}(a_{i1}, \dots, a_{i(q_i-1)}) = 1$. Pour chaque $i \in \{1, 2, 3\}$, nous considérons un entier $m_i \ge 2$.

Rappelons la définition de l'entier $r_{m,g}$ en (28). Afin d'énoncer un résultat clair, nous faisons également l'hypothèse dans ce qui suit que les entiers $r_i = r_{m_i,g_i}$ $(i = 1, 2, 3)$ sont tous égaux à 1. C'est notamment le cas dès que $\operatorname{pgcd}(m_i, q_i - 1) = 1$ pour tout $i \in \{1, 2, 3\}$.

Rappelons la notation $R(N)$ employée dans le théorème D. Usant $\mathbf{x}$ pour désigner un triplet (x_1, x_2, x_3), nous introduisons, pour tout $\mathbf{b} \in \mathbb{Z}^3$,

$$R(N,\mathbf{q},\mathbf{m},\mathbf{b}) = \sum_{\substack{n_1,n_2,n_3\\ n_1+n_2+n_3=N\\ g_i(n_i)\equiv b_i \bmod m_i,\, i\in\{1,2,3\}}} \Lambda(n_1)\Lambda(n_2)\Lambda(n_3). \tag{42}$$

THÉORÈME 6. *Sous ces hypothèses, il existe $\mu_{\mathbf{q},\mathbf{m},\mathbf{g}} > 0$ tel que pour $N \geq 2$,*

$$R(N,\mathbf{q},\mathbf{m},\mathbf{b}) = \frac{R(N)}{m_1m_2m_3} + O((\log N)^5 N^{2-\mu_{\mathbf{q},\mathbf{m},\mathbf{g}}}),$$

où la constante implicite ne dépend que de $\mathbf{q}$. *En particulier, il existe un entier N_0 dépendant de* $\mathbf{q}$, $\mathbf{m}$ *et* $\mathbf{g}$ *tel que tout entier impair $N > N_0$ s'écrit sous la forme*

$$N = p_1 + p_2 + p_3 \quad \text{avec } g_i(p_i) \equiv b_i \bmod m_i \text{ pour } i \in \{1,2,3\}, \tag{43}$$

où p_1, p_2 et p_3 sont des nombres premiers.

REMARQUE 3. Il est possible de s'affranchir de l'hypothèse faite sur les entiers caractéristiques r_1, r_2, r_3 et, sous les conditions $\operatorname{pgcd}(b_i, r_i) = 1$ pour $i \in \{1,2,3\}$, d'obtenir une formule asymptotique générale pour $R(N,\mathbf{q},\mathbf{m},\mathbf{b})$ dont le terme principal serait à un coefficient multiplicatif près la quantité

$$\sum_{\substack{n_1+n_2+n_3=N\\ n_j\equiv s_j \bmod r_j\\ j\in\{1,2,3\}}} \Lambda(n_1)\Lambda(n_2)\Lambda(n_3), \tag{44}$$

où l'on a posé pour $j \in \{1,2,3\}$, $s_j = b_j i_{r_j}(g_j(1))$, ce qui est licite puisque $\operatorname{pgcd}(g_j(1), r_j) = 1$ (cf. relation (30)). Une formule asymptotique pour la quantité (44) est contenue dans le résultat principal de [14] : pour $A > 0$, $N \geq 2$, $\operatorname{pgcd}(c_j^2, r_j) = 1$ pour $j \in \{1,2,3\}$, on a

$$\sum_{\substack{n_1+n_2+n_3=N\\ n_j\equiv c_j \bmod r_j\\ j\in\{1,2,3\}}} \Lambda(n_1)\Lambda(n_2)\Lambda(n_3) = \frac{\sigma_3(N)N^2}{2\varphi(r_1)\varphi(r_2)\varphi(r_3)} + O\bigg(\frac{N}{(\log N)^A}\bigg),$$

où φ désigne la fonction indicatrice d'Euler, et où la constante implicite est autorisée à dépendre de A, r_1, r_2 et r_3. La quantité $\sigma_3(N)$ est une série singulière issue de la méthode du cercle : la définition de $\sigma_3(N)$ étant fastidieuse, nous renvoyons à [14] pour les détails et nous nous bornons à signaler que $\sigma_3(N) = 0$ si et seulement si, soit

- $N \not\equiv c_1 + c_2 + c_3 \bmod (\operatorname{pgcd}(r_1, r_2, r_3))$, soit
- il existe un nombre premier p et un triplet d'entiers deux à deux distincts $(j,k,\ell) \in \{1,2,3\}$ tels que $p \mid \operatorname{pgcd}(r_j, r_k)$, $p \nmid r_\ell$ et $p \mid n - (c_j + c_k)$.

Démonstration du théorème 6. Nous employons ici la notation

$$T_i(x;\alpha,\beta)=\sum_{n\le x}\Lambda(n)\,\mathrm{e}(\alpha g_i(n)+\beta n)\qquad(\alpha,\beta\in\mathbb{R}).$$

Rappelons que l'on peut écrire

$$R(N)=\int_0^1\Big(\sum_{n\le N}\Lambda(n)\,\mathrm{e}(nt)\Big)^3\mathrm{e}(-Nt)\,dt. \tag{45}$$

De même, en employant l'orthogonalité des caractères additifs, on a

$$\begin{aligned}R(N,\mathbf{q},\mathbf{m},\mathbf{b})&=\int_0^1\mathrm{e}(-Nt)\prod_{i=1}^3\Big(\sum_{\substack{n\le N\\ g_i(n)\equiv b_i \bmod m_i}}\Lambda(n)\,\mathrm{e}(nt)\Big)\,dt\\&=\frac{1}{m_1m_2m_3}\sum_{\substack{0\le k_1<m_1\\0\le k_2<m_2\\0\le k_3<m_3}}\mathrm{e}\Big(-\frac{k_1b_1}{m_1}-\frac{k_2b_2}{m_2}-\frac{k_3b_3}{m_3}\Big)I_{k_1,k_2,k_3},\end{aligned}$$

où l'on a posé

$$I_{k_1,k_2,k_3}=\int_0^1\mathrm{e}(-Nt)\prod_{i=1}^3T_i\Big(N;\frac{k_i}{m_i},t\Big)\,dt.$$

En isolant le terme correspondant à $k_1=k_2=k_3=0$, nous obtenons

$$R(N,\mathbf{q},\mathbf{m},\mathbf{b})=\frac{R(N)}{m_1m_2m_3}+\frac{S}{m_1m_2m_3}, \tag{46}$$

avec

$$S=\sum_{\substack{0\le k_1<m_1\\0\le k_2<m_2\\0\le k_3<m_3\\(k_1,k_2,k_3)\ne(0,0,0)}}I_{k_1,k_2,k_3}. \tag{47}$$

Considérons un triplet (k_1,k_2,k_3) tel que $(k_1,k_2,k_3)\ne(0,0,0)$. Sans restreindre la généralité, on peut supposer que $k_1\ne0$. En utilisant l'inégalité $|ab|\le\max(|a|^2,|b|^2)$, on obtient alors

$$|I_{k_1,k_2,k_3}|\le\max_{t\in[0,1]}\Big|T_1\Big(N;\frac{k_1}{m_1},t\Big)\Big|\max_{i=2,3}\int_0^1\Big|T_i\Big(N;\frac{k_i}{m_i},t\Big)\Big|^2\,dt. \tag{48}$$

Comme r_1 vaut 1, l'ensemble J_1 (voir définition en (31)) relatif à r_1 et m_1 est réduit à $\{0\}$. Par conséquent, k_1/m_1 appartient à l'ensemble J_2 relatif à r_1 et m_1, et d'après le théorème 1, via une intégration par parties standard, on voit que

$$T_1\Big(N;\frac{k_1}{m_1},t\Big)\ll(\log N)^4N^{1-c_1\kappa_{g_1}/m_1^2}.$$

En employant l'égalité de Parseval on obtient ainsi

$$|I_{k_1,k_2,k_3}| \ll (\log N)^4 N^{1-c_1\kappa_{g_1}/m_1^2} \sum_{n\le N} \Lambda(n)^2 \ll N^{2-c_1\kappa_{g_1}/m_1^2}(\log N)^5,$$

où la dernière majoration résulte de la majoration $\Lambda(n) \le \log n$ et de l'inégalité classique de Tchebychev, $\sum_{n\le N} \Lambda(n) \ll N$. En posant

$$\mu_{\mathbf{q},\mathbf{m},\mathbf{g}} = c_1 \min_{i\in\{1,2,3\}} \frac{\kappa_{g_i}}{m_i^2} > 0, \tag{49}$$

nous obtenons

$$S \ll m_1 m_2 m_3 \, N^{2-\mu_{\mathbf{q},\mathbf{m},\mathbf{g}}} (\log N)^5. \tag{50}$$

En insérant (50) dans (46), nous obtenons bien la conclusion souhaitée. ∎

Remerciements. Ce travail a bénéficié d'une aide de l'Agence Nationale de la Recherche portant la référence « ANR-10-BLAN 0103 », MUNUM, et de Ciencia sem Fronteiras, projet PVE 407308/2013-0. Bruno Martin a également bénéficié d'un financement de l'Austrian Science Foundation FWF dans le cadre du projet S9605, faisant partie de l'Austrian National Research Network "Analytic Combinatorics and Probabilistic Number Theory".

Références

[1] P. T. Bateman and H. G. Diamond, *Analytic Number Theory. An Introductory Course*, World Sci., Hackensack, NJ, 2004.

[2] R. Bellman and H. N. Shapiro, *On a problem in additive number theory*, Ann. of Math. (2) 49 (1948), 333–340.

[3] S. Col, *Diviseurs des nombres ellipséphiques*, Period. Math. Hungar. 58 (2009), 1–23.

[4] C. Dartyge et C. Mauduit, *Nombres presque premiers dont l'écriture en base r ne comporte pas certains chiffres*, J. Number Theory 81 (2000), 270–291.

[5] 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.

[6] H. Davenport, *Multiplicative Number Theory*, 3ème éd., Grad. Texts in Math. 74, Springer, New York, 2000.

[7] C. J. de la Vallée Poussin, *Recherches analytiques sur la théorie des nombres premiers*, Brux. S. Sc. 21 (1896), 183–256, 281–362, 363–397.

[8] M. Drmota, *Subsequences of automatic sequences and uniform distribution*, dans : Uniform Distribution and Quasi-Monte Carlo Methods, Radon Ser. Comput. Appl. Math. 15, de Gruyter, Berlin, 2014, 87–104.

[9] M. Drmota and C. Mauduit, *Weyl sums over integers with affine digit restrictions*, J. Number Theory 130 (2010), 2404–2427.

[10] S. Eilenberg, *Automata, Languages, and Machines. Vol. A*, Pure Appl. Math. 58, Academic Press, New York, 1974.

[11] E. Fouvry et C. Mauduit, *Sommes des chiffres et nombres presque premiers*, Math. Ann. 305 (1996), 571–599.

[12] A. O. Gelfond, *Sur les nombres qui ont des propriétés additives et multiplicatives données*, Acta Arith. 13 (1968), 259–265.
[13] J. Hadamard, *Sur la distribution des zéros de la fonction $\zeta(s)$ et ses conséquences arithmétiques*, Bull. Soc. Math. France 24 (1896), 199–220.
[14] K. Halupczok, *On the ternary Goldbach problem with primes in independent arithmetic progressions*, Acta Math. Hungar. 120 (2008), 315–349.
[15] H. Iwaniec and E. Kowalski, *Analytic Number Theory*, Amer. Math. Soc. Colloq. Publ. 53, Amer. Math. Soc., Providence, RI, 2004.
[16] L. Kuipers and H. Niederreiter, *Uniform Distribution of Sequences*, Pure Appl. Math., Wiley-Interscience, New York, 1974.
[17] B. Martin, C. Mauduit et J. Rivat, *Théorème des nombres premiers pour les fonctions digitales*, Acta Arith. 165 (2014), 11–45.
[18] C. Mauduit, *Automates finis et ensembles normaux*, Ann. Inst. Fourier (Grenoble) 36 (1986), no. 2, 1–25.
[19] C. Mauduit et J. Rivat, *Sur un problème de Gelfond : la somme des chiffres des nombres premiers*, Ann. of Math. (2) 171 (2010), 1591–1646.
[20] C. Mauduit and J. Rivat, *Prime numbers along Rudin–Shapiro sequences*, J. Eur. Math. Soc., to appear.
[21] M. B. Nathanson, *Elementary Methods in Number Theory*, Grad. Texts in Math. 195, Springer, New York, 2000.
[22] O. Ore, *The general Chinese remainder theorem*, Amer. Math. Monthly 59 (1952), 365–370.
[23] G. Rauzy, *Propriétés statistiques de suites arithmétiques*, Le Mathématicien 15, Collection SUP, Presses Universitaires de France, Paris, 1976.
[24] I. M. Vinogradov, *The Method of Trigonometrical Sums in the Theory of Numbers*, Interscience, London, 1954.

Bruno Martin
LMPA, Centre Universitaire de la Mi-Voix
Maison de la Recherche Blaise Pascal
50 rue F. Buisson, B.P. 699
62228 Calais Cedex, France
E-mail: martin@lmpa.univ-littoral.fr

Joël Rivat
Université d'Aix-Marseille
Institut de Mathématiques de Marseille
CNRS UMR 7373
163 avenue de Luminy, Case 907
13288 Marseille Cedex 9, France
E-mail: rivat@iml.univ-mrs.fr

Christian Mauduit
Université d'Aix-Marseille
et Institut Universitaire de France
Institut de Mathématiques de Marseille
CNRS UMR 7373
163 avenue de Luminy, Case 907
13288 Marseille Cedex 9, France
E-mail: mauduit@iml.univ-mrs.fr

Reçu le 19.9.2014
et révisé le 11.5.2015 (7937)