Aix-Marseille Université
École Doctorale de Mathématiques et Informatique de Marseille
Institut de Mathématiques de Marseille

Thèse

présentée pour obtenir le grade universitaire de docteur

Discipline : Mathématiques

par

Cathy Swaenepoel

Chiffres des nombres premiers et d'autres suites remarquables

Digits of prime numbers and other remarkable sequences

Soutenue le 7 juin 2019 devant le jury composé de :

Boris Adamczewski	CNRS	Examinateur
Régis de la Bretèche	Université Paris Diderot	Rapporteur
Cécile Dartyge	Université de Lorraine	Rapporteur
Étienne Fouvry	Université Paris-Sud	Président
Florent Jouve	Université de Bordeaux	Examinateur
Bruno Martin	Université du Littoral Côte d'Opale	Examinateur
Christian Mauduit	Université d'Aix-Marseille	Examinateur
Joël Rivat	Université d'Aix-Marseille	Directeur de thèse

Résumé

Dans ce travail, nous étudions la répartition des chiffres des nombres premiers. Bourgain (2015) a obtenu une formule asymptotique pour le nombre de nombres premiers avec une proportion $c > 0$ de chiffres préassignés en base 2 (c est une constante absolue non précisée). Nous généralisons ce résultat à toute base $g \geq 2$ et nous donnons des valeurs explicites pour la proportion c en fonction de g. En adaptant, développant et précisant la stratégie introduite par Bourgain dans le cas $g = 2$, nous présentons une démonstration détaillée du cas général. La preuve est fondée sur la méthode du cercle et combine des techniques d'analyse harmonique avec des résultats sur les zéros des fonctions L de Dirichlet, notamment une région sans zéro très fine due à Iwaniec. Ce travail s'inscrit aussi dans l'étude des nombres premiers dans des ensembles « rares ».

Nous étudions également la répartition des « chiffres » (au sens de Dartyge et Sárközy) de quelques suites remarquables dans le contexte des corps finis. Ce concept de « chiffre » est à la base de la représentation des corps finis dans les logiciels de calcul formel. Nous étudions des suites variées comme les suites polynomiales, les générateurs ou encore les produits d'éléments de deux ensembles assez grands. Les méthodes développées permettent d'obtenir des estimations explicites très précises voire optimales dans certains cas. Les sommes d'exponentielles sur les corps finis jouent un rôle essentiel dans les démonstrations. Les résultats obtenus peuvent être reformulés d'un point de vue plus algébrique avec la fonction trace qui est très importante dans l'étude des corps finis.

Mots clés : chiffres, nombres premiers, méthode du cercle, sommes d'exponentielles, corps finis, trace.

Abstract

In this work, we study the distribution of prime numbers' digits. Bourgain (2015) obtained an asymptotic formula for the number of prime numbers with a proportion $c > 0$ of preassigned digits in base 2 (c is an absolute constant not specified). We generalize this result in any base $g \geq 2$ and we provide explicit admissible values for the proportion c depending on g. By adapting, developing and refining Bourgain's strategy in the case $g = 2$, we present a detailed proof for the general case. The proof is based on the circle method and combines techniques from harmonic analysis together with results on zeros of Dirichlet L-functions, notably a very sharp zero-free region due to Iwaniec. This work also falls within the study of prime numbers in sparse "sets".

In addition, we study the distribution of the "digits" (in the sense of Dartyge and Sárközy) of some sequences of interest in the context of finite fields. This concept of "digits" is fundamental in the representation of finite fields in computer algebra systems. We study various sequences such as polynomial sequences, generators as well as products of elements of two large enough sets. Our methods provide very sharp explicit estimates which are even optimal in some cases. Exponential sums over finite fields play an essential role in the proofs. Our results can be reformulated from a more algebraic point of view with the trace function which is of basic importance in the study of finite fields.

Keywords: digits, prime numbers, circle method, exponential sums, finite fields, trace.

Remerciements

Je tiens à exprimer mes plus vifs et sincères remerciements à toutes les personnes qui ont contribué à l'élaboration de ce travail et tout particulièrement à :

— Joël Rivat pour m'avoir permis, en encadrant ma thèse, de découvrir la recherche mathématique dans des conditions idéales ainsi que pour la confiance qu'il m'a accordée, les connaissances mathématiques précieuses qu'il m'a apportées, le temps qu'il a bien voulu me consacrer très fréquemment et tous les conseils avisés qu'il m'a donnés, sans lesquels ce travail n'aurait pu voir le jour,

— Christian Mauduit pour avoir suivi attentivement l'évolution de mes travaux, pour ses nombreux conseils et pour avoir accepté de faire partie du jury,

— Régis de la Bretèche et Cécile Dartyge pour l'intérêt qu'ils ont porté à mon travail et pour avoir accepté d'être rapporteurs et membres du jury,

— Étienne Fouvry pour s'être beaucoup intéressé à mes travaux, pour avoir pris du temps pour en discuter, pour ses remarques et suggestions et pour avoir accepté de faire partie du jury,

— Boris Adamczewski, Florent Jouve et Bruno Martin pour avoir accepté de faire partie du jury,

— András Sárközy pour avoir posé des questions qui ont motivé les recherches réalisées au début de ma thèse, pour l'intérêt qu'il a porté à mon travail et pour ses précieux conseils,

— Michel Balazard, Sary Drappeau et Olivier Ramaré pour s'être intéressés à mes travaux, pour toutes les connaissances qu'ils m'ont permis d'acquérir en théorie analytique des nombres et pour leur accessibilité et leur bienveillance,

— ma famille proche pour m'avoir toujours soutenue et particulièrement mon frère Tony pour la grande complicité que l'on partage.

Table des matières

I. Introduction

Depuis l'Antiquité et les travaux d'Euclide et d'Ératosthène, les nombres premiers suscitent un intérêt sans cesse renouvelé. S'ils ont une structure multiplicative extrêmement simple, les questions de nature « additive » sur les nombres premiers sont en général très difficiles à résoudre et ont mené à des problèmes célèbres tels que la primalité des nombres de Mersenne, des nombres de Fermat ou encore les conjectures des nombres premiers jumeaux et de Goldbach. L'étude des nombres premiers a également permis de développer de nombreuses applications dans des domaines très variés, aussi bien en mathématiques qu'en informatique.

Parmi ces questions de nature « additive », l'étude des chiffres des nombres premiers est d'une grande importance car elle permet de mieux comprendre comment les nombres premiers sont représentés en pratique (le plus communément en base 10 ou encore en base 2 dans les ordinateurs) et a des implications en cryptographie. Étant donné un nombre entier $g \geq 2$, tout nombre entier $k \geq 0$ s'écrit de façon unique en base g :

$$k = \sum_{j \geq 0} \varepsilon_j(k) g^j \tag{I.1}$$

où $(\varepsilon_j(k))_{j\geq 0} \in \{0, \dots, g-1\}^{\mathbb{N}}$ est la suite des chiffres de k en base g. En oubliant le chiffre ε_0 qui est particulier, les chiffres des nombres premiers semblent vérifier des propriétés statistiques similaires à celles des chiffres des nombres entiers : on parle des propriétés de pseudo-aléa des chiffres des nombres premiers. L'étude de ces propriétés est à l'origine de nombreux défis.

En 1968, Gelfond a conjecturé que la somme des chiffres des nombres premiers est bien répartie dans les progressions arithmétiques. Fouvry–Mauduit [21] et Dartyge–Tenenbaum [13] ont obtenu des résultats dans cette direction pour les nombres presque premiers. Mauduit–Rivat [44] parviennent finalement à prouver la conjecture de Gelfond en 2010 et Drmota–Mauduit–Rivat [18] obtiennent une loi limite locale pour la somme des chiffres des nombres premiers (lorsqu'elle est proche de la valeur moyenne). Plusieurs travaux ont ensuite permis d'étudier des fonctions digitales plus générales que la fonction somme des chiffres (voir par exemple [39, 40, 41, 42, 45]).

L'étude des nombres premiers avec des chiffres manquants est également restée un problème ouvert pendant de nombreuses années. Dans cette direction, Dartyge–Mauduit [9, 10] ont obtenu des résultats pour les nombres presque premiers. Maynard [46, 48] a pu montrer que, dans une base assez grande, il y a une infinité de nombres premiers avec un chiffre manquant (par exemple, il y a une infinité de nombres premiers sans chiffre 9 en base 10).

Dans le chapitre II, nous nous intéressons à l'estimation du nombre de nombres premiers ayant des chiffres préassignés. Soient $n \geq 1$ un nombre entier, $A \subset \{0, \dots, n-1\}$ un ensemble

de positions, $\boldsymbol{d} = (d_j)_{j\in A} \in \{0,\dots,g-1\}^A$ une suite de chiffres et notons

$$\mathcal{D}(n,A,\boldsymbol{d}) = \{0 \le k < g^n : \forall j \in A,\, \varepsilon_j(k) = d_j\}.$$

Le lettre p désignera toujours un nombre premier. Nous étudions la question suivante :

Question. Estimer le nombre de nombre premiers dans l'ensemble $\mathcal{D}(n,A,\boldsymbol{d})$ lorsque $|A|$ est « grand » et sans aucune restriction (ou presque) sur l'ensemble A lui-même et sur les chiffres d_j.

Comme $|\mathcal{D}(n,A,\boldsymbol{d})| = g^{n-|A|}$, l'ensemble $\mathcal{D}(n,A,\boldsymbol{d})$ est rare (i.e. de densité nulle) dès que $\lim_{n\to+\infty} |A| = +\infty$. Notre travail s'inscrit donc aussi dans le cadre de l'étude des nombres premiers dans des ensembles rares qui rassemble assez peu de résultats : par exemple, Friedlander–Iwaniec [22] ont établi l'existence d'une infinité de nombres premiers de la forme $m^2 + n^4$, suivis par Heath-Brown [31] pour les nombres premiers de la forme $m^3 + 2n^3$ mais l'existence d'une infinité de nombres premiers de la forme $2^n - 1$ (nombres de Mersenne premiers) ou de la forme $n^2 + 1$ sont encore des problèmes ouverts qui semblent actuellement hors d'atteinte.

En 2005, Wolke [70] a obtenu, sous l'hypothèse de Riemann généralisée, une formule asymptotique pour le nombre de nombres premiers dans $\mathcal{D}(n,A,\boldsymbol{d})$ lorsque $|A| \le (1-\varepsilon)\sqrt{n}$. Puis en 2008, Harman–Kátai [30] ont amélioré tous les résultats connus sur cette question (par Kátai [37], Wolke [70] et Harman [29]) en obtenant, inconditionnellement, une formule asymptotique pour le nombre de nombres premiers dans $\mathcal{D}(n,A,\boldsymbol{d})$ lorsque $|A| \ll \sqrt{n}(\log n)^{-1}$. Bourgain a ensuite fait un grand pas en avant en 2013 [4] en obtenant une formule asymptotique lorsque $|A| \ll n^{4/7}(\log n)^{-4/7}$ en base 2 et en 2015 [5], il réalise une percée spectaculaire en prouvant que cela reste vrai lorsque $|A| \le cn$ où $c > 0$ est une constante absolue (non explicitée). Il est donc possible de préassigner jusqu'à une proportion positive des chiffres binaires. La preuve dans [5] permet d'obtenir :

Théorème A. *Il existe une constante absolue $c > 0$ vérifiant la propriété suivante. Pour tout $A \subset \{0,\dots,n-1\}$ tel que $0 \in A$, $n-1 \in A$ et*

$$|A| \le cn$$

et pour tout $(d_j)_{j\in A} \in \{0,1\}^A$ tel que $d_0 = d_{n-1} = 1$,

$$|\{p < 2^n : \forall j \in A, \varepsilon_j(p) = d_j\}| = \frac{2^{n-|A|+1}}{\log 2^n}\,(1+o(1))$$

lorsque $n \to +\infty$.

Nous généralisons ce résultat à toute base en établissant une formule asymptotique pour le nombre de nombres premiers avec une proportion positive de chiffres préassignés dans une base $g \ge 2$ quelconque :

Théorème 1. *Soit $g \geq 2$ un nombre entier. Il existe une constante $c_0 = c_0(g) \in]0{,}1/2[$ explicite vérifiant la propriété suivante. Pour tout $c \in]0,c_0[$, il existe $n_0 = n_0(g,c) \geq 1$ et $\delta = \delta(g,c) > 0$ tels que pour tout nombre entier $n \geq n_0$, pour tout $A \subset \{0,\dots,n-1\}$ tel que $0 \in A$, $n-1 \in A$ et*

$$|A| \leq cn,$$

pour tout $(d_j)_{j\in A} \in \{0,\dots,g-1\}^A$ tel que $(d_0,g) = 1$ et $d_{n-1} \geq 1$, on a

$$|\{p < g^n : \forall j \in A, \varepsilon_j(p) = d_j\}| = \frac{g^{n-|A|}}{\log g^n}\frac{g}{\varphi(g)}\left(1 + O_{g,c}\left(n^{-\delta}\right)\right).$$

De plus, nous donnons des valeurs admissibles explicites de c_0 (en fonction de g), ce qui permet de mesurer la « rareté » de l'ensemble de nombres entiers dans lequel on compte les nombres premiers :

Théorème 2. *Le théorème 1 est vrai avec $c_0 = c_0(g)$ donné par :*

g	2	3	4	5	6	10	10^3	$2 \cdot 3^{100}$	2^{200}
$c_0(g) \cdot 10^3$	2,1	3,1	3,6	4,0	4,2	4,7	6,8	0,7	9,0

Ainsi, nous pouvons préassigner un peu plus de 2 millièmes des chiffres en base 2 et presque 5 millièmes en base 10.

En adaptant, développant et précisant la stratégie introduite par Bourgain dans le cas particulier $g = 2$, notre objectif est de présenter une démonstration du cas général entièrement détaillée et rigoureuse. En particulier, nous corrigeons certaines inexactitudes de [5], nous développons et complétons certains arguments, ce qui nous amène parfois à procéder différemment. La preuve est fondée sur la méthode du cercle et combine des techniques d'analyse harmonique avec des résultats sur les zéros des fonctions L de Dirichlet et en particulier une région sans zéro très fine due à Iwaniec. La méthode du cercle permet dans ce contexte de résoudre des problèmes binaires qui sont habituellement hors d'atteinte sur les nombres premiers.

Dans les chapitres III, IV et V, nous étudions dans le contexte des corps finis, la répartition des « chiffres » de quelques suites remarquables. Le concept de « chiffre » que nous considérons a été introduit et étudié par Dartyge–Sárközy [12] et il est intéressant de noter qu'il est à la base de la représentation des corps finis dans les logiciels de calcul formel. L'étude de ces « chiffres » permet donc de mieux comprendre comment certaines suites sont représentées en pratique, ce qui a des implications cryptographiques.

Soient p un nombre premier et $r \geq 2$ un nombre entier. Posons $q = p^r$ et considérons le corps fini $\mathbb{F}_q$. Si $\mathcal{B} = \{e_1,\dots,e_r\}$ est une base de $\mathbb{F}_q$ vu comme $\mathbb{F}_p$-espace vectoriel alors tout $x \in \mathbb{F}_q$ s'écrit de façon unique en base $\mathcal{B}$:

$$x = \sum_{j=1}^{r} c_j e_j \tag{I.2}$$

avec $(c_1,\dots,c_r) \in (\mathbb{F}_p)^r$. Nous appelons $c_1,\dots,c_r$ les « chiffres » de x en base $\mathcal{B}$ (de même que dans [12]). Cette dénomination apparaît naturellement en remarquant que dans le cas

particulier où $\mathcal{B}$ est une base polynomiale i.e. $\mathcal{B} = \{1,g,\dots,g^{r-1}\}$ avec $g \in \mathbb{F}_q$ tel que $\mathbb{F}_p(g) = \mathbb{F}_q$, l'écriture (I.2) devient

$$x = \sum_{j=1}^{r} c_j g^{j-1} \tag{I.3}$$

qui peut être vu comme un analogue dans les corps finis de (I.1). Par ailleurs, (I.3) est une représentation de x très largement employée dans les logiciels de calcul formel (voir par exemple [71, chapitre 6]). Les éléments de $\mathbb{F}_q$ sont donc très souvent représentés en pratique par leurs « chiffres ».

Dans ce contexte, Dartyge–Sárközy [12] ont défini la fonction somme des chiffres $s_{\mathcal{B}}$ par

$$s_{\mathcal{B}}(x) = \sum_{j=1}^{r} c_j$$

et ont étudié de façon quantitative la répartition de la somme des chiffres des carrés, des générateurs et plus généralement des suites de la forme $(P(x))_{x\in\mathbb{F}_q}$ et $(P(g))_{g\in\mathcal{G}}$ où $P \in \mathbb{F}_q[X]$ et $\mathcal{G}$ est l'ensemble des générateurs de $\mathbb{F}_q^*$. D'autres résultats sur la répartition de ces « chiffres » ont été obtenus par Dartyge–Mauduit–Sárközy [11], Dietmann–Elsholtz–Shparlinski [16] et Gabdullin [23]. En particulier, une estimation du nombre de carrés dans $\mathbb{F}_q$ avec des chiffres manquants a été prouvée dans [11] et ensuite améliorée dans [16] et [23]. La structure algébrique des corps finis permet de résoudre des problèmes dont l'analogue dans les nombres entiers est actuellement hors d'atteinte (comme la répartition de la somme des chiffres des cubes en base 2).

Dans le chapitre III (dont le contenu est publié dans [65]), nous étudions la répartition de la somme des chiffres de suites remarquables dans $\mathbb{F}_q$ comme les puissances d-ièmes ou encore les éléments d'ordre d. Pour $P \in \mathbb{F}_q[X]$ et pour $s \in \mathbb{F}_p$, nous définissons

$$\mathcal{D}(P,s) = \{x \in \mathbb{F}_q : s_{\mathcal{B}}(P(x)) = s\}.$$

Dans [12], Dartyge et Sárközy ont estimé $|\mathcal{D}(P,s)|$:

Théorème B. *Si $P \in \mathbb{F}_q[X]$ est un polynôme de degré $n \geq 1$ avec $(n,q) = 1$ alors, pour tout $s \in \mathbb{F}_p$,*

$$\left||\mathcal{D}(P,s)| - \frac{q}{p}\right| \leq (n-1)\sqrt{q}. \tag{I.4}$$

Le cas particulier où P est de la forme $P = X^d$ est particulièrement intéressant car il permet d'étudier la répartition de la somme des chiffres des puissances d-ièmes. Dans ce cas, nous obtenons dans le chapitre III :

Théorème 3. *Si d divise $q-1$ alors, pour tout $s \in \mathbb{F}_p^*$, on a en posant $\delta = (q-1)/(p-1) \in \mathbb{N}$:*

$$\left||\mathcal{D}(X^d,s)| - \frac{q}{p}\right| \leq \begin{cases} (d-1)\sqrt{q}/p & \text{si } d \mid \delta, \\ (d-1)\sqrt{q}/\sqrt{p} & \text{sinon.} \end{cases} \tag{I.5}$$

Le théorème 3 permet de gagner au moins un facteur $1/\sqrt{p}$ par rapport à (I.4). De plus, dans le cas particulier où $d = 2$ (et donc $p \geq 3$), la majoration (I.5) est la meilleure possible puisque l'on montre que (I.5) est une égalité. Dans le cas du degré 2, nous obtenons plus généralement dans le chapitre III :

Théorème 4. *Si $p \geq 3$ et si $P(X) = a_2X^2 + a_1X + a_0 \in \mathbb{F}_q[X]$ avec $a_2 \neq 0$ alors, en notant $\nu_P = s_{\mathcal{B}}(a_0 - a_1^2(4a_2)^{-1})$, on a pour tout $s \in \mathbb{F}_p$,*

$$\left||\mathcal{D}(P,s)| - \frac{q}{p}\right| = \begin{cases} \dfrac{\sqrt{q}}{\sqrt{p}} & \text{si } s \neq \nu_P \text{ et } r \text{ est impair,} \\ \dfrac{\sqrt{q}}{p} & \text{si } s \neq \nu_P \text{ et } r \text{ est pair,} \\ 0 & \text{si } s = \nu_P \text{ et } r \text{ est impair,} \\ \dfrac{p-1}{p}\sqrt{q} & \text{si } s = \nu_P \text{ et } r \text{ est pair.} \end{cases}$$

Lorsque P est un polynôme de degré 2, nous obtenons en fait une formule exacte pour $|\mathcal{D}(P,s)| - \frac{q}{p}$ qui permet d'en déterminer non seulement la valeur absolue mais aussi le signe.

Nous étudions ensuite la répartition de la somme des chiffres des générateurs et plus généralement des suites de la forme $(P(g))_{g\in\mathcal{G}}$ où $P \in \mathbb{F}_q[X]$ et $\mathcal{G}$ est l'ensemble des générateurs de $\mathbb{F}_q^*$:

Théorème 5. *Si $P \in \mathbb{F}_q[X]$ est un polynôme de degré $n \geq 1$ avec $(n,q) = 1$ alors, pour tout $s \in \mathbb{F}_p$,*

$$\left||\mathcal{G} \cap \mathcal{D}(P,s)| - \frac{\varphi(q-1)}{p}\right| < \frac{\varphi(q-1)}{q-1}\left((n2^{\omega(q-1)} - 1)\sqrt{q} + 1\right). \tag{I.6}$$

Cela améliore un résultat de Dartyge–Sárközy [12] d'un facteur $\frac{\varphi(q-1)}{q-1}$. Le cas où P est un monôme est ici encore particulièrement intéressant car il permet d'étudier la répartition de la somme des chiffres des éléments d'ordre d pour $d \,|\, q-1$. Dans ce cas, nous obtenons des estimations plus précises que (I.6).

Dans le chapitre IV (dont le contenu est publié dans [66]), nous poursuivons l'étude de la répartition des chiffres des suites remarquables $(P(x))_{x\in\mathbb{F}_q}$ et $(P(g))_{g\in\mathcal{G}}$ où $P \in \mathbb{F}_q[X]$ et $\mathcal{G}$ est l'ensemble des générateurs de $\mathbb{F}_q^*$ en estimant le nombre d'éléments de ces suites ayant des chiffres préassignés.

Pour $1 \leq j \leq r$, nous notons ε_j la fonction j-ième chiffre définie sur $\mathbb{F}_q$ par

$$\varepsilon_j\left(\sum_{i=1}^{r} c_i e_i\right) = c_j$$

pour tout $(c_1,\ldots,c_r) \in (\mathbb{F}_p)^r$. Pour $P \in \mathbb{F}_q[X]$, pour $1 \leq k \leq r$, pour $J \subset \{1,\ldots,r\}$ avec $|J| = k$ et pour $\boldsymbol{\alpha} = (\alpha_j)_{j\in J} \in (\mathbb{F}_p)^k$, nous considérons l'ensemble $\mathcal{F}_q(P,k,J,\boldsymbol{\alpha})$ formés par les éléments $x \in \mathbb{F}_q$ tels que pour tout $j \in J$, le j-ième chiffre de $P(x)$ dans la base $\mathcal{B}$ est α_j :

$$\mathcal{F}_q(P,k,J,\boldsymbol{\alpha}) = \{x \in \mathbb{F}_q : \varepsilon_j(P(x)) = \alpha_j \text{ pour tout } j \in J\}.$$

Si les chiffres de $P(x)$ se répartissent bien alors on s'attend à ce que $|\mathcal{F}_q(P,k,J,\boldsymbol{\alpha})| \approx q/p^k$, ce que nous montrons de façon quantitative :

Théorème 6. *Si $P \in \mathbb{F}_q[X]$ est un polynôme de degré $n \geq 1$ avec $(n,q) = 1$ alors, pour tout $1 \leq k \leq r$, pour tout $J \subset \{1,\dots,r\}$ avec $|J| = k$ et tout $\boldsymbol{\alpha} \in (\mathbb{F}_p)^k$, on a*

$$\left| |\mathcal{F}_q(P,k,J,\boldsymbol{\alpha})| - \frac{q}{p^k} \right| \leq \frac{p^k-1}{p^k}(n-1)\sqrt{q}. \tag{I.7}$$

En particulier, si

$$(n-1)(p^k-1) < \sqrt{q} = p^{r/2} \tag{I.8}$$

alors $\mathcal{F}_q(P,k,J,\boldsymbol{\alpha}) \neq \varnothing$.

On en déduit en prenant $P = X^2$ que si $p \geq 3$ alors pour tout $1 \leq k \leq r/2$, il existe un carré dans $\mathbb{F}_q$ avec k chiffres préassignés. Plus généralement, la condition (I.8) permet essentiellement de préassigner jusqu'à la moitié des chiffres (lorsque p est suffisamment grand par rapport à n). Le théorème 6 permet également de montrer que le nombre d'éléments $x \in \mathbb{F}_q$ tel que $P(x)$ a une proportion donnée $< 0{,}5$ de chiffres préassignés est asymptotiquement celui attendu :

Corollaire 7. *Pour tout $n \geq 1$, pour tout $\varepsilon > 0$, on a*

$$|\mathcal{F}_{p^r}(P,k,J,\boldsymbol{\alpha})| = p^{r-k}(1+o(1)) \quad (p^r \to +\infty, p \nmid n, r \geq 2)$$

uniformément pour $k \leq (1/2-\varepsilon)r$, $P \in \mathbb{F}_{p^r}[X]$ de degré n, $\mathcal{B}$ base de $\mathbb{F}_{p^r}$ sur $\mathbb{F}_p$, $J \subset \{1,\dots,r\}$ avec $|J| = k$ et $\boldsymbol{\alpha} \in (\mathbb{F}_p)^k$.

Dans le cas où $P = X^2$, nous améliorons (I.7) :

Théorème 8. *Si $p \geq 3$ alors, pour tout $1 \leq k \leq r$, pour tout $J \subset \{1,\dots,r\}$ avec $|J| = k$ et tout $\boldsymbol{\alpha} \in (\mathbb{F}_p)^k$, $\boldsymbol{\alpha} \neq 0$, on a*

$$\left| |\mathcal{F}_q(X^2,k,J,\boldsymbol{\alpha})| - \frac{q}{p^k} \right| \leq \begin{cases} \dfrac{\sqrt{q}}{\sqrt{p}} & \text{si } r \text{ est impair,} \\ \left(\dfrac{2}{p} - \dfrac{1}{p^k}\right)\sqrt{q} & \text{si } r \text{ est pair.} \end{cases} \tag{I.9}$$

Le théorème 8 permet de gagner essentiellement au moins un facteur $1/\sqrt{p}$ par rapport à (I.7). De plus, si $k = 1$ alors la majoration (I.9) est la meilleure possible puisque l'on montre que (I.9) est une égalité.

Nous estimons ensuite le nombre de générateurs g tels que $P(g)$ a des chiffres préassignés et nous en déduisons :

Corollaire 9. *Pour tout $n \geq 1$, pour tout $\varepsilon > 0$, on a*

$$|\mathcal{G} \cap \mathcal{F}_{p^r}(P,k,J,\boldsymbol{\alpha})| = \frac{\varphi(p^r-1)}{p^k}(1+o(1)) \quad (p^r \to +\infty, p \nmid n, r \geq 2)$$

uniformément pour $k \leq (1/2-\varepsilon)r$, $P \in \mathbb{F}_{p^r}[X]$ *de degré* n, $\mathcal{B}$ *base de* $\mathbb{F}_{p^r}$ *sur* $\mathbb{F}_p$, $J \subset \{1,\dots,r\}$ *avec* $|J| = k$ *et* $\boldsymbol{\alpha} \in (\mathbb{F}_p)^k$.

En particulier, le nombre de générateurs avec une proportion donnée $< 0{,}5$ de chiffres préassignés est asymptotiquement celui attendu.

Le corollaire 7 (resp. 9) implique que la connaissance de quelques chiffres de $P(x)$ (resp. $P(g)$) ne fournit (asymptotiquement) aucune information sur les autres chiffres de $P(x)$ (resp. $P(g)$), ce qui est crucial pour d'éventuelles applications en cryptographie.

Dans le chapitre V (dont le contenu est publié dans [67], à l'exception de la partie 7 dans laquelle nous présentons de nouveaux résultats), nous étudions la répartition de la trace (définie plus bas par (I.13)) des produits cd, $c \in \mathcal{C}$, $d \in \mathcal{D}$ avec $\mathcal{C},\mathcal{D} \subset \mathbb{F}_q^*$. Les résultats obtenus peuvent être formulés de façon équivalente en remplaçant la trace par la fonction somme des chiffres.

Si $\mathcal{C}$ et $\mathcal{D}$ sont deux ensembles assez grands alors les produits cd avec $c \in \mathcal{C}$ et $d \in \mathcal{D}$ devraient être « bien répartis ». Une question intéressante est alors de trouver une minoration précise de $|\mathcal{C}|$ et $|\mathcal{D}|$ qui permette d'assurer cette bonne répartition pour un critère d'aléa donné. De nombreux problèmes dans cet esprit ont été étudiés par Sárközy et ses co-auteurs. Par exemple, Rivat–Sárközy [59] ont montré que si $\mathcal{C}$ et $\mathcal{D}$ sont des sous-ensembles de $\{1,\dots,N\}$ assez grands alors la somme des chiffres de cd est bien répartie modulo m. Nous renvoyons à [59] pour une liste des articles écrits sur les propriétés arithmétiques des produits.

Soient $\mathcal{C}$ et $\mathcal{D}$ deux sous-ensembles quelconques de $\mathbb{F}_q^*$. Nous étudions la question suivante :

Question. Étant donné $\mathcal{A} \subset \mathbb{F}_p$, trouver une minoration précise de $|\mathcal{C}|$ et $|\mathcal{D}|$ qui permette d'assurer l'existence d'un produit cd avec $c \in \mathcal{C}$ et $d \in \mathcal{D}$ tel que $s_{\mathcal{B}}(cd) \in \mathcal{A}$.

Nous apportons des réponses quasi-optimales à cette question pour certains ensembles $\mathcal{A}$ « remarquables » : les singletons (pour étudier les produits dont la somme des chiffres est fixée), les sous-groupes de $\mathbb{F}_p^*$ (par exemple les carrés) et l'ensemble des générateurs de $\mathbb{F}_p^*$.

Lorsque $\mathcal{A} = \{s\}$ avec $s \in \mathbb{F}_p$, nous obtenons une estimation précise du nombre de couples $(c,d) \in \mathcal{C} \times \mathcal{D}$ tels que $s_{\mathcal{B}}(cd) = s$. Cela nous permet de répondre de façon quasi-optimale à la question précédente :

Théorème 10. *Si* $s \in \mathbb{F}_p^*$ *et si*

$$|\mathcal{C}||\mathcal{D}| \geq pq \tag{I.10}$$

alors il existe $(c,d) \in \mathcal{C} \times \mathcal{D}$ *tel que* $s_{\mathcal{B}}(cd) = s$.

La condition (I.10) est optimale à un facteur constant près : on peut construire des ensembles $\mathcal{C}$ et $\mathcal{D}$ tels que $pq/16 < |\mathcal{C}||\mathcal{D}| < pq$ et pour lesquels $s_{\mathcal{B}}(cd)$ n'est jamais égal à s.

Nous déduisons aussi de cette estimation la bonne répartition de la somme des chiffres des produits cd lorsque $\mathcal{C}$ et $\mathcal{D}$ sont assez grands :

Théorème 11. *Si* $\lim\limits_{q\to+\infty} \dfrac{|\mathcal{C}||\mathcal{D}|}{p^2q} = +\infty$ *alors les sommes des chiffres* $s_{\mathcal{B}}(cd)$ *sont bien réparties dans* $\mathbb{F}_p$.

L'étude du cas où $\mathcal{A}$ est un sous-groupe de $\mathbb{F}_p^*$ fait naturellement intervenir les quantités

$$\Delta_{\mathcal{A}}(\mathcal{C}) = \frac{|\mathcal{C}|}{q-1} - \frac{1}{m} \sum_{s \in \mathcal{A}\setminus\{1\}} \frac{|\mathcal{C} \cap s\mathcal{C}|}{|\mathcal{C}|}$$

où $m = |\mathcal{A}|$, $\mathcal{C} \subset \mathbb{F}_q^*$, $\mathcal{C} \neq \varnothing$ et nous permet d'obtenir :

Théorème 12. *Soit $\mathcal{A}$ un sous-groupe non-trivial de $\mathbb{F}_p^*$ et soit m son ordre. Si $\mathcal{C}$ et $\mathcal{D}$ vérifient*

$$|\mathcal{C}||\mathcal{D}| \geq \frac{4pq}{m^2} \tag{I.11}$$

et

$$\Delta_{\mathcal{A}}(\mathcal{C}) \geq -\frac{1}{m} \quad \textit{and} \quad \Delta_{\mathcal{A}}(\mathcal{D}) \geq -\frac{1}{m} \tag{I.12}$$

alors il existe $(c,d) \in \mathcal{C} \times \mathcal{D}$ tel que $s_{\mathcal{B}}(cd) \in \mathcal{A}$.

Ce résultat est une amélioration du théorème 1.6 du chapitre V que nous avions obtenu dans [67]. Il est démontré dans la section 7 du chapitre V.

La condition (I.11) est optimale à un facteur constant près : on peut construire des ensembles $\mathcal{C}$ et $\mathcal{D}$ vérifiant (I.12) tels que $|\mathcal{C}||\mathcal{D}| > pq/(16m^2)$ et pour lesquels $s_{\mathcal{B}}(cd)$ n'appartient jamais à $\mathcal{A}$.

Quant à la condition (I.12), nous montrons qu'elle est vraie avec une probabilité proche de 1 si q est grand (lorsque $\mathcal{C}$ et $\mathcal{D}$ parcourent des ensembles de taille fixée). Pour cela, nous étudions quelques propriétés des quantités $|\mathcal{C} \cap s\mathcal{C}|$ (voir les sections 6 et 7 du chapitre V), ce qui mène à des questions de nature combinatoire intéressantes dans les corps finis (voir les questions 1.5 et 6.2 du chapitre V).

En appliquant le théorème 12 dans le cas particulier où $p \geq 3$ et $\mathcal{A}$ est l'ensemble $\mathcal{Q}_p$ des carrés dans $\mathbb{F}_p^*$, on obtient que si

$$|\mathcal{C}||\mathcal{D}| \approx \frac{16q}{p}$$

(et si $\mathcal{C}$ et $\mathcal{D}$ vérifient une condition technique qui est très souvent vraie) alors il existe un produit cd tel que $s_{\mathcal{B}}(cd)$ est un carré. Remarquons que l'existence d'un tel produit cd n'est a priori pas du tout évidente car le nombre de $x \in \mathbb{F}_q$ tels que $s_{\mathcal{B}}(x) \notin \mathcal{Q}_p$ est $\frac{(p+1)q}{2p} \approx \frac{q}{2}$ qui est beaucoup plus grand que le nombre de produits cd (lorsque p est grand).

Les sommes d'exponentielles sur les corps finis jouent un rôle essentiel dans les chapitres III, IV et V. Les méthodes développées font intervenir des sommes de Weil, des sommes de Gauss et diverses sommes de caractères additifs et multiplicatifs de $\mathbb{F}_q$ pour lesquelles nous disposons ou nous pouvons obtenir des estimations explicites très précises voire optimales dans certains cas.

Les résultats présentés dans les chapitres III et IV peuvent être reformulés d'un point de vue plus algébrique, notamment grâce à la fonction trace $\mathrm{Tr} : \mathbb{F}_q \to \mathbb{F}_p$ définie par :

$$\mathrm{Tr}(x) = x + x^p + \cdots + x^{p^{r-1}} \tag{I.13}$$

(c'est le point de vue adopté dans le chapitre V). Cette fonction est une forme $\mathbb{F}_p$-linéaire qui est particulièrement importante dans l'étude des corps finis. Elle permet par exemple de décrire simplement toutes les formes $\mathbb{F}_p$-linéaires : pour toute forme $\mathbb{F}_p$-linéaire f, il existe un unique $b \in \mathbb{F}_q$ tel que

$$\forall x \in \mathbb{F}_q,\ f(x) = \mathrm{Tr}(bx).$$

En particulier, comme la fonction somme des chiffres $s_{\mathcal{B}}$ est une forme $\mathbb{F}_p$-linéaire, il existe un unique $b \in \mathbb{F}_q$ (b est la somme des éléments de la base duale de $\mathcal{B}$) tel que

$$\forall x \in \mathbb{F}_q,\ s_{\mathcal{B}}(x) = \mathrm{Tr}(bx),$$

ce qui permet de reformuler un résultat sur la somme des chiffres en un résultat sur la trace et vice-versa. Remarquons également que si f est une forme $\mathbb{F}_p$-linéaire non nulle alors il existe une base $\mathcal{B}$ telle que $f = s_{\mathcal{B}}$. Une propriété de la fonction $s_{\mathcal{B}}$ vraie dans toute base $\mathcal{B}$ est donc automatiquement vraie pour toute forme $\mathbb{F}_p$-linéaire non nulle, en particulier la trace.

Notons que parallèlement au concept de « chiffre » dans $\mathbb{F}_q$ qui est présenté et étudié ici, d'autres concepts de « chiffres » dans les corps finis ont fait l'objet de nombreux travaux. En particulier, dans $\mathbb{F}_q[X]$, les coefficients d'un polynôme P peuvent naturellement être appelés les chiffres de P et des résultats récents ont été obtenus concernant leur répartition.

Pollack [56] puis Ha [27] ont par exemple estimé le nombre de polynômes irréductibles dans $\mathbb{F}_q[X]$ avec des coefficients préassignés, étudiant ainsi un analogue dans $\mathbb{F}_q[X]$ du nombre de nombres premiers avec des chiffres préassignés. Plus précisément, Ha [27] a pu montrer en utilisant les techniques développées par Bourgain dans [4] l'existence d'un polynôme irréductible de degré n avec une proportion donnée $<1/4$ de coefficients préassignés (pour q assez grand). Ha a aussi obtenu une formule asymptotique pour le nombre de polynômes irréductibles de degré n avec r coefficients préassignés lorsque $r = o(n)$. L'obtention d'une telle formule lorsqu'une proportion positive des chiffres sont préassignés demeure un problème ouvert.

Dans une autre direction, Porritt [57] a estimé le nombre de polynômes irréductibles avec des coefficients manquants, étudiant ainsi un analogue dans $\mathbb{F}_q[X]$ des travaux de Maynard [48] sur les nombres premiers avec des chiffres manquants.

Plusieurs propriétés de répartition de la fonction somme des chiffres et plus généralement de fonctions Q-additives (où $Q \in \mathbb{F}_q[X]$) ont aussi été étudiées dans ce contexte notamment par Drmota–Gutenbrunner [17] et Car–Mauduit [6, 7, 8]. En particulier, Car–Mauduit [8] ont obtenu une formule asymptotique pour le nombre de polynômes irréductibles de degré n ayant un poids (nombre de coefficients non nuls) donné proche de la valeur moyenne.

II. Nombres premiers avec une proportion positive de chiffres préassignés

Le contenu de ce chapitre est soumis pour publication.

Abstract. Bourgain (2015) estimated the number of prime numbers with a proportion $c > 0$ of preassigned digits in base 2 (c is a fixed constant not specified). We establish a generalization of this result in any base $g \geq 2$ and we provide explicit admissible values for the proportion c depending on g. Our proof, which develops and enhances Bourgain's arguments, is based on the circle method and combines techniques from harmonic analysis together with results on zeros of Dirichlet L-functions, notably a very sharp zero-free region due to Iwaniec.

Table of contents

1. Introduction

Throughout this paper, g is an integer greater than or equal to 2 and the letter p denotes a prime number. Any integer $k \geq 0$ can be written uniquely in base g as

$$k = \sum_{j \geq 0} \varepsilon_j(k) g^j$$

where, for any $j \geq 0$, $\varepsilon_j(k) \in \{0, \dots, g-1\}$ is the j-th digit of k in base g. We denote by Λ the von Mangoldt function and by φ the Euler's totient function.

1.1. Pseudo-randomness of the digits of primes

The digits of integers k such that $0 \leq k < g^n$ can be seen as n independent random variables and thus possess properties in connection with this independence. When one restrict to primes p such that $0 \leq p < g^n$, the n digits are no longer independent. The general question: "For a given property of the digits of integers, do the digits of primes still possess this property?" is therefore at the source of many challenging problems. One of them is the Gelfond's conjecture about primes according to which the sum of digits of primes is well-distributed in arithmetic progressions. Fouvry–Mauduit [21] and Dartyge–Tenenbaum [13] obtained results in this direction for almost primes. Mauduit–Rivat [44] then proved Gelfond's conjecture and Drmota–Mauduit–Rivat [18] obtained a local limit law for the sum of digits of primes (when it is close to the average value).

1.2. Primes in sparse sets

Looking for primes in sparse sets of integers (i.e. sets with zero density) is a classical and important problem in Number Theory, for which there are few results. The existence of infinitely many primes of the form $2^n - 1$ (Mersenne primes) or of the form $n^2 + 1$ are still open questions which seem to be out of reach of present methods. Friedlander–Iwaniec [22] established the existence of infinitely many primes of the form $m^2 + n^4$ and Heath-Brown [31] for primes of the form $m^3 + 2n^3$. Rivat–Sargos [58] obtained an asymptotic formula for the number of primes of the form $\lfloor n^c \rfloor$ (Piatetski-Shapiro primes) for c in the range $1 < c < 1.16...$. It is natural to look for primes in sparse sets defined by digital properties. In this direction, we can mention [18] and Maynard [46, 48] who proved that, in a sufficiently large base, there are infinitely many primes with one missing digit in their digital expansion (e.g. there are infinitely many primes with no digit 9 in base 10).

1.3. Primes with preassigned digits

Let n be a large integer, $A \subset \{0, \dots, n-1\}$, $\boldsymbol{d} = (d_j)_{j \in A} \in \{0, \dots, g-1\}^A$ and denote

$$\mathcal{D}(n, A, \boldsymbol{d}) = \{0 \leq k < g^n : \forall j \in A,\ \varepsilon_j(k) = d_j\}.$$

We will focus our interest on the following question.

Question. Estimate the number of primes in $\mathcal{D}(n, A, \boldsymbol{d})$ when $|A|$ is as large as possible with (almost) no restriction on the set A itself and on the digits d_j.

Since $|\mathcal{D}(n, A, \boldsymbol{d})| = g^{n-|A|}$, the set $\mathcal{D}(n, A, \boldsymbol{d})$ is sparse whenever both $n \to \infty$ and $|A| \to \infty$. This question is thus a way to contribute to the study of primes in sparse sets (see Section 1.2). It also allows us to explore the pseudo-randomness of the digits of primes (see Section 1.1).

In 2005, Wolke [70] established an asymptotic formula for the number of primes in $\mathcal{D}(n, A, \boldsymbol{d})$ when $|A| \leq 2$ i.e. at most two digits are preassigned. He also proved that, under the Generalized Riemann Hypothesis, one can preassign up to $(1-\varepsilon)\sqrt{n}$ digits. Then, in 2006, Harman [29] obtained a lower bound for the number of primes with an arbitrarily large but fixed number of preassigned digits. Two years later, Harman–Kátai [30] corrected and improved the proofs in a previous paper [37] of Kátai who had actually already studied primes with preassigned digits in 1986. They improved all previous known results by obtaining an asymptotic formula when $|A| \ll \sqrt{n}(\log n)^{-1}$. Bourgain made an important step forward in 2013 [4] by obtaining an asymptotic formula when $|A| \ll n^{4/7}(\log n)^{-4/7}$ in base 2 and in 2015, he made an impressive breakthrough by proving that one can preassign a positive proportion of the binary digits [5].

Theorem A (Bourgain, [5])**.** *There exists an absolute constant $c > 0$ such that, for any $A \subset \{0, \dots, n-1\}$ satisfying $0 \in A$ and $|A| \leq cn$ and for any $(d_j)_{j\in A} \in \{0,1\}^A$ such that $d_0 = 1$,*

$$\sum_{\substack{0\leq k<2^n \\ \forall j\in A,\, \varepsilon_j(k)=d_j}} \Lambda(k) = 2^{n-|A|+1}\,(1+o(1))$$

as $n \to \infty$.

At the end of [5], Bourgain obtains the result above. His main result is an asymptotic formula for $|\{p < g^n : \forall j \in A,\, \varepsilon_j(k) = d_j\}|$ under the same hypotheses, but we will see in Remark 2.6 that a further hypothesis is needed.

The proportion c is not made explicit in [5] and permits us to measure how sparse the set in which we are looking for primes is. There are at least two "simple" special cases for which we already have an explicit admissible value for c. If the preassigned digits are the left-most digits then we are led to count primes in a short interval. The best estimate due to Huxley (see for instance [35, p. 265]) then allows us to preassign at most $(5/12-\varepsilon)n$ digits. If the preassigned digits are the right-most digits then we are led to count primes in arithmetic progressions. A result of Baker and Zhao (see [1, Theorem 1]) would then allow us to preassign at most $(5/12-\varepsilon)n$ digits. Even under the Generalized Riemann Hypothesis, in both cases, the best proportion of digits we are able to preassign is $1/2-\varepsilon$. Without any hypothesis on the positions of the preassigned digits, it would be very ambitious to expect obtaining a proportion larger than $1/2$.

We will provide an asymptotic formula for the number of primes with a positive proportion of preassigned digits in a general base g. Our work mainly follows the strategy introduced by Bourgain in the case $g = 2$ and the one suggested by Maynard for $g \geq 3$ in [47] with the aim to present a detailed and rigorous proof. In particular, we will correct in [5] some inaccuracies,

develop and complete some arguments and sometimes this will lead us to proceed in a different way. Moreover, we will provide explicit admissible values for c depending on g.

2. Statement of the results

For technical reasons, we will assume that the least significant digit is preassigned. Since there is a finite number of possible values, this will not be restrictive in applications. Moreover, if $d_0 \in \{0, \dots, g-1\}$ is such that $(d_0, g) > 1$ then there is at most one prime number whose least significant digit is d_0. We will therefore assume that the least significant digit is coprime to the base.

We will first establish an asymptotic formula for the mean value of the von Mangoldt function along primes with preassigned digits.

Theorem 2.1. *Let $g \geq 2$ be an integer and $\delta_0 \geq 0$ be a real number. There is an explicit $c_0 = c_0(g, \delta_0) \in]0, 1/2[$ with the following property. For any $0 < c < c_0$, there exist $n_0 = n_0(g, \delta_0, c) \geq 1$ and $\delta = \delta(g, \delta_0, c) > \delta_0$ such that for any integer $n \geq n_0$, $A \subset \{0, \dots, n-1\}$ satisfying $0 \in A$ and*

$$|A| \leq cn$$

and for any $(d_j)_{j\in A} \in \{0, \dots, g-1\}^A$ such that $(d_0, g) = 1$, we have

$$\sum_{\substack{0\leq k<g^n \\ \forall j\in A,\, \varepsilon_j(k)=d_j}} \Lambda(k) = g^{n-|A|}\frac{g}{\varphi(g)}\left(1 + O_{g,\delta_0,c}\left(n^{-\delta}\right)\right). \tag{II.1}$$

Remark 2.2. We will define an admissible $c_0 = c_0(g, \delta_0)$ in Theorem 13.3.

Remark 2.3. We will provide explicit admissible values of c_0 in Theorem 2.7. The largest value of c_0 will be obtained for $\delta_0 = 0$.

Remark 2.4. The parameter δ_0 permits us to control the accuracy of the estimate: by taking a larger δ_0, we obtain a more precise estimate but a smaller c_0.

For $A \subset \{0, \dots, n-1\}$ and $(d_j)_{j\in A} \in \{0, \dots, g-1\}^A$ such that $0 \in A$ and $(d_0, g) = 1$, we define

$$E_1 = \{p < g^n : \varepsilon_0(p) = d_0\} \quad \text{and} \quad E_2 = \{0 \leq k < g^n : \forall j \in A \setminus \{0\},\, \varepsilon_j(k) = d_j\}.$$

We have $|E_2| = g^{n-|A|+1}$ and, by the Prime Number Theorem along arithmetic progressions (see [69, p. 360]), $|E_1| \sim \frac{g^n}{\varphi(g)\log g^n}$ as $n \to \infty$. If k is a randomly chosen integer in $[0, g^n[$ then we expect the events "$k \in E_1$" and "$k \in E_2$" to be "independent" and thus, heuristically,

$$|E_1 \cap E_2| \sim g^n \frac{1}{\varphi(g)\log g^n} g^{-|A|+1} = \frac{g^{n-|A|}}{\log g^n}\frac{g}{\varphi(g)}$$

as $n \to \infty$. The following theorem establishes this in a quantitative way.

Theorem 2.5. *Let $g \geq 2$ be an integer and $\delta_0 \geq 0$ be a real number. Let $c_0 = c_0(g, \delta_0) \in]0, 1/2[$ be as in Theorem 2.1. For any $0 < c < c_0$, there exist $n_0 = n_0(g, \delta_0, c) \geq 1$ and $\delta = \delta(g, \delta_0, c) > \delta_0$ such that for any integer $n \geq n_0$, $A \subset \{0, \dots, n-1\}$ satisfying $0 \in A$, $n-1 \in A$ and*

$$|A| \leq cn,$$

for any $(d_j)_{j\in A} \in \{0, \dots, g-1\}^A$ such that $(d_0, g) = 1$ and $d_{n-1} \geq 1$, we have

$$|\{p < g^n : \forall j \in A,\ \varepsilon_j(p) = d_j\}| = \frac{g^{n-|A|}}{\log g^n} \frac{g}{\varphi(g)} \left(1 + O_{g,\delta_0,c}\left(n^{-\min(1,\delta)}\right)\right). \tag{II.2}$$

Remark 2.6. The conditions $n-1 \in A$ and $d_{n-1} \geq 1$ cannot be removed in Theorem 2.5 (they were omitted in the main theorem of [5]). Indeed, if $A = \{0, n-r, \dots, n-1\}$ (with $1 \leq r \leq n-1$), $d_{n-r} = \cdots = d_{n-1} = 0$ and d_0 is such that $0 \leq d_0 \leq g-1$ and $(d_0, g) = 1$ then, by the Prime Number Theorem along arithmetic progressions, we obtain

$$\sum_{\substack{p<g^n \\ \forall j\in A,\, \varepsilon_j(p)=d_j}} 1 = \sum_{\substack{p<g^{n-r} \\ p\equiv d_0 \bmod g}} 1 \sim \frac{g^{n-r}}{\log g^{n-r}} \frac{1}{\varphi(g)} = \frac{g^{n-|A|}}{\left(1 - \frac{r}{n}\right) \log g^n} \frac{g}{\varphi(g)}$$

as $n - r \to \infty$, which differs from (II.2) when $r \neq o(n)$.

The following theorem provides explicit admissible values of c_0 (see Section 15 for explicit admissible values of c_0 under GRH).

Theorem 2.7. *Theorem 2.1 holds with $c_0 = c_0(g, \delta_0)$ given in Table II.1.*

δ_0 \ g	2	3	4	5	6	10	10^3	$2 \cdot 3^{100}$	2^{200}
0	2.1	3.1	3.6	4.0	4.2	4.7	6.8	0.7	9.0
0.5	2.1	3.0	3.6	3.9	4.1	4.6	6.6	0.7	8.6
1	2.0	3.0	3.5	3.8	4.0	4.5	6.4	0.7	8.3
10	1.7	2.3	2.6	2.8	2.9	3.2	4.2	0.7	5.1
100	0.71	0.81	0.86	0.88	0.90	0.93	1.02	0.7	1.08

Table II.1. – $c_0(g, \delta_0) \cdot 10^3$

Remark 2.8. For general $g \geq 2$ and $\delta_0 \geq 0$, Theorem 2.1 holds with $c_0 = c_0(g, \delta_0)$ which is defined in Theorem 13.3 with the help of Lemmas 13.1 and 13.2 as the minimum between two solutions of some equations. We will establish in Section 13 the following properties of $c_0(g, \delta_0)$.

1. For any given $g \geq 2$, the largest value of $c_0(g, \delta_0)$ is obtained for $\delta_0 = 0$.
2. If $\mathcal{S} = \{p^\nu : p \text{ is prime and } \nu \geq 1\}$ then, for any $\delta_0 \geq 0$, the function $(g \in \mathcal{S}) \mapsto c_0(g, \delta_0)$ is increasing and in the special case where $\delta_0 = 0$, $\lim\limits_{\substack{g\to+\infty \\ g\in\mathcal{S}}} c_0(g, \delta_0) = 0.00927\ldots$.

3. If $a \geq 2$ is an integer then, for any $\delta_0 \geq 0$, the function $m \mapsto c_0(a^m, \delta_0)$ is increasing.
4. For any $\delta_0 \geq 0$, we have $c_0(g, \delta_0) < \frac{\log p_1^{\gamma_1}}{8 \log g}$ where $g = \prod_{i=1}^t p_i^{\gamma_i}$ with $p_1^{\gamma_1} = \min_{1 \leq i \leq t} p_i^{\gamma_i}$.

This last property explains why the values in the column corresponding to $g = 2 \cdot 3^{100}$ in Table II.1 are small.

3. Notations

We will use the following standard notations: $\mathrm{e}(x) = \exp(2i\pi x)$, $\|\theta\| = \min_{m \in \mathbb{Z}} |\theta - m|$, $\sigma_0(q) = \sum_{d \mid q} 1$, $\psi(x) = \sum_{k \leq x} \Lambda(k)$ and $\psi(x, \chi) = \sum_{k \leq x} \chi(k)\Lambda(k)$. The symbol $\sum^*_{\chi \bmod q}$ will denote a summation over all primitive characters χ mod q.

For any integer $n \geq 0$, $A \subset \mathbb{Z}$ and $\boldsymbol{d} = (d_j)_{j \in A} \in \{0, \dots, g-1\}^A$, we denote by $f_{n,A,\boldsymbol{d}}$ the indicator function of the integers $0 \leq k < g^n$ such that, for any $j \in A \cap \{0, \dots, n-1\}$, the j-th digit of k is d_j:

$$f_{n,A,\boldsymbol{d}}(k) = \begin{cases} 1 & \text{if } 0 \leq k < g^n \text{ and for any } j \in A \cap \{0, \dots, n-1\},\ \varepsilon_j(k) = d_j, \\ 0 & \text{otherwise.} \end{cases}$$

4. Structure of the proof of Theorem 2.1

Let $g \geq 2$ be a fixed integer. Let $n \geq 100$ be an integer, $A \subset \{0, \dots, n-1\}$ and $\boldsymbol{d} = (d_j)_{j \in A} \in \{0, \dots, g-1\}^A$ such that $0 \in A$ and $(d_0, g) = 1$. We denote $N = g^n$.

By using the circle method, we write

$$\sum_{1 \leq k \leq N} \Lambda(k) f_{n,A,\boldsymbol{d}}(k) = \int_0^1 S(\alpha)\overline{R(\alpha)} d\alpha \tag{II.3}$$

where

$$S(\alpha) = \sum_{1 \leq k \leq N} \Lambda(k)\, \mathrm{e}(k\alpha) \quad \text{and} \quad R(\alpha) = \sum_{1 \leq k \leq N} f_{n,A,\boldsymbol{d}}(k)\, \mathrm{e}(k\alpha).$$

The sum $R(\alpha)$ depends on digital conditions and $|S(\alpha)|$ can be large only when α is close to a rational with small denominator i.e. α is in a major arc. In order to define the major and minor arcs, we introduce two real parameters B_1 and B such that

$$g \leq B_1 \leq B < N \quad \text{and} \quad 4BB_1 < N \tag{II.4}$$

(B_1 and B will be chosen appropriately in Section 13.3 and will be small powers of N such that $B_1 = o(B)$). For $1 \leq q \leq B_1$ and $1 \leq a \leq q$ such that $(a, q) = 1$, we denote by $\mathfrak{M}(q, a)$ the interval $\left|\alpha - \frac{a}{q}\right| \leq \frac{B}{qN}$ modulo 1 i.e.

$$\mathfrak{M}(q, a) = \left(\left[\frac{a}{q} - \frac{B}{qN}, \frac{a}{q} + \frac{B}{qN} \right] + \mathbb{Z} \right) \cap [0, 1[$$

and we will say that $\mathfrak{M}(q,a)$ is a "major arc".

Lemma 4.1. *If $(q,a) \neq (q',a')$ then the major arcs $\mathfrak{M}(q,a)$ and $\mathfrak{M}(q',a')$ are disjoint.*

Proof. Since $0 < |a'q - aq'| < qq'$, we obtain

$$\left|\frac{a'}{q'} - \frac{a}{q}\right| \geq \frac{1}{qq'} \quad \text{and} \quad 1 - \left|\frac{a'}{q'} - \frac{a}{q}\right| \geq \frac{1}{qq'}.$$

Moreover, since $2BB_1 < N$,

$$\frac{B}{qN} + \frac{B}{q'N} = \frac{B}{N}\frac{q+q'}{qq'} \leq \frac{2BB_1}{Nqq'} < \frac{1}{qq'}$$

and it follows from the definition of the major arcs $\mathfrak{M}(q,a)$ and $\mathfrak{M}(q',a')$ that they are disjoint. □

We then denote by $\mathfrak{M}$ the union of these disjoint major arcs:

$$\mathfrak{M} = \bigcup_{1\leq q\leq B_1} \bigcup_{\substack{1\leq a\leq q \\ (a,q)=1}} \mathfrak{M}(q,a)$$

and by $\mathfrak{m}$ ("minor arcs") the complement in $[0,1[$ of $\mathfrak{M}$.

Remark 4.2. Our definition of $\mathfrak{M}$ differs from the one given in [5] where q runs over the larger interval $1 \leq q < B$. The interest to restrict q to run only over the interval $1 \leq q \leq B_1$ where B_1 is an additional parameter such that $B_1 = o(B)$ will appear in Remark 9.8.

We will bound the contribution of the minor arcs in Section 8 by using a very sharp estimate for the L^1-norm of the Fourier transform of $f_{n,A,\boldsymbol{d}}$. The contribution of the major arcs will be studied in Sections 9 and 11. We will switch to multiplicative characters, establish an estimate for the contribution of the principal ones (in Section 11.1) and bound the contribution of the nonprincipal ones (in Section 11.2).

For the principal characters, we will directly use a result on primes in short intervals. Compared to [5], this will allow us to avoid the use of the explicit formula for ψ, a zero-free region and a zero-density estimate for ζ. We will also need sharp estimates on the Fourier transform of $f_{n,A,\boldsymbol{d}}$.

For the contribution of the nonprincipal characters, while retaining some ideas of [5], we proceed in a different way (indeed, in [5], the fact that (4.8) can be estimated by (4.23) is not clear), see Section 11.2. We will subdivide the primitive characters χ_1 in two classes "good" and "bad" depending on the zero-free region of $L(s,\chi_1)$.

For the "good" characters (see Section 11.2.1) for which we have a good zero-free region, we will rely on zero-density estimates for Dirichlet L-functions.

For the "bad" characters (see Section 11.2.2) which form a small set of characters, we will rely on sharp estimates for the Fourier transform of $f_{n,A,\boldsymbol{d}}$. Nevertheless, the possible characters whose conductor q_1 would be such that any prime factor of q_1 divides g would be out of control.

We will show that such characters actually do not exist by using an improved zero-free region for Dirichlet L-functions to a smooth modulus. The study of the "bad" characters is the most tricky part to generalize from base 2 to a general base g. If g has several prime factors then new difficulties occur (see Remarks 5.35 and 11.12).

Sections 5, 6 and 7 are dedicated to preliminary results. All the required estimates on the Fourier transform of $f_{n,A,\boldsymbol{d}}$ will be established in Section 5. In Section 6, we will provide a precise and "ready to use" version of the improved zero-free region for L-functions to a smooth modulus which is an essential argument in the study of the "bad" characters. Indeed, this zero-free region is of independent interest and in [5], the author refers to [30] for this result but it does not appear explicitly in [30].

Since we seek for an explicit value of c_0, as large as possible, we make all involved constants explicit and we try to optimize them. In particular, we avoid as far as possible any arbitrary choices of parameters which were sufficient in [5] to establish the existence of c_0.

5. Bounds for the Fourier transform of $f_{n,A,\boldsymbol{d}}$ and consequences

For any integer $n \geq 0$, $A \subset \mathbb{Z}$ and $\boldsymbol{d} = (d_j)_{j\in A} \in \{0,\dots,g-1\}^A$, we denote by $F_{n,A,\boldsymbol{d}}$ the discrete Fourier transform of $f_{n,A,\boldsymbol{d}}$, defined for any $\lambda \in \mathbb{R}$ by

$$F_{n,A,\boldsymbol{d}}(\lambda) = g^{-n} \sum_{0\leq k<g^n} f_{n,A,\boldsymbol{d}}(k)\,\mathrm{e}\,(-k\lambda) = g^{-n} \sum_{\substack{0\leq k<g^n \\ \varepsilon_j(k)=d_j \\ \forall j\in A\cap\{0,\dots,n-1\}}} \mathrm{e}\,(-k\lambda)$$

(note that $F_{n,A,\boldsymbol{d}}$ is periodic with period 1) and by $\|F_{n,A,\boldsymbol{d}}\|_1$ the L^1-norm of $F_{n,A,\boldsymbol{d}}$:

$$\|F_{n,A,\boldsymbol{d}}\|_1 = \int_0^1 |F_{n,A,\boldsymbol{d}}(\lambda)|\,d\lambda.$$

In Section 5.1, we will establish a very sharp upper bound of $\|F_{n,A,\boldsymbol{d}}\|_1$ (see Proposition 5.11). Then, in Section 5.2, we will provide upper bounds of $|F_{n,A,\boldsymbol{d}}(a/q)|$ on average and individually. In Section 5.3, we will use a result of Section 5.2 to estimate the number of integers with preassigned digits in arithmetic progressions and derive other estimates. Finally, in Section 5.4, we will use a result of Section 5.2 to estimate character sums over integers with preassigned digits in arithmetic progressions.

5.1. Upper bound of $\|F_{n,A,\boldsymbol{d}}\|_1$

The purpose of this section is to establish Proposition 5.11 which will be essential in the study of the minor arcs. For any integer $q \geq 1$, let Φ_q be the even periodic function with

period 1 defined by

$$\Phi_q(t) = \left| \sum_{0 \le v < q} \mathrm{e}(vt) \right| = \begin{cases} \frac{|\sin \pi q t|}{|\sin \pi t|} & \text{if } t \in \mathbb{R} \setminus \mathbb{Z}, \\ q & \text{if } t \in \mathbb{Z}. \end{cases} \tag{II.5}$$

Lemma 5.1. *If $n \ge 0$, $A \subset \mathbb{Z}$, $\boldsymbol{d} = (d_j)_{j \in A} \in \{0, \dots, g-1\}^A$ then, for any $\lambda \in \mathbb{R}$,*

$$|F_{n,A,\boldsymbol{d}}(\lambda)| = P_{n,A}(\lambda)$$

where

$$P_{n,A}(\lambda) = g^{-n} \prod_{\substack{0 \le j \le n-1 \\ j \notin A}} \Phi_g\left(\lambda g^j\right) = g^{-|A \cap \{0,\dots,n-1\}|} \prod_{\substack{0 \le j \le n-1 \\ j \notin A}} \frac{\Phi_g\left(\lambda g^j\right)}{g} \ge 0. \tag{II.6}$$

Proof. For $n = 0$, we trivially have $|F_{0,A,\boldsymbol{d}}(\lambda)| = 1 = P_{0,A}(\lambda)$. For $n \ge 1$, we denote $\mathcal{A} = A \cap \{0, \dots, n-1\}$, $\mathcal{B} = \{0, \dots, n-1\} \setminus \mathcal{A}$ and we write

$$\begin{aligned} F_{n,A,\boldsymbol{d}}(\lambda) &= g^{-n} \sum_{\substack{0 \le k < g^n \\ \varepsilon_j(k) = d_j \\ \forall j \in A \cap \{0,\dots,n-1\}}} \mathrm{e}\left(-\lambda k\right) \\ &= g^{-n} \sum_{(\varepsilon_j)_{j \in \mathcal{B}} \in \{0,\dots,g-1\}^{\mathcal{B}}} \mathrm{e}\left(-\lambda \left(\sum_{j \in \mathcal{B}} \varepsilon_j g^j + \sum_{j \in \mathcal{A}} d_j g^j \right)\right) \\ &= g^{-n} \prod_{j \in \mathcal{A}} \mathrm{e}\left(-\lambda d_j g^j\right) \sum_{(\varepsilon_j)_{j \in \mathcal{B}} \in \{0,\dots,g-1\}^{\mathcal{B}}} \prod_{j \in \mathcal{B}} \mathrm{e}\left(-\lambda \varepsilon_j g^j\right) \\ &= g^{-n} \prod_{j \in \mathcal{A}} \mathrm{e}\left(-\lambda d_j g^j\right) \prod_{j \in \mathcal{B}} \sum_{0 \le \varepsilon \le g-1} \mathrm{e}\left(-\lambda \varepsilon g^j\right), \end{aligned}$$

it follows that

$$|F_{n,A,\boldsymbol{d}}(\lambda)| = g^{-n} \prod_{j \in \mathcal{B}} \Phi_g\left(\lambda g^j\right) = P_{n,A}(\lambda)$$

which completes the proof. □

In order to obtain a sharp upper bound of $\|F_{n,A,\boldsymbol{d}}\|_1$, we will first estimate

$$\sum_{0 \le h < g^n} \left| F_{n,A,\boldsymbol{d}}(hg^{-n}) \right| \tag{II.7}$$

which can be seen as the "discrete L^1-norm" of $F_{n,A,\boldsymbol{d}}$. By Lemma 5.1, this does not depend on $\boldsymbol{d}$ and is equal to $\mathcal{N}_1(n, A)$ defined by

$$\mathcal{N}_1(n, A) = \sum_{0 \le h < g^n} P_{n,A}(hg^{-n}).$$

Lemma 5.2. *If $n \geq 1$, $A \subset \mathbb{Z}$ and $0 \in A$ then*

$$\mathcal{N}_1(n, A) = \mathcal{N}_1(n-1, A-1).$$

Proof. By division of h by g^{n-1} and by (II.6),

$$\begin{aligned}\mathcal{N}_1(n, A) &= \sum_{0 \leq h < g^n} P_{n,A}(hg^{-n}) = \sum_{0 \leq r < g} \sum_{0 \leq h < g^{n-1}} P_{n,A}((h + rg^{n-1})g^{-n}) \\ &= \sum_{0 \leq r < g} \sum_{0 \leq h < g^{n-1}} g^{-n} \prod_{\substack{0 \leq j \leq n-1 \\ j \notin A}} \Phi_g\left(hg^{j-n} + rg^{j-1}\right).\end{aligned}$$

Since $0 \in A$, $j = 0$ does not contribute in the product and since Φ_g has period 1, it follows that

$$\begin{aligned}\mathcal{N}_1(n, A) &= g \sum_{0 \leq h < g^{n-1}} g^{-n} \prod_{\substack{1 \leq j \leq n-1 \\ j \notin A}} \Phi_g\left(hg^{j-n}\right) \\ &= \sum_{0 \leq h < g^{n-1}} g^{-(n-1)} \prod_{\substack{0 \leq j \leq n-2 \\ j \notin A-1}} \Phi_g\left(hg^{j-(n-1)}\right) \\ &= \sum_{0 \leq h < g^{n-1}} P_{n-1,A-1}(hg^{-(n-1)}) \\ &= \mathcal{N}_1(n-1, A-1)\end{aligned}$$

which completes the proof. □

To study the case where $0 \notin A$, we will use the following lemma.

Lemma 5.3. *For any integers $q \geq 1$, $\nu \geq 1$ and any $t \in \mathbb{R}$,*

$$\Phi_{q^\nu}(t) = \prod_{0 \leq j \leq \nu-1} \Phi_q(q^j t).$$

Proof. For $q = 1$, since $\Phi_1 = 1$, this is trivial. For $q \geq 2$, this follows immediately from (II.5) by writing v in base q. □

For any integer $q \geq 1$, we denote by Ψ_q the periodic function with period $1/q$ defined for any $t \in \mathbb{R}$ by

$$\Psi_q(t) = \frac{1}{q} \sum_{0 \leq r < q} \Phi_q\left(t + \frac{r}{q}\right) \tag{II.8}$$

and we also define

$$M(q) = \max_{t \in \mathbb{R}} \Psi_q(t). \tag{II.9}$$

Note that $\Psi_1 = 1$ and $M(1) = 1$.

Lemma 5.4. *If $1 \leq m \leq n$ and if $A \subset \mathbb{Z}$ are such that*

$$0 \leq j \leq m-1 \Rightarrow j \notin A$$

then

$$\mathcal{N}_1(n,A) = \sum_{0\le h<g^{n-m}} \Psi_{g^m}(hg^{-n}) P_{n-m,A-m}(hg^{-(n-m)}).$$

In particular,

$$\mathcal{N}_1(n,A) \le M(g^m)\,\mathcal{N}_1(n-m,A-m).$$

Proof. By division of h by g^{n-m} and by (II.6),

$$\mathcal{N}_1(n,A) = \sum_{0\le h<g^n} P_{n,A}(hg^{-n}) = \sum_{0\le r<g^m} \sum_{0\le h<g^{n-m}} g^{-n} \prod_{\substack{0\le j\le n-1\\ j\notin A}} \Phi_g\left((h+rg^{n-m})g^{j-n}\right).$$

Since $0 \le j \le m-1 \Rightarrow j \notin A$ and since Φ_g has period 1, it follows that

$$\mathcal{N}_1(n,A) = \sum_{0\le r<g^m} \sum_{0\le h<g^{n-m}} g^{-n} \left(\prod_{0\le j\le m-1} \Phi_g\left(hg^{j-n}+rg^{j-m}\right)\right)\left(\prod_{\substack{m\le j\le n-1\\ j\notin A}} \Phi_g\left(hg^{j-n}\right)\right).$$

Moreover, for any $0 \le h < g^{n-m}$, by (II.6),

$$\prod_{\substack{m\le j\le n-1\\ j\notin A}} \Phi_g\left(hg^{j-n}\right) = \prod_{\substack{0\le j\le n-m-1\\ j\notin A-m}} \Phi_g\left(hg^{j-(n-m)}\right) = g^{n-m} P_{n-m,A-m}(hg^{-(n-m)})$$

and by Lemma 5.3 and the definition of Ψ_g (see (II.8)),

$$\sum_{0\le r<g^m} \prod_{0\le j\le m-1} \Phi_g\left(hg^{j-n}+rg^{j-m}\right) = \sum_{0\le r<g^m} \Phi_{g^m}(hg^{-n}+rg^{-m}) = g^m \Psi_{g^m}(hg^{-n}).$$

This gives

$$\mathcal{N}_1(n,A) = \sum_{0\le h<g^{n-m}} \Psi_{g^m}(hg^{-n}) P_{n-m,A-m}(hg^{-(n-m)})$$

which completes the proof. □

Lemma 5.5. *If $1 \le m \le n$ and if $A \subset \mathbb{Z}$ are such that $0 \in A$ and*

$$1 \le j \le m-1 \Rightarrow j \notin A$$

then

$$\mathcal{N}_1(n,A) \le M(g^{m-1})\,\mathcal{N}_1(n-m,A-m).$$

Proof. By Lemma 5.2, since $0 \in A$,

$$\mathcal{N}_1(n, A) = \mathcal{N}_1(n-1, A-1).$$

For $m = 1$, since $M(1) = 1$, this completes the proof. For $m \geq 2$, since $0 \leq j \leq m-2$ implies $j \notin A - 1$, by Lemma 5.4,

$$\mathcal{N}_1(n-1, A-1) \leq M(g^{m-1})\mathcal{N}_1(n-m, A-m)$$

which completes the proof. □

Lemma 5.6. *Let $n \geq 1$, $0 \leq r \leq n-1$ and $0 \leq j_0 < j_1 < \cdots < j_r \leq n-1$. If $A = \{j_0, j_1, \ldots, j_r\}$ and $j_{r+1} = n$ then*

$$\mathcal{N}_1(n, A) \leq M(g^{j_0}) \prod_{s=0}^{r} M(g^{j_{s+1}-j_s-1}).$$

Proof. For $0 \leq s \leq r$, applying Lemma 5.5 with $n' = n - j_s$, $m' = j_{s+1} - j_s$ and $A' = A - j_s$ which satisfy

$$1 \leq j \leq m' - 1 \Rightarrow j \notin A',$$

we obtain

$$\mathcal{N}_1(n - j_s, A - j_s) \leq M(g^{j_{s+1}-j_s-1})\mathcal{N}_1(n - j_{s+1}, A - j_{s+1}).$$

It follows that by taking $s = 0$, then $s = 1$, ... and $s = r$,

$$\begin{aligned}
\mathcal{N}_1(n - j_0, A - j_0) &\leq M(g^{j_1-j_0-1})\mathcal{N}_1(n - j_1, A - j_1) \\
&\leq M(g^{j_1-j_0-1})M(g^{j_2-j_1-1})\mathcal{N}_1(n - j_2, A - j_2) \\
&\leq \cdots \\
&\leq M(g^{j_1-j_0-1})M(g^{j_2-j_1-1}) \cdots M(g^{j_{r+1}-j_r-1})\mathcal{N}_1(n - j_{r+1}, A - j_{r+1}) \\
&= M(g^{j_1-j_0-1})M(g^{j_2-j_1-1}) \cdots M(g^{j_{r+1}-j_r-1})
\end{aligned}$$

since $j_{r+1} = n$ and $\mathcal{N}_1(0, A - n) = 1$. When $j_0 = 0$, since $M(g^{j_0}) = 1$, this proves the lemma. When $j_0 \geq 1$, since $0 \leq j \leq j_0 - 1 \Rightarrow j \notin A$, by applying Lemma 5.4 with $m = j_0$, we obtain

$$\mathcal{N}_1(n, A) \leq M(g^{j_0})\mathcal{N}_1(n - j_0, A - j_0),$$

which completes the proof. □

Lemma 5.7. *If $\nu \geq 1$ then*

$$M(g^{\nu-1}) \leq \frac{C_1(g)}{g}\nu$$

where

$$C_1(g) = \begin{cases} g & \text{if } g = 2 \text{ or } g = 3, \\ \dfrac{g}{\pi} \log\left(\dfrac{2e^{\pi/\sqrt{2}} g}{\pi}\right) & \text{if } g = 4 \text{ or } g = 5, \\ \dfrac{2g}{\pi} \log g & \text{if } g \geq 6. \end{cases} \tag{II.10}$$

Remark 5.8. We easily see that $C_1(g) \geq g$.

Proof. If $\nu = 1$ then $M(g^{\nu-1}) = 1 \leq \frac{C_1(g)}{g}$, thus we can assume that $\nu \geq 2$. By [43, Lemma 2],

$$M(g^{\nu-1}) \leq \frac{2}{\pi} \log\left(\xi g^{\nu-1}\right)$$

where $\xi = 2e^{\pi/\sqrt{2}}/\pi \approx 5.87$. Let h_g be the function defined on $[2, +\infty[$ by

$$h_g(x) = \frac{2g}{\pi x} \log\left(\xi g^{x-1}\right) = \frac{2g}{\pi}\left(\frac{1}{x}\log\left(\frac{\xi}{g}\right) + \log g\right).$$

It suffices to establish that h_g is bounded above by $C_1(g)$. If $g \geq \xi$ then h_g is nondecreasing and thus bounded above by $\lim_{x\to\infty} h_g(x) = \frac{2g}{\pi}\log g$. If $g < \xi$ then h_g is nonincreasing and thus bounded above by $h_g(2) = \frac{g}{\pi}\log(\xi g)$. Moreover, if $2 \leq g \leq 3$ then $h_g(2) \leq g$, which completes the proof. □

We are now ready to give a sharp upper bound of $\mathcal{N}_1(n, A)$.

Lemma 5.9. *If $n \geq 1$, $A \subset \{0, \ldots, n-1\}$ and $0 \in A$ then, denoting $\rho = \frac{|A|}{n}$,*

$$\mathcal{N}_1(n, A) \leq g^{-|A|} g^{C_2(g)\rho \log\left(\frac{C_1(g)}{\rho}\right) n}$$

where

$$C_2(g) = 1/\log g. \tag{II.11}$$

Proof. Since $0 \in A$, there exist $0 \leq r \leq n-1$ and $0 = j_0 < j_1 < \cdots < j_r \leq n-1$ such that $A = \{j_0, j_1, \ldots, j_r\}$. Since $j_0 = 0$, we have $M(g^{j_0}) = 1$ and thus, by Lemma 5.6, denoting $j_{r+1} = n$,

$$\mathcal{N}_1(n, A) \leq \prod_{s=0}^{r} M(g^{j_{s+1}-j_s-1}).$$

Moreover, by Lemma 5.7, for any $0 \leq s \leq r$,

$$M(g^{j_{s+1}-j_s-1}) \leq \frac{C_1(g)}{g}(j_{s+1} - j_s)$$

and it follows that

$$\mathcal{N}_1(n,A) \le \left(\frac{C_1(g)}{g}\right)^{r+1} \prod_{s=0}^{r}(j_{s+1}-j_s).$$

By using the inequality of arithmetic and geometric means, we obtain

$$\begin{aligned}\mathcal{N}_1(n,A) &\le \left(\frac{C_1(g)}{g}\right)^{r+1}\left(\frac{1}{r+1}\sum_{s=0}^{r}(j_{s+1}-j_s)\right)^{r+1} = g^{-(r+1)}\left(C_1(g)\frac{n}{r+1}\right)^{r+1}\\ &= g^{-|A|}\left(\frac{C_1(g)}{\rho}\right)^{\rho n} = g^{-|A|}g^{\rho n\log\left(\frac{C_1(g)}{\rho}\right)\frac{1}{\log g}},\end{aligned}$$

which completes the proof. □

In order to use Lemma 5.9 to obtain a sharp upper bound of $\|F_{n,A,\boldsymbol{d}}\|_1$, we will need the following lemma.

Lemma 5.10. *If $q \ge 2$ then $\|\Phi_q\|_1 \ll \log q$.*

Proof. It suffices for instance to write

$$\|\Phi_q\|_1 = \int_{-1/2}^{1/2}\left|\sum_{0\le v<q}\mathrm{e}(vt)\right|dt \ll \int_0^{1/2}\min\left(q,\frac{1}{t}\right)dt \ll \log q.$$

□

Proposition 5.11. *If $n \ge 1$, $A \subset \{0,\dots,n-1\}$, $0 \in A$ and $\boldsymbol{d} = (d_j)_{j\in A} \in \{0,\dots,g-1\}^A$ then, denoting $\rho = \frac{|A|}{n}$,*

$$\|F_{n,A,\boldsymbol{d}}\|_1 \ll (\log g^n)\, g^{-|A|}g^{\left(C_2(g)\rho\log\left(\frac{C_1(g)}{\rho}\right)-1\right)n}.$$

Proof. For any $\lambda \in \mathbb{R}$, we can write

$$\begin{aligned}F_{n,A,\boldsymbol{d}}(\lambda) &= g^{-n}\sum_{0\le k<g^n} f_{n,A,\boldsymbol{d}}(k)\,\mathrm{e}\left(-\lambda k\right)\\ &= g^{-n}\sum_{0\le k_1,k_2<g^n} f_{n,A,\boldsymbol{d}}(k_1)\,\mathrm{e}\left(-\lambda k_2\right)g^{-n}\sum_{0\le h<g^n}\mathrm{e}\left(h(k_2-k_1)g^{-n}\right)\\ &= g^{-n}\sum_{0\le h<g^n}\left(g^{-n}\sum_{0\le k_1<g^n} f_{n,A,\boldsymbol{d}}(k_1)\,\mathrm{e}\left(-hk_1g^{-n}\right)\right)\left(\sum_{0\le k_2<g^n}\mathrm{e}\left((hg^{-n}-\lambda)k_2\right)\right)\\ &= g^{-n}\sum_{0\le h<g^n} F_{n,A,\boldsymbol{d}}(hg^{-n})\sum_{0\le k<g^n}\mathrm{e}\left((hg^{-n}-\lambda)k\right),\end{aligned}$$

hence

$$|F_{n,A,\boldsymbol{d}}(\lambda)| \le g^{-n}\sum_{0\le h<g^n}\left|F_{n,A,\boldsymbol{d}}(hg^{-n})\right|\Phi_{g^n}(hg^{-n}-\lambda).$$

By integrating over $[0,1]$, we obtain

$$\|F_{n,A,\boldsymbol{d}}\|_1 \leq g^{-n} \sum_{0\leq h<g^n} \left|F_{n,A,\boldsymbol{d}}(hg^{-n})\right| \|\Phi_{g^n}\|_1$$

and it follows from Lemma 5.1 that

$$\|F_{n,A,\boldsymbol{d}}\|_1 \leq \|\Phi_{g^n}\|_1 \, g^{-n} \sum_{0\leq h<g^n} P_{n,A}(hg^{-n}) = \|\Phi_{g^n}\|_1 \, g^{-n} \mathcal{N}_1(n,A).$$

Moreover, by Lemma 5.10, $\|\Phi_{g^n}\|_1 \ll \log g^n$ and by Lemma 5.9,

$$\mathcal{N}_1(n,A) \leq g^{-|A|} g^{C_2(g)\rho \log\left(\frac{C_1(g)}{\rho}\right)n},$$

which completes the proof. □

5.2. Upper bounds of $|F_{n,A,\boldsymbol{d}}(a/q)|$

5.2.1. Upper bound of $|F_{n,A,\boldsymbol{d}}(a/q)|$ on average over a/q

The purpose of this section is to establish Lemma 5.15 below.

Lemma 5.12. *Let m and n be integers such that $1 \leq m \leq n$, let $A \subset \{0,\dots,n-1\}$ and $\rho = \frac{|A|}{n}$. For any integer k such that $0 \leq k < \left\lfloor \frac{n}{m} \right\rfloor$, we denote*

$$I_k = [km, (k+1)m[\cap \mathbb{Z} \subset \{0,\dots,n-1\}.$$

For any real number $\kappa \geq 0$, we have

$$\left|\left\{0 \leq k < \left\lfloor \tfrac{n}{m} \right\rfloor : |I_k \cap A| > (1+\kappa)\rho m\right\}\right| < \frac{n}{(1+\kappa)m}. \tag{II.12}$$

Moreover, if $m \leq \frac{\kappa n}{2(1+\kappa)}$ then there exist k_1 and k_2 such that $0 \leq k_1 \neq k_2 < \left\lfloor \frac{n}{m} \right\rfloor$ and for $i \in \{1,2\}$, $|I_{k_i} \cap A| \leq (1+\kappa)\rho m$.

Remark 5.13. The parameter κ will be optimally chosen in Section 12 in terms of some other parameters. The simplest choice $\kappa = 1$ would be possible but would provide smaller values of c_0 in Theorem 2.7. In [5, Lemmas 3 and 4], the author considers intervals I such that $|I \cap A| \leq 2\rho m$ which corresponds to $\kappa = 1$.

Proof. Since the sets I_k are pairwise disjoint, we have

$$(1+\kappa)\rho m \sum_{\substack{0\leq k<\lfloor n/m\rfloor \\ |I_k\cap A|>(1+\kappa)\rho m}} 1 < \sum_{\substack{0\leq k<\lfloor n/m\rfloor \\ |I_k\cap A|>(1+\kappa)\rho m}} |I_k \cap A| \leq |A| = \rho n$$

which proves (II.12) when $\rho > 0$. If $\rho = 0$ then $A = \varnothing$ and the inequality (II.12) is trivial. Moreover, if $m \leq \frac{\kappa n}{2(1+\kappa)}$ then it follows from (II.12) that

$$\sum_{\substack{0 \leq k < \lfloor n/m \rfloor \\ |I_k \cap A| \leq (1+\kappa)\rho m}} 1 > \left\lfloor \frac{n}{m} \right\rfloor - \frac{n}{(1+\kappa)m} > \frac{\kappa n}{(1+\kappa)m} - 1 \geq 1$$

which completes the proof. □

Lemma 5.14. *If $n \geq 1$, $A \subset \mathbb{Z}$ and $\boldsymbol{d} \in \{0, \ldots, g-1\}^A$ then, for any real number $Q \geq 1$,*

$$\sum_{1 \leq q \leq Q} \sum_{\substack{1 \leq a \leq q \\ (a,q)=1}} \left| F_{n,A,\boldsymbol{d}}\left(\frac{a}{q}\right) \right|^2 \leq (g^n - 1 + Q^2) g^{-n-|A \cap \{0,\ldots,n-1\}|}.$$

Proof. Since the points a/q for $1 \leq q \leq Q$, $1 \leq a \leq q$, $(a,q) = 1$ are Q^{-2}-well spaced and $F_{n,A,\boldsymbol{d}}$ is the trigonometric polynomial

$$F_{n,A,\boldsymbol{d}}(\lambda) = g^{-n} \sum_{0 \leq k < g^n} f_{n,A,\boldsymbol{d}}(k)\, \mathrm{e}\left(-\lambda k\right),$$

it follows from the large sieve inequality (see for instance [49, Theorem 3]) that

$$\begin{aligned} \sum_{1 \leq q \leq Q} \sum_{\substack{1 \leq a \leq q \\ (a,q)=1}} \left| F_{n,A,\boldsymbol{d}}\left(\frac{a}{q}\right) \right|^2 &\leq (g^n - 1 + Q^2) \sum_{0 \leq k < g^n} (g^{-n} f_{n,A,\boldsymbol{d}}(k))^2 \\ &= (g^n - 1 + Q^2) g^{-n-|A \cap \{0,\ldots,n-1\}|} \end{aligned}$$

which completes the proof. □

Lemma 5.15. *Let $n \geq 1$, $A \subset \{0, \ldots, n-1\}$, $\boldsymbol{d} \in \{0, \ldots, g-1\}^A$, $\rho = \frac{|A|}{n}$, $\kappa \geq 0$ and $Q \in \mathbb{R}$. If $1 \leq Q \leq g^{\frac{\kappa n}{4(1+\kappa)}}$ then*

$$\sum_{\substack{1 \leq q \leq Q \\ (q,g)=1}} \sum_{\substack{1 \leq a \leq q \\ (a,q)=1}} g^{|A|} \left| F_{n,A,\boldsymbol{d}}\left(\frac{a}{q}\right) \right| \leq (1+g)\, Q^{2(1+\kappa)\rho}.$$

Remark 5.16. This upper bound improves the one given in Lemma 3 of [5] (for $g = 2$) where the power of Q in the right-hand side term is $C\rho \log \frac{1}{\rho}$ for some constant C.

Proof. For $1 \leq Q \leq \sqrt{g}$, it suffices to use the trivial upper bound:

$$\sum_{\substack{1 \leq q \leq Q \\ (q,g)=1}} \sum_{\substack{1 \leq a \leq q \\ (a,q)=1}} g^{|A|} \left| F_{n,A,\boldsymbol{d}}\left(\frac{a}{q}\right) \right| \leq \sum_{\substack{1 \leq q \leq Q \\ (q,g)=1}} \sum_{\substack{1 \leq a \leq q \\ (a,q)=1}} 1 \leq Q^2 \leq 1 + g \leq (1+g)\, Q^{2(1+\kappa)\rho}.$$

For $\sqrt{g} < Q \leq g^{\frac{\kappa n}{4(1+\kappa)}}$, we consider the integer m satisfying $g^m \leq Q^2 < g^{m+1}$ and thus $1 \leq m \leq \frac{\kappa n}{2(1+\kappa)} \leq \frac{n}{2}$. By Lemma 5.12, there exist two disjoint sets I_1 and I_2 of m consecutive integers such that, for any $\ell \in \{1,2\}$, $I_\ell \subset \{0,\dots,n-1\}$ and $|I_\ell \cap A| \leq (1+\kappa)\rho m$. For $\ell \in \{1,2\}$, we denote $I_\ell = \{j_\ell, \dots, j_\ell + m - 1\}$, $A_\ell = A - j_\ell$ and $\boldsymbol{d}_\ell = (0)_{j \in A_\ell}$. By applying Lemma 5.1, we obtain, for any $\lambda \in \mathbb{R}$,

$$\begin{aligned} g^{|A|} \left|F_{n,A,\boldsymbol{d}}(\lambda)\right| = \prod_{\substack{0 \leq j \leq n-1 \\ j \notin A}} \frac{\Phi_g(\lambda g^j)}{g} &\leq \prod_{\ell=1}^{2} \prod_{\substack{j \in I_\ell \\ j \notin A}} \frac{\Phi_g(\lambda g^j)}{g} = \prod_{\ell=1}^{2} \prod_{\substack{0 \leq j' \leq m-1 \\ j' \notin A_\ell}} \frac{\Phi_g\left(\lambda g^{j_\ell} g^{j'}\right)}{g} \\ &= \prod_{\ell=1}^{2} g^{|A_\ell \cap \{0,\dots,m-1\}|} \left|F_{m,A_\ell,\boldsymbol{d}_\ell}\left(\lambda g^{j_\ell}\right)\right| \end{aligned}$$

hence, by Cauchy–Schwarz inequality,

$$\begin{aligned} \sum_{\substack{1 \leq q \leq Q \\ (q,g)=1}} \sum_{\substack{1 \leq a \leq q \\ (a,q)=1}} g^{|A|} \left|F_{n,A,\boldsymbol{d}}\left(\frac{a}{q}\right)\right| &\leq \prod_{\ell=1}^{2} \left(\sum_{\substack{1 \leq q \leq Q \\ (q,g)=1}} \sum_{\substack{1 \leq a \leq q \\ (a,q)=1}} g^{2|A_\ell \cap \{0,\dots,m-1\}|} \left|F_{m,A_\ell,\boldsymbol{d}_\ell}\left(\frac{a g^{j_\ell}}{q}\right)\right|^2 \right)^{\frac{1}{2}} \\ &= \prod_{\ell=1}^{2} \left(\sum_{\substack{1 \leq q \leq Q \\ (q,g)=1}} \sum_{\substack{1 \leq a' \leq q \\ (a',q)=1}} g^{2|A_\ell \cap \{0,\dots,m-1\}|} \left|F_{m,A_\ell,\boldsymbol{d}_\ell}\left(\frac{a'}{q}\right)\right|^2 \right)^{\frac{1}{2}}. \end{aligned}$$

Moreover, by Lemma 5.14, for any $\ell \in \{1,2\}$,

$$g^{|A_\ell \cap \{0,\dots,m-1\}|} \sum_{1 \leq q \leq Q} \sum_{\substack{1 \leq a' \leq q \\ (a',q)=1}} \left|F_{m,A_\ell,\boldsymbol{d}_\ell}\left(\frac{a'}{q}\right)\right|^2 \leq (g^m - 1 + Q^2) g^{-m} < 1 + g$$

and since $|A_\ell \cap \{0,\dots,m-1\}| = |A \cap I_\ell| \leq (1+\kappa)\rho m$, we obtain

$$\begin{aligned} \sum_{\substack{1 \leq q \leq Q \\ (q,g)=1}} \sum_{\substack{1 \leq a \leq q \\ (a,q)=1}} g^{|A|} \left|F_{n,A,\boldsymbol{d}}\left(\frac{a}{q}\right)\right| &< (1+g) g^{\frac{1}{2}(|A_1 \cap \{0,\dots,m-1\}| + |A_2 \cap \{0,\dots,m-1\}|)} \\ &\leq (1+g) g^{(1+\kappa)\rho m} \leq (1+g) Q^{2(1+\kappa)\rho} \end{aligned}$$

which completes the proof. □

5.2.2. Individual upper bound of $|F_{n,A,\boldsymbol{d}}(a/q)|$

The purpose of this section is to establish Lemma 5.20 below.

Lemma 5.17. *For any integer $q \geq 2$ and for any $t \in \mathbb{R}$, we have*

$$\frac{\Phi_q(t)}{q} \leq q^{-4\|t\|^2}.$$

We note that if q is odd and $\|t\| = 1/2$ then both sides are equal to $1/q$.

Proof. Since Φ_q and $\|\cdot\|$ are even periodic functions with period 1, we can assume that $t \in [0, 1/2]$. Let $t_q = \frac{\sqrt{6}}{\pi}\frac{1}{\sqrt{q^2-1}} \leq \frac{1}{2}$. For $0 \leq t \leq t_q$, by [43, Lemma 3],

$$\frac{\Phi_q(t)}{q} \leq e^{-\frac{\pi^2}{6}(q^2-1)t^2}$$

and since $x \mapsto \frac{x^2-1}{\log x}$ is increasing on $[2, +\infty[$, we have $\frac{q^2-1}{\log q} \geq \frac{3}{\log 2} \geq \frac{24}{\pi^2}$ which gives

$$\frac{\Phi_q(t)}{q} \leq e^{-(4\log q)t^2} = q^{-4t^2}.$$

For $t_q \leq t \leq \frac{1}{2}$, we write

$$\frac{\Phi_q(t)}{q} \leq \frac{1}{q\sin \pi t} \leq \frac{1}{2qt}$$

and we consider the function h_q defined by $h_q(t) = 2qt\, e^{-(4\log q)t^2} - 1$. Clearly, $h_q(1/2) = 0$ and

$$h_q(t_q) = \frac{2\sqrt{6}}{\pi}\frac{q}{\sqrt{q^2-1}} e^{-\frac{24\log q}{\pi^2(q^2-1)}} - 1.$$

For $q = 2$, we check that $h_2(t_2) \geq 0$ and for $q \geq 3$, we have $\frac{q^2-1}{\log q} \geq \frac{8}{\log 3}$ and thus

$$h_q(t_q) \geq \frac{2\sqrt{6}}{\pi} e^{-\frac{24\log q}{\pi^2(q^2-1)}} - 1 \geq \frac{2\sqrt{6}}{\pi} e^{-\frac{3\log 3}{\pi^2}} - 1 \geq 0.$$

Moreover, h_q is increasing on $[0, (8\log q)^{-1/2}]$ and decreasing on $[(8\log q)^{-1/2}, 1/2]$. It follows that, for any $t_q \leq t \leq \frac{1}{2}$, we have $h_q(t) \geq 0$, hence

$$\frac{\Phi_q(t)}{q} \leq \frac{1}{2qt} \leq e^{-(4\log q)t^2} = q^{-4t^2}$$

which completes the proof. □

Lemma 5.18. *Let $a \geq 2$, $g \geq 2$ be integers and $x \in \mathbb{R}$. If $g^{-a-1} \leq \|x\| < g^{-a}$ then, for any $0 \leq \ell \leq a-1$, we have $g^{-a-1+\ell} \leq \left\|g^\ell x\right\| < g^{-a+\ell}$.*

Proof. We first establish that

$$g^{-a-1} \leq \|x\| < g^{-a} \quad \Rightarrow \quad g^{-a} \leq \|gx\| < g^{-a+1}. \tag{II.13}$$

Since $\|\cdot\|$ is an even periodic function with period 1, we can assume that $x \in [0, 1/2]$. If $g^{-a-1} \leq \|x\| = x < g^{-a}$ then, since $a \geq 2$ and $g \geq 2$, we obtain $g^{-a} \leq gx < g^{-a+1} \leq g^{-1} \leq 1/2$, hence $g^{-a} \leq \|gx\| = gx < g^{-a+1}$, which proves (II.13). The lemma follows by induction. □

Lemma 5.19. *If $g \geq 2$, $m \geq 1$ and $\alpha \in \mathbb{R}$ are such that, for any $0 \leq j \leq m-1$, $\|g^j\alpha\| \geq g^{-m-1}$ then, for any $1 \leq m_1 \leq m$, we have*

$$\left|\left\{0 \leq j \leq m-1 : \left\|g^j\alpha\right\| \geq g^{-m_1-1}\right\}\right| \geq m_1.$$

Proof. We assume that there exists m_1 such that $1 \leq m_1 \leq m$ and

$$\left|\left\{0 \leq j \leq m-1 : \left\|g^j\alpha\right\| \geq g^{-m_1-1}\right\}\right| \leq m_1 - 1.$$

Since for any $0 \leq j \leq m-1$, $\|g^j\alpha\| \geq g^{-m-1}$, it follows that

$$\left|\left\{0 \leq j \leq m-1 : \left\|g^j\alpha\right\| \in [g^{-m-1}, g^{-m_1-1}[\right\}\right| \geq m - m_1 + 1.$$

For any $1 \leq k \leq m$, we denote $E_k = \left[g^{-k-1}, g^{-k}\right[\subset [g^{-m-1}, g^{-1}[$. Since

$$[g^{-m-1}, g^{-m_1-1}[= \bigcup_{k=m_1+1}^{m} E_k$$

which is a union of $m - m_1$ pairwise disjoint intervals, by the pigeonhole principle, there exists k_0 such that $m_1 + 1 \leq k_0 \leq m$ and $|\{0 \leq j \leq m-1 : \|g^j\alpha\| \in E_{k_0}\}| \geq 2$. As a consequence, there exist $0 \leq j_1 < j_2 \leq m-1$ such that $\|g^{j_1}\alpha\| \in E_{k_0}$ and $\|g^{j_2}\alpha\| \in E_{k_0}$. Since $\|g^{j_1}\alpha\| \in E_{k_0}$ and $k_0 \geq 2$, by Lemma 5.18, for any $j_1 \leq j \leq j_1 + k_0 - 1$, we have $\|g^j\alpha\| \in E_{k_0-j+j_1}$. Moreover, since $\|g^{j_2}\alpha\| \in E_{k_0}$ and $j_2 > j_1$, it follows that $j_2 \geq j_1 + k_0$. Therefore, for any j such that

$$j_1 + k_0 - m_1 \leq j \leq j_1 + k_0 - 1,$$

we have $0 \leq j \leq m-1$ and $\|g^j\alpha\| \in E_{k_0-j+j_1}$, hence $\|g^j\alpha\| \geq g^{-(k_0-j+j_1)-1} \geq g^{-m_1-1}$. It follows that $|\{0 \leq j \leq m-1 : \|g^j\alpha\| \geq g^{-m_1-1}\}| \geq m_1$, which contradicts our assumption and completes the proof of the lemma. □

Lemma 5.20. *Let $n \geq 1$, $A \subset \{0, \dots, n-1\}$, $\boldsymbol{d} \in \{0, \dots, g-1\}^A$, $\rho = \frac{|A|}{n}$ and $\kappa > 0$. If $\rho \leq \frac{1}{2(1+\kappa)}$ then for any $2 \leq q \leq g^{\frac{\kappa n}{2(1+\kappa)}}$ such that $(q, g) = 1$ and any $1 \leq a \leq q$ such that $(a, q) = 1$,*

$$g^{|A|}\left|F_{n,A,\boldsymbol{d}}\left(\frac{a}{q}\right)\right| \leq \exp\left(-K_\kappa(g)\,\frac{n}{(\log q)q^{2(1+\kappa)\rho}}\right)$$

where $K_\kappa(g) = \frac{2\kappa(\log g)^2}{(1+\kappa)g^4} > 0$.

Remark 5.21. Let $\kappa > 0$ and $0 < c \leq \frac{1}{2(1+\kappa)}$. It follows from Lemma 5.20 that there exists $n_0 = n_0(g, \kappa, c)$ such that for any $n \geq n_0$, $A \subset \{0, \dots, n-1\}$ satisfying $|A| \leq cn$ and any

$\boldsymbol{d} \in \{0,\dots,g-1\}^A$, we have for any $2 \le q \le \left(\frac{n}{\log^3 n}\right)^{\frac{1}{4(1+\kappa)c}}$ such that $(q,g)=1$ and any $1 \le a \le q$ such that $(a,q)=1$,

$$g^{|A|}\left|F_{n,A,\boldsymbol{d}}\left(\frac{a}{q}\right)\right| \le g^{-\sqrt{n}}.$$

This upper bound was obtained in Lemma 4 of [5] (for $g=2$) with the smallest range $2 \le q < n^{\frac{1}{10c}}$ (note that here κ can be arbitrarily small).

Proof. (of Lemma 5.20) Combining Lemmas 5.1 and 5.17, we obtain

$$g^{|A|}\left|F_{n,A,\boldsymbol{d}}\left(\frac{a}{q}\right)\right| = \prod_{\substack{0\le j\le n-1\\ j\notin A}} \frac{\Phi_g\left(\frac{ag^j}{q}\right)}{g} \le \exp\left(-(4\log g)\sum_{\substack{0\le j\le n-1\\ j\notin A}} \left\|\frac{ag^j}{q}\right\|^2\right). \tag{II.14}$$

For any $j \ge 0$, we have $q \nmid ag^j$ hence $\left\|\frac{ag^j}{q}\right\| \ge \frac{1}{q}$ and by observing that $n-|A| = n(1-\rho) \ge \frac{n}{2}$, we obtain

$$g^{|A|}\left|F_{n,A,\boldsymbol{d}}\left(\frac{a}{q}\right)\right| \le \exp\left(-(2\log g)\frac{n}{q^2}\right).$$

Thus, for $q \le g^2$, since $\frac{q^2}{\log q} \le \frac{g^4}{\log g^2}$,

$$g^{|A|}\left|F_{n,A,\boldsymbol{d}}\left(\frac{a}{q}\right)\right| \le \exp\left(-\frac{4(\log g)^2}{g^4}\frac{n}{\log q}\right) \le \exp\left(-\frac{2\kappa(\log g)^2}{(1+\kappa)g^4}\frac{n}{(\log q)q^{2(1+\kappa)\rho}}\right).$$

For $q > g^2$, we consider the integer m such that $g^m < q \le g^{m+1}$ and since $g^2 < q \le g^{\frac{\kappa n}{2(1+\kappa)}}$, we have $2 \le m < \frac{\kappa n}{2(1+\kappa)} \le n$. By denoting, for any $0 \le k < \left\lfloor \frac{n}{m} \right\rfloor$, $I_k = [km,(k+1)m[\cap\mathbb{Z} \subset \{0,\dots,n-1\}$, we have

$$\begin{aligned}\sum_{\substack{0\le j\le n-1\\ j\notin A}} \left\|\frac{ag^j}{q}\right\|^2 \ge \sum_{\substack{0\le k<\lfloor n/m\rfloor\\ |I_k\cap A|\le(1+\kappa)\rho m}} \sum_{\substack{j\in I_k\\ j\notin A}} \left\|\frac{ag^j}{q}\right\|^2 &= \sum_{\substack{0\le k<\lfloor n/m\rfloor\\ |I_k\cap A|\le(1+\kappa)\rho m}} \sum_{\substack{0\le \ell\le m-1\\ \ell\notin A-km}} \left\|\frac{(ag^{km})g^\ell}{q}\right\|^2 \\ &\ge \xi \sum_{\substack{0\le k<\lfloor n/m\rfloor\\ |I_k\cap A|\le(1+\kappa)\rho m}} 1\end{aligned} \tag{II.15}$$

where

$$\xi = \min_{\substack{A'\subset\{0,\dots,m-1\}\\ |A'|\le(1+\kappa)\rho m}} \min_{\substack{1\le r\le q\\ (r,q)=1}} \sum_{\substack{0\le\ell\le m-1\\ \ell\notin A'}} \left\|\frac{rg^\ell}{q}\right\|^2.$$

By Lemma 5.12, since $\frac{\kappa n}{(1+\kappa)m} \geq 2$,

$$\sum_{\substack{0\leq k<\lfloor n/m\rfloor \\ |I_k\cap A|\leq(1+\kappa)\rho m}} 1 > \left\lfloor \frac{n}{m}\right\rfloor - \frac{n}{(1+\kappa)m} > \frac{\kappa n}{(1+\kappa)m} - 1 \geq \frac{\kappa n}{2(1+\kappa)m}. \tag{II.16}$$

In order to give a sharp lower bound of ξ, we consider $A' \subset \{0,\dots,m-1\}$ such that $|A'| \leq (1+\kappa)\rho m$ and $1 \leq r \leq q$ such that $(r,q)=1$. Since for any $\ell \geq 0$, $\left\|\frac{rg^\ell}{q}\right\| \geq \frac{1}{q} \geq g^{-m-1}$, by applying Lemma 5.19 with $m_1 = \lfloor (1+\kappa)\rho m\rfloor + 1 \leq \frac{m}{2}+1 \leq m$, we obtain

$$\left|\left\{0\leq \ell \leq m-1 : \left\|\tfrac{rg^\ell}{q}\right\| \geq g^{-m_1-1}\right\}\right| \geq m_1 = \lfloor (1+\kappa)\rho m\rfloor + 1.$$

Since $|A'| \leq \lfloor (1+\kappa)\rho m\rfloor$, there exists $0\leq \ell \leq m-1$ such that $\ell \notin A'$ and $\left\|\frac{rg^\ell}{q}\right\| \geq g^{-m_1-1}$ and thus

$$\sum_{\substack{0\leq \ell\leq m-1\\ \ell\notin A'}} \left\|\frac{rg^\ell}{q}\right\|^2 \geq g^{-2m_1-2} \geq g^{-4}g^{-2(1+\kappa)\rho m}.$$

It follows that

$$\xi \geq g^{-4}g^{-2(1+\kappa)\rho m}. \tag{II.17}$$

By inserting (II.16) and (II.17) into (II.15), we obtain

$$\sum_{\substack{0\leq j\leq n-1\\ j\notin A}} \left\|\frac{ag^j}{q}\right\|^2 \geq g^{-4}g^{-2(1+\kappa)\rho m}\frac{\kappa n}{2(1+\kappa)m} = \frac{\kappa}{2g^4(1+\kappa)}\,\frac{n}{mg^{2(1+\kappa)\rho m}}$$

and since $g^m < q$,

$$\sum_{\substack{0\leq j\leq n-1\\ j\notin A}} \left\|\frac{ag^j}{q}\right\|^2 \geq \frac{\kappa \log g}{2(1+\kappa)g^4}\,\frac{n}{(\log q)q^{2(1+\kappa)\rho}}$$

and therefore, by (II.14),

$$g^{|A|}\left|F_{n,A,\boldsymbol{d}}\left(\frac{a}{q}\right)\right| \leq \exp\left(-\frac{2\kappa(\log g)^2}{(1+\kappa)g^4}\,\frac{n}{(\log q)q^{2(1+\kappa)\rho}}\right)$$

which completes the proof. □

5.2.3. Upper bound for a weighted average of $|F_{n,A,\boldsymbol{d}}(a/q)|$

In this section, we combine Lemmas 5.15 and 5.20 to obtain estimates of $|F_{n,A,\boldsymbol{d}}(a/q)|$ on average over a/q with weight q^{-1} or $q^{-1/2}$.

Lemma 5.22. *Let $n \geq 100$, $A \subset \{0,\dots,n-1\}$, $\boldsymbol{d} \in \{0,\dots,g-1\}^A$, $\kappa > 0$ and $0 < c < \frac{1}{2(1+\kappa)}$. If $|A| \leq cn$ then*

$$\sum_{\substack{2\leq q\leq Q\\(q,g)=1}} \frac{1}{q} \sum_{\substack{1\leq a\leq q\\(a,q)=1}} g^{|A|} \left|F_{n,A,\boldsymbol{d}}\left(\frac{a}{q}\right)\right| \ll_{g,\kappa,c} \left(\frac{n}{\log^3 n}\right)^{1-\frac{1}{2(1+\kappa)c}}$$

where $Q = g^{\frac{\kappa n}{4(1+\kappa)}}$.

Proof. We fix a parameter $Q_0 \in \mathbb{R}$ which will be specified later on, such that $1 < Q_0 \leq Q$ and we denote by i_0 the integer such that $i_0 \geq 0$ and $Q\,2^{-(i_0+1)} < Q_0 \leq Q\,2^{-i_0}$. By subdividing the sum over $Q_0 < q \leq Q$ into dyadic ranges, we obtain

$$\begin{aligned}\sum_{\substack{Q_0<q\leq Q\\(q,g)=1}} \frac{1}{q} \sum_{\substack{1\leq a\leq q\\(a,q)=1}} g^{|A|} \left|F_{n,A,\boldsymbol{d}}\left(\frac{a}{q}\right)\right| &\leq \sum_{i=0}^{i_0} \sum_{\substack{Q\,2^{-(i+1)}<q\leq Q\,2^{-i}\\(q,g)=1}} \frac{1}{q} \sum_{\substack{1\leq a\leq q\\(a,q)=1}} g^{|A|} \left|F_{n,A,\boldsymbol{d}}\left(\frac{a}{q}\right)\right| \\ &\leq \sum_{i=0}^{i_0} \frac{2^{i+1}}{Q} \sum_{\substack{1\leq q\leq Q\,2^{-i}\\(q,g)=1}} \sum_{\substack{1\leq a\leq q\\(a,q)=1}} g^{|A|} \left|F_{n,A,\boldsymbol{d}}\left(\frac{a}{q}\right)\right|\end{aligned}$$

and since $Q2^{-i_0} \geq Q_0 \geq 1$, $Q \leq g^{\frac{\kappa n}{4(1+\kappa)}}$ and $|A| \leq cn$, it follows from Lemma 5.15 that

$$\begin{aligned}\sum_{\substack{Q_0<q\leq Q\\(q,g)=1}} \frac{1}{q} \sum_{\substack{1\leq a\leq q\\(a,q)=1}} g^{|A|} \left|F_{n,A,\boldsymbol{d}}\left(\frac{a}{q}\right)\right| &\leq \sum_{i=0}^{i_0} \frac{2^{i+1}}{Q}(1+g) \left(\frac{Q}{2^i}\right)^{2(1+\kappa)c} \\ &\ll_{g,\kappa,c} \left(\frac{2^{i_0}}{Q}\right)^{1-2(1+\kappa)c} \leq Q_0^{2(1+\kappa)c-1}.\end{aligned} \tag{II.18}$$

Moreover, it follows from Lemma 5.20 that

$$\begin{aligned}\sum_{\substack{2\leq q\leq Q_0\\(q,g)=1}} \frac{1}{q} \sum_{\substack{1\leq a\leq q\\(a,q)=1}} g^{|A|} \left|F_{n,A,\boldsymbol{d}}\left(\frac{a}{q}\right)\right| &\leq \sum_{\substack{2\leq q\leq Q_0\\(q,g)=1}} \frac{\varphi(q)}{q} \exp\left(-K_\kappa(g)\,\frac{n}{(\log q)q^{2(1+\kappa)c}}\right) \\ &\leq Q_0 \exp\left(-K_\kappa(g)\,\frac{n}{(\log Q_0)Q_0^{2(1+\kappa)c}}\right).\end{aligned} \tag{II.19}$$

We denote $Q_1 = \left(\frac{n}{\log^3 n}\right)^{\frac{1}{2(1+\kappa)c}}$ and we choose $Q_0 = \min(Q_1, Q)$ which satisfies $1 < Q_0 \leq Q$ (since $\frac{n}{\log^3 n} > 1$). If $Q_0 = Q$ then the sum in the left-hand side of (II.18) is 0 and otherwise,

we have $Q_0 = Q_1$. Thus, by (II.18),

$$\sum_{\substack{Q_0<q\le Q\\(q,g)=1}}\frac{1}{q}\sum_{\substack{1\le a\le q\\(a,q)=1}} g^{|A|}\left|F_{n,A,\boldsymbol{d}}\left(\frac{a}{q}\right)\right| \ll_{g,\kappa,c} Q_1^{2(1+\kappa)c-1} = \left(\frac{n}{\log^3 n}\right)^{1-\frac{1}{2(1+\kappa)c}}.$$

Moreover, by (II.19), since $Q_0 \le Q_1$, we obtain

$$\begin{aligned}\sum_{\substack{2\le q\le Q_0\\(q,g)=1}}\frac{1}{q}\sum_{\substack{1\le a\le q\\(a,q)=1}} g^{|A|}\left|F_{n,A,\boldsymbol{d}}\left(\frac{a}{q}\right)\right| &\le Q_1\exp\left(-K_\kappa(g)\,\frac{n}{(\log Q_1)Q_1^{2(1+\kappa)c}}\right)\\ &= Q_1\exp\left(-K_\kappa(g)\,\frac{\log^3 n}{\log Q_1}\right) \le n^{\frac{1}{2(1+\kappa)c}}\exp\left(-K_\kappa(g)\,2(1+\kappa)c\log^2 n\right)\\ &\ll_{g,\kappa,c}\left(\frac{n}{\log^3 n}\right)^{1-\frac{1}{2(1+\kappa)c}}\end{aligned}$$

which completes the proof. □

Lemma 5.23. *Let $n \ge 100$, $A \subset \{0,\dots,n-1\}$, $\boldsymbol{d} \in \{0,\dots,g-1\}^A$, $\kappa > 0$ and $0 < c < \frac{1}{4(1+\kappa)}$. If $|A| \le cn$ then*

$$\sum_{\substack{2\le q\le Q\\(q,g)=1}}\frac{1}{\sqrt{q}}\sum_{\substack{1\le a\le q\\(a,q)=1}} g^{|A|}\left|F_{n,A,\boldsymbol{d}}\left(\frac{a}{q}\right)\right| \ll_{g,\kappa,c}\left(\frac{n}{\log^3 n}\right)^{1-\frac{1}{4(1+\kappa)c}}$$

where $Q = g^{\frac{\kappa n}{4(1+\kappa)}}$.

Proof. It suffices to slightly adapt the proof of Lemma 5.22: by replacing $1/q$ by $1/\sqrt{q}$, the right-hand side of (II.18) becomes $Q_0^{2(1+\kappa)c-1/2}$ and the right-hand side of (II.19) becomes

$$Q_0^{3/2}\exp\left(-K_\kappa(g)\,\frac{n}{(\log Q_0)Q_0^{2(1+\kappa)c}}\right).$$

The same choice of Q_0 gives the result. □

5.3. Integers with preassigned digits in arithmetic progressions and consequences

The purpose of this section is to establish Lemmas 5.27 and 5.30 which will be useful for the study of the major arcs. We first provide an estimate for the number of integers with preassigned digits in arithmetic progressions.

Lemma 5.24. *Let $n \geq 100$, $A \subset \{0,\dots,n-1\}$, $\boldsymbol{d} \in \{0,\dots,g-1\}^A$, $\kappa > 0$ and $0 < c < \frac{1}{2(1+\kappa)}$. If $|A| \leq cn$ then*

$$\sum_{\substack{1\leq q\leq Q\\(q,g)=1}} \max_{0\leq r<q} \left| \sum_{\substack{0\leq k<g^n\\ k\equiv r \bmod q}} f_{n,A,\boldsymbol{d}}(k) - \frac{g^{n-|A|}}{q} \right| \ll_{g,\kappa,c} g^{n-|A|}\, n \left(\frac{n}{\log^3 n}\right)^{1-\frac{1}{2(1+\kappa)c}} \tag{II.20}$$

where $Q = g^{\frac{\kappa n}{4(1+\kappa)}}$.

Proof. For any integers $q \geq 1$ and $0 \leq r < q$, we write

$$\sum_{\substack{0\leq k<g^n\\ k\equiv r \bmod q}} f_{n,A,\boldsymbol{d}}(k) = \frac{g^n}{q} \sum_{1\leq a\leq q} \mathrm{e}\left(\frac{-ar}{q}\right) F_{n,A,\boldsymbol{d}}\left(-\frac{a}{q}\right).$$

Since the contribution of $a = q$ is

$$\frac{g^n}{q} F_{n,A,\boldsymbol{d}}(-1) = \frac{1}{q} \sum_{0\leq k<g^n} f_{n,A,\boldsymbol{d}}(k) = \frac{g^{n-|A|}}{q},$$

we obtain

$$\sum_{\substack{1\leq q\leq Q\\(q,g)=1}} \max_{0\leq r<q} \left| \sum_{\substack{0\leq k<g^n\\ k\equiv r \bmod q}} f_{n,A,\boldsymbol{d}}(k) - \frac{g^{n-|A|}}{q} \right| \leq g^{n-|A|} \sum_{\substack{1\leq q\leq Q\\(q,g)=1}} T_{n,A,\boldsymbol{d}}(q) \tag{II.21}$$

where $T_{n,A,\boldsymbol{d}}(q)$ is defined by

$$T_{n,A,\boldsymbol{d}}(q) = \frac{1}{q} \sum_{1\leq a<q} g^{|A|} \left| F_{n,A,\boldsymbol{d}}\left(\frac{a}{q}\right) \right|.$$

By splitting up the a's according to the value of (a,q), we obtain

$$\begin{aligned}
\sum_{\substack{1\leq q\leq Q\\(q,g)=1}} T_{n,A,\boldsymbol{d}}(q) &= \sum_{\substack{1\leq q\leq Q\\(q,g)=1}} \frac{1}{q} \sum_{d\,|\,q} \sum_{\substack{1\leq a<q\\(a,q)=d}} g^{|A|} \left| F_{n,A,\boldsymbol{d}}\left(\frac{a}{q}\right) \right| \\
&= \sum_{\substack{1\leq d\leq Q\\(d,g)=1}} \frac{1}{d} \sum_{\substack{1\leq q'\leq Q/d\\(q',g)=1}} \frac{1}{q'} \sum_{\substack{1\leq a'<q'\\(a',q')=1}} g^{|A|} \left| F_{n,A,\boldsymbol{d}}\left(\frac{a'}{q'}\right) \right| \\
&\ll \log Q \sum_{\substack{2\leq q'\leq Q\\(q',g)=1}} \frac{1}{q'} \sum_{\substack{1\leq a'\leq q'\\(a',q')=1}} g^{|A|} \left| F_{n,A,\boldsymbol{d}}\left(\frac{a'}{q'}\right) \right|
\end{aligned}$$

and it follows from Lemma 5.22 that

$$\sum_{\substack{1\le q\le Q\\(q,g)=1}} T_{n,A,\boldsymbol{d}}(q) \ll_{g,\kappa,c} (\log Q)\left(\frac{n}{\log^3 n}\right)^{1-\frac{1}{2(1+\kappa)c}} \ll_{g,\kappa,c} n\left(\frac{n}{\log^3 n}\right)^{1-\frac{1}{2(1+\kappa)c}}.$$

By inserting this into (II.21) we obtain (II.20). □

In order to establish Lemma 5.27, we first estimate the contribution of the q's which are coprime to g in (II.23).

Lemma 5.25. *Let $n \ge 100$, $A \subset \{0,\dots,n-1\}$, $\boldsymbol{d} \in \{0,\dots,g-1\}^A$, $\kappa > 0$ and $0 < c < \frac{1}{2(1+\kappa)}$. If $|A| \le cn$ then, for any real number $1 \le Q \le g^{\frac{\kappa n}{4(1+\kappa)}}$,*

$$\sum_{\substack{1\le q\le Q\\(q,g)=1\\ q\ sf}} \sum_{0\le k<g^n} f_{n,A,\boldsymbol{d}}(k)\frac{\mu((k,q))}{\varphi\left(\frac{q}{(k,q)}\right)} = g^{n-|A|}\left(1 + O_{g,\kappa,c}\left(n^2\log n\left(\frac{n}{\log^3 n}\right)^{1-\frac{1}{2(1+\kappa)c}}\right)\right).$$

Remark 5.26. The main term in this asymptotic formula i.e. $g^{n-|A|}$ will be provided in the proof by the contribution of $q = 1$.

Proof. By using that for any squarefree integer $\ell \ge 1$,

$$\mu(\ell)\varphi(\ell) = \mu(\ell)\sum_{d\,|\,\ell} d\mu\left(\frac{\ell}{d}\right) = \sum_{d\,|\,\ell} d\mu(d),$$

we obtain, for any squarefree integer $q \ge 1$,

$$\begin{aligned}\sum_{0\le k<g^n} f_{n,A,\boldsymbol{d}}(k)\frac{\mu((k,q))}{\varphi\left(\frac{q}{(k,q)}\right)} &= \frac{1}{\varphi(q)}\sum_{0\le k<g^n} f_{n,A,\boldsymbol{d}}(k)\sum_{d\,|\,(k,q)} d\mu(d) \qquad \text{(II.22)}\\ &= \frac{1}{\varphi(q)}\sum_{d\,|\,q} d\mu(d)\sum_{\substack{0\le k<g^n\\ d\,|\,k}} f_{n,A,\boldsymbol{d}}(k) = \frac{1}{\varphi(q)}\sum_{d\,|\,q} d\mu(d)\left(\frac{g^{n-|A|}}{d} + \Delta_{n,A,\boldsymbol{d}}(d)\right)\\ &= g^{n-|A|}\mathbf{1}_{q=1} + O\left(\frac{1}{\varphi(q)}\sum_{d\,|\,q} d\,|\Delta_{n,A,\boldsymbol{d}}(d)|\right)\end{aligned}$$

where $\Delta_{n,A,\boldsymbol{d}}(d)$ is defined by

$$\Delta_{n,A,\boldsymbol{d}}(d) = \sum_{\substack{0\le k<g^n\\ d\,|\,k}} f_{n,A,\boldsymbol{d}}(k) - \frac{g^{n-|A|}}{d}.$$

Moreover,

$$\sum_{\substack{1\le q\le Q\\(q,g)=1\\ q\text{ sf}}}\frac{1}{\varphi(q)}\sum_{d\,|\,q}d\,|\Delta_{n,A,\boldsymbol{d}}(d)|=\sum_{\substack{1\le d\le Q\\(d,g)=1\\ d\text{ sf}}}d\,|\Delta_{n,A,\boldsymbol{d}}(d)|\sum_{\substack{1\le q'\le Q/d\\(q',dg)=1\\ q'\text{ sf}}}\frac{1}{\varphi(dq')}$$
$$=\sum_{\substack{1\le d\le Q\\(d,g)=1\\ d\text{ sf}}}\frac{d}{\varphi(d)}\,|\Delta_{n,A,\boldsymbol{d}}(d)|\sum_{\substack{1\le q'\le Q/d\\(q',dg)=1\\ q'\text{ sf}}}\frac{1}{\varphi(q')}$$

and by using that for any $x\ge 2$,

$$\sum_{k\le x}\frac{1}{\varphi(k)}\ll\log x$$

(see for instance [15, p. 163]) and for any integer $k\ge 3$,

$$\frac{k}{\varphi(k)}\ll\log\log k$$

(because $\liminf_{n\to+\infty}\frac{\varphi(n)\log\log n}{n}=e^{-\gamma}$, see [28, Theorem 328]), since $Q\le g^n$, we obtain

$$\sum_{\substack{1\le q\le Q\\(q,g)=1\\ q\text{ sf}}}\frac{1}{\varphi(q)}\sum_{d\,|\,q}d\,|\Delta_{n,A,\boldsymbol{d}}(d)|\ll\sum_{\substack{1\le d\le Q\\(d,g)=1\\ d\text{ sf}}}(\log\log g^n)\,|\Delta_{n,A,\boldsymbol{d}}(d)|\,(\log g^n)$$

hence, by Lemma 5.24,

$$\sum_{\substack{1\le q\le Q\\(q,g)=1\\ q\text{ sf}}}\frac{1}{\varphi(q)}\sum_{d\,|\,q}d\,|\Delta_{n,A,\boldsymbol{d}}(d)|\ll_{g,\kappa,c}g^{n-|A|}\,n^2\log n\,\left(\frac{n}{\log^3 n}\right)^{1-\frac{1}{2(1+\kappa)c}}$$

and it follows from (II.22) that

$$\sum_{\substack{1\le q\le Q\\(q,g)=1\\ q\text{ sf}}}\sum_{0\le k<g^n}f_{n,A,\boldsymbol{d}}(k)\frac{\mu((k,q))}{\varphi\left(\frac{q}{(k,q)}\right)}=g^{n-|A|}+O_{g,\kappa,c}\left(g^{n-|A|}\,n^2\log n\,\left(\frac{n}{\log^3 n}\right)^{1-\frac{1}{2(1+\kappa)c}}\right)$$

which completes the proof. □

We are now ready to establish the following estimate.

Lemma 5.27. *Let $n \geq 100$, $A \subset \{0,\dots,n-1\}$, $\boldsymbol{d} \in \{0,\dots,g-1\}^A$ such that $0 \in A$ and $(d_0, g) = 1$. Let $\kappa > 0$ and $0 < c < \frac{1}{2(1+\kappa)}$. If $|A| \leq cn$ then, for any real number $g \leq Q \leq g^{\frac{\kappa n}{4(1+\kappa)}}$,*

$$\sum_{\substack{1\leq q\leq Q\\ q\ sf}} \sum_{0\leq k<g^n} f_{n,A,\boldsymbol{d}}(k)\frac{\mu((k,q))}{\varphi\left(\frac{q}{(k,q)}\right)} = \tag{II.23}$$

$$g^{n-|A|}\frac{g}{\varphi(g)}\left(1+O_{g,\kappa,c}\left(n^2\log n\left(\frac{n}{\log^3 n}\right)^{1-\frac{1}{2(1+\kappa)c}}\right)\right).$$

Remark 5.28. The main term in this asymptotic formula i.e. $g^{n-|A|}\frac{g}{\varphi(g)}$ will be provided in the proof by the contribution of the q's which are squarefree divisors of g.

Proof. By splitting up the q's according to the value of (q, g), we obtain

$$\sum_{\substack{1\leq q\leq Q\\ q\ \mathrm{sf}}} \sum_{0\leq k<g^n} f_{n,A,\boldsymbol{d}}(k)\frac{\mu((k,q))}{\varphi\left(\frac{q}{(k,q)}\right)} = \sum_{\substack{d\,|\,g\\ d\ \mathrm{sf}}} \sum_{\substack{1\leq q'\leq Q/d\\ (q',g)=1\\ q'\ \mathrm{sf}}} \sum_{0\leq k<g^n} f_{n,A,\boldsymbol{d}}(k)\frac{\mu((k,dq'))}{\varphi\left(\frac{dq'}{(k,dq')}\right)}.$$

Since $0 \in A$ and $(d_0, g) = 1$, we have $f_{n,A,\boldsymbol{d}}(k) = 0$ for any k such that $(k, g) > 1$. Moreover, if $(k, g) = 1$ and $d \,|\, g$ then, for any $q' \geq 1$, we have $(k, dq') = (k, q')$, hence

$$\sum_{\substack{1\leq q\leq Q\\ q\ \mathrm{sf}}} \sum_{0\leq k<g^n} f_{n,A,\boldsymbol{d}}(k)\frac{\mu((k,q))}{\varphi\left(\frac{q}{(k,q)}\right)} = \sum_{\substack{d\,|\,g\\ d\ \mathrm{sf}}} \frac{1}{\varphi(d)} \sum_{\substack{1\leq q'\leq Q/d\\ (q',g)=1\\ q'\ \mathrm{sf}}} \sum_{0\leq k<g^n} f_{n,A,\boldsymbol{d}}(k)\frac{\mu((k,q'))}{\varphi\left(\frac{q'}{(k,q')}\right)}. \tag{II.24}$$

For $1 \leq d \leq g$, since $1 \leq \frac{Q}{d} \leq g^{\frac{\kappa n}{4(1+\kappa)}}$, it follows from Lemma 5.25 that

$$\sum_{\substack{1\leq q'\leq Q/d\\ (q',g)=1\\ q'\ \mathrm{sf}}} \sum_{0\leq k<g^n} f_{n,A,\boldsymbol{d}}(k)\frac{\mu((k,q'))}{\varphi\left(\frac{q'}{(k,q')}\right)} = g^{n-|A|}\left(1+O_{g,\kappa,c}\left(n^2\log n\left(\frac{n}{\log^3 n}\right)^{1-\frac{1}{2(1+\kappa)c}}\right)\right).$$

To complete the proof of the lemma, it suffices to insert this into (II.24) and to observe that, by multiplicativity,

$$\sum_{\substack{d\,|\,g\\ d\ \mathrm{sf}}} \frac{1}{\varphi(d)} = \sum_{d\,|\,g} \frac{\mu^2(d)}{\varphi(d)} = \prod_{p\,|\,g}\left(1+\frac{1}{\varphi(p)}\right) = \prod_{p\,|\,g}\left(1-\frac{1}{p}\right)^{-1} = \frac{g}{\varphi(g)}.$$

□

In order to establish Lemma 5.30, we will need the following estimate which is a corollary of Lemma 5.24.

Lemma 5.29. *Let $n \geq 100$, $A \subset \{0,\dots,n-1\}$, $\boldsymbol{d} \in \{0,\dots,g-1\}^A$, $\kappa > 0$ and $0 < c < \frac{1}{2(1+\kappa)}$. If $|A| \leq cn$ then*

$$\sum_{\substack{1\leq q\leq Q\\(q,g)=1}} \max_{0\leq r<q} \sum_{\substack{0\leq k<g^n\\ k\equiv r \bmod q}} f_{n,A,\boldsymbol{d}}(k) \ll_{g,\kappa,c} g^{n-|A|}\, n \tag{II.25}$$

where $Q = g^{\frac{\kappa n}{4(1+\kappa)}}$.

Proof. The left-hand side of II.25 is

$$\leq \sum_{\substack{1\leq q\leq Q\\(q,g)=1}} \frac{g^{n-|A|}}{q} + \sum_{\substack{1\leq q\leq Q\\(q,g)=1}} \max_{0\leq r<q} \left| \sum_{\substack{0\leq k<g^n\\ k\equiv r \bmod q}} f_{n,A,\boldsymbol{d}}(k) - \frac{g^{n-|A|}}{q} \right|.$$

For the first term, since $Q \leq g^n$, we have

$$\sum_{\substack{1\leq q\leq Q\\(q,g)=1}} \frac{g^{n-|A|}}{q} \leq g^{n-|A|} \sum_{1\leq q\leq g^n} \frac{1}{q} \ll_g g^{n-|A|}\, n.$$

For the second term, we apply Lemma 5.24 which gives the upper bound

$$\ll_{g,\kappa,c} g^{n-|A|}\, n \left(\frac{n}{\log^3 n}\right)^{1-\frac{1}{2(1+\kappa)c}} \leq g^{n-|A|}\, n.$$

This completes the proof. □

We are now ready to establish the following estimate.

Lemma 5.30. *Let $n \geq 100$, $A \subset \{0,\dots,n-1\}$, $\boldsymbol{d} \in \{0,\dots,g-1\}^A$ such that $0 \in A$ and $(d_0, g) = 1$. Let $\kappa > 0$ and $0 < c < \frac{1}{2(1+\kappa)}$. If $|A| \leq cn$ then, for any real number $2 \leq Q \leq g^{\frac{\kappa n}{4(1+\kappa)}}$,*

$$\sum_{\substack{1\leq q\leq Q\\ q \text{ sf}}} \sum_{0\leq k<g^n} \frac{f_{n,A,\boldsymbol{d}}(k)}{\varphi\left(\frac{q}{(k,q)}\right)} \ll_{g,\kappa,c} g^{n-|A|}\, n^2.$$

Proof. By splitting up the k's according to the value of (k,q), we obtain

$$\begin{aligned}\sum_{\substack{1\leq q\leq Q\\ q \text{ sf}}} \sum_{0\leq k<g^n} \frac{f_{n,A,\boldsymbol{d}}(k)}{\varphi\left(\frac{q}{(k,q)}\right)} &= \sum_{\substack{1\leq d\leq Q\\ d \text{ sf}}} \sum_{\substack{1\leq q'\leq Q/d\\ (d,q')=1,\, q' \text{ sf}}} \frac{1}{\varphi(q')} \sum_{\substack{0\leq k<g^n\\ (k,dq')=d}} f_{n,A,\boldsymbol{d}}(k)\\ &\ll (\log Q) \sum_{1\leq d\leq Q} \sum_{\substack{0\leq k<g^n\\ d\,|\,k}} f_{n,A,\boldsymbol{d}}(k).\end{aligned}$$

Since $0 \in A$ and $(d_0, g) = 1$, we have $f_{n,A,\boldsymbol{d}}(k) = 0$ for any k such that $(k, g) > 1$ and thus if $(d, g) > 1$ then the contribution of d in the sum above is 0. Since $Q \leq g^{\frac{\kappa n}{4(1+\kappa)}}$, by Lemma 5.29, the contribution of the d's such that $(d, g) = 1$ satisfies

$$\sum_{\substack{1 \leq d \leq Q \\ (d,g)=1}} \sum_{\substack{0 \leq k < g^n \\ d \mid k}} f_{n,A,\boldsymbol{d}}(k) \ll_{g,\kappa,c} g^{n-|A|}\, n.$$

To complete the proof, it suffices to notice that $\log Q \ll_g n$. □

5.4. Character sums over integers with preassigned digits in arithmetic progressions

The purpose of this section is to establish Lemma 5.34 which will be used for the study of "bad" characters (see Section 11.2.2).

Lemma 5.31. *If f is a complex-valued function on a subset $E \subset \mathbb{R}$ and if χ is a primitive character mod $q \geq 1$ then, for any integers k_0 and q_0 such that $q_0 \geq 1$ and $(q, q_0) = 1$, we have*

$$\left| \sum_{\substack{k \in E \\ k \equiv k_0 \bmod q_0}} \chi(k) f(k) \right| \leq \frac{1}{q_0 \sqrt{q}} \sum_{q_0' \mid q_0} \sum_{\substack{a=1 \\ (a, qq_0')=1}}^{qq_0'} \left| \sum_{k \in E} \mathrm{e}\left(\frac{ak}{qq_0'}\right) f(k) \right|. \tag{II.26}$$

Proof. We denote by S the sum over k in the left-hand side of (II.26). Since χ is a primitive character mod q, we have for any integer k,

$$\chi(k)\tau(\overline{\chi}) = \sum_{a=1}^{q} \overline{\chi}(a)\, \mathrm{e}\left(\frac{ak}{q}\right)$$

and $|\tau(\overline{\chi})| = \sqrt{q}$ (see [50, Theorem 9.7 p. 287]) and it follows that

$$|S| \leq \frac{1}{\sqrt{q}} \sum_{\substack{a=1 \\ (a,q)=1}}^{q} \left| \sum_{\substack{k \in E \\ k \equiv k_0 \bmod q_0}} \mathrm{e}\left(\frac{ak}{q}\right) f(k) \right|.$$

By using that $\frac{1}{q_0} \sum_{a_0=1}^{q_0} \mathrm{e}\left(\frac{a_0(k-k_0)}{q_0}\right)$ is equal to 1 if $k \equiv k_0 \bmod q_0$ and 0 otherwise, we obtain

$$|S| \leq \frac{1}{q_0 \sqrt{q}} \sum_{\substack{a=1 \\ (a,q)=1}}^{q} \sum_{a_0=1}^{q_0} \left| \sum_{k \in E} \mathrm{e}\left(\left(\frac{a}{q} + \frac{a_0}{q_0}\right) k\right) f(k) \right|$$

and by splitting up the a_0's according to the value of (a_0, q_0), this gives

$$|S| \le \frac{1}{q_0\sqrt{q}} \sum_{q_0' \mid q_0} \sum_{\substack{a=1 \\ (a,q)=1}}^{q} \sum_{\substack{a_0'=1 \\ (a_0',q_0')=1}}^{q_0'} \left| \sum_{k\in E} \mathrm{e}\left(\left(\frac{a}{q}+\frac{a_0'}{q_0'}\right)k\right) f(k)\right|.$$

Moreover, for any divisor q_0' of q_0, since $(q, q_0) = 1$ we have $(q, q_0') = 1$ and thus, if a runs through a complete set of residues prime to q and if a_0' runs through a complete set of residues prime to q_0' then $aq_0' + a_0'q$ runs through a complete set of residues prime to qq_0' and the lemma follows. □

Notation. Let $A \subset \mathbb{Z}$ and $\boldsymbol{d} = (d_j)_{j\in A} \in \{0, \dots, g-1\}^A$. For any integer $n \ge 0$, we define

$$\mathcal{D}(n, A, \boldsymbol{d}) = \{0 \le k < g^n : \forall j \in A \cap \{0, \dots, n-1\},\ \varepsilon_j(k) = d_j\}$$

so that $f_{n,A,\boldsymbol{d}} = \mathbf{1}_{\mathcal{D}(n,A,\boldsymbol{d})}$. We also define for any integer m,

$$\tau_m(\boldsymbol{d}) = (d_{j+m})_{j\in A-m} \in \{0, \dots, g-1\}^{A-m}.$$

Lemma 5.32. *Let $A \subset \mathbb{Z}$, $\boldsymbol{d} = (d_j)_{j\in A} \in \{0, \dots, g-1\}^A$, $0 \le \nu \le m \le n$, $0 \le \ell < g^{n-m}$ and $0 \le h < g^\nu$.*

(i) If $h \in \mathcal{D}(\nu, A, \boldsymbol{d})$ and $\ell \in \mathcal{D}(n-m, A-m, \tau_m(\boldsymbol{d}))$ then, for any $0 \le k < g^{m-\nu}$,

$$f_{n,A,\boldsymbol{d}}(\ell g^m + kg^\nu + h) = f_{m-\nu, A-\nu, \tau_\nu(\boldsymbol{d})}(k).$$

(ii) If $h \notin \mathcal{D}(\nu, A, \boldsymbol{d})$ or $\ell \notin \mathcal{D}(n-m, A-m, \tau_m(\boldsymbol{d}))$ then, for any $0 \le k < g^{m-\nu}$,

$$f_{n,A,\boldsymbol{d}}(\ell g^m + kg^\nu + h) = 0.$$

Proof. If $0 \le k < g^{m-\nu}$ then, since $0 \le \ell g^m + kg^\nu + h < g^n$,

$$\begin{aligned}
\ell g^m + kg^\nu + h \in \mathcal{D}(n, A, \boldsymbol{d}) &\Leftrightarrow \forall j \in A \cap \{0, \dots, n-1\},\ \varepsilon_j(\ell g^m + kg^\nu + h) = d_j \\
&\Leftrightarrow \begin{cases} \forall j \in A \cap \{0, \dots, \nu-1\},\ \varepsilon_j(h) = d_j \\ \forall j \in A \cap \{\nu, \dots, m-1\},\ \varepsilon_{j-\nu}(k) = d_j \\ \forall j \in A \cap \{m, \dots, n-1\},\ \varepsilon_{j-m}(\ell) = d_j \end{cases} \\
&\Leftrightarrow \begin{cases} \forall j \in A \cap \{0, \dots, \nu-1\},\ \varepsilon_j(h) = d_j \\ \forall j \in (A-\nu) \cap \{0, \dots, m-\nu-1\},\ \varepsilon_j(k) = d_{j+\nu} \\ \forall j \in (A-m) \cap \{0, \dots, n-m-1\},\ \varepsilon_j(\ell) = d_{j+m} \end{cases} \\
&\Leftrightarrow \begin{cases} h \in \mathcal{D}(\nu, A, \boldsymbol{d}) \\ k \in \mathcal{D}(m-\nu, A-\nu, \tau_\nu(\boldsymbol{d})) \\ \ell \in \mathcal{D}(n-m, A-m, \tau_m(\boldsymbol{d})). \end{cases}
\end{aligned}$$

It follows that if $h \in \mathcal{D}(\nu, A, \boldsymbol{d})$ and $\ell \in \mathcal{D}(n-m, A-m, \tau_m(\boldsymbol{d}))$ then, for any $0 \le k < g^{m-\nu}$,

$$f_{n,A,\boldsymbol{d}}(\ell g^m + k g^\nu + h) = \mathbf{1}_{\mathcal{D}(n,A,\boldsymbol{d})}(\ell g^m + k g^\nu + h) = \mathbf{1}_{\mathcal{D}(m-\nu,A-\nu,\tau_\nu(\boldsymbol{d}))}(k) = f_{m-\nu,A-\nu,\tau_\nu(\boldsymbol{d})}(k)$$

while if $h \notin \mathcal{D}(\nu, A, \boldsymbol{d})$ or $\ell \notin \mathcal{D}(n-m, A-m, \tau_m(\boldsymbol{d}))$ then, for any $0 \le k < g^{m-\nu}$, we have $f_{n,A,\boldsymbol{d}}(\ell g^m + k g^\nu + h) = 0$, which completes the proof. □

Lemma 5.33. *Let $n \ge 1$, $A \subset \{0, \dots, n-1\}$ and $\boldsymbol{d} = (d_j)_{j\in A} \in \{0, \dots, g-1\}^A$. If $0 \le \nu \le m \le n$ then, for any $\alpha \in \mathbb{R}$,*

$$\sum_{0\le \ell < g^{n-m}} \sum_{0 \le h < g^\nu} \left| \sum_{\substack{\ell g^m \le k < (\ell+1) g^m \\ k \equiv h \bmod g^\nu}} \mathrm{e}(\alpha k) f_{n,A,\boldsymbol{d}}(k) \right| = g^{n-|A|} g^{|A'|} \left| F_{m-\nu,A',\boldsymbol{d}'}(\alpha g^\nu) \right| \tag{II.27}$$

where $A' = (A-\nu) \cap \{0, \dots, m-\nu-1\}$ and $\boldsymbol{d}' = (d_{j+\nu})_{j\in A'} \in \{0, \dots, g-1\}^{A'}$.

Proof. For $0 \le \ell < g^{n-m}$ and $0 \le h < g^\nu$, we define

$$E(\ell, h) = \{k \in \mathbb{Z} : \ell g^m \le k < (\ell+1) g^m, k \equiv h \bmod g^\nu\}$$

and we denote by $S(\ell, h)$ the sum over $k \in E(\ell, h)$ in the left-hand side of (II.27). If k' runs through the set $\{0, \dots, g^{m-\nu} - 1\}$ then $k = \ell g^m + k' g^\nu + h$ runs through the set $E(\ell, h)$ and thus

$$|S(\ell, h)| = \left| \sum_{0 \le k' < g^{m-\nu}} \mathrm{e}\left(\alpha k' g^\nu\right) f_{n,A,\boldsymbol{d}}(\ell g^m + k' g^\nu + h) \right|.$$

If $\ell \in \mathcal{D}(n-m, A-m, \tau_m(\boldsymbol{d}))$ and $h \in \mathcal{D}(\nu, A, \boldsymbol{d})$ then, by Lemma 5.32, for any $0 \le k' < g^{m-\nu}$, we have

$$f_{n,A,\boldsymbol{d}}(\ell g^m + k' g^\nu + h) = f_{m-\nu,A-\nu,\tau_\nu(\boldsymbol{d})}(k') = f_{m-\nu,A',\boldsymbol{d}'}(k')$$

where $A' = (A-\nu) \cap \{0, \dots, m-\nu-1\}$ and $\boldsymbol{d}' = (d_{j+\nu})_{j\in A'} \in \{0, \dots, g-1\}^{A'}$, hence

$$|S(\ell, h)| = g^{m-\nu} \left| F_{m-\nu,A',\boldsymbol{d}'}(\alpha g^\nu) \right|.$$

If $\ell \notin \mathcal{D}(n-m, A-m, \tau_m(\boldsymbol{d}))$ or $h \notin \mathcal{D}(\nu, A, \boldsymbol{d})$ then, again by Lemma 5.32, for any $0 \le k' < g^{m-\nu}$, we have $f_{n,A,\boldsymbol{d}}(\ell g^m + k' g^\nu + h) = 0$, hence $|S(\ell, h)| = 0$. It follows that

$$\sum_{0\le \ell < g^{n-m}} \sum_{0 \le h < g^\nu} |S(\ell, h)| = |\mathcal{D}(n-m, A-m, \tau_m(\boldsymbol{d}))| \, |\mathcal{D}(\nu, A, \boldsymbol{d})| \, g^{m-\nu} \left| F_{m-\nu,A',\boldsymbol{d}'}(\alpha g^\nu) \right|$$

and by observing that

$$\begin{aligned} |\mathcal{D}(n-m, A-m, \tau_m(\boldsymbol{d}))| \, |\mathcal{D}(\nu, A, \boldsymbol{d})| \, g^{m-\nu} &= g^{n-m-|(A-m)\cap\{0,\dots,n-m-1\}|} \, g^{\nu-|A\cap\{0,\dots,\nu-1\}|} \, g^{m-\nu} \\ &= g^{n-|A|} g^{|A\cap\{\nu,\dots,m-1\}|} = g^{n-|A|} g^{|A'|}, \end{aligned}$$

we obtain (II.27). □

Lemma 5.34. *Let $n \geq 1$, $A \subset \{0, \dots, n-1\}$, $\boldsymbol{d} \in \{0, \dots, g-1\}^A$ and let χ be a primitive character mod q such that q has a prime factor which does not divide g. We write $q = sq'$ where $(q', g) = 1$ and any prime factor of s is a prime factor of g. Let $\kappa > 0$ and $0 < c_1 < \frac{1}{4(1+\kappa)}$. If $\nu \geq 0$ and $m \geq 0$ are integers such that $s \mid g^\nu$, $\nu + 100 \leq m \leq n$ and $|A \cap \{\nu, \dots, m-1\}| \leq c_1(m-\nu)$ then*

$$\sum_{\substack{1 \leq q_0 \leq Q/q' \\ (q_0, qg)=1}} \sum_{0 \leq \ell < g^{n-m}} \left| \sum_{\substack{\ell g^m \leq k < (\ell+1)g^m \\ q_0 \mid k}} \chi(k) f_{n,A,\boldsymbol{d}}(k) \right| \tag{II.28}$$
$$\ll_{g,\kappa,c_1} g^{n-|A|}(m-\nu) \left(\frac{m-\nu}{\log^3(m-\nu)} \right)^{1 - \frac{1}{4(1+\kappa)c_1}}$$

where $Q = g^{\frac{\kappa(m-\nu)}{4(1+\kappa)}}$.

Remark 5.35. The most difficult part to generalize from base 2 to a general base g is the study of the character sums appearing in (II.28). In base $g = 2$, the first step to handle them is to write $q = 2^\nu q'$ with q' odd and to split the summation over k according to the values of k mod 2^ν (indeed, Bourgain proceeds in this way in [5], see (5.9)). In a general base g, we will write instead $q = sq'$ with $(q', g) = 1$ and $s \mid g^\nu$ and split the summation over k according to the values of k mod g^ν. This is in accordance with Maynard's arguments [47]. The possible multiple factors of g will be responsible for the fact that, for some bases g, we will obtain very small values of c_0 (see Remark 11.12).

Proof. For any $q_0 \geq 1$ such that $(q_0, gq) = 1$ and $0 \leq \ell < g^{n-m}$, we denote by $S(q_0, \ell)$ the sum over k in the left-hand side of (II.28). Since $(s, q') = 1$, there exist unique characters χ_s mod s and χ' mod q' such that $\chi = \chi_s \chi'$ (see for instance [50, Corollary 4.6 p. 117]). Moreover, since χ is primitive mod q, χ_s and χ' are also primitive (see for instance [50, Lemma 9.3 p. 283]). Since χ_s has period s and $s \mid g^\nu$, we can write

$$S(q_0, \ell) = \sum_{0 \leq h < g^\nu} \chi_s(h) \sum_{\substack{\ell g^m \leq k < (\ell+1)g^m \\ k \equiv h \bmod g^\nu \\ q_0 \mid k}} \chi'(k) f_{n,A,\boldsymbol{d}}(k)$$

and since $(q_0, q') = 1$, by applying Lemma 5.31 to the inner sum, we obtain

$$|S(q_0, \ell)| \leq \frac{1}{q_0 \sqrt{q'}} \sum_{q_0' \mid q_0} \sum_{\substack{a=1 \\ (a, q'q_0')=1}}^{q'q_0'} \sum_{0 \leq h < g^\nu} \left| \sum_{\substack{\ell g^m \leq k < (\ell+1)g^m \\ k \equiv h \bmod g^\nu}} \mathrm{e}\left(\frac{ak}{q'q_0'} \right) f_{n,A,\boldsymbol{d}}(k) \right|.$$

By summing over $0 \le \ell < g^{n-m}$ and applying Lemma 5.33, we get

$$\sum_{0\le \ell<g^{n-m}} |S(q_0,\ell)| \le \frac{g^{n-|A|}}{q_0\sqrt{q'}} \sum_{q_0' \mid q_0} \sum_{\substack{a=1\\(a,q'q_0')=1}}^{q'q_0'} g^{|A'|} \left| F_{m-\nu,A',\boldsymbol{d'}}\left(\frac{ag^\nu}{q'q_0'}\right)\right|$$

where $A' = (A-\nu)\cap\{0,\dots,m-\nu-1\}$ and $\boldsymbol{d'} = (d_{j+\nu})_{j\in A'} \in \{0,\dots,g-1\}^{A'}$. It follows that, for any real number $Q' \le g^{m-\nu}$,

$$\sum_{\substack{1\le q_0\le Q'\\(q_0,qg)=1}} \sum_{0\le \ell<g^{n-m}} |S(q_0,\ell)| \le \sum_{\substack{1\le q_0\le Q'\\(q_0,qg)=1}} \frac{g^{n-|A|}}{q_0\sqrt{q'}} \sum_{q_0' \mid q_0} \sum_{\substack{a'=1\\(a',q'q_0')=1}}^{q'q_0'} g^{|A'|} \left| F_{m-\nu,A',\boldsymbol{d'}}\left(\frac{a'}{q'q_0'}\right)\right|$$

(we used that $(g, q'q_0') = 1$). By interchanging the summations over q_0 and q_0', we obtain

$$\begin{aligned}\sum_{\substack{1\le q_0\le Q'\\(q_0,qg)=1}} \sum_{0\le \ell<g^{n-m}} |S(q_0,\ell)| &\ll g^{n-|A|}\log(g^{m-\nu}) \sum_{\substack{1\le q_0'\le Q'\\(q_0',qg)=1}} \frac{1}{q_0'\sqrt{q'}} \sum_{\substack{a'=1\\(a',q'q_0')=1}}^{q'q_0'} g^{|A'|} \left| F_{m-\nu,A',\boldsymbol{d'}}\left(\frac{a'}{q'q_0'}\right)\right| \\ &\le g^{n-|A|}\log(g^{m-\nu}) \sum_{\substack{q'\le q_1\le q'Q'\\(q_1,g)=1}} \frac{1}{\sqrt{q_1}} \sum_{\substack{a'=1\\(a',q_1)=1}}^{q_1} g^{|A'|} \left| F_{m-\nu,A',\boldsymbol{d'}}\left(\frac{a'}{q_1}\right)\right|.\end{aligned}$$

Moreover, since $m-\nu \ge 100$, $0 < c_1 < \frac{1}{4(1+\kappa)}$ and $|A'| \le c_1(m-\nu)$, Lemma 5.23 asserts that

$$\sum_{\substack{2\le q_1\le Q\\(q_1,g)=1}} \frac{1}{\sqrt{q_1}} \sum_{\substack{a'=1\\(a',q_1)=1}}^{q_1} g^{|A'|} \left| F_{m-\nu,A',\boldsymbol{d'}}\left(\frac{a'}{q_1}\right)\right| \ll_{g,\kappa,c_1} \left(\frac{m-\nu}{\log^3(m-\nu)}\right)^{1-\frac{1}{4(1+\kappa)c_1}}$$

where $Q = g^{\frac{\kappa(m-\nu)}{4(1+\kappa)}}$. Since q has a prime factor which does not divide g, we have $q' \ge 2$ and thus by taking $Q' = Q/q' \le g^{m-\nu}$, we obtain

$$\sum_{\substack{1\le q_0\le Q/q'\\(q_0,qg)=1}} \sum_{0\le \ell<g^{n-m}} |S(q_0,\ell)| \ll_{g,\kappa,c_1} g^{n-|A|}\log(g^{m-\nu}) \left(\frac{m-\nu}{\log^3(m-\nu)}\right)^{1-\frac{1}{4(1+\kappa)c_1}}$$

which completes the proof. □

6. Improved zero-free region for L-functions to a smooth modulus

We will see in this section that the following result of Iwaniec (see Lemma 6.1) provides an improved zero-free region for $L(s,\chi \bmod q)$ when all prime factors of q are in a given finite set

of primes (see Lemma 6.4). This zero-free region will play a crucial role in the study of the contribution of "bad" characters (see Section 11.2.2).

Lemma 6.1. *Let $q \geq 3$ be an integer. There exists at most one nonprincipal character χ mod q such that $L(s,\chi)$ has a zero $\rho = \beta + i\gamma$ in the region*

$$\beta > 1 - \frac{1}{4 \cdot 10^4 \left(\log d + (\mathscr{L}\log(2\mathscr{L}))^{3/4}\right)}$$

where $d = \prod_{p \mid q} p$ and $\mathscr{L} = \log\left(q(|\gamma|+3)\right)$. If there does exist such a character χ then χ is real and ρ is unique, real and simple.

Proof. This is [34, Theorem 2]. □

Lemma 6.2. *There is an absolute constant $\xi_0 > 0$ such that for any real character χ mod $q \geq 2$ and any real zero β of $L(s,\chi)$, we have*

$$\beta < 1 - \frac{\xi_0}{d^{1/2}(\log d)^2}$$

where $d = \prod_{p \mid q} p$.

Remark 6.3. Lemma 6.2 is a more precise version of [30, Lemma 4].

Proof. Let χ be a real character mod $q \geq 2$ and β be a real zero of $L(s,\chi)$. We assume without loss of generality that $\beta > 0$. Let q_1 be the conductor of χ and let χ_1 be the primitive character mod q_1 that induces χ. If ρ is a zero of $L(s,\chi)$ and ρ is not on the imaginary axis then ρ is a zero of $L(s,\chi_1)$ (see for instance [50, p. 334]). It follows that β is a real zero of $L(s,\chi_1)$. Moreover, we have $q_1 \geq 3$ for if $q_1 = 1$ then $L(s,\chi_1) = \zeta(s)$ has no real zero $\beta > 0$ and there is no primitive character mod 2. Since χ is real, χ_1 is also real and thus there is an absolute constant $\xi > 0$ such that

$$\beta < 1 - \frac{\xi}{q_1^{1/2}(\log q_1)^2}$$

(see [15, p. 95–96]). Furthermore, since χ_1 is a real primitive character mod q_1, there exists $k \geq 1$ odd and squarefree such that $q_1 = k, 4k$ or $8k$ (see [35, p. 47]). Since $q_1 \mid q$, it follows that if q is odd then $q_1 = k \leq d$ and if q is even then $q_1 \leq 8k \leq 8\prod_{\substack{p \mid q \\ p \neq 2}} p \leq 4d$, which completes the proof. □

Lemma 6.4. *Let $\mathcal{P}$ be a nonempty finite set of prime numbers and $d_{\mathcal{P}} = \prod_{p \in \mathcal{P}} p$. There exist an absolute constant $\xi_1 > 0$ and $T_0 = T_0(d_{\mathcal{P}}) \geq 3$ such that for any real number $T \geq T_0$, for any character χ mod $q \geq 1$ such that any prime factor of q is in $\mathcal{P}$ and for any zero $\rho = \beta + i\gamma$ of $L(s,\chi)$ such that $|\gamma| \leq T$, we have*

$$\beta < 1 - \frac{\xi_1}{(l\log l)^{3/4}}$$

where $l = \log(qT)$. One can take for instance $T_0(d_{\mathcal{P}}) = \max\left(3, \exp\left(d_{\mathcal{P}}^{2/3}(\log d_{\mathcal{P}})^{8/3}\right)\right)$.

Remark 6.5. It follows from Lemma 6.4 that there exists $\xi_1(d_{\mathcal{P}}) > 0$ which depends only on $d_{\mathcal{P}}$ such that, if $q \geq 1$ is an integer whose prime factors are in $\mathcal{P}$ then the Dirichlet L-functions to modulus q have no zero in the region

$$\beta \geq 1 - \frac{\xi_1(d_{\mathcal{P}})}{(\mathscr{L} \log \mathscr{L})^{3/4}}$$

where $\mathscr{L} = \log(q(|\gamma| + 3))$. This shows that the zero-free region obtained by Gallagher ([24, Theorem 1]) for modulus q which are a power of a given odd prime holds more generally for modulus q such that any prime factor of q is in a given finite set of prime numbers.

Proof. Let $T_0 = T_0(d_{\mathcal{P}}) \geq 3$ such that $d_{\mathcal{P}}^{1/2}(\log d_{\mathcal{P}})^2 \leq (\log T_0)^{3/4}$ and let $T \geq T_0$. Let $q \geq 1$ such that any prime factor of q is in $\mathcal{P}$, let χ be a character mod q and let $\rho = \beta + i\gamma$ be a zero of $L(s, \chi)$ such that $|\gamma| \leq T$. We denote $l = \log(qT)$.

If χ is the principal character mod q then the zeros of $L(s, \chi)$ which are not on the imaginary axis are zeros of ζ and thus, by using the zero-free region for ζ due to Vinogradov and Korobov, there are absolute constants $\xi_2, \xi_2' > 0$ such that

$$\beta < 1 - \xi_2(\log T)^{-2/3}(\log\log T)^{-1/3} \leq 1 - \xi_2'(l \log l)^{-3/4}.$$

We assume now that χ is nonprincipal, thus $q \geq 3$ and we denote $d = \prod_{p \mid q} p \leq d_{\mathcal{P}}$. If χ is real and ρ is real then, by Lemma 6.2, there are absolute constants $\xi_0, \xi_0' > 0$ such that

$$\beta < 1 - \frac{\xi_0}{d^{1/2}(\log d)^2} \leq 1 - \frac{\xi_0}{d_{\mathcal{P}}^{1/2}(\log d_{\mathcal{P}})^2} \leq 1 - \frac{\xi_0}{(\log T)^{3/4}} \leq 1 - \frac{\xi_0'}{(l \log l)^{3/4}}.$$

If χ is not real or ρ is not real then, by Lemma 6.1,

$$\beta \leq 1 - \frac{1}{4 \cdot 10^4 \left(\log d + (\mathscr{L} \log(2\mathscr{L}))^{3/4}\right)}$$

where $\mathscr{L} = \log\left(q(|\gamma| + 3)\right)$. Since $\mathscr{L} \log(2\mathscr{L}) \ll \log(qT) \log\log(qT) = l \log l$ and $(l \log l)^{3/4} \gg (\log T_0)^{3/4} \gg \log d_{\mathcal{P}} \geq \log d$, there is an absolute constant $\xi_3 > 0$ such that $\beta < 1 - \xi_3(l \log l)^{-3/4}$, which completes the proof. □

7. Other preliminaries

7.1. Smooth approximation of $\mathbf{1}_{[-1,1]}$ with small Fourier transform

We provide in this section an example of a smooth approximation w of $\mathbf{1}_{[-1,1]}$ which has a compact support and a small Fourier transform. The fact that w has a compact support will allow us in Section 9 to replace the indicator function of a major arc by an appropriate dilation of w up to an error which will be captured by the minor arcs contribution (see Lemma 9.2). The fact that $\widehat{w}$ is small will be essential in the treatment of the major arcs.

Lemma 7.1. *There is an explicit function $w : \mathbb{R} \to \mathbb{R}$ such that*

$$(i)\ 0 \le w \le 1, \quad (ii)\ w = 1 \text{ on } [-1,1], \quad (iii)\ \operatorname{supp} w \subset [-2,2], \quad (iv)\ w \in \mathcal{C}^\infty(\mathbb{R}),$$

$$(v)\ \widehat{w}(y) = O\left(e^{-|y|^{1/2}}\right) \text{ for any } y \in \mathbb{R}, \text{ where } \widehat{w}(y) = \int_{\mathbb{R}} w(u)\,\mathrm{e}(-yu)du.$$

Remark 7.2. Since w has a compact support, it follows that $\widehat{w} \in \mathcal{C}^\infty(\mathbb{R})$ and all derivatives of $\widehat{w}$ are bounded.

Proof. By using the construction of Ingham [33] (see the annex for more details), we can find an explicit function $K : \mathbb{R} \to \mathbb{R}$ such that

$$K \ge 0, \quad \operatorname{supp} K \subset \left[-\frac{1}{2}, \frac{1}{2}\right], \quad K \in \mathcal{C}^\infty(\mathbb{R}), \quad \int_{\mathbb{R}} K = 1, \quad \widehat{K}(y) = O\left(e^{-|y|^{1/2}}\right)\ (\forall y \in \mathbb{R})$$

and we define $w = K * \mathbf{1}_{\left[-\frac{3}{2},\frac{3}{2}\right]}$. If $|x| \le 1$ then for any t such that $|t| \le 1/2$, we have $|x-t| \le 3/2$ and since $\operatorname{supp} K \subset [-\frac{1}{2}, \frac{1}{2}]$, it follows that

$$w(x) = \int_{|x-t|\le 3/2} K(t)dt = \int_{\mathbb{R}} K(t)dt = 1,$$

which proves (ii). The function w satisfies (i), (iii), (iv) and (v) by elementary properties of convolutions. □

Lemma 7.3. *If $w : \mathbb{R} \to \mathbb{R}$ satisfies the conditions of Lemma 7.1 then, for any real numbers $0 < t < \frac{1}{2}$ and $v \ge 1$, we have*

$$(a) \sum_{k\in\mathbb{Z}} t\,|\widehat{w}(kt)| = O(1), \qquad (b) \sum_{|k|\ge v/t} t\,|\widehat{w}(kt)| = O\left(v^{1/2}e^{-v^{1/2}}\right), \qquad (c) \sum_{k\in\mathbb{Z}} t\widehat{w}(kt) = 1.$$

Proof. The properties (a) and (b) follow from the fact that for any $y \in \mathbb{R}$, $\widehat{w}(y) = O\left(e^{-|y|^{1/2}}\right)$ and for any $k_0 \ge 1$,

$$\sum_{|k|\le k_0} te^{-|kt|^{1/2}} = t + 2\sum_{1\le k\le k_0} te^{-(kt)^{1/2}} \ll t + \int_0^{k_0} te^{-(xt)^{1/2}}dx \ll t + \int_0^{+\infty} e^{-u^{1/2}}du \ll 1$$

and

$$\begin{aligned}\sum_{|k|\ge v/t} te^{-|kt|^{1/2}} = 2\sum_{k\ge v/t} te^{-(kt)^{1/2}} &\ll te^{-(\lceil v/t\rceil t)^{1/2}} + \int_{\lceil v/t\rceil}^{+\infty} te^{-(xt)^{1/2}}dx \\ &\ll te^{-v^{1/2}} + \int_{v/t}^{+\infty} te^{-(xt)^{1/2}}dx = te^{-v^{1/2}} + \int_v^{+\infty} e^{-u^{1/2}}du \ll v^{1/2}e^{-v^{1/2}}.\end{aligned}$$

Moreover, by defining $w_{\frac{1}{t}}(x) = \frac{1}{t} w\left(\frac{1}{t}x\right)$ and by using Poisson summation formula, we obtain

$$\sum_{k\in\mathbb{Z}} t\widehat{w}\,(kt) = \sum_{k\in\mathbb{Z}} t\widehat{w_{\frac{1}{t}}}(k) = \sum_{k\in\mathbb{Z}} t w_{\frac{1}{t}}(k) = \sum_{k\in\mathbb{Z}} w\left(\frac{1}{t}k\right) = \sum_{\left|\frac{k}{t}\right|\le 2} w\left(\frac{1}{t}k\right) = w(0) = 1$$

which completes the proof. □

7.2. Gauss sums

If χ is a Dirichlet character mod q and if k is an integer then we define

$$\tau(k,\chi) = \sum_{a=1}^{q} \chi(a)\,\mathrm{e}\left(\frac{ak}{q}\right) \quad \text{and} \quad \tau(\chi) = \tau(1,\chi) = \sum_{a=1}^{q} \chi(a)\,\mathrm{e}\left(\frac{a}{q}\right).$$

Lemma 7.4. *Let χ be a Dirichlet character mod $q \ge 1$. If q_1 is the conductor of χ, if χ_1 is the primitive character mod q_1 that induces χ and if $q_2 = q/q_1$ then*

(i) $\tau(\chi) = \mu(q_2)\chi_1(q_2)\tau(\chi_1)$,

(ii) if $(q_1,q_2) = 1$ then, for any integer k,

$$\tau(k,\chi) = c_{q_2}(k)\chi_1(q_2)\overline{\chi_1}(k)\tau(\chi_1)$$

where

$$c_{q_2}(k) := \sum_{\substack{1\le a\le q_2\\(a,q_2)=1}} \mathrm{e}\left(\frac{ak}{q_2}\right) = \frac{\mu\left(\frac{q_2}{(q_2,k)}\right)}{\varphi\left(\frac{q_2}{(q_2,k)}\right)}\varphi(q_2),$$

(iii) for any integer k,

$$\frac{1}{\varphi(q)}\overline{\tau(\chi)}\tau(k,\chi) = \begin{cases} \frac{q_1}{\varphi(q_1)}\overline{\chi_1}(k)\frac{\mu((q_2,k))}{\varphi\left(\frac{q_2}{(q_2,k)}\right)} & \text{if } (q_1,q_2)=1 \text{ and } q_2 \text{ is squarefree,}\\ 0 & \text{otherwise.}\end{cases}$$

Proof. For (i), see [50, Theorem 9.10 p. 289]. To establish (ii), we note that since $(q_1,q_2)=1$, if u runs through a complete set of residues prime to q_1 and if v runs through a complete set of residues prime to q_2 then vq_1+uq_2 runs through a complete set of residues prime to $q_1q_2 = q$ and thus

$$\begin{aligned}\tau(k,\chi) &= \sum_{\substack{1\le a\le q\\(a,q)=1}} \chi_1(a)\,\mathrm{e}\left(\frac{ak}{q}\right) = \sum_{\substack{1\le u\le q_1\\(u,q_1)=1}} \chi_1\left(uq_2\right)\mathrm{e}\left(\frac{uk}{q_1}\right)\sum_{\substack{1\le v\le q_2\\(v,q_2)=1}} \mathrm{e}\left(\frac{vk}{q_2}\right)\\ &= c_{q_2}(k)\chi_1(q_2)\tau(k,\chi_1).\end{aligned}$$

Moreover, since χ_1 is primitive,

$$\tau(k,\chi_1) = \overline{\chi_1}(k)\tau(\chi_1)$$

(see [50, Corollary 9.8 p. 288]). We refer to [50, Theorem 4.1 p. 110] for the expression of $c_{q_2}(k)$ in terms of μ and φ. The property (iii) follows from (i) and (ii) by using that $|\tau(\chi_1)|^2 = q_1$ (see [50, Theorem 9.7 p. 287]) and that if q_2 is squarefree then $\mu(q_2)\mu\left(\frac{q_2}{(q_2,k)}\right) = \mu((q_2,k))$. □

7.3. Primes in short intervals

For any real numbers $a \leq t$, we define

$$R_a(t) = \psi(t) - \psi(a) - (\lfloor t \rfloor - \lfloor a \rfloor).$$

Lemma 7.5. *If $g \in \mathcal{C}^1([a,b])$ then, by denoting $M = |g(b)| + \int_a^b |g'(t)|\,dt$,*

$$\left| \sum_{a<k\leq b} g(k)\Lambda(k) - \sum_{a<k\leq b} g(k) \right| \leq M \sup_{a<t\leq b} |R_a(t)|.$$

Proof. It suffices to write by partial summation

$$\begin{aligned}\sum_{a<k\leq b} g(k)\Lambda(k) &= \int_{a^+}^{b^+} g(t)d\left(\psi(t)-\psi(a)\right) = \int_{a^+}^{b^+} g(t)d\left(\lfloor t\rfloor - \lfloor a\rfloor\right) + \int_{a^+}^{b^+} g(t)dR_a(t)\\ &= \sum_{a<k\leq b} g(k) + g(b)R_a(b) - \int_a^b g'(t)R_a(t)dt.\end{aligned}$$

□

Lemma 7.6. *If $h \geq x^{0.75}e^{(\log x)^{0.8}}$ and $x \geq x_0 \geq 1$ then*

$$\psi(x+h) - \psi(x) = \lfloor x+h\rfloor - \lfloor x\rfloor + O\left(he^{-(\log x)^{0.1}}\right). \tag{II.29}$$

Remark 7.7. By using the arguments given by Huxley in [32, Section 28], it might be possible to obtain an asymptotic formula similar to (II.29) with the wider range $h \geq x^{7/12+\varepsilon}$ but Lemma 7.6 will be sufficient for our purpose.

Proof. By [36, Theorem 2 p. 98],

$$\psi(x+h) - \psi(x) = h + O\left(he^{-(\log x)^{0.1}}\right)$$

and

$$\lfloor x+h\rfloor - \lfloor x\rfloor = h + O(1) = h + O\left(he^{-(\log x)^{0.1}}\right).$$

□

Lemma 7.8. *If $g \in \mathcal{C}^1([a,b])$ and $b-a \geq a^{0.75}e^{(\log a)^{0.8}+(\log a)^{0.1}}\log a$, $a \geq a_0 \geq e$ then*

$$\sum_{a<k\leq b} g(k)\Lambda(k) = \sum_{a<k\leq b} g(k) + O\left(M(b-a)e^{-(\log a)^{0.1}}\right)$$

where $M = |g(b)| + \int_a^b |g'(t)|\,dt$.

Proof. Let $t_0 = a + a^{0.75}e^{(\log a)^{0.8}} \leq b$. For any $t_0 \leq t \leq b$, since $t - a \geq a^{0.75}e^{(\log a)^{0.8}}$, Lemma 7.6 gives

$$R_a(t) = O\left((t-a)e^{-(\log a)^{0.1}}\right) = O\left((b-a)e^{-(\log a)^{0.1}}\right).$$

Moreover, for any $a \leq t \leq t_0$, it follows from the definition of ψ that

$$R_a(t) = O\left((\log t)(\lfloor t \rfloor - \lfloor a \rfloor)\right) = O\left((\log a)a^{0.75}e^{(\log a)^{0.8}}\right)$$

and since $(\log a)a^{0.75}e^{(\log a)^{0.8}} \leq (b-a)\, e^{-(\log a)^{0.1}}$, we obtain for any $a \leq t \leq b$,

$$R_a(t) = O\left((b-a)e^{-(\log a)^{0.1}}\right).$$

To complete the proof, it suffices to apply Lemma 7.5. □

Lemma 7.9. *If $g \in \mathcal{C}^1([a,b])$ and if χ is a character mod $q \geq 1$ then*

$$\left|\sum_{a<k\leq b} g(k)\chi(k)\Lambda(k)\right| \leq M \sup_{a<t\leq b} |\psi(t,\chi) - \psi(a,\chi)|$$

where $M = |g(b)| + \int_a^b |g'(t)|\, dt$.

Proof. It suffices to write by partial summation

$$\begin{aligned}\sum_{a<k\leq b} g(k)\chi(k)\Lambda(k) &= \int_{a^+}^{b^+} g(t)d\left(\psi(t,\chi) - \psi(a,\chi)\right) \\ &= g(b)\left(\psi(b,\chi) - \psi(a,\chi)\right) - \int_a^b g'(t)\left(\psi(t,\chi) - \psi(a,\chi)\right)dt.\end{aligned}$$

□

Lemma 7.10. *If χ is a primitive character mod $q \geq 1$ and if $2 \leq T \leq x$ are real numbers then*

$$\psi(x,\chi) = x\mathbf{1}_{q=1} - \sum_{\substack{L(\rho,\chi)=0 \\ |\operatorname{Im}\rho|\leq T}} \frac{x^\rho - 1}{\rho} + O\left(\frac{x}{T}(\log xq)^2\right)$$

where the sum runs over all nontrivial zeros ρ of $L(s,\chi)$ (i.e. zeros ρ of $L(s,\chi)$ with $0 < \operatorname{Re}\rho < 1$) such that $|\operatorname{Im}\rho| \leq T$.

Proof. See for instance [35, Proposition 5.25]. □

Corollary 7.11. *If χ is a primitive character mod $q \geq 1$ and if $2 \leq T \leq a \leq b$ are real numbers then*

$$|\psi(b,\chi) - \psi(a,\chi) - (b-a)\mathbf{1}_{q=1}| \ll (b-a) \sum_{\substack{L(\rho,\chi)=0 \\ |\gamma|\leq T}} a^{\beta-1} + \frac{b}{T}(\log bq)^2$$

where the sum runs over all nontrivial zeros $\rho = \beta + i\gamma$ of $L(s,\chi)$ such that $|\gamma| \leq T$.

Proof. This follows from Lemma 7.10 and from the inequality

$$\left|\sum_{\substack{L(\rho,\chi)=0\\|\gamma|\leq T}}\frac{b^\rho-a^\rho}{\rho}\right|=\left|\sum_{\substack{L(\rho,\chi)=0\\|\gamma|\leq T}}\int_a^b u^{\rho-1}du\right|\leq\sum_{\substack{L(\rho,\chi)=0\\|\gamma|\leq T}}\int_a^b u^{\beta-1}du\leq(b-a)\sum_{\substack{L(\rho,\chi)=0\\|\gamma|\leq T}}a^{\beta-1}.$$

□

7.4. A zero-density estimate and a consequence

The purpose of this section is to establish Lemma 7.13 which will be used in the study of "good" characters (see Section 11.2.1). If $T\geq 0$ and $\sigma\geq 0$ are real numbers then, for any character χ, we denote by $N(\sigma,T,\chi)$ the number of zeros of $L(s,\chi)$ in the rectangle

$$\{\beta+i\gamma:\sigma\leq\beta\leq 1,\ |\gamma|\leq T\}$$

and for any set $\mathcal{C}$ of characters, we define

$$N_{\mathcal{C}}(\sigma,T)=\sum_{\chi\in\mathcal{C}}N(\sigma,T,\chi).$$

If $Q\geq 1$ is a real number and if $\mathcal{C}$ is the set of primitive characters with conductor $q\leq Q$ then we will simply write

$$N_Q(\sigma,T)=\sum_{1\leq q\leq Q}\sideset{}{^*}\sum_{\chi \bmod q}N(\sigma,T,\chi).$$

Lemma 7.12. *Let $\varepsilon>0$. If $T\geq 2$, $Q\geq 1$ and $1/2\leq\sigma\leq 1$ then*

$$N_Q(\sigma,T)\ll_\varepsilon(Q^5T^3)^{(1+\varepsilon)(1-\sigma)}.$$

Proof. See [3, p. 40] or [62, p. 615]. □

Lemma 7.13. *Let $\varepsilon>0$, $T\geq 2$, $Q\geq 1$ and $0\leq\eta\leq 1/2$ be real numbers. If $\mathcal{C}$ is a set of primitive characters with conductor $q\leq Q$ such that*

$$\sigma>1-\eta\Rightarrow N_{\mathcal{C}}(\sigma,T)=0$$

and if $a\in\mathbb{R}$ is such that $(Q^5T^3)^{1+\varepsilon}\leq a$ then

$$\sum_{\chi\in\mathcal{C}}\sum_{\substack{L(\rho,\chi)=0\\|\gamma|\leq T}}a^{\beta-1}\ll_\varepsilon\left(\frac{a}{(Q^5T^3)^{1+\varepsilon}}\right)^{-\eta}$$

where the inner sum runs over all nontrivial zeros $\rho=\beta+i\gamma$ of $L(s,\chi)$ such that $|\gamma|\leq T$.

Proof. If χ is a primitive character then the nontrivial zeros of $L(s,\chi)$ are symmetric with respect to the line $\operatorname{Re} s = 1/2$ (see for instance [50, p. 333]), hence

$$\sum_{\substack{L(\rho,\chi)=0\\ |\gamma|\le T}} a^{\beta-1} \le \sum_{\substack{L(\rho,\chi)=0\\ |\gamma|\le T,\, 1/2\le\beta\le 1}} (a^{\beta-1}+a^{-\beta}) \le 2 \sum_{\substack{L(\rho,\chi)=0\\ |\gamma|\le T,\, 1/2\le\beta\le 1}} a^{\beta-1}$$

so that it suffices to establish

$$\sum_{\chi\in\mathcal{C}} \sum_{\substack{L(\rho,\chi)=0\\ |\gamma|\le T,\, 1/2\le\beta\le 1}} a^{\beta-1} \ll_\varepsilon \left(\frac{a}{(Q^5T^3)^{1+\varepsilon}}\right)^{-\eta}. \tag{II.30}$$

By partial summation, we can write

$$\begin{aligned}\sum_{\chi\in\mathcal{C}} \sum_{\substack{L(\rho,\chi)=0\\ |\gamma|\le T,\, 1/2\le\beta\le 1}} a^{\beta-1} &= -\int_{1/2^-}^{1^+} a^{\sigma-1} d_\sigma N_{\mathcal{C}}(\sigma,T)\\ &= a^{-1/2}N_{\mathcal{C}}(1/2,T) + \log a \int_{1/2}^{1} a^{\sigma-1}N_{\mathcal{C}}(\sigma,T)d\sigma.\end{aligned}$$

Since $N_{\mathcal{C}}(\sigma,T)=0$ for any $\sigma > 1-\eta$ and $N_{\mathcal{C}}(\sigma,T) \le N_Q(\sigma,T)$ for any $1/2 \le \sigma \le 1-\eta$, we obtain

$$\sum_{\chi\in\mathcal{C}} \sum_{\substack{L(\rho,\chi)=0\\ |\gamma|\le T,\, 1/2\le\beta\le 1}} a^{\beta-1} \le a^{-1/2}N_Q(1/2,T) + \log a \int_{1/2}^{1-\eta} a^{\sigma-1}N_Q(\sigma,T)d\sigma. \tag{II.31}$$

We introduce a real parameter ε_1 such that $0<\varepsilon_1<\varepsilon$ and we denote $X = a(Q^5T^3)^{-(1+\varepsilon)}$ and $X_1 = a(Q^5T^3)^{-(1+\varepsilon_1)}$. By applying Lemma 7.12 with ε_1 in place of ε, it follows from (II.31) that

$$\sum_{\chi\in\mathcal{C}} \sum_{\substack{L(\rho,\chi)=0\\ |\gamma|\le T,\, 1/2\le\beta\le 1}} a^{\beta-1} \ll_{\varepsilon_1} X_1^{-\frac{1}{2}} + \log a \int_{1/2}^{1-\eta} X_1^{\sigma-1} d\sigma. \tag{II.32}$$

Since $1 \le X < X_1 < a$ and $0 \le \eta \le 1/2$, the right-hand side of (II.32) is

$$X_1^{-\frac{1}{2}} + \frac{\log a}{\log X_1}(X_1^{-\eta} - X_1^{-1/2}) \ll \frac{\log a}{\log X_1} X_1^{-\eta} \le \frac{\log a}{\log X_1} X^{-\eta}.$$

Moreover, since $(Q^5T^3)^{1+\varepsilon} \le a$, we have $X_1 \ge a^{1-\frac{1+\varepsilon_1}{1+\varepsilon}}$, it follows that

$$\sum_{\chi\in\mathcal{C}} \sum_{\substack{L(\rho,\chi)=0\\ |\gamma|\le T,\, 1/2\le\beta\le 1}} a^{\beta-1} \ll_{\varepsilon_1} \frac{1}{1-\frac{1+\varepsilon_1}{1+\varepsilon}} X^{-\eta}$$

which gives (II.30) by choosing for instance $\varepsilon_1 = \varepsilon/2$ and completes the proof. □

7.5. A sum involving φ on an interval

Lemma 7.14. *If $I \subset]0, +\infty[$ is a bounded interval and if $q \geq 1$ is an integer then*

$$\sum_{k \in I} \frac{1}{\varphi\left(\frac{q}{(k,q)}\right)} \leq \left(\frac{|I|}{q} + 1\right) \sigma_0(q)$$

where $\sigma_0(q)$ is the number of divisors of q.

Proof. It suffices to write

$$\sum_{k \in I} \frac{1}{\varphi\left(\frac{q}{(k,q)}\right)} = \sum_{r=1}^{q} \frac{1}{\varphi\left(\frac{q}{(r,q)}\right)} \sum_{\substack{k \in I \\ k \equiv r \bmod q}} 1 \leq \left(\frac{|I|}{q} + 1\right) \sum_{r=1}^{q} \frac{1}{\varphi\left(\frac{q}{(r,q)}\right)}$$

and to observe that

$$\sum_{r=1}^{q} \frac{1}{\varphi\left(\frac{q}{(r,q)}\right)} = \sum_{d \,|\, q} \frac{1}{\varphi\left(\frac{q}{d}\right)} \sum_{\substack{1 \leq r \leq q \\ (r,q)=d}} 1 = \sigma_0(q).$$

□

8. Minor arcs contribution

We keep the notations and all the hypothesis of Section 4. We first bound $|S(\alpha)|$ over minor arcs.

Lemma 8.1. *If $B_1 \leq N^{2/5}$ then*

$$\sup_{\alpha \in \mathfrak{m}} |S(\alpha)| \ll \frac{N}{\sqrt{B_1}} (\log N)^3. \tag{II.33}$$

Proof. Let $\alpha \in \mathfrak{m}$. By Dirichlet's theorem on Diophantine approximation (see for instance [28, Theorem 36]) there exists an irreducible fraction a/q such that $1 \leq q \leq \frac{N}{B}$ and

$$\left|\alpha - \frac{a}{q}\right| \leq \frac{B}{qN} \leq \frac{1}{q^2}.$$

Since $\alpha \in \mathfrak{m}$, we have $q > B_1$ (otherwise, $\alpha \in \mathfrak{M}(q, a)$). It follows from Vinogradov's estimate (see [35, Theorem 13.6]) that

$$|S(\alpha)| \ll \left(q^{1/2} N^{1/2} + q^{-1/2} N + N^{4/5}\right) (\log N)^3 \ll \left(\frac{N}{\sqrt{B}} + \frac{N}{\sqrt{B_1}} + N^{4/5}\right) (\log N)^3$$

and since $B_1 \leq B$ and $B_1 \leq N^{2/5}$, we obtain (II.33). □

Lemma 8.2. *Let $0 < c \leq C_1(g)e^{-1}$ where $C_1(g)$ is defined by (II.10). If $B_1 \leq N^{2/5}$ and $|A| \leq cn$ then*

$$\int_{\mathfrak{m}} \left|S(\alpha)\overline{R(\alpha)}\right| d\alpha \ll \frac{N^2}{\sqrt{B_1}} (\log N)^3 \left\|F_{n,A,\boldsymbol{d}}\right\|_1 \ll N g^{-|A|} \frac{N^{C_2(g)c\log\left(\frac{C_1(g)}{c}\right)}}{\sqrt{B_1}} (\log N)^4$$

where $C_2(g)$ is defined by (II.11).

Remark 8.3. We will choose, in Section 13.3, $B_1 \leq N^{2/5}$ such that

$$N^{2C_2(g)c\log\left(\frac{C_1(g)}{c}\right)} (\log N)^8 = o(B_1)$$

so that the contribution of the minor arcs is admissible.

Proof. Since $f_{n,A,\boldsymbol{d}}(0) = f_{n,A,\boldsymbol{d}}(N) = 0$, we have, for any $\alpha \in \mathbb{R}$,

$$\overline{R(\alpha)} = \sum_{1\leq k\leq N} f_{n,A,\boldsymbol{d}}(k)\, \mathrm{e}(-k\alpha) = N\, F_{n,A,\boldsymbol{d}}(\alpha)$$

and it follows that

$$\int_{\mathfrak{m}} \left|S(\alpha)\overline{R(\alpha)}\right| d\alpha \leq N \left\|F_{n,A,\boldsymbol{d}}\right\|_1 \sup_{\alpha\in\mathfrak{m}} |S(\alpha)|\,.$$

By using Lemma 8.1, we obtain the first inequality. For the second inequality, we apply Proposition 5.11:

$$\left\|F_{n,A,\boldsymbol{d}}\right\|_1 \ll (\log g^n)\, g^{-|A|} g^{\left(C_2(g)\rho\log\left(\frac{C_1(g)}{\rho}\right)-1\right)n} = g^{-|A|}(\log N) N^{C_2(g)\rho\log\left(\frac{C_1(g)}{\rho}\right)-1} \tag{II.34}$$

where $\rho = \frac{|A|}{n}$. Moreover, since $|A| \leq cn$, we have $\rho \leq c \leq C_1(g)e^{-1}$ and since the function $t \mapsto t\log(C_1(g)/t)$ is increasing on $]0, C_1(g)e^{-1}]$, (II.34) remains true with c in place of ρ. This completes the proof. □

9. Major arcs contribution I

The results of this section together with those of Section 11 will enable us to prove in Section 13.3 that if $|A| \leq cn$ with c small enough then we can choose B_1 and B so that the contribution of the major arcs is

$$\int_{\mathfrak{M}} S(\alpha)\overline{R(\alpha)} d\alpha = \sum_{1\leq q\leq B_1} \sum_{\substack{1\leq a\leq q\\(a,q)=1}} \int_{|\alpha-\frac{a}{q}|\leq\frac{B}{qN}} S(\alpha)\overline{R(\alpha)} d\alpha = N g^{-|A|} \frac{g}{\varphi(g)} (1+o(1))$$

(actually, we will obtain a quantitative version).

9.1. Smoothing

The first step in the major arcs analysis consists in replacing the indicator function of the interval $\left|\alpha - \frac{a}{q}\right| \leq \frac{B}{qN}$ by the smooth function

$$\alpha \mapsto w\left(\frac{qN}{B}\left(\alpha - \frac{a}{q}\right)\right)$$

where w is a function as in Lemma 7.1.

Remark 9.1. This step will allow us to replace the Fourier transform of the indicator function of the interval $[-1,1]$ by $\widehat{w}$ whose decreasing speed is much higher (see Lemma 7.1 (v)). This will be essential in the treatment of the major arcs (see Remark 9.9).

Lemma 9.2.

$$\left|\int_{\mathfrak{M}} S(\alpha)\overline{R(\alpha)}d\alpha - \sum_{1\leq q\leq B_1}\sum_{\substack{1\leq a\leq q\\(a,q)=1}}\int_{\mathbb{R}} w\left(\frac{qN}{B}\left(\alpha-\frac{a}{q}\right)\right)S(\alpha)\overline{R(\alpha)}d\alpha\right| \leq \int_{\mathfrak{m}}\left|S(\alpha)\overline{R(\alpha)}\right|d\alpha \tag{II.35}$$

Remark 9.3. Note that the right-hand side of (II.35) has already been studied in Section 8 to bound the contribution of the minor arcs.

Proof. Since $w = 1$ on $[-1,1]$,

$$\int_{\mathfrak{M}} S(\alpha)\overline{R(\alpha)}d\alpha = \sum_{1\leq q\leq B_1}\sum_{\substack{1\leq a\leq q\\(a,q)=1}}\int_{\left|\alpha-\frac{a}{q}\right|\leq\frac{B}{qN}} w\left(\frac{qN}{B}\left(\alpha-\frac{a}{q}\right)\right)S(\alpha)\overline{R(\alpha)}d\alpha$$

and thus since $\operatorname{supp} w \subset [-2,2]$ and $0 \leq w \leq 1$, the left-hand side of (II.35) is

$$\leq \sum_{1\leq q\leq B_1}\sum_{\substack{1\leq a\leq q\\(a,q)=1}}\int_{\frac{B}{qN}<\left|\alpha-\frac{a}{q}\right|\leq\frac{2B}{qN}}\left|S(\alpha)\overline{R(\alpha)}\right|d\alpha = \sum_{1\leq q\leq B_1}\sum_{\substack{1\leq a\leq q\\(a,q)=1}}\int_{\mathfrak{M}_2(q,a)\setminus\mathfrak{M}(q,a)}\left|S(\alpha)\overline{R(\alpha)}\right|d\alpha$$

where, for $1 \leq q \leq B_1$ and $1 \leq a \leq q$ such that $(a,q) = 1$, $\mathfrak{M}_2(q,a)$ is the interval $\left|\alpha - \frac{a}{q}\right| \leq \frac{2B}{qN}$ modulo 1 i.e.

$$\mathfrak{M}_2(q,a) = \left(\left[\frac{a}{q} - \frac{2B}{qN}, \frac{a}{q} + \frac{2B}{qN}\right] + \mathbb{Z}\right) \cap [0,1[. \tag{II.36}$$

Since $4BB_1 < N$, by the same argument as in the proof of Lemma 4.1, we show that if $(q,a) \neq (q',a')$ then $\mathfrak{M}_2(q,a)$ and $\mathfrak{M}_2(q',a')$ are disjoint. It follows that, for any $1 \leq q \leq B_1$ and $1 \leq a \leq q$ such that $(a,q) = 1$,

$$\mathfrak{M}_2(q,a) \setminus \mathfrak{M}(q,a) \subset \mathfrak{m}$$

and thus

$$\sum_{1\le q\le B_1}\sum_{\substack{1\le a\le q\\(a,q)=1}}\int_{\mathfrak{M}_2(q,a)\setminus\mathfrak{M}(q,a)}\left|S(\alpha)\overline{R(\alpha)}\right|d\alpha\le\int_{\mathfrak{m}}\left|S(\alpha)\overline{R(\alpha)}\right|d\alpha$$

which completes the proof. □

9.2. Switching to multiplicative characters

We switch now to multiplicative characters. As we will see in Lemma 9.4, we are led to study

$$\mathfrak{I}=\sum_{1\le q\le B_1}\sum_{\substack{\chi \bmod q\\(q_1,q_2)=1,\ q_2\ \mathrm{sf}}}\frac{q_1}{\varphi(q_1)}\sum_{1\le k_1,k_2\le N}\frac{B}{qN}\widehat{w}\left((k_2-k_1)\frac{B}{qN}\right)\chi(k_1)\Lambda(k_1)\times f_{n,A,\boldsymbol{d}}(k_2)\overline{\chi_1}(k_2)\frac{\mu((q_2,k_2))}{\varphi\left(\frac{q_2}{(q_2,k_2)}\right)} \tag{II.37}$$

where, for any character $\chi \bmod q$, q_1 is the conductor of χ, χ_1 is the primitive character mod q_1 that induces χ and $q_2=q/q_1$ and the summation over $\chi \bmod q$ is restricted to $(q_1,q_2)=1$ and q_2 squarefree (sf).

Lemma 9.4.

$$\sum_{1\le q\le B_1}\sum_{\substack{1\le a\le q\\(a,q)=1}}\int_{\mathbb{R}}w\left(\frac{qN}{B}\left(\alpha-\frac{a}{q}\right)\right)S(\alpha)\overline{R(\alpha)}d\alpha=\mathfrak{I}+O\left(N(\log N)^2\left\|F_{n,A,\boldsymbol{d}}\right\|_1\right) \tag{II.38}$$

Remark 9.5. The term in $O(\cdot)$ is $\ll\frac{N^2}{\sqrt{B_1}}(\log N)^3\left\|F_{n,A,\boldsymbol{d}}\right\|_1$ which has already been studied in Section 8 to bound the contribution of the minor arcs.

Proof. To begin, we focus on the integral

$$\int_{\mathbb{R}}w\left(\frac{qN}{B}\left(\alpha-\frac{a}{q}\right)\right)S(\alpha)\overline{R(\alpha)}d\alpha \tag{II.39}$$

for fixed $1\le q\le B_1$ and $1\le a\le q$ such that $(a,q)=1$. For any $\alpha\in\mathbb{R}$, we remind that:

$$\overline{R(\alpha)}=\sum_{1\le k\le N}f_{n,A,\boldsymbol{d}}(k)\,\mathrm{e}(-k\alpha)=N\,F_{n,A,\boldsymbol{d}}(\alpha)$$

and

$$S(\alpha)=\frac{1}{\varphi(q)}\sum_{\chi \bmod q}\tau(\overline{\chi})\chi(a)\left(\sum_{1\le k\le N}\chi(k)\Lambda(k)\,\mathrm{e}(k\beta)\right)+O((\log N)^2)$$

where $\alpha = \frac{a}{q} + \beta$ (see [15, p. 147]) and $\tau(\overline{\chi})$ is a Gauss sum defined in Section 7.2. By using also that $\operatorname{supp} w \subset [-2,2]$ and $0 \le w \le 1$, we obtain that the integral (II.39) is equal to

$$\begin{aligned}
&\frac{1}{\varphi(q)} \sum_{\chi \bmod q} \tau(\overline{\chi})\chi(a) \int_{\mathbb{R}} w\left(\frac{qN}{B}\beta\right) \left(\sum_{1\le k_1\le N} \chi(k_1)\Lambda(k_1)\,\mathrm{e}(k_1\beta)\right) \times \\
&\qquad\qquad \left(\sum_{1\le k_2\le N} f_{n,A,\boldsymbol{d}}(k_2)\,\mathrm{e}\left(\frac{-k_2 a}{q}\right)\mathrm{e}(-k_2\beta)\right) d\beta \\
&\quad + O\left(N(\log N)^2 \int_{|\alpha-\frac{a}{q}|\le \frac{2B}{qN}} |F_{n,A,\boldsymbol{d}}(\alpha)|\, d\alpha\right) \\
&= \frac{1}{\varphi(q)} \sum_{\chi \bmod q} \tau(\overline{\chi})\chi(a) \sum_{1\le k_1,k_2\le N} \chi(k_1)\Lambda(k_1) f_{n,A,\boldsymbol{d}}(k_2)\,\mathrm{e}\left(\frac{-k_2 a}{q}\right) \frac{B}{qN}\widehat{w}\left((k_2-k_1)\frac{B}{qN}\right) \\
&\quad + O\left(N(\log N)^2 \int_{\mathfrak{M}_2(q,a)} |F_{n,A,\boldsymbol{d}}(\alpha)|\, d\alpha\right)
\end{aligned}$$

where $\mathfrak{M}_2(q,a)$ is defined by (II.36).

Then, we sum over $1 \le q \le B_1$ and $1 \le a \le q$ such that $(a,q) = 1$. By using that for any character $\chi \bmod q$ and for any integer $k \ge 1$, by Lemma 7.4,

$$\frac{\tau(\overline{\chi})}{\varphi(q)} \sum_{\substack{1\le a\le q\\(a,q)=1}} \chi(a)\,\mathrm{e}\left(\frac{-ka}{q}\right) = \frac{\overline{\tau(\overline{\chi})}}{\varphi(q)}\tau(k,\overline{\chi}) = \begin{cases} \frac{q_1}{\varphi(q_1)}\overline{\chi_1}(k)\frac{\mu((q_2,k))}{\varphi\left(\frac{q_2}{(q_2,k)}\right)} & \text{if } (q_1,q_2)=1 \text{ and } q_2 \text{ sf},\\ 0 & \text{otherwise,}\end{cases}$$

where q_1 is the conductor of χ, χ_1 is the primitive character mod q_1 that induces χ and $q_2 = q/q_1$ and by recalling that if $(q,a) \ne (q',a')$ then $\mathfrak{M}_2(q,a)$ and $\mathfrak{M}_2(q',a')$ are disjoint (see the proof of Lemma 9.2), we obtain (II.38) which completes the proof. □

9.3. Localization

In $\mathfrak{I}$, the variables k_1 and k_2 run independently over the set $\{1,\dots,N\}$. Nevertheless, the decreasing speed of $\widehat{w}$ (see Lemma 7.1 (v)) and the factor $\widehat{w}\left((k_2-k_1)\frac{B}{qN}\right)$ suggest that the k_1 and k_2 which are "too far apart" should have a negligible contribution. We will establish this precisely in the following lemma.

We introduce a parameter v_N which will be chosen later and will depend only on N such that

$$(\log N)^2 \le v_N \le (\log N)^{\upsilon} \quad \text{and} \quad 4B_1 v_N \le B \tag{II.40}$$

where $\upsilon \ge 2$ is an absolute constant and we define, for any integer k,

$$I_q(k) = \left]k - \frac{qN}{B}v_N, k + \frac{qN}{B}v_N\right[.$$

We denote by $\mathfrak{I}_1$ the quantity $\mathfrak{I}$ where the summation over k_1 is restricted to $I_q(k_2)\cap\{1,\dots,N\}$:

$$\mathfrak{I}_1 = \sum_{1\le q\le B_1} \sum_{\substack{\chi \bmod q\\ (q_1,q_2)=1,\, q_2 \text{ sf}}} \frac{q_1}{\varphi(q_1)} \sum_{1\le k_2\le N} f_{n,A,\boldsymbol{d}}(k_2)\overline{\chi_1}(k_2)\frac{\mu((q_2,k_2))}{\varphi\left(\frac{q_2}{(q_2,k_2)}\right)} \times \sum_{\substack{1\le k_1\le N\\ k_1\in I_q(k_2)}} \frac{B}{qN}\widehat{w}\left((k_2-k_1)\frac{B}{qN}\right)\chi(k_1)\Lambda(k_1).$$

Lemma 9.6.

$$\mathfrak{I} = \mathfrak{I}_1 + O\left(Ng^{-|A|}(\log N)v_N^{1/2}e^{-v_N^{1/2}}B_1^2\right) \tag{II.41}$$

Remark 9.7. We will choose, in Section 12, $v_N=(\log N)^2$ so that the error term in (II.41) is $\ll Ng^{-|A|}\frac{B_1^2}{N}(\log N)^2$ and thus admissible (since we will assume that $B_1\le N^{2/5}$, see Remark 8.3).

Remark 9.8. In order to obtain sharp enough estimates for the contribution of the major arcs, we will need $|I_q(k_2)|$ to be small enough compared to N so that k_1 runs only over a short interval around k_2. Since $|I_q(k_2)|=2\frac{qN}{B}v_N\le 2\frac{B_1N}{B}v_N$, we will need in particular to choose the parameters B_1 and B so that $B_1=o(B)$. In [5], the parameter B_1 is not introduced. With our notations, this would correspond to $B_1=B$ which would not permit us to restrict the summation over k_1 for the largest values of q.

Remark 9.9. The decreasing speed of $\widehat{w}$ (see Lemma 7.1 (v)) is essential. Indeed, if we had simply chosen w such that $\widehat{w}(y)=O\left(|y|^{-C}\right)$ $(y\to\infty)$ with $C>1$ an absolute constant then we would have obtained v_N^{1-C} in place of $v_N^{1/2}e^{-v_N^{1/2}}$ in (II.41). In order to ensure that the error term in (II.41) is admissible, v_N should then be at least a small power of N, which would make many arguments below fail (see for instance the proof of Lemma 11.2 where we use that $v_N\le(\log N)^v$ or the formula for $\mathfrak{I}_{NP}$ in Lemma 11.14 where we easily see that some error terms would no longer be admissible).

Proof. It follows from the definition of $\mathfrak{I}$ and $\mathfrak{I}_1$ that

$$|\mathfrak{I}-\mathfrak{I}_1| \le \sum_{1\le q\le B_1} \sum_{\substack{\chi \bmod q\\ (q_1,q_2)=1,\, q_2 \text{ sf}}} \frac{q_1}{\varphi(q_1)} \sum_{1\le k_2\le N} f_{n,A,\boldsymbol{d}}(k_2) \sum_{\substack{1\le k_1\le N\\ k_1\notin I_q(k_2)}} \frac{B}{qN}\left|\widehat{w}\left((k_2-k_1)\frac{B}{qN}\right)\right|\Lambda(k_1).$$

Moreover, for any $1\le q\le B_1$ and $1\le k_2\le N$, by Lemma 7.3,

$$\sum_{k_1\notin I_q(k_2)} \frac{B}{qN}\left|\widehat{w}\left((k_2-k_1)\frac{B}{qN}\right)\right| \le \sum_{|k|\ge\frac{qN}{B}v_N} \frac{B}{qN}\left|\widehat{w}\left(k\frac{B}{qN}\right)\right| \ll v_N^{1/2}e^{-v_N^{1/2}}$$

and since $\sum_{1\le k_2\le N} f_{n,A,\boldsymbol{d}}(k_2)=Ng^{-|A|}$ and

$$\sum_{1\le q\le B_1}\sum_{\chi \bmod q}\frac{q_1}{\varphi(q_1)} = \sum_{1\le q\le B_1}\sum_{q_1\mid q}\frac{q_1}{\varphi(q_1)}\sideset{}{^*}\sum_{\chi_1 \bmod q_1} 1 \le \sum_{1\le q\le B_1}\sum_{q_1\mid q} q_1 \le B_1^2,$$

we obtain

$$|\mathfrak{I} - \mathfrak{I}_1| \ll Ng^{-|A|}(\log N)v_N^{1/2}e^{-v_N^{1/2}}B_1^2$$

which completes the proof. □

9.4. Other technical preparations

For technical reasons, we replace in $\mathfrak{I}_1$ the factor $\chi(k_1)$ by $\chi_1(k_1)$ and we show that this introduces a small error: denoting

$$\mathfrak{I}_2 = \sum_{1\le q\le B_1} \sum_{\substack{\chi \bmod q\\ (q_1,q_2)=1,\, q_2 \text{ sf}}} \frac{q_1}{\varphi(q_1)} \sum_{1\le k_2\le N} f_{n,A,\boldsymbol{d}}(k_2)\overline{\chi_1}(k_2)\frac{\mu((q_2,k_2))}{\varphi\left(\frac{q_2}{(q_2,k_2)}\right)} \tag{II.42}$$
$$\times \sum_{\substack{1\le k_1\le N\\ k_1\in I_q(k_2)}} \frac{B}{qN}\widehat{w}\left((k_2-k_1)\frac{B}{qN}\right)\chi_1(k_1)\Lambda(k_1),$$

we have

Lemma 9.10.

$$\mathfrak{I}_1 = \mathfrak{I}_2 + O\left(Ng^{-|A|}\frac{BB_1}{N}(\log N)^2\right).$$

Proof. For any character $\chi \bmod q$ induced by $\chi_1 \bmod q_1$, we have $\chi(k_1) = 0$ if $(k_1, q) > 1$ and $\chi(k_1) = \chi_1(k_1)$ if $(k_1, q) = 1$. It follows that in the difference between $\mathfrak{I}_2$ and $\mathfrak{I}_1$, the inner sum over k_1 is

$$\sum_{\substack{1\le k_1\le N\\ k_1\in I_q(k_2)\\ (k_1,q)>1}} \frac{B}{qN}\widehat{w}\left((k_2-k_1)\frac{B}{qN}\right)\chi_1(k_1)\Lambda(k_1) = O\left(\frac{B}{qN}\sum_{\substack{1\le k_1\le N\\ (k_1,q)>1,\,(k_1,q_1)=1}}\Lambda(k_1)\right)$$
$$= O\left(\frac{B}{qN}\sum_{\substack{p^\nu\le N\\ p\,|\,q, p\nmid q_1}}\log p\right) = O\left(\frac{B}{qN}\sum_{\substack{p^\nu\le N\\ p\,|\,q_2}}\log p\right) = O\left(\frac{B}{qN}\sum_{\substack{p\le N\\ p\,|\,q_2}}\log N\right) = O\left(\frac{B\log N}{q_1N}\right)$$

(we used that $\widehat{w}$ is bounded and $q_2 = q/q_1$). Moreover,

$$\sum_{1\le q\le B_1}\sum_{\chi \bmod q}\frac{1}{\varphi(q_1)} = \sum_{1\le q\le B_1}\sum_{q_1\,|\,q}\frac{1}{\varphi(q_1)}\sideset{}{^*}\sum_{\chi_1 \bmod q_1} 1 \le \sum_{1\le q\le B_1}\sigma_0(q) \ll B_1\log B_1,$$

and thus

$$|\mathfrak{I}_1 - \mathfrak{I}_2| \ll \sum_{1\le q\le B_1} \sum_{\substack{\chi \bmod q \\ (q_1,q_2)=1,\, q_2 \text{ sf}}} \frac{q_1}{\varphi(q_1)} N g^{-|A|} \frac{B\log N}{q_1 N} \ll N g^{-|A|} \frac{B}{N} (\log N) B_1 \log B_1$$

which completes the proof. □

In order to estimate $\mathfrak{I}_2$, we write

$$\mathfrak{I}_2 = \mathfrak{I}_P + \mathfrak{I}_{NP} \tag{II.43}$$

where $\mathfrak{I}_P$ (resp. $\mathfrak{I}_{NP}$) is the contribution of the principal (resp. nonprincipal) characters in $\mathfrak{I}_2$.

If χ_0 is the principal character mod q then the conductor of χ_0 is $q_1 = 1$ and the primitive character mod q_1 which induces χ_0 is $\chi_1 = \mathbf{1}$. It follows that the contribution of the principal characters in $\mathfrak{I}_2$ is

$$\mathfrak{I}_P = \sum_{\substack{1\le q\le B_1 \\ q \text{ sf}}} \sum_{1\le k_2\le N} f_{n,A,\boldsymbol{d}}(k_2) \frac{\mu((q,k_2))}{\varphi\left(\frac{q}{(q,k_2)}\right)} \sum_{\substack{1\le k_1\le N \\ k_1\in I_q(k_2)}} \frac{B}{qN} \widehat{w}\left((k_2-k_1)\frac{B}{qN}\right) \Lambda(k_1). \tag{II.44}$$

In order to estimate $\mathfrak{I}_P$, we will need the variable k_2 to be not "too small" and not "too large". The following lemma will allow us to reduce the study of $\mathfrak{I}_P$ to the one of $\mathfrak{I}_{P_1}$ defined by

$$\mathfrak{I}_{P_1} = \sum_{\substack{1\le q\le B_1 \\ q \text{ sf}}} \sum_{K_2(q)\le k_2\le N-K_2(q)} f_{n,A,\boldsymbol{d}}(k_2) \frac{\mu((q,k_2))}{\varphi\left(\frac{q}{(q,k_2)}\right)} \sum_{\substack{1\le k_1\le N \\ k_1\in I_q(k_2)}} \frac{B}{qN} \widehat{w}\left((k_2-k_1)\frac{B}{qN}\right) \Lambda(k_1) \tag{II.45}$$

where

$$K_2(q) = 2\frac{qN}{B} v_N. \tag{II.46}$$

Lemma 9.11.

$$\mathfrak{I}_P = \mathfrak{I}_{P_1} + O\left(\frac{NB_1}{B} v_N (\log N)^2\right)$$

Remark 9.12. We will choose later $B < N$ so that the error term above is admissible i.e.

$$g^{|A|} B_1 v_N (\log N)^2 = o(B).$$

Proof. By denoting $J_1(q) = [1, K_2(q)[$ and $J_2(q) =]N - K_2(q), N]$, we have

$$|\mathfrak{I}_P - \mathfrak{I}_{P_1}| \le \sum_{\substack{1\le q\le B_1 \\ q \text{ sf}}} \sum_{k_2\in J_1(q)\cup J_2(q)} \frac{1}{\varphi\left(\frac{q}{(q,k_2)}\right)} \sum_{\substack{1\le k_1\le N \\ k_1\in I_q(k_2)}} \frac{B}{qN} \left|\widehat{w}\left((k_2-k_1)\frac{B}{qN}\right)\right| \Lambda(k_1).$$

By Lemma 7.3, the inner sum over k_1 is $\le (\log N) \sum_{k\in\mathbb{Z}} \frac{B}{qN} \left|\widehat{w}\left(k\frac{B}{qN}\right)\right| \ll \log N$. Moreover, by

Lemma 7.14, for any $q \geq 1$,

$$\sum_{k_2 \in J_1(q) \cup J_2(q)} \frac{1}{\varphi\left(\frac{q}{(q,k_2)}\right)} \leq 2\left(\frac{K_2(q)}{q}+1\right)\sigma_0(q) \ll \frac{N}{B} v_N\, \sigma_0(q).$$

Since $\sum_{q\leq B_1} \sigma_0(q) \ll B_1 \log B_1$, we obtain

$$|\mathfrak{I}_P - \mathfrak{I}_{P_1}| \ll \frac{NB_1}{B} v_N (\log N)^2$$

which completes the proof. □

It remains to study $\mathfrak{I}_{P_1}$ and $\mathfrak{I}_{NP}$. We will provide estimates of $\mathfrak{I}_{P_1}$ and $\mathfrak{I}_{NP}$ in Section 11.

10. Conclusion of Sections 8 and 9

We summarize the results of Sections 8 and 9 in the following lemma.

Lemma 10.1. *Let $0 < c \leq C_1(g)e^{-1}$ where $C_1(g)$ is defined by (II.10). If $B_1 \leq N^{2/5}$, $v_N = (\log N)^2$ and $|A| \leq cn$ then*

$$\begin{aligned}\sum_{0\leq k<g^n} \Lambda(k) f_{n,A,\boldsymbol{d}}(k) = \mathfrak{I}_{P_1} + \mathfrak{I}_{NP} + O\left(Ng^{-|A|}\frac{N^{C_2(g)c\log\left(\frac{C_1(g)}{c}\right)}}{\sqrt{B_1}}(\log N)^4\right) \\ + O\left(Ng^{-|A|}\frac{BB_1}{N}(\log N)^2\right) + O\left(Ng^{-|A|}\frac{N^c B_1}{B}(\log N)^4\right)\end{aligned} \tag{II.47}$$

where $\mathfrak{I}_{P_1}$ is defined by (II.45), $\mathfrak{I}_{NP}$ is the contribution of the nonprincipal characters in (II.42) and $C_2(g)$ is defined by (II.11).

Proof. We saw in Section 4 that

$$\sum_{0\leq k<g^n} \Lambda(k) f_{n,A,\boldsymbol{d}}(k) = \sum_{1\leq k\leq N} \Lambda(k) f_{n,A,\boldsymbol{d}}(k) = \int_{\mathfrak{M}} S(\alpha)\overline{R(\alpha)}d\alpha + \int_{\mathfrak{m}} S(\alpha)\overline{R(\alpha)}d\alpha$$

where $S(\alpha), R(\alpha), \mathfrak{M}$ and $\mathfrak{m}$ are defined as in Section 4. Since $0 < c \leq C_1(g)e^{-1}$, $B_1 \leq N^{2/5}$ and $|A| \leq cn$, Lemma 8.2 asserts that

$$\int_{\mathfrak{m}} \left|S(\alpha)\overline{R(\alpha)}\right| d\alpha \ll \frac{N^2}{\sqrt{B_1}}(\log N)^3 \left\|F_{n,A,\boldsymbol{d}}\right\|_1 \ll Ng^{-|A|}\frac{N^{C_2(g)c\log\left(\frac{C_1(g)}{c}\right)}}{\sqrt{B_1}}(\log N)^4$$

and by Lemmas 9.2 and 9.4,

$$\int_{\mathfrak{M}} S(\alpha)\overline{R(\alpha)}d\alpha = \mathfrak{I} + O\left(N(\log N)^2 \left\|F_{n,A,\boldsymbol{d}}\right\|_1\right) + O\left(\int_{\mathfrak{m}} \left|S(\alpha)\overline{R(\alpha)}\right| d\alpha\right)$$

where $\mathfrak{I}$ is defined by (II.37). Since $N(\log N)^2 \leq \frac{N^2}{\sqrt{B_1}}(\log N)^3$, it follows that

$$\sum_{0\leq k<g^n} \Lambda(k) f_{n,A,\boldsymbol{d}}(k) = \mathfrak{I} + O\left(N g^{-|A|} \frac{N^{C_2(g)c\log\left(\frac{C_1(g)}{c}\right)}}{\sqrt{B_1}} (\log N)^4 \right).$$

By Lemmas 9.6 and 9.10, since $v_N = (\log N)^2$ and $B_1 \leq B$, we obtain

$$\mathfrak{I} = \mathfrak{I}_2 + O\left(N g^{-|A|} \frac{BB_1}{N} (\log N)^2 \right)$$

where $\mathfrak{I}_2$ is defined by (II.42). Moreover, by (II.43),

$$\mathfrak{I}_2 = \mathfrak{I}_P + \mathfrak{I}_{NP}$$

and by Lemma 9.11, since $g^{|A|} \leq N^c$,

$$\mathfrak{I}_P = \mathfrak{I}_{P_1} + O\left(\frac{NB_1}{B} (\log N)^4 \right) = \mathfrak{I}_{P_1} + O\left(N g^{-|A|} \frac{N^c B_1}{B} (\log N)^4 \right)$$

where $\mathfrak{I}_{P_1}$ is defined by (II.45), which completes the proof. □

11. Major arcs contribution II

11.1. Estimate of $\mathfrak{I}_{P_1}$

We first focus on the inner sum over k_1 in $\mathfrak{I}_{P_1}$ defined by (II.45). We remind that $K_2(q) = 2\frac{qN}{B} v_N$ (see (II.46)).

Lemma 11.1. *There exists an absolute constant N_0 such that if $N \geq N_0$ and $B \leq N^{0.2}$ then for any $1 \leq q \leq B_1$ and $K_2(q) \leq k_2 \leq N - K_2(q)$,*

$$\sum_{\substack{1\leq k_1\leq N \\ k_1 \in I_q(k_2)}} \frac{B}{qN} \widehat{w}\left((k_2 - k_1)\frac{B}{qN} \right) \Lambda(k_1) = 1 + O\left(v_N^2 e^{-c_1 (\log N)^{0.1}} \right)$$

where $c_1 > 0$ is an absolute constant.

Proof. We denote by $\Sigma(q, k_2)$ the left-hand side sum and we put $a = k_2 - \frac{qN}{B} v_N$ and $b = k_2 + \frac{qN}{B} v_N$. Since $I_q(k_2) =]a, b] \subset \left]\frac{qN}{B} v_N, N - \frac{qN}{B} v_N\right] \subset]0, N]$,

$$\Sigma(q, k_2) = \sum_{a < k_1 \leq b} \frac{B}{qN} \widehat{w}\left((k_2 - k_1)\frac{B}{qN} \right) \Lambda(k_1).$$

Since $b - a = 2\frac{qN}{B} v_N \geq \frac{N}{B} \geq N^{0.8} \geq a^{0.8}$, by Lemma 7.8, there exists an absolute constant

$a_0 \geq e$ such that if $a \geq a_0$ then

$$\Sigma(q,k_2) = \sum_{a<k_1\leq b} \frac{B}{qN}\widehat{w}\left((k_2-k_1)\frac{B}{qN}\right) + O\left(M(b-a)e^{-(\log a)^{0.1}}\right)$$

where $M \leq \frac{B}{qN}\|\widehat{w}\|_\infty + \int_a^b \left(\frac{B}{qN}\right)^2 \|\widehat{w}'\|_\infty dt \ll \frac{B}{qN}v_N$. By using that $a \geq \frac{qN}{B}v_N \geq \frac{N}{B} \geq N^{0.8}$, there exists N_0 such that if $N \geq N_0$ then

$$\Sigma(q,k_2) = \sum_{a<k_1\leq b} \frac{B}{qN}\widehat{w}\left((k_2-k_1)\frac{B}{qN}\right) + O\left(v_N^2 e^{-c_1(\log N)^{0.1}}\right) \tag{II.48}$$

where $c_1 > 0$ is an absolute constant.

Moreover, since $\mathbb{Z}\backslash\,]a,b] \subset \{k_1 : |k_2-k_1| \geq \frac{qN}{B}v_N\}$,

$$\left|\sum_{k_1\in\mathbb{Z}} \frac{B}{qN}\widehat{w}\left((k_2-k_1)\frac{B}{qN}\right) - \sum_{a<k_1\leq b} \frac{B}{qN}\widehat{w}\left((k_2-k_1)\frac{B}{qN}\right)\right| \leq \sum_{|k|\geq \frac{qN}{B}v_N} \frac{B}{qN}\left|\widehat{w}\left(k\frac{B}{qN}\right)\right|$$

and by using Lemma 7.3 and the lower bound $v_N \geq (\log N)^2$, we obtain

$$\left|1 - \sum_{a<k_1\leq b} \frac{B}{qN}\widehat{w}\left((k_2-k_1)\frac{B}{qN}\right)\right| \ll v_N^{1/2}e^{-v_N^{1/2}} \ll v_N^2 e^{-c_1(\log N)^{0.1}}.$$

To complete the proof, it suffices to insert this into (II.48). □

We are now able to study $\mathfrak{I}_{P_1}$.

Lemma 11.2. *Let $\kappa > 0$ and $0 < c < \frac{1}{2(1+\kappa)}$. There exists an absolute constant N_0 such that if $N \geq N_0$, $B_1 \leq N^{\frac{\kappa}{4(1+\kappa)}}$, $B \leq N^{0.2}$ and $|A| \leq cn$ then*

$$\mathfrak{I}_{P_1} = Ng^{-|A|}\frac{g}{\varphi(g)}\left(1 + O_{g,v,\kappa,c}\left(n^2\log n\left(\frac{n}{\log^3 n}\right)^{1-\frac{1}{2(1+\kappa)c}}\right)\right) + O\left(\frac{NB_1}{B}v_N\log N\right).$$

Proof. By Lemma 11.1, there exists an absolute constant N_0 such that if $N \geq N_0$ and $B \leq N^{0.2}$ then, for any $1 \leq q \leq B_1$ and $K_2(q) \leq k_2 \leq N - K_2(q)$,

$$\sum_{\substack{1\leq k_1\leq N\\ k_1\in I_q(k_2)}} \frac{B}{qN}\widehat{w}\left((k_2-k_1)\frac{B}{qN}\right)\Lambda(k_1) = 1 + O\left(v_N^2 e^{-c_1(\log N)^{0.1}}\right)$$

and thus, by denoting

$$\Sigma_1 = \sum_{\substack{1\leq q\leq B_1\\ q \text{ sf}}} \sum_{K_2(q)\leq k_2\leq N-K_2(q)} f_{n,A,\boldsymbol{d}}(k_2)\frac{\mu((q,k_2))}{\varphi\left(\frac{q}{(q,k_2)}\right)}$$

and

$$\Sigma_2 = \sum_{\substack{1\le q\le B_1\\ q \text{ sf}}} \sum_{K_2(q)\le k_2\le N-K_2(q)} \frac{f_{n,A,\boldsymbol{d}}(k_2)}{\varphi\left(\frac{q}{(q,k_2)}\right)},$$

and by using (II.45), we obtain

$$\mathfrak{I}_{P_1} = \Sigma_1 + O\left(v_N^2 e^{-c_1(\log N)^{0.1}}\Sigma_2\right). \tag{II.49}$$

We first study Σ_1. By denoting $J_1(q) = [1, K_2(q)[$ and $J_2(q) =]N - K_2(q), N]$, we obtain as in the proof of Lemma 9.11,

$$\sum_{\substack{1\le q\le B_1\\ q \text{ sf}}} \sum_{k_2\in J_1(q)\cup J_2(q)} \frac{1}{\varphi\left(\frac{q}{(q,k_2)}\right)} \ll \frac{NB_1}{B} v_N \log N$$

and by Lemma 5.27, since $|A| \le cn$ and $B_1 \le N^{\frac{\kappa}{4(1+\kappa)}}$,

$$\sum_{\substack{1\le q\le B_1\\ q \text{ sf}}} \sum_{1\le k\le N} f_{n,A,\boldsymbol{d}}(k) \frac{\mu((q,k))}{\varphi\left(\frac{q}{(q,k)}\right)} = Ng^{-|A|}\frac{g}{\varphi(g)}\left(1 + O_{g,\kappa,c}\left(n^2\log n\left(\frac{n}{\log^3 n}\right)^{1-\frac{1}{2(1+\kappa)c}}\right)\right).$$

It follows that

$$\Sigma_1 = Ng^{-|A|}\frac{g}{\varphi(g)}\left(1 + O_{g,\kappa,c}\left(n^2\log n\left(\frac{n}{\log^3 n}\right)^{1-\frac{1}{2(1+\kappa)c}}\right)\right) + O\left(\frac{NB_1}{B} v_N \log N\right).$$

It remains to bound Σ_2. By Lemma 5.30, we obtain

$$\Sigma_2 \le \sum_{\substack{1\le q\le B_1\\ q \text{ sf}}} \sum_{0\le k<g^n} \frac{f_{n,A,\boldsymbol{d}}(k)}{\varphi\left(\frac{q}{(k,q)}\right)} \ll_{g,\kappa,c} Ng^{-|A|}\, n^2$$

and thus, since $v_N \le (\log N)^v$ and $N = g^n$,

$$\begin{aligned} v_N^2 e^{-c_1(\log N)^{0.1}}\Sigma_2 \ll_{g,v} n^{2v} e^{-c_2 n^{0.1}}\Sigma_2 &\ll_{g,\kappa,c} Ng^{-|A|}\, n^{2+2v} e^{-c_2 n^{0.1}} \\ &\ll_{v,\kappa,c} Ng^{-|A|}\, n^2 \log n \left(\frac{n}{\log^3 n}\right)^{1-\frac{1}{2(1+\kappa)c}} \end{aligned}$$

where $c_2 > 0$ is an absolute constant. By inserting this into (II.49), we obtain

$$\mathfrak{I}_{P_1} = Ng^{-|A|}\frac{g}{\varphi(g)}\left(1 + O_{g,v,\kappa,c}\left(n^2\log n\left(\frac{n}{\log^3 n}\right)^{1-\frac{1}{2(1+\kappa)c}}\right)\right) + O\left(\frac{NB_1}{B} v_N \log N\right)$$

which completes the proof. □

11.2. Upper bound of $\mathfrak{I}_{NP}$

In this section, we study $\mathfrak{I}_{NP}$ which is the contribution of the nonprincipal characters in $\mathfrak{I}_2$ defined by (II.42). In [5], the fact that (4.8) can be estimated by (4.23) is not clear. While retaining some ideas of [5], we will thus proceed in a different way.

A character χ mod q is nonprincipal if and only if its conductor q_1 is strictly greater than 1 and thus, by splitting up the characters according to their conductor, we obtain that the contribution of the nonprincipal characters in $\mathfrak{I}_2$ is

$$\begin{aligned}\mathfrak{I}_{NP} = \sum_{1\le q\le B_1} \sum_{\substack{q_1\,|\,q\\ q_1>1\\ (q_1,q/q_1)=1,\, q/q_1 \text{ sf}}} \sideset{}{^*}\sum_{\chi_1 \bmod q_1} \frac{q_1}{\varphi(q_1)} \sum_{1\le k_2\le N} f_{n,A,\boldsymbol{d}}(k_2)\overline{\chi_1}(k_2)\frac{\mu((q/q_1,k_2))}{\varphi\left(\frac{q/q_1}{(q/q_1,k_2)}\right)} \\ \times \sum_{\substack{1\le k_1\le N\\ k_1\in I_q(k_2)}} \frac{B}{qN}\widehat{w}\left((k_2-k_1)\frac{B}{qN}\right)\chi_1(k_1)\Lambda(k_1) \qquad \text{(II.50)}\\ = \sum_{1<q_1\le B_1} \sideset{}{^*}\sum_{\chi_1 \bmod q_1} \frac{q_1}{\varphi(q_1)} \sum_{\substack{1\le q_2\le B_1/q_1\\ (q_1,q_2)=1,\, q_2 \text{ sf}}} \sum_{1\le k_2\le N} f_{n,A,\boldsymbol{d}}(k_2)\overline{\chi_1}(k_2)\frac{\mu((q_2,k_2))}{\varphi\left(\frac{q_2}{(q_2,k_2)}\right)} \\ \times \sum_{\substack{1\le k_1\le N\\ k_1\in I_{q_1q_2}(k_2)}} \frac{B}{q_1q_2N}\widehat{w}\left((k_2-k_1)\frac{B}{q_1q_2N}\right)\chi_1(k_1)\Lambda(k_1).\end{aligned}$$

We introduce two real parameters

$$T\ge 2 \quad \text{and} \quad 0<\eta_*\le 1/2$$

and we denote, for any character χ,

$$\eta(\chi,T) = \min_{\substack{L(\rho,\chi)=0\\ |\gamma|\le T}} (1-\beta)$$

where the minimum is taken over all zeros $\rho=\beta+i\gamma$ of $L(s,\chi)$ such that $0\le\beta\le 1$ and $|\gamma|\le T$. In $\mathfrak{I}_{NP}$, we subdivide the primitive characters χ_1 in two classes "good" and "bad":

$$\mathcal{G}(T,\eta_*) = \{\chi_1 \bmod q_1 \text{ primitive } : 1<q_1\le B_1 \text{ and } \eta(\chi_1,T)\ge\eta_*\},$$

$$\mathcal{B}(T,\eta_*) = \{\chi_1 \bmod q_1 \text{ primitive } : 1<q_1\le B_1 \text{ and } \eta(\chi_1,T)<\eta_*\}.$$

11.2.1. "Good" characters

In $\mathfrak{I}_{NP}$, the contribution of the characters χ_1 in $\mathcal{G}(T,\eta_*)$ is

$$\mathfrak{I}_{\mathcal{G}} = \sum_{\substack{\chi_1 \bmod q_1 \\ \in \mathcal{G}(T,\eta_*)}} \frac{q_1}{\varphi(q_1)} \sum_{\substack{1\le q_2\le B_1/q_1 \\ (q_1,q_2)=1,\, q_2 \text{ sf}}} \sum_{1\le k_2\le N} f_{n,A,\boldsymbol{d}}(k_2)\overline{\chi_1}(k_2)\frac{\mu((q_2,k_2))}{\varphi\left(\frac{q_2}{(q_2,k_2)}\right)} \tag{II.51}$$
$$\times \sum_{\substack{1\le k_1\le N \\ k_1\in I_{q_1q_2}(k_2)}} \frac{B}{q_1q_2N}\widehat{w}\left((k_2-k_1)\frac{B}{q_1q_2N}\right)\chi_1(k_1)\Lambda(k_1).$$

In order to estimate $\mathfrak{I}_{\mathcal{G}}$, we will need the variable k_2 to be not "too small". The following lemma will allow us to reduce the study of $\mathfrak{I}_{\mathcal{G}}$ to the one of $\mathfrak{I}_{\mathcal{G}_1}$ defined by

$$\mathfrak{I}_{\mathcal{G}_1} = \sum_{\substack{\chi_1 \bmod q_1 \\ \in \mathcal{G}(T,\eta_*)}} \frac{q_1}{\varphi(q_1)} \sum_{\substack{1\le q_2\le B_1/q_1 \\ (q_1,q_2)=1,\, q_2 \text{ sf}}} \sum_{K_2(q_1q_2)\le k_2\le N-K_2(q_1q_2)} f_{n,A,\boldsymbol{d}}(k_2)\overline{\chi_1}(k_2)\frac{\mu((q_2,k_2))}{\varphi\left(\frac{q_2}{(q_2,k_2)}\right)} \tag{II.52}$$
$$\times \sum_{\substack{1\le k_1\le N \\ k_1\in I_{q_1q_2}(k_2)}} \frac{B}{q_1q_2N}\widehat{w}\left((k_2-k_1)\frac{B}{q_1q_2N}\right)\chi_1(k_1)\Lambda(k_1)$$

where $K_2(q) = 2\frac{qN}{B}v_N$ is as in Section 11.1.

Lemma 11.3.

$$\mathfrak{I}_{\mathcal{G}} = \mathfrak{I}_{\mathcal{G}_1} + O\left(\frac{NB_1^3}{B}v_N(\log N)^2\right)$$

Remark 11.4. In Section 13.3, we will choose $B < N$ so that the error term above is admissible i.e.

$$g^{|A|}B_1^3v_N(\log N)^2 = o(B).$$

Proof. By denoting $J_1(q) = [1, K_2(q)[$ and $J_2(q) =]N-K_2(q), N]$, we have

$$|\mathfrak{I}_{\mathcal{G}} - \mathfrak{I}_{\mathcal{G}_1}| \le \sum_{1<q_1\le B_1} \sideset{}{^*}\sum_{\chi_1 \bmod q_1} \frac{q_1}{\varphi(q_1)} \sum_{\substack{1\le q_2\le B_1/q_1 \\ (q_1,q_2)=1,\, q_2 \text{ sf}}} \sum_{k_2\in J_1(q_1q_2)\cup J_2(q_1q_2)} \frac{1}{\varphi\left(\frac{q_2}{(q_2,k_2)}\right)}$$
$$\times \sum_{\substack{1\le k_1\le N \\ k_1\in I_{q_1q_2}(k_2)}} \frac{B}{q_1q_2N}\left|\widehat{w}\left((k_2-k_1)\frac{B}{q_1q_2N}\right)\right|\Lambda(k_1).$$

By Lemma 7.3, the inner sum over k_1 is $\le (\log N)\sum_{k\in\mathbb{Z}}\frac{B}{q_1q_2N}\left|\widehat{w}\left(k\frac{B}{q_1q_2N}\right)\right| \ll \log N$. Moreover, by Lemma 7.14, for any $q_1, q_2 \ge 1$ such that $q_1q_2 \le B_1$,

$$\sum_{k_2\in J_1(q_1q_2)\cup J_2(q_1q_2)} \frac{1}{\varphi\left(\frac{q_2}{(q_2,k_2)}\right)} \le 2\left(\frac{K_2(q_1q_2)}{q_2}+1\right)\sigma_0(q_2) \ll \frac{q_1N}{B}v_N\,\sigma_0(q_2).$$

Since for any $q_1 \le B_1$, $\sum_{q_2 \le B_1/q_1} \sigma_0(q_2) \ll \frac{B_1}{q_1}\left(1+\log\frac{B_1}{q_1}\right) \ll \frac{B_1}{q_1}\log N$, it follows that

$$|\mathfrak{I}_{\mathcal{G}} - \mathfrak{I}_{\mathcal{G}_1}| \ll \sum_{1<q_1\le B_1} \sideset{}{^*}\sum_{\chi_1 \bmod q_1} \frac{q_1}{\varphi(q_1)} \frac{q_1 N}{B} v_N \frac{B_1}{q_1} (\log N)^2 \le \frac{NB_1}{B} v_N (\log N)^2 \sum_{1<q_1\le B_1} q_1$$
$$\ll \frac{NB_1^3}{B} v_N (\log N)^2.$$

□

In order to give a sharp upper bound of $|\mathfrak{I}_{\mathcal{G}_1}|$, we define

$$U(T,\eta_*) = \sum_{\substack{\chi_1 \bmod q_1 \\ \in \mathcal{G}(T,\eta_*)}} \frac{q_1}{\varphi(q_1)} \max_{\substack{1\le q_2 \le B_1/q_1 \\ K_2(q_1q_2)\le k_2 \le N - K_2(q_1q_2)}} \left| \sum_{\substack{1\le k_1\le N \\ k_1 \in I_{q_1q_2}(k_2)}} \frac{B}{q_1q_2N} \widehat{w}\left((k_2-k_1)\frac{B}{q_1q_2N}\right) \chi_1(k_1)\Lambda(k_1) \right|$$

and we notice that

$$|\mathfrak{I}_{\mathcal{G}_1}| \le \left(\sum_{\substack{1\le q_2\le B_1 \\ q_2 \text{ sf}}} \sum_{1\le k_2\le N} \frac{f_{n,A,\boldsymbol{d}}(k_2)}{\varphi\left(\frac{q_2}{(q_2,k_2)}\right)} \right) U(T,\eta_*). \tag{II.53}$$

Remark 11.5. Under the hypothesis of Lemma 5.30 with $Q = B_1$, the double sum over q_2 and k_2 in (II.53) is $\ll_{g,\kappa,c} N g^{-|A|} (\log N)^2$.

We first focus on the inner sum over k_1 in $U(T,\eta_*)$.

Lemma 11.6. *If $T \le \frac{N}{B} v_N$ then for any primitive character $\chi_1 \bmod q_1$ such that $1 < q_1 \le B_1$ and any $1 \le q_2 \le B_1/q_1$, $K_2(q_1q_2) \le k_2 \le N - K_2(q_1q_2)$, we have*

$$\left| \sum_{\substack{1\le k_1\le N \\ k_1 \in I_{q_1q_2}(k_2)}} \frac{B}{q_1q_2N} \widehat{w}\left((k_2-k_1)\frac{B}{q_1q_2N}\right) \chi_1(k_1)\Lambda(k_1) \right| \tag{II.54}$$
$$\ll v_N^2 \sum_{\substack{L(\rho,\chi_1)=0 \\ |\gamma|\le T}} \left(\frac{N}{B} v_N\right)^{\beta-1} + \frac{B}{q_1q_2T} (\log N)^2 v_N$$

where the sum in the right-hand side runs over all nontrivial zeros $\rho = \beta + i\gamma$ of $L(s,\chi_1)$ such that $|\gamma| \le T$.

Proof. We put $q = q_1q_2$, $a = k_2 - \frac{qN}{B} v_N$ and $b = k_2 + \frac{qN}{B} v_N$ and we denote by $\Sigma(\chi_1, q_2, k_2)$ the sum in the left-hand side of (II.54). Since $I_q(k_2) =]a,b] \subset \left]\frac{qN}{B} v_N, N - \frac{qN}{B} v_N\right] \subset]0,N]$,

$$\Sigma(\chi_1,q_2,k_2) = \sum_{a<k_1\le b} \frac{B}{qN} \widehat{w}\left((k_2-k_1)\frac{B}{qN}\right) \chi_1(k_1)\Lambda(k_1)$$

and thus, by Lemma 7.9,

$$|\Sigma(\chi_1, q_2, k_2)| \ll \frac{B}{qN} v_N \sup_{a<t\leq b} |\psi(t,\chi_1) - \psi(a,\chi_1)|\,. \tag{II.55}$$

Moreover, since $a \geq \frac{qN}{B} v_N \geq T$, it follows from Corollary 7.11 that

$$\sup_{a<t\leq b} |\psi(t,\chi_1) - \psi(a,\chi_1)| \ll (b-a) \sum_{\substack{L(\rho,\chi_1)=0 \\ |\gamma|\leq T}} a^{\beta-1} + \frac{b}{T}(\log bq_1)^2$$

where the sum runs over all nontrivial zeros $\rho = \beta + i\gamma$ of $L(s,\chi_1)$ such that $|\gamma| \leq T$ and since $b - a = 2\frac{qN}{B} v_N$, $a \geq \frac{N}{B} v_N$ and $b \leq N$, we get

$$\sup_{a<t\leq b} |\psi(t,\chi_1) - \psi(a,\chi_1)| \ll \frac{qN}{B} v_N \sum_{\substack{L(\rho,\chi_1)=0 \\ |\gamma|\leq T}} \left(\frac{N}{B} v_N\right)^{\beta-1} + \frac{N}{T}(\log N)^2.$$

By inserting this into (II.55), we obtain (II.54). □

We are now able to give a sharp upper bound of $U(T,\eta_*)$.

Lemma 11.7. *Let $\varepsilon > 0$. If $(B_1^5 T^3)^{1+\varepsilon} \leq \frac{N}{B} v_N$ then*

$$U(T,\eta_*) \ll_\varepsilon \left(\frac{N v_N}{B(B_1^5 T^3)^{1+\varepsilon}}\right)^{-\eta_*} v_N^2 \log\log N + \frac{BB_1}{T}(\log N)^2 v_N.$$

Proof. Since $T \leq \frac{N}{B} v_N$, it follows from Lemma 11.6 that

$$U(T,\eta_*) \ll \sum_{\substack{\chi_1 \bmod q_1 \\ \in \mathcal{G}(T,\eta_*)}} \frac{q_1}{\varphi(q_1)} \left(v_N^2 \sum_{\substack{L(\rho,\chi_1)=0 \\ |\gamma|\leq T}} \left(\frac{N}{B} v_N\right)^{\beta-1} + \frac{B}{q_1 T}(\log N)^2 v_N \right).$$

To bound the contribution of the sum over ρ, we use that $q_1/\varphi(q_1) \ll \log\log N$ (see for instance [28, Theorem 328]) and we apply Lemma 7.13 with $Q = B_1$ and $\mathcal{C} = \mathcal{G}(T,\eta_*)$ which satisfies by definition of $\mathcal{G}(T,\eta_*)$:

$$\sigma > 1 - \eta_* \Rightarrow N_{\mathcal{C}}(\sigma, T) = 0$$

and $a = \frac{N}{B} v_N$ which satisfies $(Q^5 T^3)^{1+\varepsilon} \leq a$. We obtain

$$\sum_{\substack{\chi_1 \bmod q_1 \\ \in \mathcal{G}(T,\eta_*)}} \sum_{\substack{L(\rho,\chi_1)=0 \\ |\gamma|\leq T}} \left(\frac{N}{B} v_N\right)^{\beta-1} \ll_\varepsilon \left(\frac{N v_N}{B(B_1^5 T^3)^{1+\varepsilon}}\right)^{-\eta_*}.$$

To bound the contribution of the second term between parentheses, we simply write

$$\sum_{\substack{\chi_1 \bmod q_1\\ \in\mathcal{G}(T,\eta_*)}} \frac{q_1}{\varphi(q_1)}\frac{B}{q_1T}(\log N)^2 v_N \le \frac{B}{T}(\log N)^2 v_N \sum_{q_1\le B_1} 1 \le \frac{BB_1}{T}(\log N)^2 v_N.$$

This completes the proof. □

11.2.2. "Bad" characters

In $\mathfrak{I}_{NP}$ (see II.50), the contribution of the characters χ_1 in $\mathcal{B}(T,\eta_*)$ is

$$\mathfrak{I}_{\mathcal{B}} = \sum_{\substack{\chi_1 \bmod q_1\\ \in\mathcal{B}(T,\eta_*)}} \frac{q_1}{\varphi(q_1)} V(q_1,\chi_1) \tag{II.56}$$

where

$$V(q_1,\chi_1) = \sum_{\substack{1\le q_2\le B_1/q_1\\ (q_1,q_2)=1,\, q_2 \text{ sf}}} \sum_{1\le k_2\le N} f_{n,A,\boldsymbol{d}}(k_2)\overline{\chi_1}(k_2)\frac{\mu((q_2,k_2))}{\varphi\left(\frac{q_2}{(q_2,k_2)}\right)} \times \sum_{\substack{1\le k_1\le N\\ k_1\in I_{q_1q_2}(k_2)}} \frac{B}{q_1q_2N}\widehat{w}\left((k_2-k_1)\frac{B}{q_1q_2N}\right)\chi_1(k_1)\Lambda(k_1). \tag{II.57}$$

Since $q_1/\varphi(q_1) \ll \log\log N$ for any $1\le q_1\le N$, we obtain

$$|\mathfrak{I}_{\mathcal{B}}| \ll (\log\log N)\,|\mathcal{B}(T,\eta_*)| \max_{\substack{\chi_1 \bmod q_1\\ \in\mathcal{B}(T,\eta_*)}} |V(q_1,\chi_1)|\,. \tag{II.58}$$

In order to obtain a sharp upper bound of $|\mathfrak{I}_{\mathcal{B}}|$, we will first bound the number of "bad" characters (see Lemma 11.8), then we will establish an upper bound for $|V(q_1,\chi_1)|$ when q_1 has a prime factor which does not divide g (see Lemma 11.11) and finally, we will show that if the parameters T and η_* are judiciously chosen then the conductor of a "bad" character has always a prime factor which does not divide g (see Lemma 11.13) so that the previous upper bound of $|V(q_1,\chi_1)|$ is valid for any $(\chi_1 \bmod q_1)\in\mathcal{B}(T,\eta_*)$. In this last step, we will need an improved zero-free region for L-functions to modulus q where q is such that any prime factor of q divides the base g.

Lemma 11.8. *Let $\varepsilon>0$. We have*

$$|\mathcal{B}(T,\eta_*)| \ll_\varepsilon (B_1^5T^3)^{(1+\varepsilon)\eta_*}. \tag{II.59}$$

Proof. By definition, the elements of $\mathcal{B}(T,\eta_*)$ are the primitive characters $\chi_1 \bmod q_1$ with $1<q_1\le B_1$ such that $L(s,\chi_1)$ has a zero $\rho=\beta+i\gamma$ with $|\gamma|\le T$ and $1-\eta_*<\beta\le 1$ and

thus $N(1-\eta_*,T,\chi_1)\geq 1$. It follows that

$$|\mathcal{B}(T,\eta_*)|\leq \sum_{1<q_1\leq B_1}\sideset{}{^*}\sum_{\substack{\chi_1 \bmod q_1\\ N(1-\eta_*,T,\chi_1)\geq 1}} 1\leq \sum_{1\leq q_1\leq B_1}\sideset{}{^*}\sum_{\chi_1 \bmod q_1} N(1-\eta_*,T,\chi_1)=N_{B_1}(1-\eta_*,T).$$

Moreover, by applying Lemma 7.12, we obtain

$$N_{B_1}(1-\eta_*,T)\ll_\varepsilon (B_1^5T^3)^{(1+\varepsilon)\eta_*}$$

which completes the proof. □

Remark 11.9. In Section 11.2.3, the parameter η_* will become arbitrarily small as $N\to\infty$. Therefore, we do not actually need here a zero-density estimate which is valid for $1/2\leq\sigma\leq 1$ (as in Lemma 7.12). We could use more precise zero-density estimates valid for σ close to 1 (see for instance [55]) and obtain a slightly better upper bound in (II.59) but this would not improve significantly the final result.

We now study $\max\limits_{\substack{\chi_1 \bmod q_1\\ \in\mathcal{B}(T,\eta_*)}} |V(q_1,\chi_1)|$.

Lemma 11.10. *For any integer m such that $B_1\leq g^m\leq g^n$ and for any character χ_1 mod q_1 with $1\leq q_1\leq B_1$, we have*

$$|V(q_1,\chi_1)|$$
$$\ll v_N^2(\log N)^2(\log\log N)\sum_{\substack{1\leq q_0\leq B_1/q_1\\ (q_1g,q_0)=1,\, q_0\ sf}}\sum_{0\leq\ell<g^{n-m}}\left|\sum_{\substack{\ell g^m\leq k_2<(\ell+1)g^m\\ q_0\mid k_2}} f_{n,A,\boldsymbol{d}}(k_2)\overline{\chi_1}(k_2)\right|+\frac{Bg^m}{q_1}v_N.$$

Proof. For any $1\leq k_1\leq N$ and any $q\geq 1$, we define

$$K_2(k_1,q)=\max\left(1,k_1-\frac{qN}{B}v_N\right)\quad\text{and}\quad K_2'(k_1,q)=\min\left(N,k_1+\frac{qN}{B}v_N\right)$$

so that we have $1\leq k_2<N$ and $k_1\in I_q(k_2)$ if and only if $K_2(k_1,q)\leq k_2<K_2'(k_1,q)$ and thus, by interchanging the summations over k_1 and k_2 in (II.57), we obtain

$$V(q_1,\chi_1)=\sum_{\substack{1\leq q_2\leq B_1/q_1\\ (q_1,q_2)=1,\, q_2\ \mathrm{sf}}}\sum_{1\leq k_1\leq N}\chi_1(k_1)\Lambda(k_1)W(q_2,k_1,q_1,\chi_1)$$

where

$$W(q_2,k_1,q_1,\chi_1)=$$
$$\sum_{K_2(k_1,q_1q_2)\leq k_2<K_2'(k_1,q_1q_2)}\frac{B}{q_1q_2N}\widehat{w}\left((k_2-k_1)\frac{B}{q_1q_2N}\right)f_{n,A,\boldsymbol{d}}(k_2)\overline{\chi_1}(k_2)\frac{\mu((q_2,k_2))}{\varphi\left(\frac{q_2}{(q_2,k_2)}\right)}$$

(note that the contribution of $k_2 = N$ in (II.57) is 0), hence

$$|V(q_1,\chi_1)| \leq \sum_{\substack{1\leq q_2\leq B_1/q_1\\(q_1,q_2)=1,\, q_2 \text{ sf}}} \sum_{1\leq k_1\leq N} \Lambda(k_1)\,|W(q_2,k_1,q_1,\chi_1)|\,. \tag{II.60}$$

We first fix the variables q_2 and k_1 and we focus on $|W(q_2,k_1,q_1,\chi_1)|$. By partial summation (as in the proof of Lemma 7.9) and by observing that $K_2'(k_1,q_1q_2) - K_2(k_1,q_1q_2) \leq 2\frac{q_1q_2N}{B}v_N$, we obtain

$$\begin{aligned}&|W(q_2,k_1,q_1,\chi_1)| \\ &\ll \frac{B}{q_1q_2N}v_N \sup_{K_2(k_1,q_1q_2)<t\leq K_2'(k_1,q_1q_2)} \left|\sum_{K_2(k_1,q_1q_2)\leq k_2<t} f_{n,A,\boldsymbol{d}}(k_2)\overline{\chi_1}(k_2)\frac{\mu((q_2,k_2))}{\varphi\left(\frac{q_2}{(q_2,k_2)}\right)}\right|.\end{aligned} \tag{II.61}$$

We now fix t such that $K_2(k_1,q_1q_2) < t \leq K_2'(k_1,q_1q_2)$ and we study the term in the supremum. Since $[K_2(k_1,q_1q_2),t[\subset [0,N[$ and $[0,N[= \bigcup_{0\leq \ell<g^{n-m}} [\ell g^m,(\ell+1)g^m[$, we can write

$$[K_2(k_1,q_1q_2),t[= I_1 \cup \left(\bigcup_{\substack{0\leq\ell<g^{n-m}\\ [\ell g^m,(\ell+1)g^m[\subset[K_2(k_1,q_1q_2),t[}} [\ell g^m,(\ell+1)g^m[\right) \cup I_2$$

where I_1 and I_2 are intervals such that $0 \leq |I_1|,|I_2| \leq g^m$ and all the intervals in this decomposition are disjoint. It follows that the term in the supremum is

$$\leq \sum_{\substack{0\leq\ell<g^{n-m}\\ [\ell g^m,(\ell+1)g^m[\subset[K_2(k_1,q_1q_2),t[}} \left|\sum_{\ell g^m\leq k_2<(\ell+1)g^m} f_{n,A,\boldsymbol{d}}(k_2)\overline{\chi_1}(k_2)\frac{\mu((q_2,k_2))}{\varphi\left(\frac{q_2}{(q_2,k_2)}\right)}\right| + \sum_{k_2\in I_1\cup I_2} \frac{1}{\varphi\left(\frac{q_2}{(q_2,k_2)}\right)}$$

where, by Lemma 7.14 and the inequality $q_2 \leq B_1 \leq g^m$,

$$\sum_{k_2\in I_1\cup I_2} \frac{1}{\varphi\left(\frac{q_2}{(q_2,k_2)}\right)} \leq 2\left(\frac{g^m}{q_2}+1\right)\sigma_0(q_2) \ll g^m\,\frac{\sigma_0(q_2)}{q_2}.$$

By inserting this into (II.61) and by observing that $t \leq K_2'(k_1,q_1q_2)$, we obtain

$$\begin{aligned}&|W(q_2,k_1,q_1,\chi_1)| \\ &\ll \frac{B}{q_1q_2N}v_N \sum_{\substack{0\leq\ell<g^{n-m}\\ [\ell g^m,(\ell+1)g^m[\\ \subset[K_2(k_1,q_1q_2),K_2'(k_1,q_1q_2)[}} \left|\sum_{\ell g^m\leq k_2<(\ell+1)g^m} f_{n,A,\boldsymbol{d}}(k_2)\overline{\chi_1}(k_2)\frac{\mu((q_2,k_2))}{\varphi\left(\frac{q_2}{(q_2,k_2)}\right)}\right| \\ &\quad + \frac{B}{q_1q_2N}v_N g^m\,\frac{\sigma_0(q_2)}{q_2}.\end{aligned} \tag{II.62}$$

We then multiply (II.62) by $\Lambda(k_1)$ and we sum over $1 \le k_1 \le N$. For the contribution of the term with $\sigma_0(q_2)$, we use that $\sum_{k_1 \le N} \Lambda(k_1) = \psi(N) \ll N$ and for the contribution of the term with the summation over ℓ, we use that $\Lambda(k_1) \le \log N$, we interchange the summations over k_1 and over ℓ and we note that, given ℓ, the number of k_1 such that $[\ell g^m, (\ell+1)g^m[\subset [K_2(k_1, q_1q_2), K_2'(k_1, q_1q_2)[$ is less than the number of k_1 such that $\ell g^m - \frac{q_1q_2N}{B} v_N \le k_1 \le \ell g^m + \frac{q_1q_2N}{B} v_N$ which is $\ll \frac{q_1q_2N}{B} v_N$. We obtain

$$\sum_{1 \le k_1 \le N} \Lambda(k_1) \, |W(q_2, k_1, q_1, \chi_1)| \tag{II.63}$$

$$\ll v_N^2 (\log N) \sum_{0 \le \ell < g^{n-m}} \left| \sum_{\ell g^m \le k_2 < (\ell+1) g^m} f_{n,A,\boldsymbol{d}}(k_2) \overline{\chi_1}(k_2) \frac{\mu((q_2, k_2))}{\varphi\left(\frac{q_2}{(q_2,k_2)}\right)} \right|$$

$$+ \frac{B}{q_1 q_2} v_N g^m \frac{\sigma_0(q_2)}{q_2}.$$

We finally sum (II.63) over q_2 such that $1 \le q_2 \le B_1/q_1$, $(q_1, q_2) = 1$, q_2 sf. Since

$$\sum_{k \ge 1} \frac{\sigma_0(k)}{k^2} = \sum_{k \ge 1} \frac{1}{k^2} \sum_{d \,|\, k} 1 = \sum_{d \ge 1} \frac{1}{d^2} \sum_{k' \ge 1} \frac{1}{k'^2} = \zeta(2)^2,$$

the contribution of the term with $\sigma_0(q_2)$ is $\ll \frac{Bg^m}{q_1} v_N$. By using, as in the proof of Lemma 5.25 that for any squarefree integer $\ell \ge 1$,

$$\mu(\ell)\varphi(\ell) = \sum_{d \,|\, \ell} d\mu(d),$$

we obtain that the contribution of the term with the summation over ℓ is

$$= v_N^2 (\log N) \sum_{\substack{1 \le q_2 \le B_1/q_1 \\ (q_1,q_2)=1,\, q_2 \text{ sf}}} \frac{1}{\varphi(q_2)} \sum_{0 \le \ell < g^{n-m}} \left| \sum_{\ell g^m \le k_2 < (\ell+1) g^m} f_{n,A,\boldsymbol{d}}(k_2) \overline{\chi_1}(k_2) \sum_{q_0 \,|\, (q_2,k_2)} q_0 \mu(q_0) \right|$$

$$\le v_N^2 (\log N) \sum_{\substack{1 \le q_2 \le B_1/q_1 \\ (q_1,q_2)=1,\, q_2 \text{ sf}}} \frac{1}{\varphi(q_2)} \sum_{q_0 \,|\, q_2} q_0 \sum_{0 \le \ell < g^{n-m}} \left| \sum_{\substack{\ell g^m \le k_2 < (\ell+1) g^m \\ q_0 \,|\, k_2}} f_{n,A,\boldsymbol{d}}(k_2) \overline{\chi_1}(k_2) \right|$$

$$\ll v_N^2 (\log N)^2 (\log\log N) \sum_{\substack{1 \le q_0 \le B_1/q_1 \\ (q_1,q_0)=1,\, q_0 \text{ sf}}} \sum_{0 \le \ell < g^{n-m}} \left| \sum_{\substack{\ell g^m \le k_2 < (\ell+1) g^m \\ q_0 \,|\, k_2}} f_{n,A,\boldsymbol{d}}(k_2) \overline{\chi_1}(k_2) \right|$$

where we used for the last inequality that $q_0/\varphi(q_0) \ll \log\log N$ for any $1 \le q_0 \le N$ and

$\sum_{1\le k\le B_1} 1/\varphi(k) \ll \log B_1 \le \log N$. It follows that

$$\sum_{\substack{1\le q_2\le B_1/q_1\\(q_1,q_2)=1,\, q_2 \text{ sf}}} \sum_{1\le k_1\le N} \Lambda(k_1)\,|W(q_2,k_1,q_1,\chi_1)|$$

$$\ll v_N^2(\log N)^2(\log\log N) \sum_{\substack{1\le q_0\le B_1/q_1\\(q_1,q_0)=1,\, q_0 \text{ sf}}} \sum_{0\le \ell<g^{n-m}} \left| \sum_{\substack{\ell g^m\le k_2<(\ell+1)g^m\\ q_0\,|\,k_2}} f_{n,A,\boldsymbol{d}}(k_2)\overline{\chi_1}(k_2)\right| + \frac{Bg^m}{q_1}v_N.$$

To complete the proof, it suffices to insert this into (II.60) and to note that only the q_0's which are coprime to g can have a non zero contribution (since $0\in A$ and $(d_0,g)=1$, we have $f_{n,A,\boldsymbol{d}}(k)=0$ for any k such that $(k,g)>1$). □

Lemma 11.11. *Let $g=\prod_{i=1}^t p_i^{\gamma_i}$ be the prime decomposition of g where $p_1^{\gamma_1}=\min_{1\le i\le t} p_i^{\gamma_i}$. We assume that $n\ge 200$. Let χ_1 be a primitive character mod q_1 such that $1\le q_1\le B_1$ and q_1 has a prime factor which does not divide g. Let $\kappa>0$ and $0<c<\frac{1}{8(1+\kappa)}$. If $|A|\le cn$, $B_1\le N^{\frac{\kappa}{8(1+\kappa)}}$ and*

$$B_1 \le N^{\frac{\log p_1^{\gamma_1}}{4\log g}} \tag{II.64}$$

then

$$|V(q_1,\chi_1)| \ll_{g,\kappa,c} Ng^{-|A|}v_N^2 n^3(\log n)\left(\frac{n}{\log^3 n}\right)^{1-\frac{1}{8(1+\kappa)c}} + BN^{3/4}v_N.$$

Remark 11.12. The condition (II.64) which appears in Lemma 11.11 will be responsible for the fact that, for some bases g (for instance of the form $g=2\cdot 3^k$), we obtain a proportion c_0 which tends to 0 as g tends to ∞. Condition (II.64) permits us to ensure that there is an appropriate ν such that $s\,|\,g^\nu$ (see (II.66) and (II.67) below).

Proof. We write $q_1=sq_1'$ where $(q_1',g)=1$ and any prime factor of s is a prime factor of g. If $0<c_1<\frac{1}{4(1+\kappa)}$ and if $\nu\ge 0$ and $m\ge 0$ are integers such that $s\,|\,g^\nu$, $\nu+100\le m\le n$, $B_1\le g^{\frac{\kappa(m-\nu)}{4(1+\kappa)}}$ and $|A\cap\{\nu,\dots,m-1\}|\le c_1(m-\nu)$ then, since $B_1\le g^m$, by applying Lemma 11.10, we obtain

$$|V(q_1,\chi_1)|$$

$$\ll v_N^2(\log N)^2(\log\log N) \sum_{\substack{1\le q_0\le B_1/q_1\\(q_1g,q_0)=1,\, q_0 \text{ sf}}} \sum_{0\le \ell<g^{n-m}} \left| \sum_{\substack{\ell g^m\le k_2<(\ell+1)g^m\\ q_0\,|\,k_2}} f_{n,A,\boldsymbol{d}}(k_2)\overline{\chi_1}(k_2)\right| + \frac{Bg^m}{q_1}v_N$$

and then, since $B_1/q_1 \le B_1/q_1' \le g^{\frac{\kappa(m-\nu)}{4(1+\kappa)}}/q_1'$, it follows from Lemma 5.34 that

$$|V(q_1,\chi_1)| \tag{II.65}$$
$$\ll_{g,\kappa,c_1} v_N^2(\log N)^2(\log\log N)g^{n-|A|}(m-\nu)\left(\frac{m-\nu}{\log^3(m-\nu)}\right)^{1-\frac{1}{4(1+\kappa)c_1}} + \frac{Bg^m}{q_1}v_N.$$

We now show that the choice $c_1 = 2c$, $\nu = \lceil n/4\rceil$ and $m = \nu + \lceil n/2\rceil$ is suitable. Clearly, $0 < c_1 < \frac{1}{4(1+\kappa)}$ and since $m - \nu \ge n/2$, we have $\nu + 100 \le m \le n$, $B_1 \le g^{\frac{\kappa(m-\nu)}{4(1+\kappa)}}$ and

$$\frac{|A\cap\{\nu,\dots,m-1\}|}{m-\nu} \le \frac{|A|}{n/2} \le 2c = c_1.$$

It remains to establish that $s \mid g^\nu$. Since any prime factor of s is a prime factor of g, there exist $\sigma_1,\dots,\sigma_t \ge 0$ such that $s = \prod_{i=1}^t p_i^{\sigma_i}$ and thus

$$s \mid g^\nu \Leftrightarrow \nu \ge \max_{1\le i\le t}\frac{\sigma_i}{\gamma_i}. \tag{II.66}$$

Moreover, since $s \le q_1 \le B_1$, we have for any $1 \le i \le t$, $p_i^{\sigma_i} \le B_1$ and thus, since $B_1 \le N^{\frac{\log p_1^{\gamma_1}}{4\log g}}$,

$$\frac{\sigma_i}{\gamma_i} \le \frac{\log B_1}{\log p_i^{\gamma_i}} \le \frac{\log B_1}{\log p_1^{\gamma_1}} \le \frac{n}{4} \le \nu \tag{II.67}$$

and it follows that $s \mid g^\nu$. By (II.65), this choice of c_1, ν and m leads to

$$|V(q_1,\chi_1)| \ll_{g,\kappa,c} v_N^2(\log N)^2(\log\log N)g^{n-|A|}n\left(\frac{n}{\log^3 n}\right)^{1-\frac{1}{8(1+\kappa)c}} + \frac{Bg^{3n/4}}{q_1}v_N$$

which completes the proof. □

Lemma 11.13. *There exist an absolute constant $\xi_1 > 0$ and $T_1 = T_1(g) \ge 3$ such that if*

$$T \ge T_1 \quad \text{and} \quad \eta_* \le \xi_1\left(\log(B_1T)\log\log(B_1T)\right)^{-3/4} \tag{II.68}$$

then, for any $(\chi_1 \bmod q_1) \in \mathcal{B}(T,\eta_*)$, q_1 has a prime factor which does not divide g.

Proof. We denote by $\mathcal{P}$ the set of prime factors of g. It follows from Lemma 6.4 that there exist an absolute constant $\xi_1 > 0$ and $T_1 = T_1(g) \ge 3$ such that if T and η_* satisfy (II.68) then, for any primitive character $\chi_1 \bmod q_1$ such that $1 < q_1 \le B_1$ and such that the prime factors of q_1 are in $\mathcal{P}$, we have for any zero $\rho = \beta + i\gamma$ of $L(s,\chi_1)$ such that $|\gamma| \le T$:

$$\beta < 1 - \xi_1\left(\log(q_1T)\log\log(q_1T)\right)^{-3/4} \le 1 - \xi_1\left(\log(B_1T)\log\log(B_1T)\right)^{-3/4} \le 1 - \eta_*$$

and thus $(\chi_1 \bmod q_1) \notin \mathcal{B}(T,\eta_*)$, which completes the proof. □

11.2.3. Conclusion for $\mathfrak{I}_{NP}$

We summarize the results of Sections 11.2.1 and 11.2.2 in the following lemma.

Lemma 11.14. *Let $g = \prod_{i=1}^{t} p_i^{\gamma_i}$ be the prime decomposition of g where $p_1^{\gamma_1} = \min_{1\le i\le t} p_i^{\gamma_i}$. Let b_1 such that $B_1 = N^{b_1}$ and b such that $B = N^b$. Let $0 < t < 1$, $\alpha > 0$, $\varepsilon > 0$ and $c > 0$. There exists $n_1 = n_1(t, \alpha, g) \ge 1$ such that if $n \ge n_1$, $|A| \le cn$,*

$$c + b_1 < 1/8, \qquad b_1 \le \frac{\log p_1^{\gamma_1}}{4\log g}, \qquad b + (1+\varepsilon)(5b_1 + 3t) \le 1 \tag{II.69}$$

then

$$\begin{aligned}\mathfrak{I}_{NP} &= O_{g,c,\varepsilon,b_1}\left(Ng^{-|A|}\left(v_N^2\, n^{4-\frac{1}{8c}+\frac{b_1}{c}+\alpha(1+\varepsilon)(5b_1+3t)}(\log n)^{\frac{3}{8c}} + \frac{v_N\, n^{\alpha(1+\varepsilon)(5b_1+3t)}\log n}{N^{1/4-b-c}}\right)\right)\\ &+ O_{g,c,\varepsilon}\left(Ng^{-|A|}\left(v_N^2\, n^{2-\alpha(1-b-(1+\varepsilon)(5b_1+3t))}\log n + \frac{v_N(\log N)^4}{N^{t-b-b_1}}\right)\right)\\ &+ O\left(Ng^{-|A|}\,\frac{v_N(\log N)^2}{N^{b-3b_1-c}}\right).\end{aligned}$$

Proof. Let $T = N^t$ and $\eta_* = \frac{\alpha}{\log g}\frac{\log n}{n} = \alpha\frac{\log n}{\log N}$. There exists $n_1 = n_1(g, t, \alpha) \ge 200$ such that if $n \ge n_1$ then

$$T \ge T_1 \ge 3 \quad \text{and} \quad 0 < \eta_* \le \xi_1\left(\log(N^2)\log\log(N^2)\right)^{-3/4} \le 1/2$$

where T_1 and ξ_1 are as in Lemma 11.13 (T_1 depends only on g and $\xi_1 > 0$ is an absolute constant). We henceforth assume that $n \ge n_1$. In order to estimate $\mathfrak{I}_{NP}$, we first note that

$$\mathfrak{I}_{NP} = \mathfrak{I}_{\mathcal{G}} + \mathfrak{I}_{\mathcal{B}}$$

where $\mathfrak{I}_{\mathcal{G}}$ and $\mathfrak{I}_{\mathcal{B}}$ are defined by (II.51) and (II.56) respectively.

By (II.58) and Lemma 11.8, we obtain

$$\begin{aligned}|\mathfrak{I}_{\mathcal{B}}| &\ll_{\varepsilon} (\log\log N)\,(B_1^5T^3)^{(1+\varepsilon)\eta_*}\max_{\substack{\chi_1 \bmod q_1\\ \in\mathcal{B}(T,\eta_*)}}|V(q_1,\chi_1)|\\ &\ll_{g,\varepsilon} (\log n)\, n^{\alpha(1+\varepsilon)(5b_1+3t)}\max_{\substack{\chi_1 \bmod q_1\\ \in\mathcal{B}(T,\eta_*)}}|V(q_1,\chi_1)|\end{aligned}$$

where $V(q_1, \chi_1)$ is defined by (II.57). Let $(\chi_1 \bmod q_1) \in \mathcal{B}(T, \eta_*)$. Since $B_1T \le N^2$, T and η_* satisfy (II.68) and it follows from Lemma 11.13 that q_1 has a prime factor which does not divide g. Since $B_1 \le N^{\frac{\log p_1^{\gamma_1}}{4\log g}}$, we are allowed to apply Lemma 11.11 with $\kappa = \frac{8b_1}{1-8b_1} > 0$ which

satisfies $c < \frac{1}{8} - b_1 = \frac{1}{8(1+\kappa)}$ and $B_1 = N^{\frac{\kappa}{8(1+\kappa)}}$ and we obtain

$$|V(q_1,\chi_1)| \ll_{g,b_1,c} Ng^{-|A|}v_N^2\, n^3(\log n)\left(\frac{n}{\log^3 n}\right)^{1-\frac{1}{8c}+\frac{b_1}{c}} + BN^{3/4}v_N.$$

It follows that

$$\begin{aligned}|\mathfrak{I}_{\mathcal{B}}| &\ll_{g,c,\varepsilon,b_1} (\log n)\, n^{\alpha(1+\varepsilon)(5b_1+3t)}\left(Ng^{-|A|}v_N^2\, n^3(\log n)\left(\frac{n}{\log^3 n}\right)^{1-\frac{1}{8c}+\frac{b_1}{c}} + BN^{3/4}v_N\right)\\ &\le Ng^{-|A|}\left(v_N^2\, n^{4-\frac{1}{8c}+\frac{b_1}{c}+\alpha(1+\varepsilon)(5b_1+3t)}(\log n)^{\frac{3}{8c}} + \frac{v_N\, n^{\alpha(1+\varepsilon)(5b_1+3t)}\log n}{N^{1/4-b-c}}\right)\end{aligned}$$

(for the right-hand side term, we used the inequality $g^{|A|} \le N^c$).

It remains to estimate $\mathfrak{I}_{\mathcal{G}}$. By Lemma 11.3,

$$\mathfrak{I}_{\mathcal{G}} = \mathfrak{I}_{\mathcal{G}_1} + O\left(\frac{NB_1^3}{B}v_N(\log N)^2\right) = \mathfrak{I}_{\mathcal{G}_1} + O\left(Ng^{-|A|}\,\frac{v_N(\log N)^2}{N^{b-3b_1-c}}\right)$$

where $\mathfrak{I}_{\mathcal{G}_1}$ is defined by (II.52). Since $c + b_1 < 1/8$, we have $c < 1/4$ and $B_1 \le N^{1/8}$. It follows from (II.53) and Lemma 5.30 with $Q = B_1$ and $\kappa = 1$ that

$$|\mathfrak{I}_{\mathcal{G}_1}| \ll_{g,c} Ng^{-|A|}n^2\, U(T,\eta_*).$$

Moreover, since $b + (1+\varepsilon)(5b_1+3t) \le 1$, we have $(B_1^5T^3)^{1+\varepsilon} \le \frac{N}{B} \le \frac{N}{B}v_N$ and thus, by Lemma 11.7,

$$\begin{aligned}U(T,\eta_*) &\ll_\varepsilon \left(\frac{N}{B(B_1^5T^3)^{1+\varepsilon}}\right)^{-\eta_*} v_N^2\log\log N + \frac{BB_1}{T}(\log N)^2 v_N\\ &= n^{-\alpha(1-b-(1+\varepsilon)(5b_1+3t))}v_N^2\log\log N + \frac{(\log N)^2 v_N}{N^{t-b-b_1}},\end{aligned}$$

hence

$$|\mathfrak{I}_{\mathcal{G}_1}| \ll_{g,c,\varepsilon} Ng^{-|A|}\left(v_N^2\, n^{2-\alpha(1-b-(1+\varepsilon)(5b_1+3t))}\log n + \frac{v_N(\log N)^4}{N^{t-b-b_1}}\right)$$

This completes the proof. □

12. Conclusion of minor and major arcs

In this section, we will combine the previous results regarding the contribution of the minor and major arcs to obtain:

Proposition 12.1. *Let $g \geq 2$ be an integer and $g = \prod_{i=1}^{t} p_i^{\gamma_i}$ be the prime decomposition of g where $p_1^{\gamma_1} = \min_{1\leq i\leq t} p_i^{\gamma_i}$. Let b_1, b, t, α, ε and c be positive real numbers such that*

$$b_1 < b \leq 1/5, \qquad c + b_1 < 1/8, \qquad b_1 \leq \frac{\log p_1^{\gamma_1}}{4\log g}, \qquad b + (1+\varepsilon)(5b_1 + 3t) \leq 1. \tag{II.70}$$

There exists $n_0 = n_0(g, b_1, b, t, \alpha) \geq 200$ such that for any $n \geq n_0$, $A \subset \{0, \dots, n-1\}$ satisfying $0 \in A$ and $|A| \leq cn$ and for any $\boldsymbol{d} = (d_j)_{j\in A} \in \{0, \dots, g-1\}^A$ such that $(d_0, g) = 1$, we have

$$\begin{aligned}
&\sum_{0\leq k<g^n} \Lambda(k) f_{n,A,\boldsymbol{d}}(k) = \\
&Ng^{-|A|}\frac{g}{\varphi(g)}\Bigg[1 + O_{g,c,\varepsilon}\left(n^{6-\alpha(1-b-(1+\varepsilon)(5b_1+3t))}\log n + \frac{(\log N)^6}{N^{t-b-b_1}}\right) \\
&\qquad + O_{g,c,\varepsilon,b_1}\left(n^{8-\frac{1}{8c}+\frac{b_1}{c}+\alpha(1+\varepsilon)(5b_1+3t)}(\log n)^{\frac{3}{8c}} + \frac{n^{2+\alpha(1+\varepsilon)(5b_1+3t)}\log n}{N^{1/4-b-c}}\right) \\
&\qquad + O_{g,c,b_1}\left(n^{3-\frac{1}{2c}+\frac{2b_1}{c}}(\log n)^{\frac{3}{2c}}\right) + O\left(\frac{(\log N)^4}{N^{b-3b_1-c}}\right) \\
&\qquad + O\left(\frac{(\log N)^4}{N^{\frac{b_1}{2}-C_2(g)c\log\left(\frac{C_1(g)}{c}\right)}}\right)\Bigg]
\end{aligned}$$

where $N = g^n$ and $C_1(g)$ and $C_2(g)$ are defined respectively by (II.10) and (II.11).

Proof. Let $n \geq 1$, $N = g^n$, $B_1 = N^{b_1}$, $B = N^b$ and $v_N = (\log N)^2$. There exists $n_2 = n_2(b_1, b) \geq 200$ such that if $n \geq n_2$ then

$$g \leq B_1, \quad 4B_1(\log N)^2 \leq B < \frac{N}{4B_1}$$

so that B_1 and B satisfy the condition (II.4) and v_N satisfies (II.40). We henceforth assume that $n \geq \max(n_2, \frac{\log N_0}{\log g}, n_1)$ where N_0 is the same absolute constant as in Lemma 11.2 and $n_1 = n_1(t, \alpha, g)$ is as in Lemma 11.14. Let $A \subset \{0, \dots, n-1\}$ such that $0 \in A$ and $|A| \leq cn$ and let $\boldsymbol{d} = (d_j)_{j\in A} \in \{0, \dots, g-1\}^A$ such that $(d_0, g) = 1$.

Since $0 < c < 1/8 \leq 2e^{-1} \leq C_1(g)e^{-1}$, $B_1 \leq N^{1/8} \leq N^{2/5}$ and $|A| \leq cn$, it follows from Lemma 10.1 that

$$\begin{aligned}
\sum_{0\leq k<g^n} \Lambda(k) f_{n,A,\boldsymbol{d}}(k) &= \mathfrak{I}_{P_1} + \mathfrak{I}_{NP} \\
&\quad + O\left(Ng^{-|A|}\frac{(\log N)^4}{N^{\frac{b_1}{2}-C_2(g)c\log\left(\frac{C_1(g)}{c}\right)}}\right) + O\left(Ng^{-|A|}\frac{(\log N)^4}{N^{b-b_1-c}}\right)
\end{aligned} \tag{II.71}$$

where $\mathfrak{I}_{P_1}$ is defined by (II.45) and $\mathfrak{I}_{NP}$ is the contribution of the nonprincipal characters in (II.42) (note that, since $b \leq 1/2$, the second $O(\cdot)$ in (II.47) enters in the third one).

Since $c+2b_1 < 1/8+1/8 < 1/2$, $N \geq N_0$ and $b \leq 0.2$, we are allowed to apply Lemma 11.2 with $\kappa = \frac{4b_1}{1-4b_1} > 0$ which satisfies $c < \frac{1}{2(1+\kappa)}$ and $B_1 = N^{\frac{\kappa}{4(1+\kappa)}}$ and we obtain

$$\mathfrak{I}_{P_1} = Ng^{-|A|}\frac{g}{\varphi(g)}\left(1+O_{g,c,b_1}\left(n^{3-\frac{1}{2c}+\frac{2b_1}{c}}(\log n)^{\frac{3}{2c}}\right)\right)+O\left(Ng^{-|A|}\frac{(\log N)^3}{N^{b-b_1-c}}\right)$$

(for the rightmost term, we used that $g^{|A|} \leq N^c$).

Since $n \geq n_1$ and (II.69) is satisfied, it follows from Lemma 11.14 that

$$\begin{aligned}\mathfrak{I}_{NP} = {} & O_{g,c,\varepsilon,b_1}\left(Ng^{-|A|}\left(n^{8-\frac{1}{8c}+\frac{b_1}{c}+\alpha(1+\varepsilon)(5b_1+3t)}(\log n)^{\frac{3}{8c}}+\frac{n^{2+\alpha(1+\varepsilon)(5b_1+3t)}\log n}{N^{1/4-b-c}}\right)\right)\\ & + O_{g,c,\varepsilon}\left(Ng^{-|A|}\left(n^{6-\alpha(1-b-(1+\varepsilon)(5b_1+3t))}\log n+\frac{(\log N)^6}{N^{t-b-b_1}}\right)\right)\\ & + O\left(Ng^{-|A|}\frac{(\log N)^4}{N^{b-3b_1-c}}\right).\end{aligned}$$

To complete the proof, it suffices to insert these estimates of $\mathfrak{I}_{P_1}$ and $\mathfrak{I}_{NP}$ into (II.71). □

13. Completion of the proof of Theorem 2.1 and Theorem 2.7

In this section, we will complete the proof of Theorem 2.1 by providing an explicit admissible value of $c_0(g,\delta_0)$ for general integer $g \geq 2$ and real number $\delta_0 \geq 0$ (see Theorem 13.3). We will then be able to prove Theorem 2.7.

In order to define an admissible value of $c_0(g,\delta_0)$, we will need the following two lemmas (they will be proved in Sections 13.1 and 13.2).

Lemma 13.1. *For $g \geq 2$, $\delta_0 \geq 0$ and $x > 0$, we denote*

$$y_g(x) = \frac{2}{\log g}\,x\log\left(\frac{C_1(g)}{x}\right) \tag{II.72}$$

where $C_1(g)$ is defined by (II.10) and

$$h_{g,\delta_0}(x) = x(8+\delta_0)+y_g(x)+\frac{(6+\delta_0)\,x(17y_g(x)+3x)}{1-20y_g(x)-4x}. \tag{II.73}$$

For any $g \geq 2$ and $\delta_0 \geq 0$,

(i) the equation $20y_g(x)+4x = 1$ has a unique solution $x = x_1(g)$ on $]0,1/2[$,

(ii) the equation $h_{g,\delta_0}(x) = \frac{1}{8}$ has a unique solution $x = c_1(g,\delta_0)$ on $]0,x_1(g)[$,

(iii) if $x \in]0,1/2[$ satisfies $20y_g(x)+4x < 1$ and $h_{g,\delta_0}(x) \leq \frac{1}{8}$ then $x \leq c_1(g,\delta_0)$.

Moreover,

(iv) for any $g \geq 2$, $c_1(g, \delta_0)$ is a decreasing function of δ_0,

(v) for any $\delta_0 \geq 0$, $c_1(g, \delta_0)$ is an increasing function of g,

(vi) for $\delta_0 = 0$, $c_1(g, \delta_0)$ tends to $\ell_0 \approx 0.00927$ as $g \to \infty$.

Lemma 13.2. *Let $g \geq 2$ be an integer and $g = \prod_{i=1}^{t} p_i^{\gamma_i}$ be the prime decomposition of g where $p_1^{\gamma_1} = \min_{1 \leq i \leq t} p_i^{\gamma_i}$. Let y_g be the function defined by (II.72) and $\beta_g = \frac{\log p_1^{\gamma_1}}{4 \log g}$.*

(i) The equation $y_g(x) = \beta_g$ has a unique solution $x = c_2(g)$ on $]0, 1/2[$.

(ii) If $0 < x < 1/2$ satisfies $y_g(x) \leq \beta_g$ then $x \leq c_2(g)$.

(iii) $c_2(g) < \frac{\beta_g}{2}$.

(iv) If $g \geq 6$ then $c_2(g) \geq \left(\frac{\beta_g}{2}\left(\frac{2}{\pi}\log g\right)^{-\frac{1}{\log g}}\right)^{\frac{1}{1-\frac{1}{\log g}}} \sim \frac{\beta_g}{2}$ as $g \to \infty$.

(v) If $(g_i)_i$ is a strictly increasing sequence of integers larger than or equal to 2 such that $(\beta_{g_i})_i$ is constant then the sequence $(c_2(g_i))_i$ is increasing.

(vi) If g is a prime power then, for any $\delta_0 \geq 0$, $c_1(g, \delta_0) \leq c_2(g)$.

We will then establish in Section 13.3:

Theorem 13.3. *For any $g \geq 2$ and $\delta_0 \geq 0$, Theorem 2.1 holds with $c_0 = \min(c_1, c_2)$ where $c_1 = c_1(g, \delta_0)$ is defined in Lemma 13.1 (ii) and $c_2 = c_2(g)$ is defined in Lemma 13.2 (i).*

Theorem 2.1 is an immediate corollary of Theorem 13.3. The c_0 in Theorem 13.3 satisfies the properties stated in Remark 2.8:

1. It follows from Lemma 13.1 (iv) that, for any given $g \geq 2$, the largest value of c_0 is obtained for $\delta_0 = 0$.
2. If g is a prime power then, for any $\delta_0 \geq 0$, it follows from Lemma 13.2 (vi) that $c_0 = c_1$ which is an increasing function of g (see Lemma 13.1 (v)). Moreover, in the special case where $\delta_0 = 0$, c_1 tends to 0.00927... as $g \to \infty$ (see Lemma 13.1 (vi)).
3. If $a \geq 2$ is an integer then $(\beta_{a^i})_i$ is constant and thus, by Lemma 13.1 (v) and Lemma 13.2 (v), for any $\delta_0 \geq 0$, the function $i \mapsto c_0(a^i, \delta_0)$ is increasing.
4. For any $\delta_0 \geq 0$, we have $c_0 \leq c_2 < \beta_g/2$ by Lemma 13.2 (iii).

We will finally obtain Theorem 2.7 as a consequence of Theorem 13.3 in Section 13.4.

13.1. Proof of Lemma 13.1

(i) An elementary calculation shows that the functions y_g and $\widetilde{y}_g : x \mapsto 20 y_g(x) + 4x$ are strictly increasing on $]0, 1/2] \subset]0, C_1(g) e^{-1}]$. Moreover, $\widetilde{y}_g(x)$ tends to 0 as x tends to 0 and $\widetilde{y}_g(1/2) \geq 4 \cdot 1/2 > 1$. As a consequence, there is a unique $x_1 = x_1(g) \in]0, 1/2[$ such that $\widetilde{y}_g(x_1) = 1$.

(ii) If $0 < x < x_1 = x_1(g)$ then $\widetilde{y}_g(x) < \widetilde{y}_g(x_1) = 1$ so that $h_{g,\delta_0}(x)$ is well defined. Since y_g and $\widetilde{y}_g$ are strictly increasing on $]0, x_1[$, h_{g,δ_0} is also strictly increasing on $]0, x_1[$. Moreover, $h_{g,\delta_0}(x)$ tends to 0 as x tends to 0 and $h_{g,\delta_0}(x)$ tends to $+\infty$ as x tends to x_1. As a consequence, there is a unique $c_1 = c_1(g, \delta_0) \in]0, x_1[$ such that $h_{g,\delta_0}(c_1) = 1/8$.

(iii) If $0 < x < 1/2$ satisfies $20y_g(x) + 4x < 1$ then, since $\widetilde{y}_g$ is increasing on $]0, 1/2]$ and $\widetilde{y}_g(x_1) = 1$, we have $x < x_1$. Moreover, since h_{g,δ_0} is strictly increasing on $]0, x_1[$ and $h_{g,\delta_0}(x) \leq \frac{1}{8} = h_{g,\delta_0}(c_1)$, it follows that $x \leq c_1$.

(iv) Let $g \geq 2$ and $\delta_0' \geq \delta_0 \geq 0$. By denoting $c_1 = c_1(g, \delta_0)$ and $c_1' = c_1(g, \delta_0')$, we have

$$h_{g,\delta_0}(c_1') \leq h_{g,\delta_0'}(c_1') = 1/8 = h_{g,\delta_0}(c_1)$$

and since h_{g,δ_0} is strictly increasing on $]0, x_1(g)[$, it follows that $c_1' \leq c_1$.

(v) For $x > 0$ and $t > 1$, we define $z_x(t) = \frac{1}{\log t} \log\left(\frac{2}{\pi x} \log t\right)$. By an elementary calculation, z_x is decreasing on $\left[\exp\left(\frac{e\pi x}{2}\right), +\infty\right[$. Moreover, for $g \geq 6$, $y_g(x) = 2x(1 + z_x(g))$ and it follows that if $0 < x \leq \frac{2\log 6}{e\pi}$ then $(g \geq 6 \mapsto y_g(x))$ is decreasing. For $2 \leq g \leq 6$, we check that if $0 < x < 1/2$ then $y_2(x) \geq y_3(x) \geq y_4(x) \geq y_5(x) \geq y_6(x)$ (we leave the details to the reader). This proves that if $0 < x \leq \frac{2\log 6}{e\pi}$ then $(g \geq 2 \mapsto y_g(x))$ is decreasing.

Let $g' \geq g \geq 2$, $x_1 = x_1(g)$ and $x_1' = x_1(g')$. Since $4x_1 \leq 20y_g(x_1) + 4x_1 = 1$, we have $x_1 \leq 1/4 \leq \frac{2\log 6}{e\pi}$ and thus $y_{g'}(x_1) \leq y_g(x_1)$. It follows that

$$\widetilde{y}_{g'}(x_1) \leq \widetilde{y}_g(x_1) = 1 = \widetilde{y}_{g'}(x_1')$$

and since $\widetilde{y}_{g'}$ is strictly increasing on $]0, 1/2[$, we deduce that $x_1' \geq x_1$.

Let $\delta_0 \geq 0$, $c_1 = c_1(g, \delta_0)$ and $c_1' = c_1(g', \delta_0)$. Since $c_1 < x_1 \leq \frac{2\log 6}{e\pi}$, we have $y_{g'}(c_1) \leq y_g(c_1)$ and thus also $\widetilde{y}_{g'}(c_1) \leq \widetilde{y}_g(c_1) < \widetilde{y}_g(x_1) = 1$. It follows that

$$h_{g',\delta_0}(c_1) \leq h_{g,\delta_0}(c_1) = 1/8 = h_{g',\delta_0}(c_1')$$

and since h_{g',δ_0} is strictly increasing on $]0, x_1'[$ and $c_1 < x_1 \leq x_1'$, it follows that $c_1' \geq c_1$.

(vi) Let $\delta_0 \geq 0$. For $g \geq 2$, since $1/8 = h_{g,\delta_0}(c_1(g, \delta_0)) \geq 8c_1(g, \delta_0)$, on a $c_1(g, \delta_0) \leq 1/64$. Since $c_1(g, \delta_0)$ is an increasing function of g and $c_1(g, \delta_0) \geq c_1(2, \delta_0) > 0$, there exists $0 < \ell_{\delta_0} \leq 1/64$ such that $c_1(g, \delta_0)$ tends to ℓ_{δ_0} as $g \to \infty$. Moreover, for $g \geq 6$, $y_g(c_1(g, \delta_0)) = 2c_1(g, \delta_0)\left(1 + \frac{1}{\log g} \log\left(\frac{2}{\pi c_1(g,\delta_0)} \log g\right)\right)$ and thus $y_g(c_1(g, \delta_0))$ tends to $2\ell_{\delta_0}$ as $g \to \infty$. It follows that $h_{g,\delta_0}(c_1(g, \delta_0))$ tends to

$$\frac{1}{8} = \ell_{\delta_0}(8 + \delta_0) + 2\ell_{\delta_0} + \frac{(6 + \delta_0)\,\ell_{\delta_0}(17 \cdot 2\ell_{\delta_0} + 3\ell_{\delta_0})}{1 - 20 \cdot 2\ell_{\delta_0} - 4\ell_{\delta_0}} = \ell_{\delta_0}\left(10 + \delta_0 + \frac{37(6 + \delta_0)\ell_{\delta_0}}{1 - 44\ell_{\delta_0}}\right)$$

as $g \to \infty$. In particular, for $\delta_0 = 0$, $\ell_{\delta_0} = \ell_0$ is a solution of $218\,\ell_0^2 - \frac{31}{2}\ell_0 + \frac{1}{8} = 0$ and thus $\ell_0 = \frac{31 \pm 5\sqrt{21}}{872}$. Since $\ell_0 \leq 1/64$, we obtain $\ell_0 = \frac{31 - 5\sqrt{21}}{872} \approx 0.00927$.

13.2. Proof of Lemma 13.2

(i) The function y_g is strictly increasing on $]0,1/2]$. Moreover, $y_g(x)$ tends to 0 as $x \to 0$ and $y_g(1/2) \geq \frac{1}{\log g}\log 2g > 1 > \frac{\log p_1^{\gamma_1}}{4\log g} = \beta_g$. As a consequence, there is a unique $c_2 = c_2(g) \in]0,1/2[$ such that $y_g(c_2) = \beta_g$.

(ii) If $0 < x < 1/2$ is such that $y_g(x) \leq \beta_g$ then, since y_g is strictly increasing on $]0,1/2]$, we have $x \leq c_2$.

(iii) It follows from the inequality $C_1(g) \geq g$ that if $0 < x < 1$ then $y_g(x) > 2x$ and thus $2c_2 < y_g(c_2) = \beta_g$.

(iv) Since $g \geq 6$ and $y_g(c_2) = \beta_g$, we obtain by using the inequality $\log(1+u) \leq u$:

$$\log\left(\frac{\beta_g}{2}\right) = \log c_2 + \log\left(1 + \frac{1}{\log g}\log\left(\frac{2\log g}{\pi c_2}\right)\right) \leq \log c_2 + \frac{1}{\log g}\log\left(\frac{2\log g}{\pi c_2}\right),$$

hence

$$\frac{\beta_g}{2} \leq c_2^{1-\frac{1}{\log g}}\left(\frac{2\log g}{\pi}\right)^{\frac{1}{\log g}}$$

and the lower bound of c_2 claimed in (iv) follows. We then note that

$$\left(\frac{2}{\pi}\log g\right)^{-\frac{1}{\log g}\frac{1}{1-\frac{1}{\log g}}} = \exp\left(-\frac{1}{\log g - 1}\log\left(\frac{2}{\pi}\log g\right)\right) \to 1, \quad \text{as } g \to \infty,$$

and since $\left|\log\left(\frac{\beta_g}{2}\right)\right| = \log\left(\frac{2}{\beta_g}\right) \leq \log\left(\frac{8\log g}{\log 2}\right)$, we obtain $\left|\left(\frac{1}{1-\frac{1}{\log g}} - 1\right)\log\frac{\beta_g}{2}\right| \ll \frac{\log\log g}{\log g}$ and thus

$$\left(\frac{\beta_g}{2}\right)^{\frac{1}{1-\frac{1}{\log g}}} \sim \frac{\beta_g}{2}, \quad \text{as } g \to \infty$$

which completes the proof of (iv).

(v) Let $(g_i)_i$ be a strictly increasing sequence of integers larger than or equal to 2 such that $(\beta_{g_i})_i$ is constant, say equal to β. Let $i \leq i'$ and denote $c_2 = c_2(g_i)$ and $c_2' = c_2(g_{i'})$. By (iii), $c_2 < \frac{\beta_{g_i}}{2} \leq \frac{1}{8}$. In the proof of Lemma 13.1 (v), we established that if $0 < x \leq \frac{2\log 6}{e\pi}$ then $(g \geq 2 \mapsto y_g(x))$ is decreasing. It follows that

$$y_{g_{i'}}(c_2) \leq y_{g_i}(c_2) = \beta = y_{g_{i'}}(c_2')$$

and since $y_{g_{i'}}$ is strictly increasing on $]0,1/2[$, we deduce that $c_2' \geq c_2$.

(vi) Let $\delta_0 \geq 0$ and denote $c_1 = c_1(g,\delta_0)$. In the proof of Lemma 13.1, we established that $c_1 < x_1 = x_1(g) < 1/2$, $\widetilde{y}_g : x \mapsto 20y_g(x) + 4x$ is strictly increasing on $]0,1/2]$ and $\widetilde{y}_g(x_1) = 1$. It follows that

$$20y_g(c_1) \leq \widetilde{y}_g(c_1) < \widetilde{y}_g(x_1) = 1$$

and thus $y_g(c_1) < 1/20$. Moreover, if g is a prime power then $\beta_g = 1/4$ and thus $y_g(c_1) < \beta_g$ which implies by (ii) that $c_1 \leq c_2$.

13.3. Proof of Theorem 13.3

We are now ready to prove Theorem 13.3. Let $\delta_0 \geq 0$, $g \geq 2$ be an integer and $g = \prod_{i=1}^{t} p_i^{\gamma_i}$ be the prime decomposition of g where $p_1^{\gamma_1} = \min_{1\leq i\leq t} p_i^{\gamma_i}$. Let $c_0 = \min(c_1, c_2) \in]0, 1/2[$ where $c_1 = c_1(g, \delta_0)$ is defined in Lemma 13.1 and $c_2 = c_2(g)$ is defined in Lemma 13.2 and let c such that $0 < c < c_0$.

Using the function y_g defined by (II.72), we denote for $0 < x < 1/2$ and $\varepsilon \geq 0$,

$$\begin{aligned} b_1(x,\varepsilon) &= y_g(x) + \varepsilon, \\ b(x,\varepsilon) &= 3b_1(x,\varepsilon) + x + \varepsilon, \\ t(x,\varepsilon) &= b(x,\varepsilon) + b_1(x,\varepsilon) + \varepsilon, \\ b_2(x,\varepsilon) &= (1+\varepsilon)(5b_1(x,\varepsilon) + 3t(x,\varepsilon)) \end{aligned}$$

and we define

$$\begin{aligned} &h_1(x,\varepsilon) = b(x,\varepsilon) + b_2(x,\varepsilon), \\ &h_2(x,\varepsilon) = x(8+\delta_0+\varepsilon) + b_1(x,\varepsilon) + \frac{(6+\delta_0+\varepsilon)\, x\, b_2(x,\varepsilon)}{1-h_1(x,\varepsilon)} \qquad (\text{if } h_1(x,\varepsilon) < 1). \end{aligned}$$

We check that, for $\varepsilon = 0$, $h_1(x,0) = 20y_g(x) + 4x$ and $h_2(x,0) = h_{g,\delta_0}(x)$ where h_{g,δ_0} is defined by (II.73).

Let $x_1 = x_1(g)$ be defined by Lemma 13.1 (i). The function $h_1(\cdot, 0)$ is strictly increasing on $]0, x_1]$ (see the proof of Lemma 13.1) and since $c < c_0 \leq c_1 < x_1$ and $h_1(x_1, 0) = 1$, we have $h_1(c, 0) < 1$. Since $h_1(c, \varepsilon)$ tends to $h_1(c, 0)$ as $\varepsilon \to 0$, there exists $\varepsilon_1 = \varepsilon_1(g, c) > 0$ such that if $0 \leq \varepsilon < \varepsilon_1$ then $h_1(c, \varepsilon) < 1$ and thus $h_2(c, \varepsilon)$ is well defined.

Moreover, $h_2(\cdot, 0)$ is strictly increasing on $]0, x_1[$ (see the proof of Lemma 13.1) and thus $h_2(c, 0) < h_2(c_1, 0) = 1/8$. Since $h_2(c, \varepsilon)$ is well defined for $0 \leq \varepsilon < \varepsilon_1$ and $h_2(c, \varepsilon)$ tends to $h_2(c, 0) < 1/8$ as $\varepsilon \to 0$, there exists $\varepsilon_2 = \varepsilon_2(g, \delta_0, c)$ such that $0 < \varepsilon_2 < \varepsilon_1$ and if $0 \leq \varepsilon < \varepsilon_2$ then $h_2(c, \varepsilon) < 1/8$.

Since $c < c_0 \leq c_2$ and since $b_1(\cdot, 0) = y_g$ is strictly increasing on $]0, 1/2[$, we have $b_1(c, 0) < b_1(c_2, 0) = y_g(c_2) = \frac{\log p_1^{\gamma_1}}{4 \log g}$ (see Lemma 13.2). Since $b_1(c, \varepsilon)$ tends to $b_1(c, 0)$ as $\varepsilon \to 0$, we deduce there exists $\varepsilon_3 = \varepsilon_3(g, c) > 0$ such that if $0 \leq \varepsilon < \varepsilon_3$ then $b_1(c, \varepsilon) < \frac{\log p_1^{\gamma_1}}{4 \log g}$.

We henceforth take $\varepsilon = \min(\frac{\varepsilon_2}{2}, \frac{\varepsilon_3}{2}, \frac{1}{64}) > 0$ and we put

$$b_1 = b_1(c,\varepsilon),\ b = b(c,\varepsilon) = 3b_1 + c + \varepsilon,\ t = t(c,\varepsilon) = b + b_1 + \varepsilon,\ b_2 = b_2(c,\varepsilon) = (1+\varepsilon)(5b_1 + 3t),$$

$$h_1 = h_1(c,\varepsilon) = b + b_2,\ h_2 = h_2(c,\varepsilon),\ \alpha = \frac{6+\delta_0+\varepsilon}{1-h_1} \tag{II.74}$$

which satisfy

$$(a)\ h_1 < 1, \qquad (b)\ h_2 < 1/8, \qquad (c)\ b_1 < \frac{\log p_1^{\gamma_1}}{4 \log g}.$$

Moreover, we check that $h_1 \geq 20 b_1$. By (a), this implies $b_1 < 1/20$. We also check that

$h_2 \geq c(8+\delta_0+\varepsilon)+b_1 \geq 8c$, which implies by (b) that $c<1/64$ and

$$c(3+\delta_0+\varepsilon)+2b_1 \leq h_2+b_1 < 1/8+1/20 < 1/2. \tag{II.75}$$

We also deduce that

$$b_1+c<1/8, \quad 3b_1+2c<1/4, \quad b<1/5.$$

In particular, b_1, b, t, ε and c satisfy (II.70). In addition, ε, b_1, b, t, b_2 and α are positive and we can check that they depend only on g, δ_0 and c. It follows from Proposition 12.1 that there exists $n_0=n_0(g,\delta_0,c)\geq 200$ such that for any $n\geq n_0$, $A\subset\{0,\dots,n-1\}$ satisfying $0\in A$ and $|A|\leq cn$ and for any $\boldsymbol{d}=(d_j)_{j\in A}\in\{0,\dots,g-1\}^A$ such that $(d_0,g)=1$, we have

$$\begin{aligned}
&\sum_{0\leq k<g^n}\Lambda(k)f_{n,A,\boldsymbol{d}}(k)=\\
&\quad Ng^{-|A|}\frac{g}{\varphi(g)}\left[1+O_{g,\delta_0,c}\left(n^{6-\alpha(1-b-(1+\varepsilon)(5b_1+3t))}\log n+\frac{(\log N)^6}{N^{t-b-b_1}}\right)\right.\\
&\qquad\qquad +O_{g,\delta_0,c}\left(n^{8-\frac{1}{8c}+\frac{b_1}{c}+\alpha(1+\varepsilon)(5b_1+3t)}(\log n)^{\frac{3}{8c}}+\frac{n^{2+\alpha(1+\varepsilon)(5b_1+3t)}\log n}{N^{1/4-b-c}}\right)\\
&\qquad\qquad +O_{g,\delta_0,c}\left(n^{3-\frac{1}{2c}+\frac{2b_1}{c}}(\log n)^{\frac{3}{2c}}\right)+O\left(\frac{(\log N)^4}{N^{b-3b_1-c}}\right)\\
&\qquad\qquad \left.+O\left(\frac{(\log N)^4}{N^{\frac{b_1}{2}-\frac{1}{2}y_g(c)}}\right)\right]
\end{aligned}$$

where $N=g^n$ and thus, by (II.74) and by using that $h_2=c(8+\delta_0+\varepsilon)+b_1+\frac{(6+\delta_0+\varepsilon)\,c\,b_2}{1-h_1}$, we obtain

$$\begin{aligned}
&\sum_{0\leq k<g^n}\Lambda(k)f_{n,A,\boldsymbol{d}}(k)=\\
&\quad Ng^{-|A|}\frac{g}{\varphi(g)}\left[1+O_{g,\delta_0,c}\left(n^{-\delta_0-\varepsilon}\log n+\frac{(\log N)^6}{N^{\varepsilon}}\right)\right.\\
&\qquad\qquad +O_{g,\delta_0,c}\left(n^{\frac{1}{c}\left(h_2-\frac{1}{8}\right)-\delta_0-\varepsilon}(\log n)^{\frac{3}{8c}}+\frac{n^{2+\alpha b_2}\log n}{N^{1/4-b-c}}\right)\\
&\qquad\qquad +O_{g,\delta_0,c}\left(n^{3-\frac{1}{2c}+\frac{2b_1}{c}}(\log n)^{\frac{3}{2c}}\right)+O\left(\frac{(\log N)^4}{N^{\varepsilon}}\right)\\
&\qquad\qquad \left.+O\left(\frac{(\log N)^4}{N^{\varepsilon/2}}\right)\right].
\end{aligned}$$

By using the inequalities $h_2<1/8$, $b+c<1/5+1/64<1/4$, the fact that α, b_2, b and ε depend only on g, δ_0 and c and the inequality (II.75), it follows that

$$\sum_{0\leq k<g^n}\Lambda(k)f_{n,A,\boldsymbol{d}}(k)=Ng^{-|A|}\frac{g}{\varphi(g)}\left[1+O_{g,\delta_0,c}\left(n^{-\delta_0-\varepsilon}(\log n)^{\frac{3}{2c}}\right)\right].$$

By taking $\delta = \delta_0 + \varepsilon/2 > \delta_0$, δ depends only on g, δ_0 and c and the term in $O(\cdot)$ is $\ll_{g,\delta_0,c} n^{-\delta}$, which establishes (II.1) and thus completes the proof of Theorem 13.3.

13.4. Proof of Theorem 2.7

We use the notations of Lemmas 13.1 and 13.2. For each pair (g, δ_0), we check numerically that the corresponding value of c_0 in Table II.1 satisfies $c_0 \in]0, 1/2[$, $20y_g(c_0) + 4c_0 < 1$, $h_{g,\delta_0}(c_0) \leq \frac{1}{8}$ and $y_g(c_0) \leq \beta_g$. By Lemma 13.1 (iii) and Lemma 13.2 (ii), this implies that $c_0 \leq c_1(g, \delta_0)$ and $c_0 \leq c_2(g)$. It follows from Theorem 13.3 that Theorem 2.1 holds with c_0.

14. Proof of Theorem 2.5

We will need the following corollary of Theorem 2.1.

Corollary 14.1. *Let $g \geq 2$ be an integer and $\delta_0 \geq 0$ be a real number. Let $c_0 = c_0(g, \delta_0) \in]0, 1/2[$ be as in Theorem 2.1. For any $0 < c < c_0$, there exist $n_0 = n_0(g, \delta_0, c) \geq 1$ and $\delta = \delta(g, \delta_0, c) > \delta_0$ such that for any integer $n \geq n_0$, $A \subset \{0, \dots, n-1\}$ satisfying $0 \in A$ and*

$$|A| \leq cn$$

and for any $(d_j)_{j\in A} \in \{0, \dots, g-1\}^A$ such that $(d_0, g) = 1$, we have

$$\sum_{\substack{p<g^n \\ \forall j\in A,\, \varepsilon_j(p)=d_j}} \log p = g^{n-|A|}\frac{g}{\varphi(g)}\left(1 + O_{g,\delta_0,c}\left(n^{-\delta}\right)\right). \tag{II.76}$$

Proof. It suffices to write

$$\left| \sum_{\substack{0\leq k<g^n \\ \forall j\in A,\, \varepsilon_j(k)=d_j}} \Lambda(k) - \sum_{\substack{p<g^n \\ \forall j\in A,\, \varepsilon_j(p)=d_j}} \log p \right| \leq \sum_{\substack{p^\nu<g^n \\ \nu\geq 2}} \log p \leq \pi\left(\sqrt{g^n}\right)\log g^n \ll \sqrt{g^n}$$

and to note that since $|A| \leq cn$, we have $\sqrt{g^n} \leq g^{n-|A|}g^{(c-1/2)n}$ and since $c - 1/2 < c_0 - 1/2 < 0$ and δ depends only on g, δ_0 and c, we have $g^{(c-1/2)n} \ll_{g,\delta_0,c} n^{-\delta}$. □

We are now ready to prove Theorem 2.5. Let $n \geq 2$, $A \subset \{0, \dots, n-1\}$ and $(d_j)_{j\in A} \in \{0, \dots, g-1\}^A$. By partial summation, we obtain

$$\begin{aligned}\sum_{g^{n-1}\leq p<g^n} f_{n,A,\boldsymbol{d}}(p) = \frac{1}{\log g^n} \sum_{g^{n-1}\leq p<g^n} f_{n,A,\boldsymbol{d}}(p)\log p \\ + \int_{g^{n-1}}^{g^n} \frac{1}{t(\log t)^2}\left(\sum_{g^{n-1}\leq p<t} f_{n,A,\boldsymbol{d}}(p)\log p\right) dt\end{aligned}$$

where the integral is

$$\ll \left(\int_{g^{n-1}}^{g^n} \frac{dt}{t(\log t)^2}\right) \sum_{g^{n-1}\le p<g^n} f_{n,A,\boldsymbol{d}}(p)\log p = \frac{1}{\log g^n}\frac{1}{n-1}\sum_{g^{n-1}\le p<g^n} f_{n,A,\boldsymbol{d}}(p)\log p.$$

Moreover, if $n-1\in A$ and $d_{n-1}\ge 1$ then, for any $k<g^{n-1}$, we have $f_{n,A,\boldsymbol{d}}(k)=0$, hence

$$\sum_{p<g^n} f_{n,A,\boldsymbol{d}}(p) = \frac{1}{\log g^n}\left(1+O\left(\frac{1}{n}\right)\right)\sum_{p<g^n} f_{n,A,\boldsymbol{d}}(p)\log p. \tag{II.77}$$

Theorem 2.5 then follows immediately from (II.77) and Corollary 14.1.

15. Explicit admissible values of c_0 under GRH

The purpose of this section is to provide explicit admissible values of c_0 under GRH (Generalized Riemann Hypothesis).

Theorem 15.1. *Assume GRH. Theorem 2.1 holds with $c_0 = c_0(g,\delta_0)$ given in Table II.2.*

δ_0 \ g	2	3	4	5	6	10	10^3	$2\cdot 3^{100}$	2^{200}
0	16	24	29	31	33	37	52	68	69
0.5	15	23	28	30	32	35	49	64	64
1	15	23	27	29	31	34	47	60	60
10	11	15	17	18	19	20	25	28	29
100	3.5	3.9	4	4.1	4.1	4.2	4.5	4.6	4.6

Table II.2. – $c_0(g,\delta_0)\cdot 10^3$ under GRH

We will prove Theorem 15.1 in Section 15.3.3.

Remark 15.2. For general $g\ge 2$ and $\delta_0\ge 0$, we will show that under GRH, Theorem 2.1 holds with $c_0 = c_0(g,\delta_0)$ which is defined as a solution of an equation (see Lemma 15.9 and Theorem 15.10). For any given $g\ge 2$, the largest value of $c_0(g,\delta_0)$ is obtained for $\delta_0=0$. Moreover, for any $\delta_0\ge 0$, $c_0(g,\delta_0)$ is an increasing function of g and tends to $\frac{1}{2(7+\delta_0)}$ as $g\to\infty$. In particular, for $\delta_0=0$, $c_0(g,\delta_0)$ tends to $1/14\approx 0.07142$ as $g\to\infty$.

15.1. Major arcs contribution under GRH

In this section, we will see that assuming GRH permits us to obtain stronger results regarding $\mathfrak{I}_{P_1}$ and $\mathfrak{I}_{NP}$ (than those obtained unconditionally in Section 11).

15.1.1. Estimate of $\mathfrak{I}_{P_1}$ under RH

We will need the following lemma.

Lemma 15.3. *Assume RH. If $g \in \mathcal{C}^1([a,b])$ and $a \geq 2$ then*

$$\sum_{a<k\leq b} g(k)\Lambda(k) = \sum_{a<k\leq b} g(k) + O\left(Mb^{1/2}(\log b)^2\right)$$

where $M = |g(b)| + \int_a^b |g'(t)|\,dt$.

Proof. Since we assume RH, we have for any $x \geq 2$,

$$\psi(x) = \lfloor x \rfloor + O\left(x^{1/2}(\log x)^2\right)$$

(see for instance [50, Theorem 13.1 p. 419]) and it follows that for any $a \leq t \leq b$,

$$\psi(t) - \psi(a) - (\lfloor t \rfloor - \lfloor a \rfloor) = O\left(b^{1/2}(\log b)^2\right).$$

To complete the proof, it suffices to apply Lemma 7.5. □

We are now able to establish a more precise version of Lemma 11.1 under RH.

Lemma 15.4. *Assume RH. For any $1 \leq q \leq B_1$ and $K_2(q) \leq k_2 \leq N - K_2(q)$, we have*

$$\sum_{\substack{1\leq k_1\leq N\\ k_1\in I_q(k_2)}} \frac{B}{qN}\widehat{w}\left((k_2-k_1)\frac{B}{qN}\right)\Lambda(k_1) = 1 + O\left(\frac{B}{qN^{1/2}}v_N(\log N)^2\right). \tag{II.78}$$

Proof. We denote by $\Sigma(q,k_2)$ the left-hand side sum and we put $a = k_2 - \frac{qN}{B}v_N$ and $b = k_2 + \frac{qN}{B}v_N$. As in the proof of Lemma 11.1, since $I_q(k_2) =]a,b] \subset \left]\frac{qN}{B}v_N, N - \frac{qN}{B}v_N\right] \subset]0,N]$, we have

$$\Sigma(q,k_2) = \sum_{a<k_1\leq b} \frac{B}{qN}\widehat{w}\left((k_2-k_1)\frac{B}{qN}\right)\Lambda(k_1)$$

and since $b - a = 2\frac{qN}{B}v_N$, it follows from Lemma 15.3 that

$$\Sigma(q,k_2) = \sum_{a<k_1\leq b} \frac{B}{qN}\widehat{w}\left((k_2-k_1)\frac{B}{qN}\right) + O\left(\frac{B}{qN}v_N N^{1/2}(\log N)^2\right).$$

Moreover, as in the proof of Lemma 11.1, since $K_2(q) \leq k_2 \leq N - K_2(q)$, we obtain

$$\left|1 - \sum_{a<k_1\leq b} \frac{B}{qN}\widehat{w}\left((k_2-k_1)\frac{B}{qN}\right)\right| \ll v_N^{1/2}e^{-v_N^{1/2}},$$

and since $1 \le (\log N)^2 \le v_N$,

$$v_N^{1/2} e^{-v_N^{1/2}} \le \frac{v_N}{N} \le \frac{B}{qN} v_N N^{1/2} (\log N)^2,$$

which completes the proof. □

We derive the following estimate of $\mathfrak{I}_{P_1}$ (defined by (II.45)) under RH.

Lemma 15.5. *Assume RH. Let $\kappa > 0$ and $0 < c < \frac{1}{2(1+\kappa)}$. If $B_1 \le N^{\frac{\kappa}{4(1+\kappa)}}$ and $|A| \le cn$ then*

$$\mathfrak{I}_{P_1} = N g^{-|A|} \frac{g}{\varphi(g)} \left(1 + O_{g,\kappa,c} \left(n^2 \log n \left(\frac{n}{\log^3 n} \right)^{1 - \frac{1}{2(1+\kappa)c}} \right) + O_{g,\kappa,c} \left(\frac{B}{N^{1/2}} v_N (\log N)^4 \right) \right) + O\left(\frac{NB_1}{B} v_N \log N \right).$$

Proof. It follows from (II.45) and (II.78) that

$$\mathfrak{I}_{P_1} = \Sigma_1 + O\left(\frac{B}{N^{1/2}} v_N (\log N)^2 \Sigma_2 \right)$$

where Σ_1 and Σ_2 are defined as in the proof of Lemma 11.2. Moreover, since $|A| \le cn$ and $B_1 \le N^{\frac{\kappa}{4(1+\kappa)}}$, we obtain as in the proof of Lemma 11.2

$$\Sigma_1 = N g^{-|A|} \frac{g}{\varphi(g)} \left(1 + O_{g,\kappa,c} \left(n^2 \log n \left(\frac{n}{\log^3 n} \right)^{1 - \frac{1}{2(1+\kappa)c}} \right) \right) + O\left(\frac{NB_1}{B} v_N \log N \right)$$

and

$$\Sigma_2 \le \sum_{\substack{1 \le q \le B_1 \\ q \text{ sf}}} \sum_{0 \le k < g^n} \frac{f_{n,A,\boldsymbol{d}}(k)}{\varphi\left(\frac{q}{(k,q)} \right)} \ll_{g,\kappa,c} N g^{-|A|} n^2$$

which completes the proof. □

15.1.2. Upper bound of $\mathfrak{I}_{NP}$ under GRH

Lemma 15.6. *Assume GRH. If $\chi_1 \bmod q_1$ is a primitive character such that $1 < q_1 \le B_1$ and if $1 \le q_2 \le B_1/q_1$ and $1 \le k_2 \le N$ then*

$$\left| \sum_{\substack{1 \le k_1 \le N \\ k_1 \in I_{q_1 q_2}(k_2)}} \frac{B}{q_1 q_2 N} \widehat{w}\left((k_2 - k_1) \frac{B}{q_1 q_2 N} \right) \chi_1(k_1) \Lambda(k_1) \right| \ll \frac{B}{q_1 q_2 N^{1/2}} v_N (\log N)^2. \tag{II.79}$$

Proof. We denote by $\Sigma(\chi_1, q_2, k_2)$ the sum in the left-hand side of (II.79) and we put $q = q_1 q_2$, $a = \max(k_2 - \frac{qN}{B} v_N, 1)$ and $b = \min(k_2 + \frac{qN}{B} v_N, N)$ so that

$$\Sigma(\chi_1, q_2, k_2) = \sum_{a < k_1 \le b} \frac{B}{qN} \widehat{w}\left((k_2 - k_1)\frac{B}{qN}\right) \chi_1(k_1)\Lambda(k_1).$$

Since $b - a \le 2\frac{qN}{B} v_N$, it follows from Lemma 7.9 that

$$|\Sigma(\chi_1, q_2, k_2)| \ll \frac{B}{qN} v_N \sup_{a < t \le b} |\psi(t, \chi_1) - \psi(a, \chi_1)|.$$

Since we assume GRH and χ_1 is nonprincipal, we have for any $x \ge 2$,

$$\psi(x, \chi_1) = O\left(x^{1/2}(\log x)(\log q_1 x)\right)$$

(see for instance [50, Theorem 13.7 p. 425]) and it follows that

$$|\Sigma(\chi_1, q_2, k_2)| \ll \frac{B}{qN} v_N\, b^{1/2}(\log b)(\log q_1 b) \ll \frac{B}{qN^{1/2}} v_N (\log N)^2.$$

□

We derive the following estimate of $\mathfrak{I}_{NP}$ (defined by (II.50)) under GRH.

Lemma 15.7. *Assume GRH. Let $\kappa > 0$ and $0 < c < \frac{1}{2(1+\kappa)}$. If $B_1 \le N^{\frac{\kappa}{4(1+\kappa)}}$ and $|A| \le cn$ then*

$$\mathfrak{I}_{NP} = O_{g,\kappa,c}\left(N g^{-|A|} \frac{BB_1}{N^{1/2}} v_N (\log N)^4\right).$$

Proof. It follows from (II.50) that

$$|\mathfrak{I}_{NP}| \le \left(\sum_{\substack{1 \le q_2 \le B_1 \\ q_2 \text{ sf}}} \sum_{1 \le k_2 \le N} \frac{f_{n,A,\boldsymbol{d}}(k_2)}{\varphi\left(\frac{q_2}{(q_2, k_2)}\right)}\right) U \tag{II.80}$$

where U is defined by

$$U = \sum_{1 < q_1 \le B_1} \sideset{}{^*}\sum_{\chi_1 \bmod q_1} \frac{q_1}{\varphi(q_1)} \max_{\substack{1 \le q_2 \le B_1/q_1 \\ 1 \le k_2 \le N}} \left| \sum_{\substack{1 \le k_1 \le N \\ k_1 \in I_{q_1 q_2}(k_2)}} \frac{B}{q_1 q_2 N} \widehat{w}\left((k_2 - k_1)\frac{B}{q_1 q_2 N}\right) \chi_1(k_1)\Lambda(k_1) \right|.$$

Moreover, by Lemma 15.6,

$$U \ll \sum_{1 < q_1 \le B_1} \sideset{}{^*}\sum_{\chi_1 \bmod q_1} \frac{q_1}{\varphi(q_1)} \frac{B}{q_1 N^{1/2}} v_N (\log N)^2 \le \frac{BB_1}{N^{1/2}} v_N (\log N)^2$$

and by Lemma 5.30, since $B_1 \le N^{\frac{\kappa}{4(1+\kappa)}}$ and $|A| \le cn$, the double sum over q_2 and k_2 in the right-hand side of (II.80) is

$$\ll_{g,\kappa,c} Ng^{-|A|}(\log N)^2$$

which completes the proof. □

15.2. Conclusion of minor and major arcs under GRH

Proposition 15.8. *Assume GRH. Let $g \ge 2$ be an integer and $c > 0$ be a real number. Let $n \ge 100$, $A \subset \{0, \dots, n-1\}$ and $\boldsymbol{d} = (d_j)_{j\in A} \in \{0, \dots, g-1\}^A$ such that $0 \in A$ and $(d_0, g) = 1$. We denote $N = g^n$. If $|A| \le cn$ then for any real numbers $\kappa > 0$, B_1 and B satisfying*

$$g \le B_1 \le N^{\frac{\kappa}{4(1+\kappa)}}, \quad 4B_1(\log N)^2 \le B < \frac{N}{4B_1} \quad \text{and} \quad c < \frac{1}{2(1+\kappa)},$$

we have

$$\sum_{0\le k<g^n} \Lambda(k) f_{n,A,\boldsymbol{d}}(k) =$$
$$Ng^{-|A|}\frac{g}{\varphi(g)}\left[1 + O_{g,\kappa,c}\left(n^2 \log n \left(\frac{n}{\log^3 n}\right)^{1-\frac{1}{2(1+\kappa)c}}\right) + O_{g,\kappa,c}\left(\frac{BB_1}{N^{1/2}}(\log N)^6\right)\right.$$
$$\left. + O\left(\frac{N^{C_2(g)c\log\left(\frac{C_1(g)}{c}\right)}}{B_1^{1/2}}(\log N)^4\right) + O\left(\frac{N^c B_1}{B}(\log N)^4\right)\right]$$

where $C_1(g)$ and $C_2(g)$ are defined respectively by (II.10) and (II.11).

Proof. The parameters B_1 and B clearly satisfy the condition (II.4). We put $v_N = (\log N)^2$ which satisfies (II.40). Since $0 < c < \frac{1}{2(1+\kappa)} < \frac{1}{2} \le 2e^{-1} \le C_1(g)e^{-1}$, $B_1 \le N^{1/4} \le N^{2/5}$ and $|A| \le cn$, Lemma 10.1 asserts that

$$\sum_{0\le k<g^n} \Lambda(k) f_{n,A,\boldsymbol{d}}(k) = \mathfrak{I}_{P_1} + \mathfrak{I}_{NP} + O\left(Ng^{-|A|}\frac{N^{C_2(g)c\log\left(\frac{C_1(g)}{c}\right)}}{\sqrt{B_1}}(\log N)^4\right) \tag{II.81}$$
$$+ O\left(Ng^{-|A|}\frac{BB_1}{N}(\log N)^2\right) + O\left(Ng^{-|A|}\frac{N^c B_1}{B}(\log N)^4\right)$$

where $\mathfrak{I}_{P_1}$ is defined by (II.45) and $\mathfrak{I}_{NP}$ is the contribution of the nonprincipal characters

in (II.42). Since we assume GRH, it follows from Lemma 15.5 that

$$\mathfrak{I}_{P_1} = Ng^{-|A|}\frac{g}{\varphi(g)}\left(1 + O_{g,\kappa,c}\left(n^2\log n\left(\frac{n}{\log^3 n}\right)^{1-\frac{1}{2(1+\kappa)c}}\right) + O_{g,\kappa,c}\left(\frac{B}{N^{1/2}}(\log N)^6\right)\right) + O\left(\frac{NB_1}{B}(\log N)^3\right)$$

and by Lemma 15.7,

$$\mathfrak{I}_{NP} = O_{g,\kappa,c}\left(Ng^{-|A|}\,\frac{BB_1}{N^{1/2}}(\log N)^6\right).$$

To complete the proof, it suffices to insert these estimates of $\mathfrak{I}_{P_1}$ and $\mathfrak{I}_{NP}$ into (II.81) and to use that $g^{|A|} \le N^c$. □

15.3. Completion of the proof of Theorem 15.1

In this section, we will provide an explicit admissible value of $c_0(g,\delta_0)$ under GRH for general integer $g \ge 2$ and real number $\delta_0 \ge 0$ (see Theorem 15.10). We will then be able to prove Theorem 15.1.

In order to define an admissible value of $c_0(g,\delta_0)$, we will need the following lemma (it will be proved in Section 15.3.1).

Lemma 15.9. *For $g \ge 2$ and $x > 0$, let $y_g(x)$ be defined by (II.72). For any $g \ge 2$ and $\delta_0 \ge 0$,*

(i) the equation $4y_g(x) + 2x(3+\delta_0) = 1$ has a unique solution $x = c_0(g,\delta_0)$ on $]0,1/2[$,

(ii) if $x \in]0,1/2[$ satisfies $4y_g(x) + 2x(3+\delta_0) \le 1$ then $x \le c_0(g,\delta_0)$.

Moreover,

(iii) for any $g \ge 2$, $c_0(g,\delta_0)$ is a decreasing function of δ_0,

(iv) for any $\delta_0 \ge 0$, $c_0(g,\delta_0)$ is an increasing function of g,

(v) for any $\delta_0 \ge 0$, $c_0(g,\delta_0)$ tends to $\frac{1}{2(7+\delta_0)}$ as $g \to \infty$.

We will then establish in Section 15.3.2:

Theorem 15.10. *Assume GRH. For any $g \ge 2$ and $\delta_0 \ge 0$, Theorem 2.1 holds with $c_0 = c_0(g,\delta_0)$ defined in Lemma 15.9 (i).*

We will finally obtain Theorem 15.1 as a consequence of Theorem 15.10 in Section 15.3.3.

15.3.1. Proof of Lemma 15.9

For $g \ge 2$, $\delta_0 \ge 0$ and $x > 0$, we define $k_{g,\delta_0}(x) = 4y_g(x) + 2x(3+\delta_0)$.

(i) An elementary calculation shows that the functions y_g and k_{g,δ_0} are strictly increasing on $]0,1/2] \subset]0, C_1(g)e^{-1}]$. Moreover, $k_{g,\delta_0}(x)$ tends to 0 as $x \to 0$ and $k_{g,\delta_0}(1/2) \ge 6 \cdot 1/2 > 1$. As a consequence, there is a unique $c_0 = c_0(g,\delta_0) \in]0,1/2[$ such that $k_{g,\delta_0}(c_0) = 1$.

(ii) If $0 < x < 1/2$ is such that $k_{g,\delta_0}(x) \leq 1$ then, since k_{g,δ_0} is strictly increasing on $]0, 1/2]$, we have $x \leq c_0$.

(iii) Let $g \geq 2$ and $\delta_0' \geq \delta_0 \geq 0$. By denoting $c_0 = c_0(g, \delta_0)$ and $c_0' = c_0(g, \delta_0')$, we have

$$k_{g,\delta_0}(c_0') \leq k_{g,\delta_0'}(c_0') = 1 = k_{g,\delta_0}(c_0)$$

and since k_{g,δ_0} is strictly increasing on $]0, 1/2[$, it follows that $c_0' \leq c_0$.

(iv) Let $\delta_0 \geq 0$ and $g' \geq g \geq 2$. We denote $c_0 = c_0(g, \delta_0)$ and $c_0' = c_0(g', \delta_0)$. We established in Section 13.1 (v) that if $0 < x \leq \frac{2\log 6}{e\pi}$ then $(g \geq 2 \mapsto y_g(x))$ is decreasing. Since $6c_0 \leq k_{g,\delta_0}(c_0) = 1$, we have $c_0 \leq 1/6 \leq \frac{2\log 6}{e\pi}$ and it follows that

$$k_{g',\delta_0}(c_0) \leq k_{g,\delta_0}(c_0) = 1 = k_{g',\delta_0}(c_0').$$

Since k_{g',δ_0} is strictly increasing on $]0, 1/2[$, we deduce that $c_0' \geq c_0$.

(v) Let $\delta_0 \geq 0$. Since $c_0(g, \delta_0)$ is an increasing function of g and $c_0(g, \delta_0) \geq c_0(2, \delta_0) > 0$, there exists $\ell_{\delta_0} > 0$ such that $c_0(g, \delta_0)$ tends to ℓ_{δ_0} as $g \to \infty$. Moreover, for $g \geq 6$, $y_g(c_0(g, \delta_0)) = 2c_0(g, \delta_0)\left(1 + \frac{1}{\log g}\log\left(\frac{2}{\pi c_0(g,\delta_0)}\log g\right)\right)$ and thus $y_g(c_0(g, \delta_0))$ tends to $2\ell_{\delta_0}$ as $g \to \infty$. It follows that $k_{g,\delta_0}(c_0(g, \delta_0))$ tends to $1 = 8\ell_{\delta_0} + 2\ell_{\delta_0}(3 + \delta_0)$ as $g \to \infty$, hence $\ell_{\delta_0} = \frac{1}{2(7+\delta_0)}$.

15.3.2. Proof of Theorem 15.10

Let $g \geq 2$, $\delta_0 \geq 0$ and $c_0 \in]0, 1/2[$ where $c_0 = c_0(g, \delta_0)$ is defined in Lemma 15.9. Assume GRH and take any c such that $0 < c < c_0$. Let k_{g,δ_0} be the function defined in Section 15.3.1. Since k_{g,δ_0} is strictly increasing on $]0, 1/2]$, we have $k_{g,\delta_0}(c) < k_{g,\delta_0}(c_0) = 1$ and thus there exists $\Delta = \Delta(g, \delta_0, c) > 0$ such that

$$y_g(c) + \frac{3 + \delta_0}{2}c + \Delta < \frac{1}{4}.$$

We define $b_1 = y_g(c) + \Delta$ which satisfies $b_1 + \frac{3+\delta_0}{2}c < 1/4$ and we easily see that there exists $n_0 = n_0(g, b_1) \geq 100$ such that for any $n \geq n_0$, by denoting $N = g^n$, we have $g \leq N^{b_1}$ and $4(\log N)^3 \leq N^{\frac{1}{4}-b_1}$. Note that n_0 depends only on g, δ_0 and c. We assume now that $n \geq n_0$ and we define

$$B_1 = N^{b_1}, \quad B = \frac{N^{\frac{c}{2}+\frac{1}{4}}}{\log N} \quad \text{and} \quad \kappa = \frac{4b_1}{1 - 4b_1} > 0.$$

The choice of n_0 guarantees that $g \leq B_1$ and $4B_1(\log N)^2 \leq \frac{N^{1/4}}{\log N} \leq B$. Moreover, since $b_1 + \frac{c}{2} < 1/4$, we have $4BB_1 < \frac{4}{\log N}N^{1/2} < N$ and we can easily check that $b_1 = \frac{\kappa}{4(1+\kappa)}$ and $2(1 + \kappa)c < 1$. It follows from Proposition 15.8 that if $A \subset \{0, \ldots, n-1\}$ is such that $0 \in A$

and $|A| \leq cn$ and if $\boldsymbol{d} = (d_j)_{j\in A} \in \{0, \dots, g-1\}^A$ is such that $(d_0, g) = 1$ then

$$\sum_{0\leq k<g^n} \Lambda(k) f_{n,A,\boldsymbol{d}}(k) = Ng^{-|A|}\frac{g}{\varphi(g)}\left[1 + O_{g,\kappa,c}\left(n^2 \log n \left(\frac{n}{\log^3 n}\right)^{1-\frac{1}{2(1+\kappa)c}}\right)\right.$$
$$\left. + O_{g,\kappa,c}\left(\frac{(\log N)^5}{N^{1/4-b_1-c/2}}\right) + O\left(\frac{(\log N)^4}{N^{\Delta/2}}\right)\right].$$

The power of n in the term in the first $O_{g,\kappa,c}(\cdot)$ is $E := 3 - \frac{1}{2(1+\kappa)c}$ and since $1/4 - b_1 - c/2 > 0$ and $\Delta > 0$, we obtain for any δ such that $E < -\delta$,

$$\sum_{0\leq k<g^n} \Lambda(k) f_{n,A,\boldsymbol{d}}(k) = Ng^{-|A|}\frac{g}{\varphi(g)}\left(1 + O_{g,\kappa,c,\delta,b_1,\Delta}\left(n^{-\delta}\right)\right).$$

Moreover, since $b_1 + \frac{3+\delta_0}{2}c < 1/4$, we have $E < -\delta_0$. This allows us to choose $\delta = \frac{1}{2}(\delta_0 - E)$ so that $E < -\delta$ and $\delta > \delta_0$. Since Δ, b_1, κ and δ depend only on g, δ_0 and c, we obtain

$$\sum_{0\leq k<g^n} \Lambda(k) f_{n,A,\boldsymbol{d}}(k) = Ng^{-|A|}\frac{g}{\varphi(g)}\left(1 + O_{g,\delta_0,c}\left(n^{-\delta}\right)\right)$$

which completes the proof of Theorem 15.10.

15.3.3. Proof of Theorem 15.1

For each pair (g, δ_0), we check numerically that the corresponding value of c_0 in Table II.2 satisfies $c_0 \in]0, 1/2[$ and $4y_g(c_0) + 2c_0(3 + \delta_0) \leq 1$ where y_g be defined by (II.72). It follows from Lemma 15.9 (ii) and Theorem 15.10 that if we assume GRH then Theorem 2.1 holds with c_0.

III. Somme des chiffres de certaines suites dans les corps finis

Le contenu de ce chapitre est publié dans « Monatshefte für Mathematik » [65].

Abstract. In $\mathbb{F}_q$, Dartyge and Sárközy introduced the notion of digits and studied some properties of the sum of digits function. We will provide sharp estimates for the number of elements of special sequences of $\mathbb{F}_q$ whose sum of digits is prescribed. Such special sequences of particular interest include the set of n-th powers for each $n \geq 1$ and the set of elements of order d in $\mathbb{F}_q^*$ for each divisor d of $q-1$. We provide an optimal estimate for the number of squares whose sum of digits is prescribed. Our methods combine A. Weil bounds with character sums, Gaussian sums and exponential sums.

Table of contents

1. Introduction

1.1. Motivation

Let $g \geq 2$ be an integer. Every $n \in \mathbb{N}$ can be written uniquely in base g:

$$n = \sum_{j=0}^{r} c_j g^j \tag{III.1}$$

where the digits c_j belong to $\{0, \ldots, g-1\}$ and $c_r \geq 1$. The study of the connection between the arithmetic properties of n and the properties of its digits in a given basis produces a lot of interesting and difficult questions and many papers have been devoted to this topic. In particular, Gelfond [25] proved an asymptotic formula for the number of integers of an arithmetic progression whose sum of digits modulo m is fixed. More recently, Mauduit and Rivat [43], [44] obtained an asymptotic formula for the number of prime numbers and also for the number of squares whose sum of digits modulo m is fixed. In another direction, Maynard [48] showed in a recent work that there are infinitely many prime numbers with one missing digit (e.g. no digit 9) in their decimal expansion.

In [12], Dartyge and Sárközy initiated the study of the concept of digits in the context of finite fields. The algebraic structure of finite fields permits us to formulate and study new problems of interest which might be out of reach in the context of integers [38], [52]. Let p be a prime number, let $q = p^r$ with $r \geq 2$ and consider the finite field $\mathbb{F}_q$. Let $\mathcal{B} = \{e_1, \ldots, e_r\}$ be a basis of the vector space $\mathbb{F}_q$ over $\mathbb{F}_p$. Then every $x \in \mathbb{F}_q$ can be written uniquely in base $\mathcal{B}$:

$$x = \sum_{j=1}^{r} c_j e_j \tag{III.2}$$

with $c_1, \ldots, c_r \in \mathbb{F}_p$. As in [12], we will call $c_1, \ldots, c_r$ the "digits" of x by analogy with the special case where the basis $\mathcal{B}$ consists of the first r powers of a generator (i.e. primitive element) g of $\mathbb{F}_q^*$ since in this situation (III.2) becomes

$$x = \sum_{j=1}^{r} c_j g^{j-1},$$

which reminds us of (III.1). Then Dartyge and Sárközy introduced the function $s_{\mathcal{B}}$ defined over $\mathbb{F}_q$ by

$$s_{\mathcal{B}}(x) = \sum_{j=1}^{r} c_j \tag{III.3}$$

which may be called the "sum of digits" function and they estimated the number of squares in $\mathbb{F}_q$ whose sum of digits is prescribed. Beyond squares, they also obtained results for sequences in $\mathbb{F}_q$ of the form $(P(x))_{x \in \mathbb{F}_q}$ and $(P(g))_{g \in \mathcal{G}}$ where $P \in \mathbb{F}_q[X]$ and $\mathcal{G}$ is the set of generators of $\mathbb{F}_q^*$. Further problems on digits in finite fields have been studied by Dartyge, Mauduit, Sárközy [11], Dietmann, Elsholtz, Shparlinski [16] and Gabdullin [23]. In particular, an estimate

of the number of squares in $\mathbb{F}_q$ with restricted digits has been proved in [11] and then improved in [16] and [23].

In this paper, our goal is to provide sharp estimates for the number of elements of special sequences of $\mathbb{F}_q$ whose sum of digits is prescribed. Such special sequences of particular interest include the set of n-th powers for each $n \geq 1$ and the set of elements of order d in $\mathbb{F}_q^*$ for each divisor d of $q-1$. We will provide an optimal estimate for the number of squares whose sum of digits is prescribed.

1.2. Statement of results

Let p be a prime number, let $q = p^r$ with $r \geq 2$, let $\mathcal{B} = \{e_1, \ldots, e_r\}$ be a basis of $\mathbb{F}_q$ over $\mathbb{F}_p$ and let $s_{\mathcal{B}}$ be the sum of digits function defined by (III.3).

1.2.1. Sum of digits of polynomial values

For $P \in \mathbb{F}_q[X]$ and for $s \in \mathbb{F}_p$, we define

$$\mathcal{D}(P, s) = \{x \in \mathbb{F}_q : s_{\mathcal{B}}(P(x)) = s\}.$$

In [12], Dartyge and Sárközy obtained the following estimate for $|\mathcal{D}(P, s)|$:

Theorem A. *If $P \in \mathbb{F}_q[X]$ is a polynomial of degree $n \geq 1$ with $(n, q) = 1$ then, for any $s \in \mathbb{F}_p$,*

$$\left| |\mathcal{D}(P, s)| - \frac{q}{p} \right| \leq (n-1)\sqrt{q}.$$

In the special case where $n = 2$, we will improve optimally this result by giving an exact formula for $||\mathcal{D}(P, s)| - q/p|$:

Theorem 1.1. *If $p \geq 3$ and if $P(X) = a_2X^2 + a_1X + a_0 \in \mathbb{F}_q[X]$ with $a_2 \neq 0$ then, writing $\nu_P = s_{\mathcal{B}}(a_0 - a_1^2(4a_2)^{-1})$, we have, for any $s \in \mathbb{F}_p$,*

$$\left| |\mathcal{D}(P, s)| - \frac{q}{p} \right| = \begin{cases} \dfrac{\sqrt{q}}{\sqrt{p}} & \text{if } s \neq \nu_P \text{ and } r \text{ is odd,} \\ \dfrac{\sqrt{q}}{p} & \text{if } s \neq \nu_P \text{ and } r \text{ is even,} \\ 0 & \text{if } s = \nu_P \text{ and } r \text{ is odd,} \\ \dfrac{p-1}{p}\sqrt{q} & \text{if } s = \nu_P \text{ and } r \text{ is even.} \end{cases}$$

The fact that $|\mathcal{D}(P, s)| = q/p$ for $s = \nu_P$ and $r \equiv 1 \bmod 2$ does not seem to be obvious at first sight; this will follow from the proof. We will see in Remark 3.2 that if $p = 2$ then $|\mathcal{D}(P, s)|$ is equal to q/p or 0 or q.

Theorem 1.1 will be a consequence of a more precise result (see Theorem 3.1 in Section 3.1) which provides an exact formula for $|\mathcal{D}(P, s)|$.

Our next purpose will be to improve Theorem A in the special case where P is a monomial. We will see in Section 3.2 that for any monomial $aX^n \in \mathbb{F}_q[X]$ and for any $s \in \mathbb{F}_p$, we have $|\mathcal{D}(aX^n, s)| = |\mathcal{D}(aX^d, s)|$ where $d = (n, q-1)$. Thus, it suffices to study $|\mathcal{D}(P, s)|$ for monomials P whose degree divides $q-1$. In this last case, the statement of Theorem A becomes: if d divides $q-1$ and if $a \in \mathbb{F}_q^*$ then, for any $s \in \mathbb{F}_p$,

$$\left| |\mathcal{D}(aX^d, s)| - \frac{q}{p} \right| \leq (d-1)\sqrt{q}. \tag{III.4}$$

We will obtain the following sharper estimate for $|\mathcal{D}(aX^d, s)|$:

Theorem 1.2. *If d divides $q-1$ and if $a \in \mathbb{F}_q^*$ then, for any $s \in \mathbb{F}_p^*$,*

$$\left| \left|\mathcal{D}(aX^d, s)\right| - \frac{q}{p} \right| \leq \begin{cases} (d-1)\sqrt{q}/p & \text{if } d \mid \delta, \\ (d-1)\sqrt{q}/\sqrt{p} & \text{otherwise,} \end{cases}$$

where δ is the integer defined by $\delta = (q-1)/(p-1)$ and for $s = 0$,

$$\left| \left|\mathcal{D}(aX^d, 0)\right| - \frac{q}{p} \right| \leq \frac{p-1}{p} \left((d, \delta) - 1\right) \sqrt{q}.$$

For $s \neq 0$, Theorem 1.2 permits us to improve (III.4) by a factor at least $1/\sqrt{p}$. In the special case where $d = 2$ (and so $p \geq 3$), a comparison between Theorem 1.2 and Theorem 1.1 shows that the upper bounds obtained in Theorem 1.2 are the best possible (indeed, $d = 2$ divides δ if and only if r is even).

Theorem 1.2 will be proved in Section 3.2 and it will appear as a consequence of a slightly more precise estimate for $\left|\mathcal{D}(aX^d, s)\right|$ (see Theorem 3.7).

We will see that Theorem 1.2 provides a sharp estimate for the number of n-th powers in $\mathbb{F}_q$ whose sum of digits is prescribed. For $s \in \mathbb{F}_p$, we define

$$\mathcal{F}_s = \{x \in \mathbb{F}_q : s_{\mathcal{B}}(x) = s\}$$

and $\mathcal{F}_s^* = \mathcal{F}_s \setminus \{0\}$. For $n \geq 1$, we denote by $\mathcal{A}_n$ the set of n-th powers in $\mathbb{F}_q$:

$$\mathcal{A}_n = \{x^n : x \in \mathbb{F}_q\}.$$

Since $\mathcal{A}_n = \mathcal{A}_d$ where $d = (n, q-1)$ (see for instance Lemma 2D p. 13 of [61]), the study of $|\mathcal{F}_s \cap \mathcal{A}_n|$ is reduced to the study of $|\mathcal{F}_s \cap \mathcal{A}_d|$ where d is a divisor of $q-1$. In Section 3.3, we will deduce from Theorem 1.2 the following estimate for $|\mathcal{F}_s \cap \mathcal{A}_d|$:

Corollary 1.3. *If d divides $q-1$ then, for any $s \in \mathbb{F}_p^*$,*

$$\left| |\mathcal{F}_s \cap \mathcal{A}_d| - \frac{|\mathcal{F}_s|}{d} \right| \leq \begin{cases} \dfrac{d-1}{d}\dfrac{\sqrt{q}}{p} & \text{if } d \mid \delta, \\ \dfrac{d-1}{d}\dfrac{\sqrt{q}}{\sqrt{p}} & \text{otherwise,} \end{cases} \tag{III.5}$$

where δ is the integer defined by $\delta = (q-1)/(p-1)$ and for $s = 0$,

$$\left| |\mathcal{F}_0 \cap \mathcal{A}_d| - \left(\frac{|\mathcal{F}_0^*|}{d} + 1 \right) \right| \leq \frac{p-1}{p} \frac{(d,\delta)-1}{d} \sqrt{q}. \tag{III.6}$$

Note that the term $|\mathcal{F}_s|/d$ in (III.5) (resp. $|\mathcal{F}_0^*|/d + 1$ in (III.6)) is the expected value for $|\mathcal{F}_s \cap \mathcal{A}_d|$ when $s \neq 0$ (resp. for $|\mathcal{F}_0 \cap \mathcal{A}_d|$): the proportion of d-th powers in $\mathbb{F}_q^*$ is $1/d$ and thus if d-th powers were reasonably well distributed then we would expect this proportion to be preserved in $\mathcal{F}_s^*$.

In the special case of squares, we will deduce from Theorem 1.1 the following optimal result:

Corollary 1.4. *If $p \geq 3$ then, for any $s \in \mathbb{F}_p^*$,*

$$\left| |\mathcal{F}_s \cap \mathcal{A}_2| - \frac{|\mathcal{F}_s|}{2} \right| = \begin{cases} \dfrac{\sqrt{q}}{2\sqrt{p}} & \text{if } r \text{ is odd,} \\ \dfrac{\sqrt{q}}{2p} & \text{if } r \text{ is even,} \end{cases}$$

and for $s = 0$,

$$\left| |\mathcal{F}_0 \cap \mathcal{A}_2| - \left(\frac{|\mathcal{F}_0^*|}{2} + 1 \right) \right| = \begin{cases} 0 & \text{if } r \text{ is odd,} \\ \dfrac{p-1}{2p}\sqrt{q} & \text{if } r \text{ is even.} \end{cases}$$

Our next goal will be to generalize Theorem A in the case of several polynomials. For $P_1, \dots, P_\ell \in \mathbb{F}_q[X]$ and for $s_1, \dots, s_\ell \in \mathbb{F}_p$, we define

$$\mathcal{D}(P_1, \dots, P_\ell, s_1, \dots, s_\ell) = \{x \in \mathbb{F}_q : s_{\mathcal{B}}(P_j(x)) = s_j \text{ for all } 1 \leq j \leq \ell\}.$$

We will obtain in Section 3.4:

Theorem 1.5. *For any integer $1 \leq \ell \leq r$, if $P_1, \dots, P_\ell \in \mathbb{F}_q[X]$ are polynomials of same degree $n \geq 1$ with $(n, q) = 1$ and whose leading coefficients are $\mathbb{F}_p$-linearly independent then, for any $s_1, \dots, s_\ell \in \mathbb{F}_p$,*

$$\left| |\mathcal{D}(P_1, \dots, P_\ell, s_1, \dots, s_\ell)| - \frac{q}{p^\ell} \right| \leq (n-1)\sqrt{q};$$

in particular, if $(n-1)p^\ell < \sqrt{q}$ then $\mathcal{D}(P_1, \dots, P_\ell, s_1, \dots, s_\ell) \neq \varnothing$.

Note that, taking $\ell = 1$ in this theorem, we end up with Theorem A.

1.2.2. Sum of digits of rational values

In order to extend Theorem A to rational functions, we define, for a rational function $R = P/Q$ over $\mathbb{F}_q$ and for $s \in \mathbb{F}_p$:

$$\mathcal{D}(R, s) = \{x \in \mathbb{F}_q : Q(x) \neq 0 \text{ and } s_{\mathcal{B}}(R(x)) = s\}.$$

We will obtain in Section 4 the following estimate for $|D(R,s)|$:

Theorem 1.6. *If $R = P/Q$ is a rational function over $\mathbb{F}_q$ satisfying*

$$\begin{cases} P \neq 0, \\ \deg(P) - \deg(Q) \not\equiv 0 \bmod p \text{ or } \deg(P) < \deg(Q), \\ Q \text{ is not divisible by the } p\text{-th power of a nonconstant} \\ \text{polynomial over } \overline{\mathbb{F}_q}, \end{cases} \tag{III.7}$$

then, for any $s \in \mathbb{F}_p$,

$$\left| |\mathcal{D}(R,s)| - \frac{v}{p} \right| \leq ((\max(\deg P, \deg Q) + \alpha^* - 2)\sqrt{q} + \beta)$$

where

- $v = |\{x \in \mathbb{F}_q : Q(x) \neq 0\}|$,
- *α is the number of distinct roots of the polynomial Q in the algebraic closure $\overline{\mathbb{F}_q}$ of $\mathbb{F}_q$,*
- *$(\alpha^*, \beta) = (\alpha, 1)$ if $\deg P \leq \deg Q$ and $(\alpha^*, \beta) = (\alpha + 1, 0)$ otherwise.*

Note that, taking $Q = 1$ in this theorem, we end up with Theorem A.

1.2.3. Sum of digits of polynomial values with generator arguments

We denote by $\mathcal{G}$ the set of generators (i.e. primitive elements) of $\mathbb{F}_q^*$. The Euler's totient function will be denoted by φ and for $m \geq 1$, the number of distinct prime factors of m will be denoted by $\omega(m)$. For $P \in \mathbb{F}_q[X]$ and for $s \in \mathbb{F}_p$, we define

$$\mathcal{D}_{\mathcal{G}}(P,s) = \{g \in \mathcal{G} : s_{\mathcal{B}}(P(g)) = s\} = \mathcal{D}(P,s) \cap \mathcal{G}.$$

In [12], Dartyge and Sárközy obtained an estimate for $|\mathcal{D}_{\mathcal{G}}(P,s)|$ for any $s \in \mathbb{F}_p$ and for any polynomial $P \in \mathbb{F}_q[X]$ whose degree is coprime with q. Their proof leads to

Theorem B. *If $P \in \mathbb{F}_q[X]$ is a polynomial of degree $n \geq 1$ with $(n,q) = 1$ then, for any $s \in \mathbb{F}_p$,*

$$\left| |\mathcal{D}_{\mathcal{G}}(P,s)| - \frac{\varphi(q-1)}{p} \right| \leq (n2^{\omega(q-1)} - 1)\sqrt{q} + \frac{\varphi(q-1)}{q-1}. \tag{III.8}$$

In this paper, we will improve (III.8) and obtain in Section 5.2:

Theorem 1.7. *If $P \in \mathbb{F}_q[X]$ is a polynomial of degree $n \geq 1$ with $(n,q) = 1$ then, for any $s \in \mathbb{F}_p$,*

$$\left| |\mathcal{D}_{\mathcal{G}}(P,s)| - \frac{\varphi(q-1)}{p} \right| < \frac{\varphi(q-1)}{q-1} \left((n2^{\omega(q-1)} - 1)\sqrt{q} + 1 \right). \tag{III.9}$$

In the special case where P is a monomial, we will be able to further improve the upper bound in (III.9). We will show in Section 5.3 that for any monomial $aX^n \in \mathbb{F}_q[X]$ and for any

$s \in \mathbb{F}_p$, we have $|\mathcal{D}_{\mathcal{G}}(aX^n, s)| = |\mathcal{D}_{\mathcal{G}}(aX^d, s)|$ where $d = (n, q-1)$. Thus, it suffices to study $|\mathcal{D}_{\mathcal{G}}(P, s)|$ for monomials P whose degree divides $q-1$. We will obtain the following sharper estimate for $|\mathcal{D}_{\mathcal{G}}(aX^d, s)|$:

Theorem 1.8. *If d divides $q-1$ and if $a \in \mathbb{F}_q^*$ then, for any $s \in \mathbb{F}_p^*$,*

$$\left| \left|\mathcal{D}_{\mathcal{G}}(aX^d, s)\right| - \frac{q}{p}\frac{\varphi(q-1)}{q-1} \right| \leq \frac{\varphi(q-1)}{q-1}\left(d\, 2^{\omega\left(\frac{q-1}{d}\right)} - 1\right)\frac{\sqrt{q}}{\sqrt{p}},$$

and for $s = 0$,

$$\left| \left|\mathcal{D}_{\mathcal{G}}(aX^d, 0)\right| - \left(\frac{q}{p} - 1\right)\frac{\varphi(q-1)}{q-1} \right| \leq \frac{\varphi(q-1)}{q-1}\frac{p-1}{p}\left((d,\delta)2^{\omega\left(\frac{\delta}{(d,\delta)}\right)} - 1\right)\sqrt{q}$$

where δ is the integer defined by $\delta = (q-1)/(p-1)$.

For $s \neq 0$, Theorem 1.8 permits us to improve (III.9) by a factor at least $1/\sqrt{p}$.

Theorem 1.8 will be proved in Section 5.3 and it will appear as a consequence of a slightly more precise estimate for $\left|\mathcal{D}_{\mathcal{G}}(aX^d, s)\right|$ (see Theorem 5.6).

We will see that, for any divisor d of $q-1$, Theorem 1.8 provides an estimate for the number of elements of order d whose sum of digits is prescribed. For any divisor d of $q-1$, we denote by $\mathcal{O}_d$ the set of elements of order d in $\mathbb{F}_q^*$. In Section 5.4, we will deduce the following estimate for $|\mathcal{F}_s \cap \mathcal{O}_d|$:

Corollary 1.9. *If d divides $q-1$ then, for any $s \in \mathbb{F}_p^*$,*

$$\left| |\mathcal{F}_s \cap \mathcal{O}_d| - |\mathcal{F}_s|\frac{\varphi(d)}{q-1} \right| \leq \frac{\varphi(d)}{q-1}\left(\frac{q-1}{d}\, 2^{\omega(d)} - 1\right)\frac{\sqrt{q}}{\sqrt{p}}, \tag{III.10}$$

and for $s = 0$,

$$\left| |\mathcal{F}_0 \cap \mathcal{O}_d| - |\mathcal{F}_0^*|\frac{\varphi(d)}{q-1} \right| \leq \frac{\varphi(d)}{q-1}\frac{p-1}{p}\left((d',\delta)2^{\omega\left(\frac{\delta}{(d',\delta)}\right)} - 1\right)\sqrt{q} \tag{III.11}$$

where δ is the integer defined by $\delta = (q-1)/(p-1)$ and $d' = (q-1)/d$.

Note that the term $|\mathcal{F}_s|\varphi(d)/(q-1)$ in (III.10) (resp. $|\mathcal{F}_0^*|\varphi(d)/(q-1)$ in (III.11)) is the expected value for $|\mathcal{F}_s \cap \mathcal{O}_d|$ when $s \neq 0$ (resp. for $|\mathcal{F}_0 \cap \mathcal{O}_d|$): the proportion of elements of order d in $\mathbb{F}_q^*$ is $\varphi(d)/(q-1)$ and thus if elements of order d were reasonably well distributed then we would expect this proportion to be preserved in $\mathcal{F}_s^*$.

In order to extend Theorem 1.7, we will finally provide an estimate for the number of generators $g \in \mathcal{G}$ such that $s_{\mathcal{B}}(P(g))$ is prescribed for several polynomials P i.e. an estimate for $|\mathcal{D}_{\mathcal{G}}(P_1, \ldots, P_\ell, s_1, \ldots, s_\ell)|$ where $P_1, \ldots, P_\ell \in \mathbb{F}_q[X]$, $s_1, \ldots, s_\ell \in \mathbb{F}_p$ and $\mathcal{D}_{\mathcal{G}}(P_1, \ldots, P_\ell, s_1, \ldots, s_\ell)$ is the set defined by

$$\mathcal{D}_{\mathcal{G}}(P_1, \ldots, P_\ell, s_1, \ldots, s_\ell) = \{g \in \mathcal{G} : s_{\mathcal{B}}(P_j(g)) = s_j \text{ for all } 1 \leq j \leq \ell\}.$$

We will obtain in Section 5.5:

Theorem 1.10. *For any integer $1 \leq \ell \leq r$, if $P_1, \dots, P_\ell \in \mathbb{F}_q[X]$ are polynomials of same degree $n \geq 1$ with $(n, q) = 1$ and whose leading coefficients are $\mathbb{F}_p$-linearly independent then, for any $s_1, \dots, s_\ell \in \mathbb{F}_p$,*

$$\left| |\mathcal{D}_{\mathcal{G}}(P_1, \dots, P_\ell, s_1, \dots, s_\ell)| - \frac{\varphi(q-1)}{p^\ell} \right| < \frac{\varphi(q-1)}{q-1} \left((n 2^{\omega(q-1)} - 1)\sqrt{q} + 1 \right);$$

in particular, if

$$np^\ell \leq \sqrt{q}/2^{\omega(q-1)} \tag{III.12}$$

then $\mathcal{D}_{\mathcal{G}}(P_1, \dots, P_\ell, s_1, \dots, s_\ell) \neq \varnothing$.

Note that, taking $\ell = 1$ in this theorem, we end up with Theorem 1.7.

Remark 1.11. One may wonder if condition (III.12) is not too restrictive. Heuristically, according to the normal order of the ω function (see [28], Theorem 431), for almost all values of q, it is expected that $\omega(q-1) = O(\log\log q)$. Under this assumption, condition (III.12) would become

$$np^\ell \leq \frac{\sqrt{q}}{(\log q)^K}$$

for some constant $K > 0$, so that in most cases condition (III.12) is not too restrictive as $q \to \infty$.

1.3. Notations

We use the notation $\mathrm{e}(t) = \exp(2i\pi t)$.

The trivial additive character of $\mathbb{F}_q$ is denoted by ψ_0 and the trivial multiplicative character of $\mathbb{F}_q$ is denoted by χ_0. The trivial multiplicative character of $\mathbb{F}_p$ is simply denoted by 1. The field $\mathbb{F}_p$ will be seen as a subfield of $\mathbb{F}_q$ so that every multiplicative character χ of $\mathbb{F}_q$ induces a multiplicative character of $\mathbb{F}_p$ denoted by $\chi_{|\mathbb{F}_p^*}$.

We introduce the following notations for Gaussian sums. If χ is a multiplicative character of $\mathbb{F}_p$, let $\tau(\chi)$ be the Gaussian sum

$$\tau(\chi) = \sum_{j \in \mathbb{F}_p^*} \mathrm{e}\left(\frac{j}{p}\right) \chi(j).$$

If ψ is an additive character of $\mathbb{F}_q$ and if χ is a multiplicative character of $\mathbb{F}_q$, let $G(\chi, \psi)$ be the Gaussian sum

$$G(\chi, \psi) = \sum_{x \in \mathbb{F}_q^*} \chi(x)\psi(x).$$

For $s \in \mathbb{F}_p$ and for a multiplicative character χ of $\mathbb{F}_q$, we denote by $S(\chi, s)$ the sum

$$S(\chi, s) = \sum_{\substack{x \in \mathbb{F}_q^* \\ s_{\mathcal{B}}(x) = s}} \chi(x). \tag{III.13}$$

The trace Tr of $\mathbb{F}_q$ over $\mathbb{F}_p$ defined for $x \in \mathbb{F}_q$ by:

$$\mathrm{Tr}(x) = x + x^p + \cdots + x^{p^{r-1}}$$

is an $\mathbb{F}_p$-linear form (see Theorem 2.23 of [38]) and permits defining the canonical additive character ψ_1 of $\mathbb{F}_q$ by:

$$\psi_1(x) = \mathrm{e}\left(\frac{\mathrm{Tr}(x)}{p}\right). \tag{III.14}$$

We define $\mathbb{1}_{X=Y}$ by

$$\mathbb{1}_{X=Y} = \begin{cases} 1 & \text{if } X = Y, \\ 0 & \text{otherwise.} \end{cases}$$

2. Preparations

The following Weil bound will play an important role in the proofs.

Theorem 2.1 (Weil)**.** *Let $P \in \mathbb{F}_q[X]$ be of degree $n \geq 1$ with $(n, q) = 1$ and let ψ be a nontrivial additive character of $\mathbb{F}_q$. Then,*

$$\left| \sum_{x \in \mathbb{F}_q} \psi(P(x)) \right| \leq (n-1)\sqrt{q}.$$

Proof. See [38], Theorem 5.38 p. 223. □

Lemma 2.2. *If ψ is an additive character of $\mathbb{F}_q$ and χ is a multiplicative character of $\mathbb{F}_q$ then*

$$G(\chi, \psi) = \begin{cases} q-1 & \text{if } \chi = \chi_0 \text{ and } \psi = \psi_0, \\ -1 & \text{if } \chi = \chi_0 \text{ and } \psi \neq \psi_0, \\ 0 & \text{if } \chi \neq \chi_0 \text{ and } \psi = \psi_0, \end{cases}$$

and $|G(\chi, \psi)| = \sqrt{q}$ if $\chi \neq \chi_0$ and $\psi \neq \psi_0$.

In the special case where χ is a multiplicative character of $\mathbb{F}_p$, $|\tau(\chi)| = \sqrt{p}$ if χ is nontrivial and $\tau(\chi) = -1$ if χ is trivial.

Proof. See Theorem 5.11 of [38]. □

The following lemma will be of basic interest in the proof of most of our results.

Lemma 2.3. *If χ is a nontrivial multiplicative character of $\mathbb{F}_q$ and if $s \in \mathbb{F}_p$ then*

$$S(\chi, s) = \begin{cases} \overline{\chi}(b)\chi(s)\,\dfrac{G(\chi,\psi_1)}{\tau(\chi_{|\mathbb{F}_p^*})} & \text{if } s \neq 0 \text{ and } \chi_{|\mathbb{F}_p^*} \neq 1, \\ -\overline{\chi}(b)\,\dfrac{G(\chi,\psi_1)}{p} & \text{if } s \neq 0 \text{ and } \chi_{|\mathbb{F}_p^*} = 1, \\ 0 & \text{if } s = 0 \text{ and } \chi_{|\mathbb{F}_p^*} \neq 1, \\ \overline{\chi}(b)\,\dfrac{p-1}{p} G(\chi,\psi_1) & \text{if } s = 0 \text{ and } \chi_{|\mathbb{F}_p^*} = 1, \end{cases} \tag{III.15}$$

where ψ_1 is defined by (III.14) and b is the element of $\mathbb{F}_q^*$ such that for any $x \in \mathbb{F}_q$, $s_{\mathcal{B}}(x) = \mathrm{Tr}(bx)$.

The existence of a unique $b \in \mathbb{F}_q^*$ such that, for any $x \in \mathbb{F}_q$, $s_{\mathcal{B}}(x) = \mathrm{Tr}(bx)$ follows from the fact that $s_{\mathcal{B}}$ is a linear form and from Theorem 2.24 of [38].

Proof. Let χ be a nontrivial multiplicative character of $\mathbb{F}_q$. As in [2], we define the Eisentein sum $E(\chi)$ by

$$E(\chi) = \sum_{\substack{x \in \mathbb{F}_q^* \\ \mathrm{Tr}(x)=1}} \chi(x).$$

If $s \in \mathbb{F}_p^*$ then the sum $S(\chi, s)$ is related to $E(\chi)$ by

$$S(\chi, s) = \sum_{\substack{x \in \mathbb{F}_q^* \\ \mathrm{Tr}(s^{-1}bx)=1}} \chi(x) = \sum_{\substack{y \in \mathbb{F}_q^* \\ \mathrm{Tr}(y)=1}} \chi(sb^{-1}y) = \overline{\chi}(b)\chi(s)E(\chi).$$

Moreover, by Theorem 12.1.1 of [2],

$$E(\chi) = \begin{cases} \dfrac{G(\chi,\psi_1)}{\tau(\chi_{|\mathbb{F}_p^*})} & \text{if } \chi_{|\mathbb{F}_p^*} \neq 1, \\ \dfrac{-G(\chi,\psi_1)}{p} & \text{if } \chi_{|\mathbb{F}_p^*} = 1. \end{cases} \tag{III.16}$$

This proves (III.15) in the case where $s \in \mathbb{F}_p^*$ (note that if $\chi_{|\mathbb{F}_p^*} = 1$ then $\chi(s) = 1$). For $s = 0$, we write

$$S(\chi, 0) = \sum_{\substack{x \in \mathbb{F}_q^* \\ \mathrm{Tr}(bx)=0}} \chi(x) = \overline{\chi}(b) \sum_{\substack{y \in \mathbb{F}_q^* \\ \mathrm{Tr}(y)=0}} \chi(y)$$

where by Lemma 12.0.2 of [2] and by (III.16)

$$\sum_{\substack{y \in \mathbb{F}_q^* \\ \mathrm{Tr}(y)=0}} \chi(x) = \begin{cases} 0 & \text{if } \chi_{|\mathbb{F}_p^*} \neq 1, \\ -(p-1)E(\chi) = \dfrac{(p-1)G(\chi,\psi_1)}{p} & \text{if } \chi_{|\mathbb{F}_p^*} = 1. \end{cases}$$

This proves (III.15) in the case where $s = 0$. □

We deduce from Lemma 2.3 and Lemma 2.2 an exact formula for the absolute value of character sums over elements whose sum of digits is fixed.

Corollary 2.4. *If χ is a nontrivial multiplicative character of $\mathbb{F}_q$ and if $s \in \mathbb{F}_p$ then*

$$|S(\chi, s)| = \begin{cases} \dfrac{\sqrt{q}}{\sqrt{p}} & \text{if } s \neq 0 \text{ and } \chi_{|\mathbb{F}_p^*} \neq 1, \\ \dfrac{\sqrt{q}}{p} & \text{if } s \neq 0 \text{ and } \chi_{|\mathbb{F}_p^*} = 1, \\ 0 & \text{if } s = 0 \text{ and } \chi_{|\mathbb{F}_p^*} \neq 1, \\ \dfrac{p-1}{p}\sqrt{q} & \text{if } s = 0 \text{ and } \chi_{|\mathbb{F}_p^*} = 1. \end{cases}$$

Proof. Since $\chi \neq \chi_0$ and $\psi_1 \neq \psi_0$, this result follows immediately from Lemma 2.3 and Lemma 2.2. □

From now on, g_0 denotes a generator of the cyclic group $\mathbb{F}_q^*$. The following lemmas regarding the structure of multiplicative characters of $\mathbb{F}_q$ will also play an important role in the proofs.

Lemma 2.5. *The multiplicative characters of $\mathbb{F}_q$ are $\chi_1, \ldots, \chi_{q-1}$ where, for every $1 \leq j \leq q-1$, χ_j is defined by*

$$\chi_j(g_0^k) = \mathrm{e}\left(\frac{jk}{q-1}\right) \tag{III.17}$$

for any $1 \leq k \leq q-1$.

Proof. See Theorem 5.8 of [38]. □

Lemma 2.6. *For any $1 \leq j \leq q-1$, the multiplicative character χ_j of $\mathbb{F}_q$ defined by (III.17) satisfies: $\chi_{j\,|\mathbb{F}_p^*} = 1$ if and only if $p-1$ divides j.*

Proof. We consider $g_1 = g_0^{\frac{q-1}{p-1}} \in \mathbb{F}_p^*$. Since g_0 is a generator of $\mathbb{F}_q^*$, g_1 is a generator of $\mathbb{F}_p^*$. It follows that for $1 \leq j \leq q-1$, $\chi_{j\,|\mathbb{F}_p^*} = 1$ if and only if $\chi_j(g_1) = 1$. Moreover, by (III.17), $\chi_j(g_1) = \mathrm{e}\left(\frac{j}{p-1}\right)$ and thus $\chi_j(g_1) = 1$ if and only if $p-1$ divides j, which completes the proof. □

3. Sum of digits of polynomial values

3.1. Proof of Theorem 1.1

In this section, we denote by η the quadratic character of $\mathbb{F}_q$. Theorem 1.1 will be an immediate consequence of the following result which provides an exact formula for $|\mathcal{D}(P, s)|$:

Theorem 3.1. *If $p \geq 3$ and if $P(X) = a_2X^2 + a_1X + a_0 \in \mathbb{F}_q[X]$ with $a_2 \neq 0$ then, for any $s \in \mathbb{F}_p$,*

$$|\mathcal{D}(P,s)| - \frac{q}{p} = \begin{cases} I_p^{r-1}\eta(a_2b(s-\nu_P))\dfrac{\sqrt{q}}{\sqrt{p}} & \text{if } s \neq \nu_P \text{ and } r \text{ is odd,} \\ I_p^r\eta(a_2b)\dfrac{\sqrt{q}}{p} & \text{if } s \neq \nu_P \text{ and } r \text{ is even,} \\ 0 & \text{if } s = \nu_P \text{ and } r \text{ is odd,} \\ -I_p^r\eta(a_2b)\dfrac{p-1}{p}\sqrt{q} & \text{if } s = \nu_P \text{ and } r \text{ is even,} \end{cases}$$

where

- $\nu_P = s_{\mathcal{B}}(a_0 - a_1^2(4a_2)^{-1})$,
- $I_p = 1$ *if* $p \equiv 1 \bmod 4$ *and* $I_p = i$ *if* $p \equiv 3 \bmod 4$,
- b *is the element of* $\mathbb{F}_q^*$ *such that for any* $x \in \mathbb{F}_q$, $s_{\mathcal{B}}(x) = \mathrm{Tr}(bx)$.

Remark 3.2. If $p = 2$ then any element of $\mathbb{F}_q$ is a square (the mapping F defined by $F(x) = x^2$ for $x \in \mathbb{F}_{2^r}$ is the Frobenius automorphism of $\mathbb{F}_{2^r}$ over $\mathbb{F}_2$); in particular there exists $\alpha \in \mathbb{F}_q$ such that $ba_2 = \alpha^2$ and thus, since $\mathrm{Tr}(y^2) = \mathrm{Tr}(y)$ for any $y \in \mathbb{F}_{2^r}$ (see Theorem 2.23 of [38]):

$$s_{\mathcal{B}}(a_2x^2 + a_1x) = \mathrm{Tr}((\alpha x)^2 + ba_1x) = \mathrm{Tr}((\alpha + ba_1)x)$$

and it follows that if $\alpha + ba_1 \neq 0$ then $|\mathcal{D}(a_2X^2 + a_1X + a_0, s)| = q/p$ and if $\alpha + ba_1 = 0$ then $|\mathcal{D}(a_2X^2 + a_1X + a_0, s)| = q\,\mathbb{1}_{s - s_{\mathcal{B}}(a_0) = 0}$.

Remark 3.3. In [38], the existence of b is proved by a counting argument. One may wonder how to construct b. For instance, we can consider a generator g of $\mathbb{F}_q^*$ and the associated basis $\mathcal{B}_g = \{1, g, \ldots, g^{r-1}\}$ of $\mathbb{F}_q$. Then, writing $s_{\mathcal{B}}(g^k) = \mathrm{Tr}(bg^k)$ for all $0 \leq k \leq r-1$, we end up with a linear system of r equations and r variables $b, b^p, \ldots, b^{p^{r-1}}$ that can be solved by inverting a Vandermonde matrix.

To prove Theorem 3.1, we will need the two following lemmas.

Lemma 3.4. *For any $p \geq 3$, the quadratic character η of $\mathbb{F}_q$ satisfies*

$$\eta_{|\mathbb{F}_p^*} = \begin{cases} \gamma & \text{if } r \text{ is odd,} \\ 1 & \text{if } r \text{ is even,} \end{cases}$$

where γ is the quadratic character of $\mathbb{F}_p$.

Proof. See for instance [66], Lemma 5.1. □

Lemma 3.5. *For any $p \geq 3$, the Gaussian sums $G(\eta, \psi_1)$ and $\tau(\gamma)$ satisfy*

$$G(\eta, \psi_1) = (-1)^{r-1}I_p^r\sqrt{q} \quad \text{and} \quad \tau(\gamma) = I_p\sqrt{p}$$

where $I_p = 1$ if $p \equiv 1 \bmod 4$ and $I_p = i$ if $p \equiv 3 \bmod 4$.

Proof. See Theorem 5.15 of [38]. □

We will first prove the following result which establishes Theorem 3.1 in the case where $P(X) = aX^2$ with $a \in \mathbb{F}_q^*$.

Proposition 3.6. *If $p \geq 3$ and if $a \in \mathbb{F}_q^*$ then, for any $s \in \mathbb{F}_p$,*

$$|\mathcal{D}(aX^2, s)| - \frac{q}{p} = \begin{cases} I_p^{r-1}\eta(abs)\dfrac{\sqrt{q}}{\sqrt{p}} & \text{if } s \neq 0 \text{ and } r \text{ is odd,} \\ I_p^r\eta(ab)\dfrac{\sqrt{q}}{p} & \text{if } s \neq 0 \text{ and } r \text{ is even,} \\ 0 & \text{if } s = 0 \text{ and } r \text{ is odd,} \\ -I_p^r\eta(ab)\dfrac{p-1}{p}\sqrt{q} & \text{if } s = 0 \text{ and } r \text{ is even,} \end{cases}$$

where

- *$I_p = 1$ if $p \equiv 1 \bmod 4$ and $I_p = i$ if $p \equiv 3 \bmod 4$,*
- *b is the element of $\mathbb{F}_q^*$ such that for any $x \in \mathbb{F}_q$, $s_{\mathcal{B}}(x) = \mathrm{Tr}(bx)$.*

Proof. Let $a \in \mathbb{F}_q^*$ and $s \in \mathbb{F}_p$. The number of $x \in \mathbb{F}_q$ such that $s_{\mathcal{B}}(ax^2) = s$ is given by

$$\begin{aligned} |\mathcal{D}(aX^2, s)| &= \sum_{\substack{y \in \mathbb{F}_q \\ s_{\mathcal{B}}(y) = s}} \sum_{x \in \mathbb{F}_q} \mathbb{1}_{ax^2 = y} = \mathbb{1}_{s_{\mathcal{B}}(0) = s} \sum_{x \in \mathbb{F}_q} \mathbb{1}_{ax^2 = 0} + \sum_{\substack{y \in \mathbb{F}_q^* \\ s_{\mathcal{B}}(y) = s \\ a^{-1}y \text{ is a square}}} 2 \\ &= \mathbb{1}_{s=0} + \sum_{\substack{y \in \mathbb{F}_q^* \\ s_{\mathcal{B}}(y) = s}} (1 + \eta(a^{-1}y)) \end{aligned}$$

thus, since the number of $y \in \mathbb{F}_q$ such that $s_{\mathcal{B}}(y) = s$ is q/p,

$$|\mathcal{D}(aX^2, s)| = \frac{q}{p} + \eta(a)S(\eta, s)$$

where $S(\eta, s)$ is defined by (III.13). By Lemma 2.3 and Lemma 3.4, $S(\eta, s)$ is given by

$$S(\eta, s) = \begin{cases} \eta(b)\eta(s)\,\dfrac{G(\eta, \psi_1)}{\tau(\gamma)} & \text{if } s \neq 0 \text{ and } r \text{ is odd,} \\ -\eta(b)\,\dfrac{G(\eta, \psi_1)}{p} & \text{if } s \neq 0 \text{ and } r \text{ is even,} \\ 0 & \text{if } s = 0 \text{ and } r \text{ is odd,} \\ \eta(b)\,\dfrac{p-1}{p}G(\eta, \psi_1) & \text{if } s = 0 \text{ and } r \text{ is even,} \end{cases} \tag{III.18}$$

where b is defined as in Lemma 2.3. To complete the proof of Proposition 3.6, it suffices to insert the expressions of $G(\eta, \psi_1)$ and $\tau(\gamma)$ given by Lemma 3.5 into (III.18). □

Theorem 3.1 is then a straightforward consequence of Proposition 3.6. Let $P(X) = a_2X^2 + a_1X + a_0 \in \mathbb{F}_q[X]$ with $a_2 \neq 0$ and let $s \in \mathbb{F}_p$. Since $P(X) = a_2(X-\alpha)^2 + \beta$ where $\alpha = -a_1(2a_2)^{-1}$ and $\beta = a_0 - a_1^2(4a_2)^{-1}$, denoting $\nu_P = s_{\mathcal{B}}(\beta)$, we have

$$|\mathcal{D}(P,s)| = |\{x \in \mathbb{F}_q : s_{\mathcal{B}}\left(a_2(x-\alpha)^2\right) = s - \nu_P\}| = |\mathcal{D}(a_2X^2, s-\nu_P)|.$$

Applying Proposition 3.6 to $|\mathcal{D}(a_2X^2, s-\nu_P)|$, we obtain the expected exact formula for $|\mathcal{D}(P,s)|$, which completes the proof of Theorem 3.1.

3.2. Sum of digits of monomials and proof of Theorem 1.2

We first show that the study of $|\mathcal{D}(P,s)|$ where P is a monomial may be reduced to the case where the degree of P divides $q-1$. Let $n \geq 1$ and denote $d = (n, q-1)$. The set of n-th powers in $\mathbb{F}_q^*$ equals the set of d-th powers in $\mathbb{F}_q^*$ and for any n-th power $y \in \mathbb{F}_q^*$, there are exactly d elements $x \in \mathbb{F}_q^*$ such that $y = x^n$ (see Lemma 2D p. 13 of [61]). It follows that for any $a \in \mathbb{F}_q^*$ and for any $s \in \mathbb{F}_p$,

$$\begin{aligned} |\mathcal{D}(aX^n, s) \setminus \{0\}| &= d \cdot |\mathcal{A}_n \cap \{y \in \mathbb{F}_q^* : s_{\mathcal{B}}(ay) = s\}| \\ &= d \cdot |\mathcal{A}_d \cap \{y \in \mathbb{F}_q^* : s_{\mathcal{B}}(ay) = s\}| \\ &= |\mathcal{D}(aX^d, s) \setminus \{0\}| \end{aligned} \tag{III.19}$$

where $\mathcal{A}_n$ (resp. $\mathcal{A}_d$) is the set of n-th (resp. d-th) powers in $\mathbb{F}_q$ and thus

$$|\mathcal{D}(aX^n, s)| = |\mathcal{D}(aX^d, s)|.$$

We will now obtain the following result which provides a sharp estimate for $|\mathcal{D}(aX^d, s)|$ as soon as d divides $q-1$.

Theorem 3.7. *If d divides $q-1$ and if $a \in \mathbb{F}_q^*$ then, for any $s \in \mathbb{F}_p^*$,*

$$\left| \left|\mathcal{D}(aX^d, s)\right| - \frac{q}{p} \right| \leq \left(d - (d,\delta)\left(1 - \frac{1}{\sqrt{p}}\right) - \frac{1}{\sqrt{p}} \right) \frac{\sqrt{q}}{\sqrt{p}}$$

where δ is the integer defined by $\delta = (q-1)/(p-1)$ and for $s = 0$,

$$\left| \left|\mathcal{D}(aX^d, 0)\right| - \frac{q}{p} \right| \leq \frac{p-1}{p}\left((d,\delta) - 1\right)\sqrt{q}.$$

Theorem 1.2 is an immediate consequence of Theorem 3.7. To prove Theorem 3.7, we will need the following lemma.

Lemma 3.8. *For any integer $1 \leq j \leq q-1$, the multiplicative character χ_j of $\mathbb{F}_q$ defined by (III.17) satisfies for any $n \geq 1$:*

$$\sum_{x \in \mathbb{F}_q^*} \chi_j^n(x) = \begin{cases} q-1 & \text{if } q-1 \,|\, nj, \\ 0 & \text{otherwise.} \end{cases}$$

Proof. It suffices to write

$$\sum_{x \in \mathbb{F}_q^*} \chi_j^n(x) = \sum_{1 \leq k \leq q-1} \chi_j^n\left(g_0^k\right) = \sum_{1 \leq k \leq q-1} \mathrm{e}\left(\frac{njk}{q-1}\right)$$

which is equal to $q-1$ if $q-1 \,|\, nj$ and 0 otherwise. □

We are now able to prove Theorem 3.7. Let d be a divisor of $q-1$, let $a \in \mathbb{F}_q^*$ and $s \in \mathbb{F}_p$. Since $\mathcal{D}(aX^d, s) = \{x \in \mathbb{F}_q : s_{\mathcal{B}}(ax^d) = s\}$, we have

$$\left|\mathcal{D}(aX^d, s)\right| = \sum_{\substack{y \in \mathbb{F}_q \\ s_{\mathcal{B}}(y)=s}} \sum_{x \in \mathbb{F}_q} \mathbb{1}_{ax^d=y} = \mathbb{1}_{s_{\mathcal{B}}(0)=s} \sum_{x \in \mathbb{F}_q} \mathbb{1}_{ax^d=0} + \sum_{\substack{y \in \mathbb{F}_q^* \\ s_{\mathcal{B}}(y)=s}} \sum_{x \in \mathbb{F}_q^*} \mathbb{1}_{ax^d=y}.$$

Since $\sum_{x \in \mathbb{F}_q} \mathbb{1}_{ax^d=0} = 1$, using the orthogonality relations for multiplicative characters of $\mathbb{F}_q$ to detect the equality $ax^d = y$, we obtain:

$$\begin{aligned} \left|\mathcal{D}(aX^d, s)\right| &= \mathbb{1}_{s=0} + \frac{1}{q-1} \sum_{\chi} \left(\sum_{x \in \mathbb{F}_q^*} \chi(ax^d) \right) \left(\sum_{\substack{y \in \mathbb{F}_q^* \\ s_{\mathcal{B}}(y)=s}} \overline{\chi}(y) \right) \\ &= \mathbb{1}_{s=0} + \frac{1}{q-1} \sum_{\chi} \chi(a) \left(\sum_{x \in \mathbb{F}_q^*} \chi^d(x) \right) S(\overline{\chi}, s) \end{aligned}$$

where $S(\overline{\chi}, s)$ is defined by (III.13). In the right-hand side sum, the main term is provided by $\chi = \chi_0$ and since the number of $y \in \mathbb{F}_q$ such that $s_{\mathcal{B}}(y) = s$ is q/p,

$$\left|\mathcal{D}(aX^d, s)\right| = \frac{q}{p} + \frac{1}{q-1} \sum_{\chi \neq \chi_0} \chi(a) \left(\sum_{x \in \mathbb{F}_q^*} \chi^d(x) \right) S(\overline{\chi}, s).$$

The nontrivial multiplicative characters of $\mathbb{F}_q$ are $\chi_1, \ldots, \chi_{q-2}$ defined by (III.17) and it follows that

$$\left|\mathcal{D}(aX^d, s)\right| - \frac{q}{p} = \frac{1}{q-1} \sum_{1 \leq j < q-1} \chi_j(a) \left(\sum_{x \in \mathbb{F}_q^*} \chi_j^d(x) \right) S(\overline{\chi_j}, s)$$

and by Lemma 3.8

$$\left|\mathcal{D}(aX^d, s)\right| - \frac{q}{p} = \sum_{\substack{1 \leq j < q-1 \\ q-1 \,|\, dj}} \chi_j(a) S(\overline{\chi_j}, s).$$

Moreover, by Lemma 2.6, for $1 \le j \le q-1$, $\chi_{j\,|\mathbb{F}_p^*} = 1$ if and only if $p-1$ divides j. Thus, by Corollary 2.4, if $s \neq 0$ then

$$\left|\left|\mathcal{D}(aX^d, s)\right| - \frac{q}{p}\right| \le \frac{\sqrt{q}}{\sqrt{p}} \sum_{\substack{1\le j\le q-1 \\ q-1\,|\,dj \\ p-1\nmid j}} 1 + \frac{\sqrt{q}}{p} \sum_{\substack{1\le j<q-1 \\ q-1\,|\,dj \\ p-1\,|\,j}} 1 \tag{III.20}$$

and for $s = 0$,

$$\left|\left|\mathcal{D}(aX^d, 0)\right| - \frac{q}{p}\right| \le \frac{p-1}{p}\sqrt{q} \sum_{\substack{1\le j<q-1 \\ q-1\,|\,dj \\ p-1\,|\,j}} 1. \tag{III.21}$$

Since $\delta = (q-1)/(p-1)$, writing

$$\sum_{\substack{1\le j\le q-1 \\ q-1\,|\,dj \\ p-1\,|\,j}} 1 = \sum_{\substack{1\le u\le \delta \\ q-1\,|\,du(p-1)}} 1 = \sum_{\substack{1\le u\le \delta \\ \delta\,|\,du}} 1 = \sum_{\substack{1\le u\le \delta \\ \frac{\delta}{(d,\delta)}\,|\,u}} 1 = (d,\delta)$$

and

$$\sum_{\substack{1\le j\le q-1 \\ q-1\,|\,dj \\ p-1\nmid j}} 1 = \sum_{\substack{1\le j\le q-1 \\ q-1\,|\,dj}} 1 - \sum_{\substack{1\le j\le q-1 \\ q-1\,|\,dj \\ p-1\,|\,j}} 1 = d - (d,\delta),$$

(III.20) becomes, for $s \neq 0$,

$$\left|\left|\mathcal{D}(aX^d, s)\right| - \frac{q}{p}\right| \le \frac{\sqrt{q}}{\sqrt{p}}(d - (d,\delta)) + \frac{\sqrt{q}}{p}((d,\delta) - 1)$$

and (III.21) becomes

$$\left|\left|\mathcal{D}(aX^d, 0)\right| - \frac{q}{p}\right| \le \frac{p-1}{p}\sqrt{q}((d,\delta) - 1)$$

which completes the proof of Theorem 3.7.

3.3. Proof of Corollaries 1.3 and 1.4

To prove Corollary 1.3 (resp. Corollary 1.4), it suffices to remark that if d divides $q-1$ then, by (III.19), we have:

- for $s \in \mathbb{F}_p^*$, $|\mathcal{F}_s| = q/p$ and $|\mathcal{D}(X^d, s)| = d \cdot |\mathcal{F}_s \cap \mathcal{A}_d|$,
- for $s = 0$, $|\mathcal{F}_0^*| = q/p - 1$ and $|\mathcal{D}(X^d, 0)| = d(|\mathcal{F}_0 \cap \mathcal{A}_d| - 1) + 1$

and to apply Theorem 1.2 (resp. Theorem 1.1).

3.4. Proof of Theorem 1.5

For each $1 \le j \le \ell$, the condition $s_{\mathcal{B}}(P_j(x)) = s_j$ can be handled with an exponential sum by using the classical equality:

$$\frac{1}{p}\sum_{j=0}^{p-1} \mathrm{e}\left(\frac{ja}{p}\right) = \begin{cases} 1 & \text{if } a \equiv 0 \bmod p, \\ 0 & \text{otherwise.} \end{cases}$$

This permits us to detect the elements of $\mathcal{D}(P_1, \dots, P_\ell, s_1, \dots, s_\ell)$ by a product of exponential sums as follows:

$$\begin{aligned} |\mathcal{D}(P_1, \dots, P_\ell, s_1, \dots, s_\ell)| &= \sum_{x \in \mathbb{F}_q} \prod_{j=1}^{\ell} \left(\frac{1}{p} \sum_{h_j=0}^{p-1} \mathrm{e}\left(\frac{h_j(s_{\mathcal{B}}(P_j(x)) - s_j)}{p}\right)\right) \\ &= \frac{1}{p^\ell} \sum_{0 \le h_1, \dots, h_\ell \le p-1} \mathrm{e}\left(\frac{-1}{p}\sum_{j=1}^{\ell} h_j s_j\right) \sum_{x \in \mathbb{F}_q} \psi_{\mathcal{B}}\left(\sum_{j=1}^{\ell} h_j P_j(x)\right) \end{aligned}$$

where $\psi_{\mathcal{B}}$ is the additive character of $\mathbb{F}_q$ defined by $\psi_{\mathcal{B}}(y) = \mathrm{e}\left(s_{\mathcal{B}}(y)/p\right)$ for any $y \in \mathbb{F}_q$. The contribution of $(h_1, \dots, h_\ell) = (0, \dots, 0)$ is q/p^ℓ. Since all the P_j have degree n and their leading coefficients are $\mathbb{F}_p$-linearly independent, it is enough that one of the h_j in not 0 to ensure that the polynomial $\sum_{j=1}^{\ell} h_j P_j(x)$ has degree n and it follows from Theorem 2.1 that:

$$\left| |\mathcal{D}(P_1, \dots, P_\ell, s_1, \dots, s_\ell)| - \frac{q}{p^\ell} \right| \le \frac{p^\ell - 1}{p^\ell}(n-1)\sqrt{q} \le (n-1)\sqrt{q}.$$

In particular, if $(n-1)p^\ell < \sqrt{q}$ then $|\mathcal{D}(P_1, \dots, P_\ell, s_1, \dots, s_\ell)| > 0$, which completes the proof of Theorem 1.5.

4. Sum of digits of rational values

To prove Theorem 1.6, we will need the following result.

Theorem 4.1. *Let ψ be a nontrivial additive character of $\mathbb{F}_q$ and let $R = P/Q$ be a rational function over $\mathbb{F}_q$. Let α be the number of distinct roots of the polynomial Q in the algebraic closure $\overline{\mathbb{F}_q}$ of $\mathbb{F}_q$. If R satisfies*

$$R \text{ is not of the form } A^p - A \text{ where } A \text{ is a rational function over } \overline{\mathbb{F}_q} \tag{III.22}$$

then

$$\left| \sum_{\substack{x \in \mathbb{F}_q \\ Q(x) \neq 0}} \psi\left(R(x)\right) \right| \le (\max(\deg P, \deg Q) + \alpha^* - 2)\sqrt{q} + \beta$$

where $(\alpha^*, \beta) = (\alpha, 1)$ if $\deg P \le \deg Q$ and $(\alpha^*, \beta) = (\alpha + 1, 0)$ otherwise.

Proof. See [51], Theorem 2. □

Moreover, by Lemma 2 of [53], if a rational function $R = P/Q$ over $\mathbb{F}_q$ satisfies condition (III.7) then it also satisfies (III.22).

Then, to prove Theorem 1.6, it suffices to follow the same arguments as in the proof of Theorem A and to use Theorem 4.1 instead of Weil's Theorem 2.1.

5. Sum of digits of polynomial values with generator arguments

5.1. Preliminary results

Lemma 5.1. *For any integers $j \geq 1$ and $m \geq 1$, the Ramanujan sum $c_m(j)$ defined by*

$$c_m(j) = \sum_{\substack{1 \leq k \leq m \\ (k,m)=1}} \mathrm{e}\left(\frac{jk}{m}\right),$$

satisfies

$$c_m(j) = \frac{\mu}{\varphi}\left(\frac{m}{(j,m)}\right)\varphi(m)$$

where μ is the Möbius function.

Proof. See [28], Theorem 272. □

Lemma 5.2. *For any integers $m \geq 1$ and $n \geq 1$, we have*

$$\sum_{\ell=1}^{m} \frac{\mu^2}{\varphi}\left(\frac{m}{(n\ell,m)}\right) = (n,m)2^{\omega\left(\frac{m}{(n,m)}\right)}.$$

Proof. We write

$$\sum_{\ell=1}^{m} \frac{\mu^2}{\varphi}\left(\frac{m}{(n\ell,m)}\right) = \sum_{d \,|\, m} \frac{\mu^2}{\varphi}(d) \sum_{\substack{1 \leq \ell \leq m \\ (n\ell,m)=\frac{m}{d}}} 1 \tag{III.23}$$

and we define $D = (n,m)$, $n' = n/D$ and $m' = m/D$. If $d \,|\, m'$ then $(n\ell,m) = \frac{m}{d}$ if and only if $(n'\ell,m') = \frac{m'}{d}$ i.e. $(\ell,m') = \frac{m'}{d}$ (since $(n',m') = 1$). If $d \nmid m'$ then the contribution of d in (III.23) is 0. Hence,

$$\begin{aligned}\sum_{\ell=1}^{m} \frac{\mu^2}{\varphi}\left(\frac{m}{(n\ell,m)}\right) &= \sum_{d \,|\, m'} \frac{\mu^2}{\varphi}(d) \sum_{\substack{1 \leq \ell \leq m \\ (\ell,m')=\frac{m'}{d}}} 1 = \sum_{d \,|\, m'} \frac{\mu^2}{\varphi}(d) \sum_{\substack{1 \leq u \leq dD \\ (u,d)=1}} 1 \\ &= D \sum_{d \,|\, m'} \mu^2(d) = D\, 2^{\omega(m')}\end{aligned}$$

where the last equality holds by Theorem 264 of [28]. This completes the proof of Lemma 5.2. □

Lemma 5.3. *For any integer $1 \le j \le q-1$, the multiplicative character χ_j of $\mathbb{F}_q$ defined by (III.17) satisfies for any $n \ge 1$:*

$$\sum_{g\in\mathcal{G}} \chi_j^n(g) = \frac{\mu}{\varphi}\left(\frac{q-1}{(nj, q-1)}\right)\varphi(q-1).$$

Proof. The set $\mathcal{G}$ can be described in terms of g_0: $\mathcal{G} = \{g_0^k : 1 \le k \le q-1 \text{ and } (k, q-1) = 1\}$ and it follows

$$\sum_{g\in\mathcal{G}} \chi_j^n(g) = \sum_{\substack{1\le k\le q-1\\(k,q-1)=1}} \chi_j^n\left(g_0^k\right) = \sum_{\substack{1\le k\le q-1\\(k,q-1)=1}} \mathrm{e}\left(\frac{njk}{q-1}\right).$$

The last sum is the Ramanujan sum $c_{q-1}(nj)$ and thus, by Lemma 5.1,

$$\sum_{g\in\mathcal{G}} \chi_j^n(g) = \frac{\mu}{\varphi}\left(\frac{q-1}{(nj, q-1)}\right)\varphi(q-1).$$

□

5.2. Proof of Theorem 1.7

Theorem 1.7 improves Theorem 1.3 in [12]. This improvement can be obtained by using the following result [66, Proposition 6.1]:

Proposition 5.4. *If $P \in \mathbb{F}_q[X]$ is a polynomial of degree $n \ge 1$ with $(n, q) = 1$ and if ψ is a nontrivial additive character of $\mathbb{F}_q$ then we have the upper bound*

$$\left|\sum_{g\in\mathcal{G}} \psi(P(g))\right| \le \frac{\varphi(q-1)}{q-1}\left((n2^{\omega(q-1)} - 1)\sqrt{q} + 1\right).$$

To prove Theorem 1.7, it suffices to follow the same arguments as in the proof of Theorem 1.3 in [12] and to use Proposition 5.4 instead of Lemma 4.1 of [12].

5.3. Sum of digits of monomials with generator arguments and proof of Theorem 1.8

We first show that the study of $|\mathcal{D}_{\mathcal{G}}(P, s)|$ where P is a monomial may be reduced to the case where the degree of P divides $q-1$. We will need the following lemma.

Lemma 5.5. *If $m \ge 2$ is an integer and if $d \ge 2$ divides m then the morphism*

$$\begin{array}{rcl} f : (\mathbb{Z}/m\mathbb{Z})^* & \to & (\mathbb{Z}/d\mathbb{Z})^* \\ k \bmod m & \mapsto & k \bmod d \end{array}$$

is surjective and the preimage of each $x \in (\mathbb{Z}/d\mathbb{Z})^*$ has exactly $\frac{\varphi(m)}{\varphi(d)}$ elements.

Proof. If $1 \leq k' \leq d-1$ satisfies $(k', d) = 1$, by Dirichlet's theorem on arithmetic progressions (see for instance Theorem 15 in [28]), there are infinitely many prime numbers p such that $p \equiv k' \bmod d$, thus, there exists a prime p such that $p \nmid m$ (m has finitely many prime factors) and $p \equiv k' \bmod d$. This shows that f is surjective. Therefore, the quotient group $(\mathbb{Z}/m\mathbb{Z})^*/\ker f$ is isomorphic to $(\mathbb{Z}/d\mathbb{Z})^*$ and it follows that $|\ker f| = \varphi(m)/\varphi(d)$. Moreover, the preimage of each $x \in (\mathbb{Z}/d\mathbb{Z})^*$ by f is $x_0 \ker f$, where x_0 is an element of $(\mathbb{Z}/m\mathbb{Z})^*$ satisfying $f(x_0) = x$. It follows that the preimage of each $x \in (\mathbb{Z}/d\mathbb{Z})^*$ by f has exactly $\varphi(m)/\varphi(d)$ elements, which completes the proof of Lemma 5.5. □

Let $n \geq 1$ and denote $d = (n, q-1)$ and $d' = (q-1)/d$. For any generator g, the order of g^n is d'. Moreover, we will see that Lemma 5.5 permits us to show that, for any $x \in \mathbb{F}_q^*$ of order d', there are exactly $\varphi(q-1)/\varphi(d')$ generators g such that $x = g^n$. Indeed, there exists $1 \leq k_0 \leq d'$ such that $(k_0, d') = 1$ and $x = g_0^{k_0 d}$ (where g_0 is a fixed generator of $\mathbb{F}_q^*$) and since $\mathcal{G} = \{g_0^k : 1 \leq k \leq q-1, (k, q-1) = 1\}$, the number of generators g such that $g^n = x$ is the number of integers $1 \leq k \leq q-1$ such that $(k, q-1) = 1$ and $kn \equiv k_0 d \bmod (q-1)$ i.e. $k\frac{n}{d} \equiv k_0 \bmod d'$ which may be written as

$$k \equiv k_0 i_{d'}\left(\frac{n}{d}\right) \bmod d'$$

where $i_{d'}\left(\frac{n}{d}\right)$ is the inverse of $\frac{n}{d}$ modulo d'. By Lemma 5.5, there are exactly $\varphi(q-1)/\varphi(d')$ such integers k. It follows that

$$|\mathcal{D}_{\mathcal{G}}(aX^n, s)| = \frac{\varphi(q-1)}{\varphi(d')} |\mathcal{O}_{d'} \cap \{y \in \mathbb{F}_q : s_{\mathcal{B}}(ay) = s\}| \tag{III.24}$$

and in particular, $|\mathcal{D}_{\mathcal{G}}(aX^n, s)| = |\mathcal{D}_{\mathcal{G}}(aX^d, s)|$.

We will now obtain the following result which provides a sharp estimate for $|\mathcal{D}_{\mathcal{G}}(aX^d, s)|$ as soon as d divides $q-1$.

Theorem 5.6. *If d divides $q-1$ and if $a \in \mathbb{F}_q^*$ then, for any $s \in \mathbb{F}_p^*$,*

$$\left| \left| \mathcal{D}_{\mathcal{G}}(aX^d, s) \right| - \frac{q}{p} \frac{\varphi(q-1)}{q-1} \right| \leq$$
$$\frac{\varphi(q-1)}{q-1} \left(d\, 2^{\omega\left(\frac{q-1}{d}\right)} - (d, \delta)\, 2^{\omega\left(\frac{\delta}{(d,\delta)}\right)} \left(1 - \frac{1}{\sqrt{p}}\right) - \frac{1}{\sqrt{p}} \right) \frac{\sqrt{q}}{\sqrt{p}}$$

where δ is the integer defined by $\delta = (q-1)/(p-1)$ and for $s = 0$,

$$\left| \left| \mathcal{D}_{\mathcal{G}}(aX^d, 0) \right| - \left(\frac{q}{p} - 1\right) \frac{\varphi(q-1)}{q-1} \right| \leq \frac{\varphi(q-1)}{q-1} \frac{p-1}{p} \left((d, \delta)\, 2^{\omega\left(\frac{\delta}{(d,\delta)}\right)} - 1 \right) \sqrt{q}.$$

Theorem 1.8 is an immediate consequence of Theorem 5.6.

Proof. Let $d \,|\, q-1$, let $a \in \mathbb{F}_q^*$ and $s \in \mathbb{F}_p$. Since $\mathcal{D}_{\mathcal{G}}(aX^d, s) = \{g \in \mathcal{G} : s_{\mathcal{B}}(ag^d) = s\}$, by the

same arguments as in the proof of Theorem 3.7,

$$\begin{aligned}\left|\mathcal{D}_{\mathcal{G}}(aX^d,s)\right| &= \sum_{\substack{y\in\mathbb{F}_q^*\\ s_{\mathcal{B}}(y)=s}}\sum_{g\in\mathcal{G}}\mathbb{1}_{ag^d=y}\\ &= \frac{1}{q-1}\sum_{\chi}\chi(a)\left(\sum_{g\in\mathcal{G}}\chi^d(g)\right)S(\overline{\chi},s)\end{aligned}$$

where $S(\overline{\chi},s)$ is defined by (III.13). The main term is provided by $\chi=\chi_0$:

$$\left|\mathcal{D}_{\mathcal{G}}(aX^d,s)\right| = M_s + \frac{1}{q-1}\sum_{\chi\neq\chi_0}\chi(a)\left(\sum_{g\in\mathcal{G}}\chi^d(g)\right)S(\overline{\chi},s)$$

where

$$M_s = \frac{|\mathcal{G}|}{q-1}\left|\{y\in\mathbb{F}_q^* : s_{\mathcal{B}}(y)=s\}\right| = \begin{cases}\dfrac{q}{p}\dfrac{\varphi(q-1)}{q-1} & \text{if } s\neq 0,\\ \left(\dfrac{q}{p}-1\right)\dfrac{\varphi(q-1)}{q-1} & \text{if } s=0.\end{cases} \tag{III.25}$$

The nontrivial multiplicative characters of $\mathbb{F}_q$ are $\chi_1,\dots,\chi_{q-2}$ defined by (III.17). It follows that

$$\left|\mathcal{D}_{\mathcal{G}}(aX^d,s)\right| - M_s = \frac{1}{q-1}\sum_{j=1}^{q-2}\chi_j(a)\left(\sum_{g\in\mathcal{G}}\chi_j^d(g)\right)S(\overline{\chi_j},s)$$

and by Lemma 5.3

$$\left|\mathcal{D}_{\mathcal{G}}(aX^d,s)\right| - M_s = \frac{\varphi(q-1)}{q-1}\sum_{j=1}^{q-2}\chi_j(a)\frac{\mu}{\varphi}\left(\frac{q-1}{(dj,q-1)}\right)S(\overline{\chi_j},s).$$

Moreover, by Lemma 2.6, for $1\le j\le q-1$, $\chi_{j\,|\mathbb{F}_p^*}=1$ if and only if $p-1$ divides j. Thus, by Corollary 2.4, if $s\neq 0$ then

$$\begin{aligned}\left|\left|\mathcal{D}_{\mathcal{G}}(aX^d,s)\right| - M_s\right| \le{}& \frac{\varphi(q-1)}{q-1}\frac{\sqrt{q}}{\sqrt{p}}\sum_{\substack{1\le j\le q-1\\ p-1\nmid j}}\frac{\mu^2}{\varphi}\left(\frac{q-1}{(dj,q-1)}\right)\\ &+\frac{\varphi(q-1)}{q-1}\frac{\sqrt{q}}{p}\sum_{\substack{1\le j<q-1\\ p-1\mid j}}\frac{\mu^2}{\varphi}\left(\frac{q-1}{(dj,q-1)}\right)\end{aligned} \tag{III.26}$$

and for $s=0$,

$$\left|\left|\mathcal{D}_{\mathcal{G}}(aX^d,0)\right| - M_0\right| \le \frac{\varphi(q-1)}{q-1}\frac{(p-1)\sqrt{q}}{p}\sum_{\substack{1\le j<q-1\\ p-1\mid j}}\frac{\mu^2}{\varphi}\left(\frac{q-1}{(dj,q-1)}\right). \tag{III.27}$$

Lemma 5.2 permits us to compute each sum over j in (III.26) and (III.27):

$$\sum_{\substack{1\le j<q-1\\ p-1\,|\,j}} \frac{\mu^2}{\varphi}\left(\frac{q-1}{(dj,q-1)}\right) = \sum_{1\le \ell<\delta} \frac{\mu^2}{\varphi}\left(\frac{\delta}{(d\ell,\delta)}\right) = (d,\delta)\,2^{\omega\left(\frac{\delta}{(d,\delta)}\right)} - 1 \tag{III.28}$$

where $\delta = (q-1)/(p-1)$ and thus, also by Lemma 5.2,

$$\begin{aligned}
&\sum_{\substack{1\le j\le q-1\\ p-1\nmid j}} \frac{\mu^2}{\varphi}\left(\frac{q-1}{(dj,q-1)}\right)\\
&\qquad = \sum_{1\le j\le q-1} \frac{\mu^2}{\varphi}\left(\frac{q-1}{(dj,q-1)}\right) - \sum_{\substack{1\le j\le q-1\\ p-1\,|\,j}} \frac{\mu^2}{\varphi}\left(\frac{q-1}{(dj,q-1)}\right)\\
&\qquad = d\,2^{\omega\left(\frac{q-1}{d}\right)} - (d,\delta)\,2^{\omega\left(\frac{\delta}{(d,\delta)}\right)}.
\end{aligned} \tag{III.29}$$

To complete the proof of Theorem 5.6, it suffices to insert (III.28), (III.29) and (III.25) into (III.26) for $s\neq 0$ and to insert (III.28) and (III.25) into (III.27) for $s=0$. □

5.4. Proof of Corollary 1.9

If d divides $q-1$, it follows from (III.24) that:

$$\left|\mathcal{D}_{\mathcal{G}}(X^{d'},s)\right| = \frac{\varphi(q-1)}{\varphi(d)}\,|\mathcal{F}_s\cap\mathcal{O}_d| \tag{III.30}$$

where $d'=(q-1)/d$. Then, to prove Corollary 1.9, it suffices to insert (III.30) into Theorem 1.8.

5.5. Proof of Theorem 1.10

By the same argument as in the proof of Theorem 1.5, $|\mathcal{D}_{\mathcal{G}}(P_1,\dots,P_\ell,s_1,\dots,s_\ell)|$ is given by:

$$|\mathcal{D}_{\mathcal{G}}(P_1,\dots,P_\ell,s_1,\dots,s_\ell)| = \frac{1}{p^\ell}\sum_{0\le h_1,\dots,h_\ell\le p-1} \mathrm{e}\left(\frac{-1}{p}\sum_{j=1}^{\ell} h_j s_j\right)\times \sum_{g\in\mathcal{G}}\psi_{\mathcal{B}}\left(\sum_{j=1}^{\ell} h_j P_j(g)\right).$$

The contribution of $(h_1,\dots,h_\ell)=(0,\dots,0)$ is $\varphi(q-1)/p^\ell$. Again, by the same argument as in the proof of Theorem 1.5, if at least one of the h_j is not 0 then the polynomial $\sum_{j=1}^{\ell} h_j P_j(x)$

has degree n and by Proposition 5.4,

$$\left||\mathcal{D}_{\mathcal{G}}(P_1,\dots,P_\ell,s_1,\dots,s_\ell)|-\frac{\varphi(q-1)}{p^\ell}\right|<\frac{\varphi(q-1)}{q-1}\left((n2^{\omega(q-1)}-1)\sqrt{q}+1\right)$$
$$<\frac{\varphi(q-1)}{q-1}\left(n2^{\omega(q-1)}\sqrt{q}-\frac{1}{p^\ell}\right),$$

and thus, if $np^\ell\leq\sqrt{q}/2^{\omega(q-1)}$ then $|\mathcal{D}_{\mathcal{G}}(P_1,\dots,P_\ell,s_1,\dots,s_\ell)|>0$, which completes the proof of Theorem 1.10.

IV. Chiffres préassignés dans les corps finis

Le contenu de ce chapitre est publié dans « Journal of Number Theory » [66].

Abstract. Let p be a prime number, $q = p^r$ with $r \geq 2$ and $P \in \mathbb{F}_q[X]$. In this paper, we first estimate the number of $x \in \mathbb{F}_q$ such that $P(x)$ has prescribed digits (in the sense of Dartyge and Sárközy). In particular, for a given proportion < 0.5 of prescribed digits, we show that this number is asymptotically as expected. Then, we obtain similar results when x is allowed to run only in the set of generators (primitive elements) of $\mathbb{F}_q^*$. In the case of special interest where P is a monomial of degree 2, our estimate for the number of $x \in \mathbb{F}_q$ such that $P(x)$ has prescribed digits is sharper than the estimate following from the Weil bound. We will need to study exponential sums of independent interest such as multiplicative character sums over affine subspaces and additive character sums with generator arguments.

Table of contents

1. Introduction

1.1. Motivation

Let $g \geq 2$ be an integer. Every integer $n \in \mathbb{N}$ can be written uniquely in base g:

$$n = \sum_{j=0}^{r} c_j g^j \tag{IV.1}$$

where the digits c_j belong to $\{0, \ldots, g-1\}$ and $c_r \geq 1$. The study of the connection between the arithmetic properties of n and the properties of its digits in a given basis produces a lot of interesting and difficult questions. Many results have been obtained on this topic for instance by Gelfond [25], Erdős–Mauduit–Sárközy [19, 20], Dartyge–Tenenbaum [13, 14], Mauduit–Rivat [43, 44], Wolke [70], Harman–Kátai [30], Bourgain [4, 5], Maynard [46, 48]....

In [12], Dartyge and Sárközy initiated the study of the concept of digits in the context of finite fields. The algebraic structure of finite fields permits us to formulate and study new problems of interest which might be out of reach in the context of integers [38], [52]. Let p be a prime number, let $q = p^r$ with $r \geq 2$ and consider the finite field $\mathbb{F}_q$. Let $\mathcal{B} = \{e_1, \ldots, e_r\}$ be a basis of the vector space $\mathbb{F}_q$ over $\mathbb{F}_p$. Then every $x \in \mathbb{F}_q$ can be written uniquely in base $\mathcal{B}$:

$$x = \sum_{j=1}^{r} c_j e_j \tag{IV.2}$$

with $c_1, \ldots, c_r \in \mathbb{F}_p$. As in [12], we will call $c_1, \ldots, c_r$ the "digits" of x by analogy with the special case where the basis $\mathcal{B}$ consists of the first r powers of a generator (i.e. primitive element) g of $\mathbb{F}_q^*$ since in this situation (IV.2) becomes

$$x = \sum_{j=1}^{r} c_j g^{j-1},$$

which reminds us of (IV.1). In [12], Dartyge and Sárközy estimated the number of $x \in \mathbb{F}_q$ such that the sum of digits of $P(x)$ is prescribed where $P \in \mathbb{F}_q[X]$ is a given polynomial. They also obtained similar results when x is allowed to run only in the set of generators of $\mathbb{F}_q^*$. Further problems on digits in finite fields have been studied by Dartyge, Mauduit, Sárközy [11], Dietmann, Elsholtz, Shparlinski [16] and Gabdullin [23]. In particular, an estimate of the number of squares in $\mathbb{F}_q$ with restricted digits has been proved in [11] and then improved in [16] and [23].

In general, the study of elements of some special sequences of integers with prescribed digits is quite difficult [4], [5], [16], [29], [30], [63], [70]. In particular, Bourgain [5] obtained an asymptotic formula for the number of prime numbers with a positive proportion of prescribed digits. We notice that the distribution of sequences with prescribed digits may have important consequences in cryptography. In the context of finite fields, as in [12], it is natural to consider polynomial values. We will estimate the number of $x \in \mathbb{F}_q$ such that $P(x)$ has prescribed digits. In particular, for a given proportion < 0.5 of prescribed digits, we show that this number is

asymptotically as expected. As in [12], we will also consider the situation where x is allowed to run only in the set of generators of $\mathbb{F}_q^*$ and obtain similar results. In the case of special interest where P is a monomial of degree 2, our estimate for the number of $x \in \mathbb{F}_q$ such that $P(x)$ has prescribed digits will be sharper than the estimate for more general P following from the Weil bound. In order to prove these results, we will need to study exponential sums of independent interest such as multiplicative character sums over affine subspaces and additive character sums with generator arguments.

1.2. Statement of results

Let p be a prime number, let $q = p^r$ with $r \geq 2$ and let $\mathcal{B} = \{e_1, \dots, e_r\}$ be a basis of $\mathbb{F}_q$ over $\mathbb{F}_p$. For $1 \leq j \leq r$, we define the j-th digit function ε_j on $\mathbb{F}_q$ by

$$\varepsilon_j\left(\sum_{i=1}^{r} c_i e_i\right) = c_j$$

for any $(c_1, \dots, c_r) \in (\mathbb{F}_p)^r$.

1.2.1. Prescribing the digits of $P(x)$

For $P \in \mathbb{F}_q[X]$, for $1 \leq k \leq r$, for $J \subset \{1, \dots, r\}$ with $|J| = k$ and for $\boldsymbol{\alpha} = (\alpha_j)_{j \in J} \in (\mathbb{F}_p)^k$, we consider the set $\mathcal{F}_q(P, k, J, \boldsymbol{\alpha})$ formed by all elements $x \in \mathbb{F}_q$ such that for any $j \in J$, the j-th digit of $P(x)$ in base $\mathcal{B}$ is α_j:

$$\mathcal{F}_q(P, k, J, \boldsymbol{\alpha}) = \{x \in \mathbb{F}_q : \varepsilon_j(P(x)) = \alpha_j \text{ for all } j \in J\}.$$

Heuristically, since $\boldsymbol{\alpha}$ can take p^k values, we would expect $|\mathcal{F}_q(P, k, J, \boldsymbol{\alpha})| \approx q/p^k$. We will prove this in a quantitative way by obtaining in Section 3.1 the following estimate for $|\mathcal{F}_q(P, k, J, \boldsymbol{\alpha})|$.

Theorem 1.1. *If $P \in \mathbb{F}_q[X]$ is a polynomial of degree $n \geq 1$ with $(n, q) = 1$ then, for any $1 \leq k \leq r$, for any $J \subset \{1, \dots, r\}$ with $|J| = k$ and any $\boldsymbol{\alpha} \in (\mathbb{F}_p)^k$, we have*

$$\left| |\mathcal{F}_q(P, k, J, \boldsymbol{\alpha})| - \frac{q}{p^k} \right| \leq \frac{p^k - 1}{p^k}(n-1)\sqrt{q}; \tag{IV.3}$$

in particular, if

$$(n-1)(p^k - 1) < \sqrt{q} = p^{r/2} \tag{IV.4}$$

then $\mathcal{F}_q(P, k, J, \boldsymbol{\alpha}) \neq \varnothing$.

If $P \in \mathbb{F}_q[X]$ is a polynomial of degree 2 and if $p \geq 3$ then Theorem 1.1 permits us to prescribe up to half of the digits: for any $1 \leq k \leq r/2$, for any $J \subset \{1, \dots, r\}$ with $|J| = k$ and for any $\boldsymbol{\alpha} \in (\mathbb{F}_p)^k$, we have $\mathcal{F}_q(P, k, J, \boldsymbol{\alpha}) \neq \varnothing$.

For fixed $n \geq 3$, condition (IV.4) allows us to prescribe essentially up to half of the digits.

The main argument in the proof of Theorem 1.1 is the classical Weil bound.

Note that $|\mathcal{F}_q(P,k,J,\boldsymbol{\alpha})|$ is the number of $x \in \mathbb{F}_q$ such that $P(x)$ belongs to an affine subspace of $\mathbb{F}_q$. For more general results on polynomial values in affine subspaces, see for instance [54].

Theorem 1.1 will enable us to show that the number of $x \in \mathbb{F}_q$ such that $P(x)$ has a given proportion < 0.5 of prescribed digits is asymptotically as expected:

Corollary 1.2. *For any $n \geq 1$, for any $\varepsilon > 0$, we have*

$$|\mathcal{F}_{p^r}(P,k,J,\boldsymbol{\alpha})| = p^{r-k}(1+o(1)) \quad (p^r \to +\infty, p \nmid n, r \geq 2)$$

uniformly over $k \leq (1/2-\varepsilon)r$, $P \in \mathbb{F}_{p^r}[X]$ of degree n, basis $\mathcal{B}$ of $\mathbb{F}_{p^r}$ over $\mathbb{F}_p$, $J \subset \{1,\dots,r\}$ with $|J| = k$ and $\boldsymbol{\alpha} \in (\mathbb{F}_p)^k$.

1.2.2. Squares with prescribed digits

Let $\mathcal{Q}$ be the set of squares in $\mathbb{F}_q$: $\mathcal{Q} = \{x^2 : x \in \mathbb{F}_q\}$. Since each square in $\mathbb{F}_q^*$ has exactly two roots, one can easily see that the number of squares $x \in \mathbb{F}_q$ such that $\varepsilon_j(x) = \alpha_j$ for all $j \in J$, that is $|\mathcal{Q} \cap \mathcal{F}_q(X,k,J,\boldsymbol{\alpha})|$, satisfies:

$$|\mathcal{F}_q(X^2,k,J,\boldsymbol{\alpha})| = \begin{cases} 2 \cdot |\mathcal{Q} \cap \mathcal{F}_q(X,k,J,\boldsymbol{\alpha})| & \text{if } \boldsymbol{\alpha} \neq \mathbf{0}, \\ 2 \cdot |\mathcal{Q} \cap \mathcal{F}_q(X,k,J,\boldsymbol{\alpha})| - 1 & \text{if } \boldsymbol{\alpha} = \mathbf{0}. \end{cases}$$

It follows that the study of the number of squares with k prescribed digits is reduced to the study of $|\mathcal{F}_q(P,k,J,\boldsymbol{\alpha})|$ for $P = X^2$. In this special case and more generally for $P = aX^2$ where $a \in \mathbb{F}_q^*$, we will be able to improve (IV.3) and we will obtain in Section 5.1:

Theorem 1.3. *If $p \geq 3$ then, for any $a \in \mathbb{F}_q^*$, for any $1 \leq k \leq r$, for any $J \subset \{1,\dots,r\}$ with $|J| = k$ and any $\boldsymbol{\alpha} \in (\mathbb{F}_p)^k$, we have*

$$\left| |\mathcal{F}_q(aX^2,k,J,\boldsymbol{\alpha})| - \frac{q}{p^k} \right| \leq \begin{cases} \dfrac{\sqrt{q}}{\sqrt{p}} & \text{if } \boldsymbol{\alpha} \neq \mathbf{0} \text{ and } r \text{ is odd}, \\ \left(\dfrac{2}{p} - \dfrac{1}{p^k}\right)\sqrt{q} & \text{if } \boldsymbol{\alpha} \neq \mathbf{0} \text{ and } r \text{ is even}, \\ 0 & \text{if } \boldsymbol{\alpha} = \mathbf{0} \text{ and } r \text{ is odd}, \\ \dfrac{p^k-1}{p^k}\sqrt{q} & \text{if } \boldsymbol{\alpha} = \mathbf{0} \text{ and } r \text{ is even}. \end{cases} \tag{IV.5}$$

For $\boldsymbol{\alpha} \neq \mathbf{0}$, (IV.5) improves (IV.3) by a factor $1/\sqrt{p}$ if r is odd and by a factor $2/p$ if r is even. We will see in Section 5.1 that if $k = 1$ then (IV.5) is an equality and that for $k = 2$ or $k = 3$ there are nontrivial cases where (IV.5) is again an equality. This shows the sharpness of (IV.5). Note that, for $p = 2$, since the mapping $x \mapsto x^2$ is a bijection of $\mathbb{F}_{2^r}$ (Frobenius automorphism of $\mathbb{F}_{2^r}$ over $\mathbb{F}_2$), we have $|\mathcal{F}_q(aX^2,k,J,\boldsymbol{\alpha})| = |\mathcal{F}_q(aX,k,J,\boldsymbol{\alpha})| = q/p^k$ by Theorem 1.1.

To prove Theorem 1.3, we will first obtain a sharp upper bound for multiplicative character sums over affine subspaces of $\mathbb{F}_q$ which is of independent interest (see Proposition 4.4).

Theorem 1.3 will enable us to improve Corollary 1.2 in the special case where $P = aX^2$. If r is even, we will obtain:

Corollary 1.4. *For any $\varepsilon > 0$, we have*

$$|\mathcal{F}_{p^r}(aX^2, k, J, \boldsymbol{\alpha})| = p^{r-k}(1 + o(1)) \quad (p^r \to +\infty, p \geq 3, r \geq 2, r \text{ even})$$

uniformly over $k \leq (1/2 - \varepsilon)r + 1$, $a \in \mathbb{F}_{p^r}^*$, basis $\mathcal{B}$ of $\mathbb{F}_{p^r}$ over $\mathbb{F}_p$, $J \subset \{1, \dots, r\}$ with $|J| = k$ and $\boldsymbol{\alpha} \in (\mathbb{F}_p)^k$, $\boldsymbol{\alpha} \neq \mathbf{0}$.

And if r is odd, we will obtain:

Corollary 1.5. *For any $\varepsilon > 0$, we have*

$$|\mathcal{F}_{p^r}(aX^2, k, J, \boldsymbol{\alpha})| = p^{r-k}(1 + o(1)) \quad (p^r \to +\infty, p \geq 3, r \geq 2, r \text{ odd})$$

uniformly over $k \leq (1/2 - \varepsilon)r + 1/2$, $a \in \mathbb{F}_{p^r}^*$, basis $\mathcal{B}$ of $\mathbb{F}_{p^r}$ over $\mathbb{F}_p$, $J \subset \{1, \dots, r\}$ with $|J| = k$ and $\boldsymbol{\alpha} \in (\mathbb{F}_p)^k$, $\boldsymbol{\alpha} \neq \mathbf{0}$.

1.2.3. Prescribing the digits of $P(g)$

We denote by $\mathcal{G}$ the set of generators (or primitive elements) of $\mathbb{F}_q^*$. The Euler's totient function will be denoted by φ and for $m \geq 1$, the number of distinct prime factors of m will be denoted by $\omega(m)$. For $P \in \mathbb{F}_q[X]$, for $1 \leq k \leq r$, for $J \subset \{1, \dots, r\}$ with $|J| = k$ and for $\boldsymbol{\alpha} = (\alpha_j)_{j \in J} \in (\mathbb{F}_p)^k$, we are interested in the number of elements of

$$\mathcal{G} \cap \mathcal{F}_q(P, k, J, \boldsymbol{\alpha}) = \{g \in \mathcal{G} : \varepsilon_j(P(g)) = \alpha_j \text{ for all } j \in J\}.$$

Heuristically, since $|\mathcal{G}| = \varphi(q-1)$ and since there are p^k possible values for $\boldsymbol{\alpha}$, we would expect $|\mathcal{G} \cap \mathcal{F}_q(P, k, J, \boldsymbol{\alpha})| \approx \varphi(q-1)/p^k$. We will prove this in a quantitative way by obtaining in Section 6.2 the following estimate for $|\mathcal{G} \cap \mathcal{F}_q(P, k, J, \boldsymbol{\alpha})|$.

Theorem 1.6. *If $P \in \mathbb{F}_q[X]$ is a polynomial of degree $n \geq 1$ with $(n, q) = 1$ then, for any $1 \leq k \leq r$, for any $J \subset \{1, \dots, r\}$ with $|J| = k$ and any $\boldsymbol{\alpha} \in (\mathbb{F}_p)^k$, we have*

$$\left| |\mathcal{G} \cap \mathcal{F}_q(P, k, J, \boldsymbol{\alpha})| - \frac{\varphi(q-1)}{p^k} \right| \leq \frac{p^k - 1}{p^k} \frac{\varphi(q-1)}{q-1} \left((n 2^{\omega(q-1)} - 1)\sqrt{q} + 1 \right); \tag{IV.6}$$

in particular, if

$$n(p^k - 1) < \sqrt{q}/2^{\omega(q-1)} \tag{IV.7}$$

then $\mathcal{G} \cap \mathcal{F}_q(P, k, J, \boldsymbol{\alpha}) \neq \varnothing$.

Remark 1.7. One may wonder if condition (IV.7) is not too restrictive. Heuristically, according to the normal order of the ω function (see [28], Theorem 431), for almost all values of q, it is expected that $\omega(q-1) = O(\log\log q)$. Under this assumption, condition (IV.7) would become $n(p^k - 1) \leq \sqrt{q}/(\log q)^K$ for some constant $K > 0$, so that in most cases condition (IV.7) is not too restrictive as $q \to \infty$.

To prove Theorem 1.6, we will establish in Section 6.1 a sharp upper bound for the absolute value of character sums of the form

$$\sum_{g\in\mathcal{G}} \psi(P(g))$$

where ψ is an additive character of $\mathbb{F}_q$ and $P \in \mathbb{F}_q[X]$, which is of independent interest. Our upper bound will be sharper than the one obtained in [12] (see Lemma 4.1) and used in [11].

Theorem 1.1 will enable us to obtain in Section 6.3:

Corollary 1.8. *For any $n \geq 1$, for any $\varepsilon > 0$, we have*

$$|\mathcal{G} \cap \mathcal{F}_{p^r}(P, k, J, \boldsymbol{\alpha})| = \frac{\varphi(p^r-1)}{p^k}(1+o(1)) \quad (p^r \to +\infty, p \nmid n, r \geq 2)$$

uniformly over $k \leq (1/2-\varepsilon)r$, $P \in \mathbb{F}_{p^r}[X]$ of degree n, basis $\mathcal{B}$ of $\mathbb{F}_{p^r}$ over $\mathbb{F}_p$, $J \subset \{1,\dots,r\}$ with $|J| = k$ and $\boldsymbol{\alpha} \in (\mathbb{F}_p)^k$.

In particular, the number of generators with a given proportion < 0.5 of prescribed digits is asymptotically as expected.

1.3. Notations

We use the notation $\mathrm{e}(t) = \exp(2i\pi t)$.

The trivial additive character of $\mathbb{F}_q$ is denoted by ψ_0 and the trivial multiplicative character of $\mathbb{F}_q$ is denoted by χ_0. The trivial multiplicative character of $\mathbb{F}_p$ is simply denoted by 1. The field $\mathbb{F}_p$ will be seen as a subfield of $\mathbb{F}_q$ so that every multiplicative character χ of $\mathbb{F}_q$ induces a multiplicative character of $\mathbb{F}_p$ denoted by $\chi_{|\mathbb{F}_p^*}$.

We introduce the following notations for Gaussian sums. If χ is a multiplicative character of $\mathbb{F}_p$, let $\tau(\chi)$ be the Gaussian sum

$$\tau(\chi) = \sum_{j\in\mathbb{F}_p^*} \chi(j)\,\mathrm{e}\left(\frac{j}{p}\right).$$

If ψ is an additive character of $\mathbb{F}_q$ and if χ is a multiplicative character of $\mathbb{F}_q$, let $G(\chi,\psi)$ be the Gaussian sum

$$G(\chi,\psi) = \sum_{x\in\mathbb{F}_q^*} \chi(x)\psi(x).$$

We define $\mathbb{1}_{X=Y}$ by

$$\mathbb{1}_{X=Y} = \begin{cases} 1 & \text{if } X = Y, \\ 0 & \text{otherwise.} \end{cases}$$

2. Preparations

To detect the equality of two elements of $\mathbb{F}_p$, we will often use the classical equality

$$\frac{1}{p}\sum_{j=0}^{p-1} \mathrm{e}\left(\frac{ja}{p}\right) = \begin{cases} 1 & \text{if } a \equiv 0 \bmod p, \\ 0 & \text{otherwise.} \end{cases} \tag{IV.8}$$

The following results regarding exponential sums will play an important role in the proofs.

Theorem 2.1 (Weil). *Let $P \in \mathbb{F}_q[X]$ be of degree $n \geq 1$ with $(n, q) = 1$ and let ψ be a nontrivial additive character of $\mathbb{F}_q$. Then,*

$$\left|\sum_{x\in\mathbb{F}_q} \psi(P(x))\right| \leq (n-1)\sqrt{q}.$$

Moreover, if χ is a nontrivial multiplicative character of $\mathbb{F}_q^*$, then

$$\left|\sum_{x\in\mathbb{F}_q^*} \psi(P(x))\chi(x)\right| \leq n\sqrt{q}.$$

Proof. See [38], Theorem 5.38, p. 223 and [61], Theorem 2G, p. 45. □

Lemma 2.2. *If ψ is an additive character of $\mathbb{F}_q$ and χ is a multiplicative character of $\mathbb{F}_q$ then*

$$G(\chi,\psi) = \begin{cases} q-1 & \text{if } \chi = \chi_0 \text{ and } \psi = \psi_0, \\ -1 & \text{if } \chi = \chi_0 \text{ and } \psi \neq \psi_0, \\ 0 & \text{if } \chi \neq \chi_0 \text{ and } \psi = \psi_0, \end{cases}$$

and $|G(\chi,\psi)| = \sqrt{q}$ if $\chi \neq \chi_0$ and $\psi \neq \psi_0$.

In the special case where χ is a multiplicative character of $\mathbb{F}_p$, $|\tau(\chi)| = \sqrt{p}$ if χ is nontrivial and $\tau(\chi) = -1$ if χ is trivial.

Proof. See Theorem 5.11 of [38]. □

3. Prescribing the digits of $P(x)$

3.1. Proof of Theorem 1.1

We will provide a short and direct proof of Theorem 1.1. In [54], Ostafe establishes an estimate for the number of x in a given affine subset of $\mathbb{F}_q$ such that $P(x)$ also belongs to a given affine subset of $\mathbb{F}_q$ (see Theorem 15). The proof of this result could also be used to obtain Theorem 1.1.

For each $j \in J$, the condition $\varepsilon_j(P(x)) = \alpha_j$ can be handled with an exponential sum by (IV.8). Considering products of such sums, we can detect the elements of the set

$\mathcal{F}_q(P,k,J,\boldsymbol{\alpha})$ as follows:

$$|\mathcal{F}_q(P,k,J,\boldsymbol{\alpha})| = \sum_{x\in\mathbb{F}_q}\prod_{j\in J}\left(\frac{1}{p}\sum_{h\in\mathbb{F}_p}\mathrm{e}\left(\frac{h\left(\varepsilon_j(P(x))-\alpha_j\right)}{p}\right)\right)$$
$$= \frac{1}{p^k}\sum_{\mathbf{h}=(h_j)_{j\in J}\in(\mathbb{F}_p)^k}\mathrm{e}\left(\frac{-1}{p}\sum_{j\in J}h_j\alpha_j\right)\sum_{x\in\mathbb{F}_q}\psi_{\mathbf{h}}(P(x))$$

where, for any $\mathbf{h}=(h_j)_{j\in J}\in(\mathbb{F}_p)^k$, $\psi_{\mathbf{h}}$ is the additive character of $\mathbb{F}_q$ defined by

$$\psi_{\mathbf{h}}(y) = \mathrm{e}\left(\frac{1}{p}\sum_{j\in J}h_j\varepsilon_j(y)\right).$$

The contribution of $\mathbf{h}=\mathbf{0}$ is q/p^k. Since the linear forms ε_j for $j\in J$ are linearly independent, the character $\psi_{\mathbf{h}}$ is trivial if and only if $\mathbf{h}=\mathbf{0}$ and it follows from Theorem 2.1 that

$$\left||\mathcal{F}_q(P,k,J,\boldsymbol{\alpha})| - \frac{q}{p^k}\right| \le \frac{p^k-1}{p^k}(n-1)\sqrt{q}.$$

In particular, if $(n-1)(p^k-1)<\sqrt{q}$ then $|\mathcal{F}_q(P,k,J,\boldsymbol{\alpha})|>0$, which completes the proof of Theorem 1.1.

3.2. Proof of Corollary 1.2

Let $n\ge 1$ be an integer and let $\varepsilon>0$. If p is a prime number such that $p\nmid n$, if $r\ge 2$, if $k\le(1/2-\varepsilon)r$, if $P\in\mathbb{F}_{p^r}[X]$ is of degree n, if $\mathcal{B}$ is a basis of $\mathbb{F}_{p^r}$ over $\mathbb{F}_p$, if $J\subset\{1,\dots,r\}$ is such that $|J|=k$ and if $\boldsymbol{\alpha}\in(\mathbb{F}_p)^k$ then, by Theorem 1.1,

$$p^{-(r-k)}\left||\mathcal{F}_{p^r}(P,k,J,\boldsymbol{\alpha})| - p^{r-k}\right| \le p^{k-r/2}(n-1) \le p^{-\varepsilon r}(n-1) = o(1)$$

as $p^r\to+\infty$, which completes the proof of Corollary 1.2.

4. Multiplicative character sums over affine subspaces

In this section, we will obtain a sharp upper bound for multiplicative character sums over affine subspaces of $\mathbb{F}_q$ (see Proposition 4.4) which is of independent interest. This will enable us to prove Theorem 1.3 in Section 5.

Let Tr be the trace of $\mathbb{F}_q$ over $\mathbb{F}_p$ defined by

$$\mathrm{Tr}(x) = x + x^p + \cdots + x^{p^{r-1}}.$$

We first establish the two following lemmas.

Lemma 4.1. *If χ is a nontrivial multiplicative character of $\mathbb{F}_q$ then for any $1 \leq k \leq r$, any $\mathbf{b} = (b_1, \ldots, b_k) \in (\mathbb{F}_q)^k$ such that $b_1, \ldots, b_k$ are linearly independent over $\mathbb{F}_p$ and any $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_k) \in (\mathbb{F}_p)^k$, the sum $S_\chi(k, \mathbf{b}, \boldsymbol{\alpha})$ defined by*

$$S_\chi(k, \mathbf{b}, \boldsymbol{\alpha}) = \sum_{\substack{x \in \mathbb{F}_q^* \\ \mathrm{Tr}(b_j x) = \alpha_j, \forall\, 1 \leq j \leq k}} \chi(x) \tag{IV.9}$$

satisfies

$$|S_\chi(k, \mathbf{b}, \boldsymbol{\alpha})| = \frac{\sqrt{q}}{p^k} \, |T_\chi(k, \mathbf{b}, \boldsymbol{\alpha})| \tag{IV.10}$$

where $T_\chi(k, \mathbf{b}, \boldsymbol{\alpha})$ is defined by

$$T_\chi(k, \mathbf{b}, \boldsymbol{\alpha}) = \sum_{\substack{(h_1, \ldots, h_k) \in (\mathbb{F}_p)^k \\ (h_1, \ldots, h_k) \neq 0}} \chi\left(\sum_{j=1}^k h_j b_j\right) \mathrm{e}\left(\frac{1}{p} \sum_{j=1}^k h_j \alpha_j\right). \tag{IV.11}$$

Proof. For each $1 \leq j \leq k$, using (IV.8) to detect the elements of $\mathbb{F}_q^*$ satisfying $\mathrm{Tr}(b_j x) = \alpha_j$, we obtain:

$$\begin{aligned} S_\chi(k, \mathbf{b}, \boldsymbol{\alpha}) &= \sum_{x \in \mathbb{F}_q^*} \chi(x) \prod_{j=1}^k \left(\frac{1}{p} \sum_{h=0}^{p-1} \mathrm{e}\left(\frac{h\,(\mathrm{Tr}(b_j x) - \alpha_j)}{p}\right)\right) \\ &= \frac{1}{p^k} \sum_{0 \leq h_1, \ldots, h_k \leq p-1} \mathrm{e}\left(\frac{-1}{p} \sum_{j=1}^k h_j \alpha_j\right) \Delta(h_1, \ldots, h_k) \end{aligned} \tag{IV.12}$$

where

$$\Delta(h_1, \ldots, h_k) = \sum_{x \in \mathbb{F}_q^*} \chi(x) \, \mathrm{e}\left(\frac{1}{p} \sum_{j=1}^k h_j \, \mathrm{Tr}(b_j x)\right). \tag{IV.13}$$

Since Tr is a linear form (see Theorem 2.23 of [38]), (IV.13) becomes

$$\Delta(h_1, \ldots, h_k) = \sum_{x \in \mathbb{F}_q^*} \chi(x) \psi_1\left(\left(\sum_{j=1}^k h_j b_j\right) x\right)$$

where ψ_1 is the canonical additive character of $\mathbb{F}_q$ defined by

$$\psi_1(x) = \mathrm{e}\left(\frac{\mathrm{Tr}(x)}{p}\right).$$

Since the elements $b_1, \ldots, b_k$ are linearly independent, it is enough that one of the h_j is not 0

to ensure that $\sum_{j=1}^{k} h_j b_j \neq 0$. It follows that for $(h_1, \ldots, h_k) \neq 0$,

$$\Delta(h_1, \ldots, h_k) = \overline{\chi}\left(\sum_{j=1}^{k} h_j b_j\right) G(\chi, \psi_1).$$

Note also that, since χ is nontrivial, $\Delta(0, \ldots, 0) = 0$. Thus, (IV.12) becomes

$$S_\chi(k, \mathbf{b}, \boldsymbol{\alpha}) = \frac{G(\chi, \psi_1)}{p^k}\,\overline{T_\chi(k, \mathbf{b}, \boldsymbol{\alpha})}$$

where $T_\chi(k, \mathbf{b}, \boldsymbol{\alpha})$ is defined by (IV.11). It follows from Lemma 2.2 that

$$|S_\chi(k, \mathbf{b}, \boldsymbol{\alpha})| = \frac{\sqrt{q}}{p^k}\,|T_\chi(k, \mathbf{b}, \boldsymbol{\alpha})|,$$

which completes the proof of Lemma 4.1. □

Remark 4.2. Since $|T_\chi(k, \mathbf{b}, \boldsymbol{\alpha})|$ is trivially bounded by $p^k - 1$, it follows from (IV.10) that

$$|S_\chi(k, \mathbf{b}, \boldsymbol{\alpha})| \leq \frac{p^k - 1}{p^k}\sqrt{q} \tag{IV.14}$$

and that any improvement of the trivial bound $p^k - 1$ for $|T_\chi(k, \mathbf{b}, \boldsymbol{\alpha})|$ would give a more precise upper bound for $|S_\chi(k, \mathbf{b}, \boldsymbol{\alpha})|$ than (IV.14).

We establish now the following nontrivial upper bound for $|T_\chi(k, \mathbf{b}, \boldsymbol{\alpha})|$.

Lemma 4.3. *If χ is a multiplicative character of $\mathbb{F}_q$ then for any $1 \leq k \leq r$, for any $\mathbf{b} = (b_1, \ldots, b_k) \in (\mathbb{F}_q)^k$ such that $b_1, \ldots, b_k$ are linearly independent over $\mathbb{F}_p$ and for any $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_k) \in (\mathbb{F}_p)^k$, the sum $T_\chi(k, \mathbf{b}, \boldsymbol{\alpha})$ defined by (IV.11) satisfies for $\boldsymbol{\alpha} \neq \mathbf{0}$,*

$$|T_\chi(k, \mathbf{b}, \boldsymbol{\alpha})| \leq \begin{cases} p^{k-1}\sqrt{p} & \text{if } \chi_{|\mathbb{F}_p^*} \neq 1, \\ 2p^{k-1} - 1 & \text{if } \chi_{|\mathbb{F}_p^*} = 1, \end{cases} \tag{IV.15}$$

and for $\boldsymbol{\alpha} = \mathbf{0}$,

$$|T_\chi(k, \mathbf{b}, \boldsymbol{\alpha})| \leq \begin{cases} 0 & \text{if } \chi_{|\mathbb{F}_p^*} \neq 1, \\ p^k - 1 & \text{if } \chi_{|\mathbb{F}_p^*} = 1. \end{cases} \tag{IV.16}$$

Proof. We proceed by induction on k. Assume first that $k = 1$. If $\boldsymbol{\alpha} = \mathbf{0}$ then

$$|T_\chi(1, \mathbf{b}, \boldsymbol{\alpha})| = \left|\sum_{h \in \mathbb{F}_p^*} \chi(h)\right| = \begin{cases} 0 & \text{if } \chi_{|\mathbb{F}_p^*} \neq 1, \\ p - 1 & \text{if } \chi_{|\mathbb{F}_p^*} = 1, \end{cases}$$

and if $\boldsymbol{\alpha} \neq \mathbf{0}$ then

$$T_\chi(1, \mathbf{b}, \boldsymbol{\alpha}) = \sum_{h \in \mathbb{F}_p^*} \chi(hb_1)\,\mathrm{e}\left(\frac{h\alpha_1}{p}\right) = \chi(b_1)\overline{\chi(\alpha_1)}\tau(\chi_{|\mathbb{F}_p^*}),$$

hence, by Lemma 2.2,

$$|T_\chi(1,\mathbf{b},\boldsymbol{\alpha})| = \begin{cases} \sqrt{p} & \text{if } \chi_{|\mathbb{F}_p^*} \neq 1, \\ 1 & \text{if } \chi_{|\mathbb{F}_p^*} = 1, \end{cases}$$

which proves (IV.15) and (IV.16) for $k = 1$.

Assume now that $2 \leq k \leq r$. Distinguishing the cases $h_k \neq 0$ and $h_k = 0$, write:

$$T_\chi(k,\mathbf{b},\boldsymbol{\alpha}) = U_\chi(k,\mathbf{b},\boldsymbol{\alpha}) + T_\chi(k-1,\mathbf{b}',\boldsymbol{\alpha}') \tag{IV.17}$$

where $\mathbf{b}' = (b_1,\dots,b_{k-1})$, $\boldsymbol{\alpha}' = (\alpha_1,\dots,\alpha_{k-1})$ and

$$U_\chi(k,\mathbf{b},\boldsymbol{\alpha}) = \sum_{h_k\in\mathbb{F}_p^*} \sum_{(h_1,\dots,h_{k-1})\in\mathbb{F}_p^{k-1}} \chi\left(\sum_{j=1}^k h_j b_j\right) \mathrm{e}\left(\frac{1}{p}\sum_{j=1}^k h_j\alpha_j\right).$$

Substituting $h_j \to u_j h_k$ for all $1 \leq j \leq k-1$, we get

$$\begin{aligned} &U_\chi(k,\mathbf{b},\boldsymbol{\alpha}) \\ &= \sum_{h_k\in\mathbb{F}_p^*} \chi(h_k) \sum_{(u_1,\dots,u_{k-1})\in\mathbb{F}_p^{k-1}} \chi\left(b_k + \sum_{j=1}^{k-1} u_j b_j\right) \mathrm{e}\left(\frac{h_k}{p}\left(\alpha_k + \sum_{j=1}^{k-1} u_j\alpha_j\right)\right) \\ &= \sum_{(u_1,\dots,u_{k-1})\in\mathbb{F}_p^{k-1}} \chi\left(b_k + \sum_{j=1}^{k-1} u_j b_j\right) \sum_{h\in\mathbb{F}_p^*} \chi(h)\,\mathrm{e}\left(\frac{h}{p}\left(\alpha_k + \sum_{j=1}^{k-1} u_j\alpha_j\right)\right), \end{aligned}$$

so that

$$\begin{aligned} &U_\chi(k,\mathbf{b},\boldsymbol{\alpha}) \\ &= \tau(\chi_{|\mathbb{F}_p^*}) \sum_{\substack{(u_1,\dots,u_{k-1})\in\mathbb{F}_p^{k-1} \\ \alpha_k+\sum_{j=1}^{k-1} u_j\alpha_j\neq 0}} \chi\left(b_k + \sum_{j=1}^{k-1} u_j b_j\right) \overline{\chi}\left(\alpha_k + \sum_{j=1}^{k-1} u_j\alpha_j\right) \\ &\quad + (p-1)\mathbb{1}_{\chi_{|\mathbb{F}_p^*}=1} \sum_{\substack{(u_1,\dots,u_{k-1})\in\mathbb{F}_p^{k-1} \\ \alpha_k+\sum_{j=1}^{k-1} u_j\alpha_j=0}} \chi\left(b_k + \sum_{j=1}^{k-1} u_j b_j\right). \end{aligned} \tag{IV.18}$$

If $\boldsymbol{\alpha} = \mathbf{0}$ and if $\chi_{|\mathbb{F}_p^*} \neq 1$ then $U_\chi(k,\mathbf{b},\boldsymbol{\alpha}) = 0$ and since $T_\chi(k-1,\mathbf{b}',\boldsymbol{\alpha}') = 0$ by induction hypothesis, we end up with $T_\chi(k,\mathbf{b},\boldsymbol{\alpha}) = 0$ which proves (IV.16) (note that $T_\chi(k,\mathbf{b},\boldsymbol{\alpha})$ is always trivially bounded by $p^k - 1$). Assume now $\boldsymbol{\alpha} \neq \mathbf{0}$. It follows from (IV.18) that

$$U_\chi(k,\mathbf{b},\boldsymbol{\alpha}) \leq |\tau(\chi_{|\mathbb{F}_p^*})|(p^{k-1} - N(\boldsymbol{\alpha})) + (p-1)\mathbb{1}_{\chi_{|\mathbb{F}_p^*}=1} N(\boldsymbol{\alpha})$$

where $N(\boldsymbol{\alpha})$ denotes the number of solutions $(u_1,\dots,u_{k-1}) \in \mathbb{F}_p^{k-1}$ of the equation $\alpha_k + \sum_{j=1}^{k-1} u_j\alpha_j = 0$. If $\boldsymbol{\alpha}' = \mathbf{0}$ then $N(\boldsymbol{\alpha}) = 0$ and if $\boldsymbol{\alpha}' \neq \mathbf{0}$ then $N(\boldsymbol{\alpha}) = p^{k-2}$. We

finally deduce that, by Lemma 2.2, by the induction hypothesis and by (IV.17),

- for $\chi_{|\mathbb{F}_p^*} \neq 1$ and $\boldsymbol{\alpha}' \neq \mathbf{0}$, $|U_\chi(k, \mathbf{b}, \boldsymbol{\alpha})| \leq \sqrt{p}(p^{k-1} - p^{k-2})$ and $|T_\chi(k-1, \mathbf{b}', \boldsymbol{\alpha}')| \leq p^{k-2}\sqrt{p}$ which implies that $|T_\chi(k, \mathbf{b}, \boldsymbol{\alpha})| \leq p^{k-1}\sqrt{p}$,
- for $\chi_{|\mathbb{F}_p^*} \neq 1$ and $\boldsymbol{\alpha}' = \mathbf{0}$, $|U_\chi(k, \mathbf{b}, \boldsymbol{\alpha})| \leq p^{k-1}\sqrt{p}$ and $|T_\chi(k-1, \mathbf{b}', \boldsymbol{\alpha}')| = 0$ which implies that $|T_\chi(k, \mathbf{b}, \boldsymbol{\alpha})| \leq p^{k-1}\sqrt{p}$,
- for $\chi_{|\mathbb{F}_p^*} = 1$ and $\boldsymbol{\alpha}' \neq \mathbf{0}$, $|U_\chi(k, \mathbf{b}, \boldsymbol{\alpha})| \leq p^{k-1} - p^{k-2} + (p-1)p^{k-2}$, $|T_\chi(k-1, \mathbf{b}', \boldsymbol{\alpha}')| \leq 2p^{k-2} - 1$ which implies that $|T_\chi(k, \mathbf{b}, \boldsymbol{\alpha})| \leq 2p^{k-1} - 1$,
- for $\chi_{|\mathbb{F}_p^*} = 1$ and $\boldsymbol{\alpha}' = \mathbf{0}$, $|U_\chi(k, \mathbf{b}, \boldsymbol{\alpha})| \leq p^{k-1}$ and $|T_\chi(k-1, \mathbf{b}', \boldsymbol{\alpha}')| \leq p^{k-1} - 1$ which implies that $|T_\chi(k, \mathbf{b}, \boldsymbol{\alpha})| \leq 2p^{k-1} - 1$.

This shows (IV.15) and completes the proof of Lemma 4.3. □

Combining Lemma 4.1 and Lemma 4.3, we immediately obtain the following upper bound for multiplicative character sum over an affine subspace of $\mathbb{F}_q$:

Proposition 4.4. *If χ is a nontrivial multiplicative character of $\mathbb{F}_q$ then for any $1 \leq k \leq r$, any $\mathbf{b} = (b_1, \dots, b_k) \in (\mathbb{F}_q)^k$ such that $b_1, \dots, b_k$ are linearly independent over $\mathbb{F}_p$ and any $\boldsymbol{\alpha} = (\alpha_1, \dots, \alpha_k) \in (\mathbb{F}_p)^k$, the sum $S_\chi(k, \mathbf{b}, \boldsymbol{\alpha})$ defined by (IV.9) satisfies*

$$|S_\chi(k, \mathbf{b}, \boldsymbol{\alpha})| \leq \begin{cases} \dfrac{\sqrt{q}}{\sqrt{p}} & \text{if } \boldsymbol{\alpha} \neq \mathbf{0} \text{ and } \chi_{|\mathbb{F}_p^*} \neq 1, \\ \left(\dfrac{2}{p} - \dfrac{1}{p^k}\right)\sqrt{q} & \text{if } \boldsymbol{\alpha} \neq \mathbf{0} \text{ and } \chi_{|\mathbb{F}_p^*} = 1, \\ 0 & \text{if } \boldsymbol{\alpha} = \mathbf{0} \text{ and } \chi_{|\mathbb{F}_p^*} \neq 1, \\ \dfrac{p^k - 1}{p^k}\sqrt{q} & \text{if } \boldsymbol{\alpha} = \mathbf{0} \text{ and } \chi_{|\mathbb{F}_p^*} = 1. \end{cases} \tag{IV.19}$$

Remark 4.5. For $k = 1$, the proof of Lemma 4.3 shows that (IV.15) and (IV.16) are always equalities and thus, by Lemma 4.1, (IV.19) is also always an equality.

For $k = 2$ or $k = 3$, we will see in Remark 5.2 that if χ is the quadratic character of $\mathbb{F}_q$ then there are nontrivial cases for which (IV.19) is again an equality (if (IV.5) is an equality then, by (IV.20), (IV.21) is also an equality).

5. Squares with prescribed digits

5.1. Proof of Theorem 1.3

We first prove the following lemma.

Lemma 5.1. *For any $p \geq 3$, the quadratic character η of $\mathbb{F}_q$ satisfies*

$$\eta_{|\mathbb{F}_p^*} = \begin{cases} \gamma & \text{if } r \text{ is odd}, \\ 1 & \text{if } r \text{ is even}, \end{cases}$$

where γ is the quadratic character of $\mathbb{F}_p$.

Proof. If $s \in \mathbb{F}_p^*$ then $\eta(s) = s^{\frac{q-1}{2}}$ and $\gamma(s) = s^{\frac{p-1}{2}}$ (see for example [38], exercise 2.13). It follows that $\eta_{|\mathbb{F}_p^*} = \gamma^\delta$ where $\delta = \frac{q-1}{p-1} = \sum_{i=0}^{r-1} p^i$. Thus, since $\gamma^2 = 1$, $\eta_{|\mathbb{F}_p^*} = \gamma$ if δ is odd and $\eta_{|\mathbb{F}_p^*} = 1$ if δ is even. Moreover, since p is odd, $\delta \equiv r \bmod 2$, which ends the proof of Lemma 5.1. □

We are now ready to prove Theorem 1.3. Let $p \geq 3$, let $1 \leq k \leq r$, let $a \in \mathbb{F}_q^*$, let $J \subset \{1, \dots, r\}$ with $|J| = k$ and let $\boldsymbol{\alpha} = (\alpha_j)_{j\in J} \in (\mathbb{F}_p)^k$. Using the quadratic character η of $\mathbb{F}_q$ to detect the squares of $\mathbb{F}_q^*$, we obtain

$$\begin{aligned}|\mathcal{F}_q(aX^2, k, J, \boldsymbol{\alpha})| &= \sum_{\substack{x\in\mathbb{F}_q \\ \varepsilon_j(ax^2)=\alpha_j, \forall\, j\in J}} 1 = \mathbb{1}_{\boldsymbol{\alpha}=\mathbf{0}} + \sum_{\substack{y\in\mathbb{F}_q^* \\ \varepsilon_j(ay)=\alpha_j, \forall\, j\in J}} (1+\eta(y)) \\ &= \frac{q}{p^k} + \sum_{\substack{y\in\mathbb{F}_q^* \\ \varepsilon_j(ay)=\alpha_j, \forall\, j\in J}} \eta(y) = \frac{q}{p^k} + \eta(a) \sum_{\substack{x\in\mathbb{F}_q^* \\ \varepsilon_j(x)=\alpha_j, \forall\, j\in J}} \eta(x).\end{aligned}$$

For each $j \in J$, since ε_j is a $\mathbb{F}_p$-linear form, by Theorem 2.24 of [38], there exists a unique $b_j \in \mathbb{F}_q$ such that, for any $x \in \mathbb{F}_q$, $\varepsilon_j(x) = \mathrm{Tr}(b_j x)$. Hence, with the notation (IV.9), we have

$$\left||\mathcal{F}_q(aX^2, k, J, \boldsymbol{\alpha})| - q/p^k\right| = |S_\eta(k, \mathbf{b}, \boldsymbol{\alpha})| \tag{IV.20}$$

where $\mathbf{b} = (b_j)_{j\in J}$ and $\boldsymbol{\alpha} = (\alpha_j)_{j\in J}$. Moreover, since $\{\varepsilon_j,\ j \in J\}$ is a set of independent linear forms, one can easily see that $\{b_j,\ j \in J\}$ is a set of linearly independent elements. It follows from Proposition 4.4 applied with $\chi = \eta$ and from Lemma 5.1 that

$$|S_\eta(k, \mathbf{b}, \boldsymbol{\alpha})| \leq \begin{cases} \dfrac{\sqrt{q}}{\sqrt{p}} & \text{if } \boldsymbol{\alpha} \neq \mathbf{0} \text{ and } r \text{ is odd,} \\ \left(\dfrac{2}{p} - \dfrac{1}{p^k}\right)\sqrt{q} & \text{if } \boldsymbol{\alpha} \neq \mathbf{0} \text{ and } r \text{ is even,} \\ 0 & \text{if } \boldsymbol{\alpha} = \mathbf{0} \text{ and } r \text{ is odd,} \\ \dfrac{p^k-1}{p^k}\sqrt{q} & \text{if } \boldsymbol{\alpha} = \mathbf{0} \text{ and } r \text{ is even.} \end{cases} \tag{IV.21}$$

To complete the proof of Theorem 1.3, it suffices to insert this into (IV.20).

Remark 5.2. For $k = 1$, by Remark 4.5, (IV.21) is always an equality and thus, by (IV.20), (IV.5) is also always an equality. For $k = 2$ or $k = 3$, there are nontrivial cases where (IV.5) is again an equality. For instance, in each of the following situations, Sage permits us to check that (IV.5) is an equality for any $a \in \mathbb{F}_q^*$ ($f \in \mathbb{F}_p[X]$ is an irreducible polynomial of degree r, $\mathbb{F}_q = \mathbb{F}_{p^r} = \mathbb{F}_p(x_0)$ where x_0 is a root of f and we consider the basis $\mathcal{B} = \{e_1, \dots, e_r\}$ of $\mathbb{F}_q$ over $\mathbb{F}_p$ where for any $1 \leq j \leq r$, $e_j = x_0^{j-1}$):

- $p = 5$, $r = 7$, $f = X^7 + 3X + 3$, $J = \{1, 6\}$ and $\boldsymbol{\alpha} = (2, 4)$,
- $p = 3$, $r = 10$, $f = X^{10} + 2X^6 + 2X^5 + 2X^4 + X + 2$, $J = \{1, 3\}$ and $\boldsymbol{\alpha} = (0, 0)$ or $J = \{1, 4\}$ and $\boldsymbol{\alpha} = (1, 0)$,
- $p = 3$, $r = 11$, $f = X^{11} + 2X^2 + 1$, $J = \{1, 2, 5\}$ and $\boldsymbol{\alpha} = (0, 2, 1)$.

5.2. Proof of Corollaries 1.4 and 1.5

Let $\varepsilon > 0$. If p is a prime number such that $p \geq 3$, if $r \geq 2$ is even, if $k \leq (1/2 - \varepsilon)r + 1$, if $a \in \mathbb{F}_q^*$, if $\mathcal{B}$ is a basis of $\mathbb{F}_{p^r}$ over $\mathbb{F}_p$, if $J \subset \{1, \dots, r\}$ is such that $|J| = k$ and if $\boldsymbol{\alpha} \in (\mathbb{F}_p)^k$, $\boldsymbol{\alpha} \neq \mathbf{0}$ then, by Theorem 1.3,

$$p^{-(r-k)} \left| |\mathcal{F}_{p^r}(aX^2, k, J, \boldsymbol{\alpha})| - p^{r-k} \right| \leq 2p^{k-r/2-1} \leq p^{-\varepsilon r} = o(1)$$

as $p^r \to +\infty$, which completes the proof of Corollary 1.4. Corollary 1.5 can be proved similarly.

6. Prescribing the digits of $P(g)$

6.1. Additive character sums with generator arguments

The proof of Lemma 4.1 in [12] permits us to show that: if $P \in \mathbb{F}_q[X]$ is a polynomial of degree n with $(n, q) = 1$ and if ψ is a nontrivial additive character of $\mathbb{F}_q$ then we have the upper bound

$$\left| \sum_{g \in \mathcal{G}} \psi(P(g)) \right| \leq (n2^{\omega(q-1)} - 1)\sqrt{q} + \frac{\varphi(q-1)}{q-1}. \tag{IV.22}$$

In this section, we will obtain the following result which improves the main term in the right-hand side of (IV.22) by a factor $\frac{\varphi(q-1)}{q-1}$.

Proposition 6.1. *If $P \in \mathbb{F}_q[X]$ is a polynomial of degree n with $(n, q) = 1$ and if ψ is a nontrivial additive character of $\mathbb{F}_q$ then we have the upper bound*

$$\left| \sum_{g \in \mathcal{G}} \psi(P(g)) \right| \leq \frac{\varphi(q-1)}{q-1} \left((n2^{\omega(q-1)} - 1)\sqrt{q} + 1 \right). \tag{IV.23}$$

Let us first observe that the upper bound in (IV.23) is sharp. For that purpose, we consider the nontrivial case where $p = 3$, $r = 2$ and $P(X) = X$. Let α be a root of the irreducible polynomial $X^2 + 2X + 2 \in \mathbb{F}_3[X]$ and let $\mathbb{F}_9 = \mathbb{F}_3(\alpha)$. Then, the set $\{1, \alpha\}$ is a basis of $\mathbb{F}_9$ as a $\mathbb{F}_3$-vector space. The generators of $\mathbb{F}_9^*$ are α, $\alpha^3 = 1 + 2\alpha$, $\alpha^5 = 2\alpha$ and $\alpha^7 = \alpha + 2$. On the one hand, if ψ is the additive character of $\mathbb{F}_9$ defined by $\psi(1) = 1$ and $\psi(\alpha) = \mathrm{e}\left(\frac{1}{3}\right)$, then

$$\sum_{g \in \mathcal{G}} \psi(g) = \mathrm{e}\left(\frac{1}{3}\right) + \mathrm{e}\left(\frac{2}{3}\right) + \mathrm{e}\left(\frac{2}{3}\right) + \mathrm{e}\left(\frac{1}{3}\right) = -2.$$

On the other hand, $\frac{\varphi(q-1)}{q-1}\left((n2^{\omega(q-1)} - 1)\sqrt{q} + 1\right) = 2$. Thus, (IV.23) may be an equality, which shows the sharpness of the upper bound in (IV.23).

Proof of Proposition 6.1. Let $P \in \mathbb{F}_q[X]$ be a polynomial of degree n with $(n, q) = 1$ and let ψ be a nontrivial additive character of $\mathbb{F}_q$. Orthogonality relations for multiplicative characters

of $\mathbb{F}_q$ permit us to detect the generators of $\mathbb{F}_q^*$:

$$\sum_{g\in\mathcal{G}}\psi(P(g)) = \sum_{x\in\mathbb{F}_q^*}\psi(P(x))\sum_{g\in\mathcal{G}}\frac{1}{q-1}\sum_{\chi}\chi(x)\overline{\chi(g)},$$

hence,

$$\left|\sum_{g\in\mathcal{G}}\psi(P(g))\right| \leq \frac{1}{q-1}\sum_{\chi}\left|\sum_{g\in\mathcal{G}}\chi(g)\right|\left|\sum_{x\in\mathbb{F}_q^*}\psi(P(x))\chi(x)\right|. \tag{IV.24}$$

Moreover, by Theorem 2.1,

$$\left|\sum_{x\in\mathbb{F}_q^*}\psi(P(x))\chi(x)\right| \leq \begin{cases} (n-1)\sqrt{q}+1 & \text{if } \chi=\chi_0,\\ n\sqrt{q} & \text{otherwise.}\end{cases}$$

Isolating the term corresponding to $\chi=\chi_0$ in (IV.24), we deduce

$$\left|\sum_{g\in\mathcal{G}}\psi(P(g))\right| \leq \frac{\varphi(q-1)}{q-1}((n-1)\sqrt{q}+1) + \frac{n\sqrt{q}}{q-1}\sum_{\chi\neq\chi_0}\left|\sum_{g\in\mathcal{G}}\chi(g)\right|. \tag{IV.25}$$

If g_0 is a fixed generator of $\mathbb{F}_q^*$ then the $q-1$ multiplicative characters of $\mathbb{F}_q$ are $\chi_1,\ldots,\chi_{q-1}$ where, for any $j\in\{1,\ldots,q-1\}$, χ_j is given by $\chi_j(g_0)=\mathrm{e}\left(\frac{j}{q-1}\right)$ (see Theorem 5.8 of [38]), hence

$$\sum_{\chi}\left|\sum_{g\in\mathcal{G}}\chi(g)\right| = \sum_{j=1}^{q-1}\left|\sum_{\substack{1\leq k\leq q-1\\(k,q-1)=1}}\mathrm{e}\left(\frac{jk}{q-1}\right)\right| = \varphi(q-1)\sum_{j=1}^{q-1}\frac{\mu^2}{\varphi}\left(\frac{q-1}{(j,q-1)}\right) \tag{IV.26}$$

where the last equality holds by Theorem 272 of [28]. Moreover,

$$\sum_{j=1}^{q-1}\frac{\mu^2}{\varphi}\left(\frac{q-1}{(j,q-1)}\right) = \sum_{d|q-1}\frac{\mu^2}{\varphi}(d)\sum_{\substack{1\leq j\leq q-1\\(j,q-1)=\frac{q-1}{d}}}1 = \sum_{d|q-1}\mu^2(d) = 2^{\omega(q-1)}$$

where the last equality holds by Theorem 264 of [28]. It follows that (IV.26) equals $\varphi(q-1)2^{\omega(q-1)}$ and inserting this into (IV.25), we finally obtain

$$\left|\sum_{g\in\mathcal{G}}\psi(P(g))\right| \leq \frac{\varphi(q-1)}{q-1}\left((n2^{\omega(q-1)}-1)\sqrt{q}+1\right)$$

which completes the proof of Proposition 6.1. □

6.2. Proof of Theorem 1.6

To obtain (IV.6), it suffices to adapt the proof of Theorem 1.1 by replacing the sums over $x \in \mathbb{F}_q$ by sums over $g \in \mathcal{G}$ and by using Proposition 6.1 instead of Theorem 2.1.

If $n(p^k-1) < \sqrt{q}/2^{\omega(q-1)}$ then it follows from (IV.6) that

$$\begin{aligned}\left||\mathcal{G} \cap \mathcal{F}_q(P,k,J,\boldsymbol{\alpha})| - \frac{\varphi(q-1)}{p^k}\right| &\leq \frac{p^k-1}{p^k}\frac{\varphi(q-1)}{q-1}\left(n2^{\omega(q-1)}\sqrt{q} - \frac{1}{p^k-1}\right)\\ &< \frac{p^k-1}{p^k}\frac{\varphi(q-1)}{q-1}\left(\frac{q}{p^k-1} - \frac{1}{p^k-1}\right)\\ &= \frac{\varphi(q-1)}{p^k}\end{aligned}$$

and thus $|\mathcal{G} \cap \mathcal{F}_q(P,k,J,\boldsymbol{\alpha})| \neq \varnothing$, which completes the proof of Theorem 1.6.

6.3. Proof of Corollary 1.8

Let $n \geq 1$ and let $\varepsilon > 0$. If p is a prime number such that $p \nmid n$, if $r \geq 2$, if $k \leq (1/2-\varepsilon)r$, if $P \in \mathbb{F}_{p^r}[X]$ is of degree n, if $\mathcal{B}$ is a basis of $\mathbb{F}_{p^r}$ over $\mathbb{F}_p$, if $J \subset \{1,\dots,r\}$ is such that $|J| = k$ and if $\boldsymbol{\alpha} \in (\mathbb{F}_p)^k$ then, by Theorem 1.6,

$$\begin{aligned}\frac{p^k}{\varphi(q-1)}\left||\mathcal{G} \cap \mathcal{F}_{p^r}(P,k,J,\boldsymbol{\alpha})| - \frac{\varphi(q-1)}{p^k}\right| &\leq \frac{p^k-1}{q-1}\left((n2^{\omega(q-1)}-1)\sqrt{q}+1\right)\\ &\leq \frac{2p^k}{q}\,n2^{\omega(q-1)}\sqrt{q} \leq 2n\,\frac{2^{\omega(q-1)}}{q^{\varepsilon}}\end{aligned}$$

and since $2^{\omega(q-1)} \leq \tau(q-1) = O_\varepsilon(q^{\varepsilon/2})$ where $\tau(q-1)$ is the number of divisors of $q-1$ (see for instance Theorem 315 of [28]), $2n\,2^{\omega(q-1)}q^{-\varepsilon} = o(1)$ as $q = p^r \to +\infty$, which completes the proof of Corollary 1.8.

V. Trace de produits dans les corps finis

Le contenu de ce chapitre est publié dans « Finite Fields and Their Applications » [67] à l'exception de la partie 7 dans laquelle on présente de nouveaux résultats.

ABSTRACT. Let p be a prime number and let $q = p^r$. If $\mathcal{C}$ and $\mathcal{D}$ are large subsets of $\mathbb{F}_q^*$ we study the trace of products cd with $c \in \mathcal{C}$ and $d \in \mathcal{D}$ and show that it is well distributed in $\mathbb{F}_p$. We give an optimal condition (up to an absolute constant factor) on the size of the subsets $\mathcal{C}$ and $\mathcal{D}$ to ensure that the trace of products cd takes any given value in $\mathbb{F}_p$. We also give a condition (optimal up to an absolute constant factor in most cases) on the size of the subsets $\mathcal{C}$ and $\mathcal{D}$ to ensure that the trace of cd meets the set of k-th powers for $k \geq 1$, respectively the set of generators. Our method will enable us to take sets $\mathcal{C}$ and $\mathcal{D}$ whose size is substantially below $\sqrt{q}$. Character sums and Gaussian sums over $\mathbb{F}_p$ and $\mathbb{F}_q$ will play an important role in the proofs. Some estimates lead to interesting combinatorial questions in finite fields.

Table of contents

1. Introduction

1.1. Motivation

The study of the connection between the arithmetic properties of an integer and the properties of its digits in a given basis produces a lot of interesting questions and a lot of papers have been devoted to this topic. In particular, Gelfond [25] proved an asymptotic formula for the number of integers of an arithmetic progression whose sum of digits modulo m is fixed. More recently, Mauduit and Rivat [43, 44] obtained an asymptotic formula for the number of prime numbers and also for the number of squares whose sum of digits modulo m is fixed. In another direction, Maynard [48] showed in a recent work that there are infinitely many prime numbers with one missing digit (e.g. no digit 9) in their decimal expansion.

In the context of finite fields, the algebraic structure permits us to formulate and study new problems of interest which might be out of reach in the context of natural integers [38, 52]. In [12], Dartyge and Sárközy initiated the study of the concept of digits in the context of finite fields. Let p be a prime number, let $q = p^r$ with $r \geq 2$ and consider the finite field $\mathbb{F}_q$. If $\mathcal{B} = \{e_1, \ldots, e_r\}$ is a basis of $\mathbb{F}_q$ viewed as a $\mathbb{F}_p$-vector space then every $x \in \mathbb{F}_q$ can be written uniquely in base $\mathcal{B}$:

$$x = \sum_{j=1}^{r} c_j e_j \tag{V.1}$$

with $c_1, \ldots, c_r \in \mathbb{F}_p$. In [12], $c_1, \ldots, c_r$ are called the "digits" of x and the function $s_{\mathcal{B}}$ defined on $\mathbb{F}_q$ by

$$s_{\mathcal{B}}(x) = \sum_{j=1}^{r} c_j \tag{V.2}$$

is called the "sum of digits" function. Dartyge and Sárközy estimated the number of squares in $\mathbb{F}_q$ whose sum of digits is fixed and also obtained results for polynomial values, resp. polynomial values with generator arguments whose sum of digits is fixed. Further problems on digits in finite fields have been studied by Dartyge, Mauduit, Sárközy [11], Dietmann, Elsholtz, Shparlinski [16] and Gabdullin [23]. In particular, an estimate of the number of squares in $\mathbb{F}_q$ with restricted digits has been proved in [11] and then improved in [16] and [23].

In [59], Rivat and Sárközy provided a "possibly complete" list of the papers written on arithmetic properties of products and showed that if $\mathcal{C}$ and $\mathcal{D}$ are large subsets of $\{1, \ldots, N\}$ then the sum of digits of the products cd with $c \in \mathcal{C}$ and $d \in \mathcal{D}$ is well distributed modulo m. We will study a local analog of this result in the context of finite fields. Instead of the sum of digits function $s_{\mathcal{B}}$, we will consider the trace function Tr from $\mathbb{F}_q$ to $\mathbb{F}_p$ which is of basic importance in finite fields (see [38, 52]) and can be used to describe all $\mathbb{F}_p$-linear forms on $\mathbb{F}_q$. In particular, given a basis $\mathcal{B}$, there exists $\alpha \in \mathbb{F}_q^*$ (α is the sum of the elements of the dual basis of $\mathcal{B}$) such that, for any $x \in \mathbb{F}_q$,

$$s_{\mathcal{B}}(x) = \mathrm{Tr}(\alpha x).$$

Therefore, any question on $s_{\mathcal{B}}$ can be reduced to a question on the trace (see below). We will

estimate the number of pairs $(c,d) \in \mathcal{C} \times \mathcal{D}$ such that the trace of the product cd is fixed and we will deduce that if $\mathcal{C}$ and $\mathcal{D}$ are large subsets of $\mathbb{F}_q^*$ then $\mathrm{Tr}(cd)$ is well distributed in $\mathbb{F}_p$.

The study of integers whose sum of digits belongs to a specific sequence is quite difficult. Beyond arithmetic progressions (Gelfond), it would be interesting to consider the case of prime values and square or polynomial values, but these problems seem to be out of reach of present methods. In the context of finite fields, we will be able to study products cd whose trace belongs to some interesting subsets of $\mathbb{F}_p$. More precisely, for some subsets $\mathcal{A}$ of $\mathbb{F}_p$, we will give a nontrivial condition on the "size" of the sets $\mathcal{C}$ and $\mathcal{D}$ to ensure that there exists $(c,d) \in \mathcal{C} \times \mathcal{D}$ such that $\mathrm{Tr}(cd)$ belongs to $\mathcal{A}$. The set $\mathcal{A}$ will be either a singleton, or any subgroup of $\mathbb{F}_p^*$ (for instance the set of squares or more generally the set of k-th powers) or the set of generators of $\mathbb{F}_p^*$. In most of these situations, we will prove that our result is optimal up to an absolute constant factor.

More generally, since any $\mathbb{F}_p$-linear form can be expressed with the help of the trace function, we will see that the study of products whose image by a given nonzero $\mathbb{F}_p$-linear form belongs to $\mathcal{A}$ can be reduced to the study of products whose trace belongs to $\mathcal{A}$.

1.2. Statement of results

Let p be a prime number, let $q = p^r$ with $r \geq 2$ and let Tr be the trace from $\mathbb{F}_q$ to $\mathbb{F}_p$ defined for $x \in \mathbb{F}_q$ by:

$$\mathrm{Tr}(x) = x + x^p + \cdots + x^{p^{r-1}}.$$

Note that Tr is an $\mathbb{F}_p$-linear form (see [38, Theorem 2.23]). Let $\mathcal{A}$ be a nonempty subset of $\mathbb{F}_p$. If f is a nonzero $\mathbb{F}_p$-linear form on $\mathbb{F}_q$ then there exists $\alpha \in \mathbb{F}_q^*$ such that, for any $x \in \mathbb{F}_q$, $f(x) = \mathrm{Tr}(\alpha x)$ (see [38, Theorem 2.24]) and thus, for any nonempty subsets $\mathcal{C}'$ and $\mathcal{D}'$ of $\mathbb{F}_q^*$,

$$|\{(c',d') \in \mathcal{C}' \times \mathcal{D}' : f(c'd') \in \mathcal{A}\}| = |\{(c,d) \in \mathcal{C} \times \mathcal{D} : \mathrm{Tr}(cd) \in \mathcal{A}\}|$$

where $\mathcal{C} = \alpha\mathcal{C}'$ and $\mathcal{D} = \mathcal{D}'$; it follows that the study of the number of pairs $(c',d') \in \mathcal{C}' \times \mathcal{D}'$ such that $f(c'd') \in \mathcal{A}$ can be reduced to the study of $|\mathcal{E}_\mathcal{A}|$ where $\mathcal{E}_\mathcal{A}$ is defined by

$$\mathcal{E}_\mathcal{A} = \{(c,d) \in \mathcal{C} \times \mathcal{D} : \mathrm{Tr}(cd) \in \mathcal{A}\}$$

for nonempty subsets $\mathcal{C}$ and $\mathcal{D}$ of $\mathbb{F}_q^*$. Throughout this paper, we will study the cardinality of $\mathcal{E}_\mathcal{A}$ for some interesting sets $\mathcal{A}$. If $\mathcal{A}$ contains only one element s, we will simply write $\mathcal{E}_s$ in place of $\mathcal{E}_{\{s\}}$.

First, we will obtain a sharp estimate of the number of pairs $(c,d) \in \mathcal{C} \times \mathcal{D}$ such that the trace of cd is fixed.

Theorem 1.1. *Let s be any element of $\mathbb{F}_p$. The cardinality of the set $\mathcal{E}_s$ satisfies*

$$\left| |\mathcal{E}_s| - \frac{|\mathcal{C}||\mathcal{D}|}{p} \right| \leq \sqrt{q}\sqrt{|\mathcal{C}||\mathcal{D}|}. \tag{V.3}$$

It follows that the traces $\mathrm{Tr}(cd)$ are well distributed in $\mathbb{F}_p$ as soon as $p^2 q = o(|\mathcal{C}||\mathcal{D}|)$. This

provides a very big range of admissible values of $|\mathcal{C}||\mathcal{D}|$. In particular, if $|\mathcal{C}| = |\mathcal{D}|$ it is sufficient to suppose $p\sqrt{q} = o(|\mathcal{C}|)$ to ensure the well distribution of $\mathrm{Tr}(cd)$ in $\mathbb{F}_p$.

Theorem 1.1 will be proved in Section 3.5. We will first show an estimate of $|\mathcal{E}_s|$ when $s \neq 0$ (see Proposition 3.1) and then an estimate of $|\mathcal{E}_0|$ (see Proposition 3.2). We will also show in Section 3.6 that the upper bound in (V.3) is optimal up to an absolute constant factor: we can construct sets $\mathcal{C}$ and $\mathcal{D}$ such that

$$\left| |\mathcal{E}_0| - \frac{|\mathcal{C}||\mathcal{D}|}{p} \right| > \frac{1}{\sqrt{128}} \sqrt{q} \sqrt{|\mathcal{C}||\mathcal{D}|}.$$

Another immediate consequence of Theorem 1.1 is that if $s \in \mathbb{F}_p$ and if

$$|\mathcal{C}||\mathcal{D}| > p^2 q \tag{V.4}$$

then the set $\mathcal{E}_s$ is nonempty which means that the traces $\mathrm{Tr}(cd)$ take the value s. Considering separately the cases $s \neq 0$ and $s = 0$ and using directly the corresponding estimate of $|\mathcal{E}_s|$ (see Propositions 3.1 and 3.2), we are able to show that this still holds true with a lower bound sharper than (V.4):

Theorem 1.2. *Let $s \in \mathbb{F}_p^*$. If $\mathcal{C}$ and $\mathcal{D}$ are nonempty subsets of $\mathbb{F}_q^*$ satisfying*

$$|\mathcal{C}||\mathcal{D}| \geq pq \tag{V.5}$$

then there exists $(c, d) \in \mathcal{C} \times \mathcal{D}$ such that $\mathrm{Tr}(cd) = s$.

We will see in Section 3.2 that condition (V.5) is optimal up to an absolute constant factor: we can find explicit sets $\mathcal{C}$ and $\mathcal{D}$ such that $pq/16 < |\mathcal{C}||\mathcal{D}| < pq$ and for which $\mathcal{E}_s = \varnothing$.

To study the special case where $s = 0$, we define for any nonempty set $\mathcal{C} \subset \mathbb{F}_q^*$,

$$\Delta_0(\mathcal{C}) = \frac{|\mathcal{C}|}{q-1} - \frac{1}{p-1} \sum_{s \in \mathbb{F}_p^* \setminus \{1\}} \frac{|\mathcal{C} \cap s\mathcal{C}|}{|\mathcal{C}|} \tag{V.6}$$

and we will obtain the following result.

Theorem 1.3. *If $\mathcal{C}$ and $\mathcal{D}$ are nonempty subsets of $\mathbb{F}_q^*$ satisfying*

$$|\mathcal{C}||\mathcal{D}| > q \left(\frac{q-1}{q-p} \right)^2 \tag{V.7}$$

and

$$\Delta_0(\mathcal{C}) \geq 0 \quad \text{and} \quad \Delta_0(\mathcal{D}) \geq 0 \tag{V.8}$$

then there exists $(c, d) \in \mathcal{C} \times \mathcal{D}$ such that $\mathrm{Tr}(cd) = 0$.

Remark 1.4. Since $\frac{q-1}{q-p} < 2$, Theorem 1.3 holds true with condition (V.7) replaced by:

$$|\mathcal{C}||\mathcal{D}| \geq 4q. \tag{V.9}$$

Again, we will see in Section 3.4 that conditions (V.7) and (V.9) are optimal up to an absolute constant factor: we can construct sets $\mathcal{C}$ and $\mathcal{D}$ satisfying (V.8) such that

$$\frac{q}{32}\left(\frac{q-1}{q-p}\right)^2 < \frac{q}{8} < |\mathcal{C}||\mathcal{D}| \leq q\left(\frac{q-1}{q-p}\right)^2 < 4q$$

and for which $\mathcal{E}_0 = \varnothing$.

The rather technical condition (V.8) arises naturally from the proof. We will study this condition in Section 6 where some estimates will lead to interesting combinatorial questions. An explicit formula for the average of $|\mathcal{C} \cap s\mathcal{C}|$ over all subsets $\mathcal{C} \subset \mathbb{F}_q^*$ with fixed cardinality will be proved in Section 6.1. In Section 6.2, we will show that (V.8) is true "on average" and then, in Section 6.3, we will give explicit examples of subsets of $\mathbb{F}_q^*$ satisfying (V.8).

It would be interesting to go further in the study of the quantity $|\mathcal{C} \cap s\mathcal{C}|$. Gowers asked whether, if G is an abelian group of prime order p and if $\mathcal{C}$ is a subset of G of size $\lfloor p/2 \rfloor$, there exists $x \in G$ such that

$$||\mathcal{C} \cap x\mathcal{C}| - p/4| = o(p).$$

Note that $p/4$ is the expected value of $|\mathcal{C} \cap x\mathcal{C}|$. Green and Konyagin [26] considered a generalization of Gowers' question in a quantitative way and proved that: if $|\mathcal{C}| = \gamma p$ then there exists $x \in G$ such that

$$\left||\mathcal{C} \cap x\mathcal{C}| - \gamma^2 p\right| = O\left(p(\log\log p/\log p)^{1/3}\right).$$

One appealing feature of Gowers' question is that similar statements do not hold if $G = \mathbb{F}_q^*$. For instance, for $p \geq 3$, if $\mathcal{C}$ is the subgroup of squares in $\mathbb{F}_q^*$ then $|\mathcal{C}| = \gamma|G|$ with $\gamma = 1/2$ and since $\mathcal{C} \cap x\mathcal{C} = \varnothing$ or $\mathcal{C}$, clearly, there is no $x \in G$ such that

$$\left||\mathcal{C} \cap x\mathcal{C}| - \gamma^2|G|\right| = o(|G|). \tag{V.10}$$

This leads to ask the following:

Question 1.5. Characterize the subsets $\mathcal{C}$ of $G = \mathbb{F}_q^*$ such that $|\mathcal{C}| = \gamma|G|$ and for which $\mathcal{C} \cap x\mathcal{C}$ never satisfies (V.10).

This seems to be a difficult open question.

In Sections 4 and 5, we will consider products cd whose trace is in some interesting subsets $\mathcal{A}$ of $\mathbb{F}_p$. In each situation, we will provide an estimate of $|\mathcal{E}_{\mathcal{A}}|$ (see Propositions 4.1 and 5.2) by a similar method but some new difficulties will arise when trying to take advantage of the structure of the set $\mathcal{A}$. In particular, we will need to compute character sums over $\mathcal{A}$. Our method will enable us to take sets $\mathcal{C}$ and $\mathcal{D}$ whose size is substantially below $\sqrt{q}$.

For a subgroup $\mathcal{A}$ of $\mathbb{F}_p^*$ with $|\mathcal{A}| = m$, we define for any nonempty set $\mathcal{C} \subset \mathbb{F}_q^*$

$$\Delta_{\mathcal{A}}(\mathcal{C}) = \frac{|\mathcal{C}|}{q-1} - \frac{1}{m}\sum_{s \in \mathcal{A}\setminus\{1\}} \frac{|\mathcal{C} \cap s\mathcal{C}|}{|\mathcal{C}|} \tag{V.11}$$

and we will obtain the following result.

Theorem 1.6. *Let m be any divisor of $p-1$ and let $\mathcal{A}$ be the subgroup of $\mathbb{F}_p^*$ of order m. If $\mathcal{C}$ and $\mathcal{D}$ are nonempty subsets of $\mathbb{F}_q^*$ satisfying*

$$|\mathcal{C}||\mathcal{D}| \geq \frac{pq}{m^2} \tag{V.12}$$

and

$$\Delta_{\mathcal{A}}(\mathcal{C}) \geq 0 \quad \text{and} \quad \Delta_{\mathcal{A}}(\mathcal{D}) \geq 0 \tag{V.13}$$

then there exists $(c,d) \in \mathcal{C} \times \mathcal{D}$ such that $\mathrm{Tr}(cd) \in \mathcal{A}$.

Here also condition (V.13) arises naturally from the proof (see Section (4.2)). As for Theorem 1.3, we will show in Section 6.2 that this condition is true "on average".

If $p = 2$ then $\mathcal{A} = \{1\}$ and condition (V.13) is trivially satisfied. Thus, for $p = 2$, Theorem 1.6 is exactly Theorem 1.2 with $s = 1$. For $p \geq 3$ and $m \neq p-1$, we will see in Section 4.3 that condition (V.12) is optimal up to an absolute constant factor: we can find explicit sets $\mathcal{C}$ and $\mathcal{D}$ satisfying (V.13) such that $pq/(16m^2) < |\mathcal{C}||\mathcal{D}| < pq/m^2$ and for which $\mathrm{Tr}(cd)$ never belongs to $\mathcal{A}$. For $p \geq 3$ and $m = p-1$, we will see in Section 4.3 that condition (V.12) is sharp up to a factor $4p$: we can find explicit sets $\mathcal{C}$ and $\mathcal{D}$ satisfying (V.13) such that $q/(4(p-1)^2) < |\mathcal{C}||\mathcal{D}| = q/p^2 < pq/(p-1)^2$ and for which $\mathrm{Tr}(cd)$ is always 0.

Applying this result with $\mathcal{A} = \mathcal{A}_k$ where $\mathcal{A}_k$ is the set of k-th powers in $\mathbb{F}_p^*$, we will obtain

Corollary 1.7. *Assume $p \geq 3$ and let $k \geq 1$ be an integer. If $\mathcal{C}$ and $\mathcal{D}$ are nonempty subsets of $\mathbb{F}_q^*$ satisfying condition (V.13) with $\mathcal{A} = \mathcal{A}_k$ and such that*

$$|\mathcal{C}||\mathcal{D}| \geq \frac{p(k,p-1)^2}{(p-1)^2}\, q \tag{V.14}$$

then there exists $(c,d) \in \mathcal{C} \times \mathcal{D}$ such that $\mathrm{Tr}(cd)$ is a k-th power in $\mathbb{F}_p^*$.

We will see in Section 4.4 that if $(k, p-1) \neq 1$ then (V.14) is optimal up to an absolute constant factor.

In the special case where $k = 2$, Corollary 1.7 becomes

Corollary 1.8. *Assume $p \geq 3$ and let $\mathcal{Q}_p$ be the set of squares in $\mathbb{F}_p^*$. If $\mathcal{C}$ and $\mathcal{D}$ are nonempty subsets of $\mathbb{F}_q^*$ satisfying condition (V.13) with $\mathcal{A} = \mathcal{Q}_p$ and such that*

$$|\mathcal{C}||\mathcal{D}| \geq \frac{4pq}{(p-1)^2} \tag{V.15}$$

then there exists $(c,d) \in \mathcal{C} \times \mathcal{D}$ such that $\mathrm{Tr}(cd)$ is a square in $\mathbb{F}_p^*$.

In particular, if $|\mathcal{C}| = |\mathcal{D}|$ it is sufficient to suppose $|\mathcal{C}| \geq \frac{2\sqrt{p}}{p-1}\sqrt{q}$ to ensure that condition (V.15) is satisfied. Thus, Corollary 1.8 can be applied to sets $\mathcal{C}$ and $\mathcal{D}$ whose size is substantially below $\sqrt{q}$.

The optimality up to an absolute constant factor of condition (V.14) implies that condition (V.15) is also optimal up to an absolute constant factor. In Section 4.5, we will give explicit

examples of sets $\mathcal{C}$ and $\mathcal{D}$ satisfying (V.13) with $\mathcal{A} = \mathcal{Q}_p$ such that $\frac{pq}{4(p-1)^2} < |\mathcal{C}||\mathcal{D}| = \frac{q}{p} < \frac{4pq}{(p-1)^2}$ and for which $\mathrm{Tr}(cd)$ is never a square.

Finally, we study the case where $\mathcal{A}$ is the set $\mathcal{G}_p$ of generators of $\mathbb{F}_p^*$. We denote by $\omega(n)$ the number of distinct prime factors of n and we define for $k \geq 1$,

$$m_k = 2^{\omega((k,p-1))} \prod_{\substack{p' \mid p-1 \\ p' \nmid k}} \frac{p'-2}{p'-1} \tag{V.16}$$

where the product runs over all prime divisors p' of $p-1$ not dividing k. We define also for any $g_0 \in \mathcal{G}_p$ and any nonempty set $\mathcal{C} \subset \mathbb{F}_q^*$

$$\Delta_{\mathcal{G}}(g_0, \mathcal{C}) = \frac{|\mathcal{C}|}{q-1} - \frac{1}{p-1} \sum_{k=1}^{p-2} \frac{|\mathcal{C} \cap g_0^k \mathcal{C}|}{|\mathcal{C}|} m_k \tag{V.17}$$

and we will show in Lemma 5.1 that $\Delta_{\mathcal{G}}(g_0, \mathcal{C})$ does not depend on $g_0 \in \mathcal{G}_p$, thus we may write $\Delta_{\mathcal{G}}(\mathcal{C}) = \Delta_{\mathcal{G}}(g_0, \mathcal{C})$. We will obtain the following result.

Theorem 1.9. *If $\mathcal{C}$ and $\mathcal{D}$ are nonempty subsets of $\mathbb{F}_q^*$ satisfying*

$$|\mathcal{C}||\mathcal{D}| \geq 4q \frac{2^{2\omega(p-1)}}{p} \tag{V.18}$$

and

$$\Delta_{\mathcal{G}}(\mathcal{C}) \geq 0 \quad \text{and} \quad \Delta_{\mathcal{G}}(\mathcal{D}) \geq 0 \tag{V.19}$$

then there exists $(c, d) \in \mathcal{C} \times \mathcal{D}$ such that $\mathrm{Tr}(cd) \in \mathcal{G}_p$.

Using the inequality $\omega(n) \leq (1 + o(1)) \log n / \log \log n$ (see [68, p. 122]), (V.18) becomes

$$|\mathcal{C}||\mathcal{D}| \geq \frac{q}{p} p^{o(1)}.$$

Remark 1.10. Heuristically, according to the normal order of $\omega(n)$ (see [28, Theorem 431]), for almost all values of p, it is expected that $\omega(p-1) = O(\log \log p)$. Under this assumption, (V.18) becomes

$$|\mathcal{C}||\mathcal{D}| \geq \frac{4q}{p} (\log p)^K$$

for some constant $K > 0$.

The condition (V.19) and the coefficients m_k arise naturally from the proof. If $p \geq 3$, it follows immediately from (V.16) that only the even k can have a contribution in the sum appearing in (V.17). We will show in Section 6.2 that condition (V.19) is true "on average" and we will give at the end of Section 5.2 an explicit example of sets $\mathcal{C}$ and $\mathcal{D}$ satisfying (V.19) such that $|\mathcal{C}||\mathcal{D}| = q/p$ and for which $\mathrm{Tr}(cd)$ never meets the set $\mathcal{G}_p$ (for $p \geq 3$).

1.3. Notations

We use the notation $\mathrm{e}(t) = \exp(2i\pi t)$.

The trivial additive character of $\mathbb{F}_q$ is denoted by ψ_0 and the trivial multiplicative character of $\mathbb{F}_q$ is denoted by χ_0. The trivial multiplicative character of $\mathbb{F}_p$ is simply denoted by 1. The field $\mathbb{F}_p$ will be seen as a subfield of $\mathbb{F}_q$ so that every multiplicative character χ of $\mathbb{F}_q$ induces a multiplicative character of $\mathbb{F}_p$ denoted by $\chi_{|\mathbb{F}_p^*}$.

The trace Tr from $\mathbb{F}_q$ to $\mathbb{F}_p$ is an $\mathbb{F}_p$-linear form and permits defining the canonical additive character ψ_1 of $\mathbb{F}_q$ by:

$$\psi_1(x) = \mathrm{e}\left(\frac{\mathrm{Tr}(x)}{p}\right). \tag{V.20}$$

The character ψ_1 will be of particular interest to handle conditions on the trace.

We introduce the following notations for Gaussian sums. If χ is a multiplicative character of $\mathbb{F}_p$, let $\tau(\chi)$ be the Gaussian sum

$$\tau(\chi) = \sum_{j\in\mathbb{F}_p^*} \mathrm{e}\left(\frac{j}{p}\right)\chi(j).$$

If ψ is an additive character of $\mathbb{F}_q$ and if χ is a multiplicative character of $\mathbb{F}_q$, let $G(\chi,\psi)$ be the Gaussian sum

$$G(\chi,\psi) = \sum_{x\in\mathbb{F}_q^*} \chi(x)\psi(x).$$

If χ is a multiplicative character of $\mathbb{F}_q$ and if $\mathcal{C}$ is any subset of $\mathbb{F}_q^*$, we write

$$S_{\mathcal{C}}(\chi) = \sum_{x\in\mathcal{C}} \chi(x).$$

We define $\mathbb{1}_{X=Y}$ and $\mathbb{1}_{a|b}$ by

$$\mathbb{1}_{X=Y} = \begin{cases} 1 & \text{if } X = Y, \\ 0 & \text{otherwise,} \end{cases} \qquad \text{and} \qquad \mathbb{1}_{a|b} = \begin{cases} 1 & \text{if } a \text{ divides } b, \\ 0 & \text{otherwise.} \end{cases}$$

The set of squares in $\mathbb{F}_p^*$ is denoted by $\mathcal{Q}_p$ and the set of generators of $\mathbb{F}_p^*$ (i.e. primitive elements) is denoted by $\mathcal{G}_p$.

2. Preparations

In this section, $\mathcal{A}$ denotes a nonempty subset of $\mathbb{F}_p$ and $\mathcal{C}$ and $\mathcal{D}$ are nonempty subsets of $\mathbb{F}_q^*$.

2.1. Number of pairs (c,d) such that $\mathrm{Tr}(cd) \in \mathcal{A}$

Our goal is to give an estimate of the cardinality of the set

$$\mathcal{E}_{\mathcal{A}} = \{(c,d) \in \mathcal{C} \times \mathcal{D} : \mathrm{Tr}(cd) \in \mathcal{A}\}.$$

Consider the set

$$\mathcal{H}_{\mathcal{A}} = \left\{x \in \mathbb{F}_q^* : \mathrm{Tr}(x) \in \mathcal{A}\right\}.$$

The elements of $\mathcal{E}_{\mathcal{A}}$ are the elements of the set $\{(\alpha,\beta) \in \mathbb{F}_q^* \times \mathbb{F}_q^* : \alpha\beta \in \mathcal{H}_{\mathcal{A}}\}$ which are in $\mathcal{C} \times \mathcal{D}$. For each element $h \in \mathcal{H}_{\mathcal{A}}$ and each $\alpha \in \mathbb{F}_q^*$, there is a unique $\beta \in \mathbb{F}_q^*$ such that $\alpha\beta = h$. Therefore the proportion of pairs $(\alpha,\beta) \in \mathbb{F}_q^* \times \mathbb{F}_q^*$ such that $\alpha\beta \in \mathcal{H}_{\mathcal{A}}$ is $|\mathcal{H}_{\mathcal{A}}|/(q-1)$. If the pairs (c,d) were reasonably well distributed then we would expect this proportion to be preserved in $\mathcal{C} \times \mathcal{D}$. In order to establish this property in a quantitative form, the following lemma will constitute a crucial step.

Lemma 2.1. *The set $\mathcal{E}_{\mathcal{A}}$ satisfies*

$$|\mathcal{E}_{\mathcal{A}}| = \frac{|\mathcal{C}||\mathcal{D}|}{q-1}\,|\mathcal{H}_{\mathcal{A}}| + R_{\mathcal{A}}$$

with

$$R_{\mathcal{A}} = \frac{1}{q-1} \sum_{\chi \neq \chi_0} \overline{S_{\mathcal{H}_{\mathcal{A}}}(\chi)} S_{\mathcal{C}}(\chi) S_{\mathcal{D}}(\chi) \tag{V.21}$$

where the sum runs over all nontrivial multiplicative characters of $\mathbb{F}_q$.

The study of the character sums appearing in (V.21) will enable us to give an upper bound of $|R_{\mathcal{A}}|$.

Proof. Since $0 \notin \mathcal{C}$ and $0 \notin \mathcal{D}$, we have

$$|\mathcal{E}_{\mathcal{A}}| = \sum_{x \in \mathcal{H}_{\mathcal{A}}} \sum_{(c,d) \in \mathcal{C} \times \mathcal{D}} \mathbb{1}_{cd=x}.$$

We use the orthogonality relations for multiplicative characters of $\mathbb{F}_q$ to handle the equality $cd = x$:

$$\begin{aligned} |\mathcal{E}_{\mathcal{A}}| &= \sum_{x \in \mathcal{H}_{\mathcal{A}}} \sum_{(c,d) \in \mathcal{C} \times \mathcal{D}} \frac{1}{q-1} \sum_{\chi} \chi(cd)\overline{\chi(x)} = \frac{1}{q-1} \sum_{\chi} \sum_{x \in \mathcal{H}_{\mathcal{A}}} \overline{\chi(x)} \sum_{c \in \mathcal{C}} \chi(c) \sum_{d \in \mathcal{D}} \chi(d) \\ &= \frac{1}{q-1} \sum_{\chi} \overline{S_{\mathcal{H}_{\mathcal{A}}}(\chi)} S_{\mathcal{C}}(\chi) S_{\mathcal{D}}(\chi). \end{aligned}$$

The term corresponding to $\chi = \chi_0$ in the previous sum is

$$\frac{|\mathcal{C}||\mathcal{D}|}{q-1}\,|\mathcal{H}_{\mathcal{A}}|$$

and the sum of the remaining terms is $R_{\mathcal{A}}$. This completes the proof of Lemma 2.1. □

2.2. Character sums over elements whose trace belongs to $\mathcal{A}$

Let us first consider the crucial case where $\mathcal{A} = \{s\}$. Then the sum $S_{\mathcal{H}_\mathcal{A}}(\chi)$ appearing in (V.21) is given by

$$S_{\mathcal{H}_\mathcal{A}}(\chi) = \sum_{\substack{x \in \mathbb{F}_q^* \\ \mathrm{Tr}(x)=s}} \chi(x).$$

We will express this sum with the help of Gaussian sums over $\mathbb{F}_q$ and over $\mathbb{F}_p$ (see Proposition 2.2). We will deduce an expression for $S_{\mathcal{H}_\mathcal{A}}(\chi)$ for any $\mathcal{A} \subset \mathbb{F}_p^*$ (see Corollary 2.5).

Proposition 2.2. *If χ is a nontrivial multiplicative character of $\mathbb{F}_q$ and if s is any element of $\mathbb{F}_p$ then we have*

$$\sum_{\substack{x \in \mathbb{F}_q^* \\ \mathrm{Tr}(x)=s}} \chi(x) = \begin{cases} \dfrac{\chi(s)\overline{\tau(\chi_{|\mathbb{F}_p^*})}}{p} G(\chi, \psi_1) & \text{if } s \neq 0, \\ \dfrac{p-1}{p} G(\chi, \psi_1) \mathbb{1}_{\chi_{|\mathbb{F}_p^*}=1} & \text{if } s = 0, \end{cases}$$

where ψ_1 is the additive character of $\mathbb{F}_q$ defined by (V.20).

Proposition 2.2 can be proved using Eisenstein sums (for instance by combining results in [2, p. 389–391]). Nevertheless, for the convenience of the reader, we give a short and elementary proof of this result.

Proof. We detect the elements x of $\mathbb{F}_q^*$ such that $\mathrm{Tr}(x) = s$ by the classical equality

$$\frac{1}{p} \sum_{j=0}^{p-1} \mathrm{e}\left(\frac{ja}{p}\right) = \begin{cases} 1 & \text{if } a \equiv 0 \bmod p, \\ 0 & \text{otherwise.} \end{cases}$$

It gives

$$\sum_{\substack{x \in \mathbb{F}_q^* \\ \mathrm{Tr}(x)=s}} \chi(x) = \frac{1}{p} \sum_{j=0}^{p-1} \mathrm{e}\left(\frac{-js}{p}\right) \sum_{x \in \mathbb{F}_q^*} \chi(x) \, \mathrm{e}\left(\frac{j \, \mathrm{Tr}(x)}{p}\right).$$

Since χ is nontrivial, the term corresponding to $j = 0$ in the last sum is 0. Thus,

$$\begin{aligned} \sum_{\substack{x \in \mathbb{F}_q^* \\ \mathrm{Tr}(x)=s}} \chi(x) &= \frac{1}{p} \sum_{j \in \mathbb{F}_p^*} \mathrm{e}\left(\frac{-js}{p}\right) \overline{\chi(j)} \sum_{x \in \mathbb{F}_q^*} \chi(jx) \, \mathrm{e}\left(\frac{\mathrm{Tr}(jx)}{p}\right) \\ &= \frac{1}{p} \sum_{j \in \mathbb{F}_p^*} \mathrm{e}\left(\frac{-js}{p}\right) \overline{\chi(j)} \sum_{x \in \mathbb{F}_q^*} \chi(x) \, \mathrm{e}\left(\frac{\mathrm{Tr}(x)}{p}\right). \end{aligned}$$

Each sum over $x \in \mathbb{F}_q^*$ is then the Gaussian sum $G(\chi, \psi_1)$ of the multiplicative character χ

of $\mathbb{F}_q$ and the additive character ψ_1 of $\mathbb{F}_q$ defined by (V.20). Moreover, if $s \neq 0$,

$$\sum_{j\in\mathbb{F}_p^*} \mathrm{e}\left(\frac{-js}{p}\right)\overline{\chi(j)} = \overline{\overline{\chi(s)}\sum_{j\in\mathbb{F}_p^*} \mathrm{e}\left(\frac{js}{p}\right)\chi(js)} = \chi(s)\overline{\tau(\chi_{|\mathbb{F}_p^*})}$$

and if $s = 0$,

$$\sum_{j\in\mathbb{F}_p^*} \mathrm{e}\left(\frac{-js}{p}\right)\overline{\chi(j)} = \sum_{j\in\mathbb{F}_p^*} \overline{\chi(j)} = (p-1)\mathbb{1}_{\chi_{|\mathbb{F}_p^*}=1},$$

which completes the proof of Proposition 2.2. □

We will need the following classical result about Gaussian sums.

Lemma 2.3. *If ψ is an additive character of $\mathbb{F}_q$ and χ is a multiplicative character of $\mathbb{F}_q$ then*

$$G(\chi,\psi) = \begin{cases} q-1 & \text{if } \chi = \chi_0 \text{ and } \psi = \psi_0, \\ -1 & \text{if } \chi = \chi_0 \text{ and } \psi \neq \psi_0, \\ 0 & \text{if } \chi \neq \chi_0 \text{ and } \psi = \psi_0, \end{cases}$$

and $|G(\chi,\psi)| = \sqrt{q}$ if $\chi \neq \chi_0$ and $\psi \neq \psi_0$.

In the special case where χ is a multiplicative character of $\mathbb{F}_p$, $|\tau(\chi)| = \sqrt{p}$ if χ is nontrivial and $\tau(\chi) = -1$ if χ is trivial.

Proof. See [38, Theorem 5.11]. □

We deduce from Proposition 2.2 and Lemma 2.3 an exact formula for the absolute value of character sums over elements whose trace is fixed.

Corollary 2.4. *If χ is a nontrivial multiplicative character of $\mathbb{F}_q$ and if s is any element of $\mathbb{F}_p$ then*

$$\left|\sum_{\substack{x\in\mathbb{F}_q^* \\ \mathrm{Tr}(x)=s}} \chi(x)\right| = \begin{cases} \dfrac{\sqrt{q}}{\sqrt{p}} & \text{if } s \neq 0 \text{ and } \chi_{|\mathbb{F}_p^*} \neq 1, \\ \dfrac{\sqrt{q}}{p} & \text{if } s \neq 0 \text{ and } \chi_{|\mathbb{F}_p^*} = 1, \\ \dfrac{\sqrt{q}(p-1)}{p}\mathbb{1}_{\chi_{|\mathbb{F}_p^*}=1} & \text{if } s = 0. \end{cases}$$

Proof. Since $\chi \neq \chi_0$ and $\psi_1 \neq \psi_0$, this result follows immediately from Proposition 2.2 and Lemma 2.3. □

Let $\mathcal{A}$ be any nonempty subset of $\mathbb{F}_p^*$. Proposition 2.2 enables us to give an expression for the sum $S_{\mathcal{H}_\mathcal{A}}(\chi)$ depending on Gaussian sums and character sums over elements of $\mathcal{A}$.

Corollary 2.5. *If χ is a nontrivial multiplicative character of $\mathbb{F}_q$ then we have*

$$S_{\mathcal{H}_{\mathcal{A}}}(\chi) = \begin{cases} \dfrac{1}{p}\overline{\tau(\chi_{|\mathbb{F}_p^*})}G(\chi,\psi_1)\displaystyle\sum_{s\in\mathcal{A}}\chi(s) & \text{if } 0\notin\mathcal{A}, \\ \dfrac{1}{p}\overline{\tau(\chi_{|\mathbb{F}_p^*})}G(\chi,\psi_1)\displaystyle\sum_{s\in\mathcal{A}\setminus\{0\}}\chi(s) & \text{if } 0\in\mathcal{A} \text{ and } \chi_{|\mathbb{F}_p^*}\neq 1, \\ \dfrac{p-|\mathcal{A}|}{p}G(\chi,\psi_1) & \text{if } 0\in\mathcal{A} \text{ and } \chi_{|\mathbb{F}_p^*}=1. \end{cases}$$

Proof. It suffices to write

$$S_{\mathcal{H}_{\mathcal{A}}}(\chi) = \sum_{\substack{x\in\mathbb{F}_q^* \\ \mathrm{Tr}(x)\in\mathcal{A}}}\chi(x) = \sum_{s\in\mathcal{A}}\sum_{\substack{x\in\mathbb{F}_q^* \\ \mathrm{Tr}(x)=s}}\chi(x)$$

and to use Proposition 2.2 which gives an expression for each inner sum. Moreover, when $\chi_{|\mathbb{F}_p^*}=1$, the Gaussian sum $\tau(\chi_{|\mathbb{F}_p^*})=-1$ and $\sum_{s\in\mathcal{A}\setminus\{0\}}\chi(s)=|\mathcal{A}|-1$, which gives the expected equality in the last case. □

2.3. Further results on exponential sums

The following results are based on orthogonality relations for characters. They will be useful to give an upper bound of $|R_{\mathcal{A}}|$ where $R_{\mathcal{A}}$ is defined by (V.21). As in Section 2.1, if $\mathcal{C}\subset\mathbb{F}_q^*$ and if χ is a multiplicative character of $\mathbb{F}_q$ then $S_{\mathcal{C}}(\chi)$ denotes the character sum

$$S_{\mathcal{C}}(\chi) = \sum_{c\in\mathcal{C}}\chi(c).$$

Lemma 2.6. *If $\mathcal{C}$ is a subset of $\mathbb{F}_q^*$ then*

$$\sum_{\chi\neq\chi_0}|S_{\mathcal{C}}(\chi)|^2 = (q-1)|\mathcal{C}|-|\mathcal{C}|^2$$

where the sum runs over all nontrivial multiplicative characters of $\mathbb{F}_q$.

Proof. It suffices to write

$$\sum_{\chi\neq\chi_0}|S_{\mathcal{C}}(\chi)|^2 = \sum_{(c_1,c_2)\in\mathcal{C}^2}\sum_{\chi\neq\chi_0}\chi(c_1)\overline{\chi(c_2)}$$

and to use orthogonality relations for multiplicative characters of $\mathbb{F}_q$

$$\sum_{\chi\neq\chi_0}|S_{\mathcal{C}}(\chi)|^2 = \sum_{(c_1,c_2)\in\mathcal{C}^2}[(q-1)\mathbb{1}_{c_1=c_2}-1] = (q-1)|\mathcal{C}|-|\mathcal{C}|^2.$$ □

Lemma 2.7. *If $\mathcal{C}$ and $\mathcal{D}$ are subsets of $\mathbb{F}_q^*$ then*

$$\sum_{\chi\neq\chi_0}|S_{\mathcal{C}}(\chi)S_{\mathcal{D}}(\chi)|\leq(q-1)\sqrt{|\mathcal{C}||\mathcal{D}|}\left(1-\frac{|\mathcal{C}|}{q-1}\right)^{1/2}\left(1-\frac{|\mathcal{D}|}{q-1}\right)^{1/2}.$$

Proof. Using the Cauchy–Schwarz inequality, we can write

$$\sum_{\chi\neq\chi_0}|S_{\mathcal{C}}(\chi)S_{\mathcal{D}}(\chi)|\leq\left(\sum_{\chi\neq\chi_0}|S_{\mathcal{C}}(\chi)|^2\right)^{1/2}\left(\sum_{\chi\neq\chi_0}|S_{\mathcal{D}}(\chi)|^2\right)^{1/2}.$$

By Lemma 2.6,

$$\sum_{\chi\neq\chi_0}|S_{\mathcal{C}}(\chi)S_{\mathcal{D}}(\chi)|\leq\left((q-1)|\mathcal{C}|-|\mathcal{C}|^2\right)^{1/2}\left((q-1)|\mathcal{D}|-|\mathcal{D}|^2\right)^{1/2},$$

which completes the proof of Lemma 2.7. □

Lemma 2.8. *If $\mathcal{C}$ is a subset of $\mathbb{F}_q^*$ and if λ is any multiplicative character of $\mathbb{F}_p$ then we have*

$$\sum_{\substack{\chi\neq\chi_0\\ \chi_{|\mathbb{F}_p^*}=\lambda}}|S_{\mathcal{C}}(\chi)|^2=\frac{q-1}{p-1}\sum_{s\in\mathbb{F}_p^*}\lambda(s)|\mathcal{C}\cap s\mathcal{C}|-|\mathcal{C}|^2\mathbb{1}_{\lambda=1}.$$

Proof. We detect the condition $\chi_{|\mathbb{F}_p^*}=\lambda$ thanks to the orthogonality relations for multiplicative characters of $\mathbb{F}_p$:

$$\begin{aligned}
\sum_{\substack{\chi\neq\chi_0\\ \chi_{|\mathbb{F}_p^*}=\lambda}}|S_{\mathcal{C}}(\chi)|^2&=\sum_{(c_1,c_2)\in\mathcal{C}^2}\sum_{\substack{\chi\neq\chi_0\\ \chi_{|\mathbb{F}_p^*}=\lambda}}\chi(c_1)\overline{\chi(c_2)}\\
&=\frac{1}{p-1}\sum_{(c_1,c_2)\in\mathcal{C}^2}\sum_{\chi\neq\chi_0}\chi(c_1)\overline{\chi(c_2)}\sum_{s\in\mathbb{F}_p^*}\lambda(s)\overline{\chi(s)}\\
&=\frac{1}{p-1}\sum_{s\in\mathbb{F}_p^*}\lambda(s)\sum_{(c_1,c_2)\in\mathcal{C}^2}\sum_{\chi\neq\chi_0}\chi(c_1)\overline{\chi(sc_2)}\\
&=\frac{1}{p-1}\sum_{s\in\mathbb{F}_p^*}\lambda(s)\sum_{(c_1,c_2)\in\mathcal{C}^2}((q-1)\mathbb{1}_{c_1=sc_2}-1)\\
&=\frac{1}{p-1}\sum_{s\in\mathbb{F}_p^*}\lambda(s)\left((q-1)|\mathcal{C}\cap s\mathcal{C}|-|\mathcal{C}|^2\right)\\
&=\frac{q-1}{p-1}\sum_{s\in\mathbb{F}_p^*}\lambda(s)|\mathcal{C}\cap s\mathcal{C}|-|\mathcal{C}|^2\mathbb{1}_{\lambda=1}.
\end{aligned}$$

□

3. Products cd whose trace is fixed

For $s \in \mathbb{F}_p$, we recall the notation $\mathcal{E}_s = \{(c,d) \in \mathcal{C} \times \mathcal{D} : \mathrm{Tr}(cd) = s\}$. We will first prove Theorems 1.2 and 1.3. Then, we will be able to prove Theorem 1.1. We will also show that these results are optimal up to an absolute constant factor.

3.1. Proof of Theorem 1.2

We first estimate $|\mathcal{E}_s|$ for $s \neq 0$.

Proposition 3.1. *For any $s \in \mathbb{F}_p^*$, the set $\mathcal{E}_s$ satisfies*

$$|\mathcal{E}_s| = \frac{|\mathcal{C}||\mathcal{D}|}{(q-1)}\frac{q}{p} + R_s$$

where

$$|R_s| \leq \frac{\sqrt{q}}{\sqrt{p}}\sqrt{|\mathcal{C}||\mathcal{D}|}\left(1 - \frac{|\mathcal{C}|}{q-1}\right)^{1/2}\left(1 - \frac{|\mathcal{D}|}{q-1}\right)^{1/2}.$$

Proof. We take $\mathcal{A} = \{s\}$. By Lemma 2.1, $|\mathcal{E}_s| = |\mathcal{E}_{\mathcal{A}}|$ is the sum of a main term

$$P_s = \frac{|\mathcal{C}||\mathcal{D}|}{q-1}|\{x \in \mathbb{F}_q^* : \mathrm{Tr}(x) = s\}|$$

and a second term R_s given by (V.21). The number of elements x of $\mathbb{F}_q^*$ such that $\mathrm{Tr}(x) = s$ is q/p. Hence we have

$$P_s = \frac{|\mathcal{C}||\mathcal{D}|}{(q-1)}\frac{q}{p}.$$

Moreover, by (V.21),

$$R_s = \frac{1}{q-1}\sum_{\chi \neq \chi_0} \overline{S_{\mathcal{H}_{\mathcal{A}}}(\chi)} S_{\mathcal{C}}(\chi) S_{\mathcal{D}}(\chi)$$

and by Corollary 2.4, if $\chi \neq \chi_0$,

$$|S_{\mathcal{H}_{\mathcal{A}}}(\chi)| \leq \frac{\sqrt{q}}{\sqrt{p}}.$$

It follows

$$|R_s| \leq \frac{\sqrt{q}}{(q-1)\sqrt{p}}\sum_{\chi \neq \chi_0} |S_{\mathcal{C}}(\chi) S_{\mathcal{D}}(\chi)|,$$

and using Lemma 2.7, we conclude

$$|R_s| \leq \frac{\sqrt{q}}{\sqrt{p}}\sqrt{|\mathcal{C}||\mathcal{D}|}\left(1 - \frac{|\mathcal{C}|}{q-1}\right)^{1/2}\left(1 - \frac{|\mathcal{D}|}{q-1}\right)^{1/2}.$$

□

We are now ready to prove Theorem 1.2. Given $s \in \mathbb{F}_p^*$, it follows from Proposition 3.1 that

$$\left| |\mathcal{E}_s| - \frac{|\mathcal{C}||\mathcal{D}|}{(q-1)} \frac{q}{p} \right| \leq \frac{\sqrt{q}}{\sqrt{p}} \sqrt{|\mathcal{C}||\mathcal{D}|}.$$

In particular, this implies

$$|\mathcal{E}_s| > \frac{|\mathcal{C}||\mathcal{D}|}{p} - \frac{\sqrt{q}}{\sqrt{p}} \sqrt{|\mathcal{C}||\mathcal{D}|},$$

thus if $|\mathcal{C}||\mathcal{D}| \geq pq$ we have $|\mathcal{E}_s| > 0$ which completes the proof of Theorem 1.2.

3.2. Optimality of Theorem 1.2

Condition (V.5) is optimal up to an absolute constant factor. Indeed, given $s \in \mathbb{F}_p^*$, we can find explicit sets $\mathcal{C}$ and $\mathcal{D}$ such that

$$pq/16 < |\mathcal{C}||\mathcal{D}| < pq \tag{V.22}$$

for which $\mathcal{E}_s = \varnothing$. To show this, we will give a construction based on the set $\mathcal{Q}_p$ formed by the squares in $\mathbb{F}_p^*$.

If $p \geq 3$ and if $s \in \mathcal{Q}_p$, we can take for instance $\mathcal{C} = \left\{x \in \mathbb{F}_q^* : \mathrm{Tr}(x) \in \mathcal{Q}_p\right\}$ and $\mathcal{D} = \mathbb{F}_p^* \setminus \mathcal{Q}_p$. The number of squares in $\mathbb{F}_p^*$ is $(p-1)/2$ and for each $t \in \mathbb{F}_p^*$, the number of elements $x \in \mathbb{F}_q^*$ such that $\mathrm{Tr}(x) = t$ is q/p. Hence $|\mathcal{D}| = \frac{p-1}{2}$ and $|\mathcal{C}| = \frac{p-1}{2}\frac{q}{p}$ and thus (V.22) is satisfied. Moreover, if $(c,d) \in \mathcal{C} \times \mathcal{D}$ then $d \in \mathbb{F}_p$ thus $\mathrm{Tr}(cd) = d\,\mathrm{Tr}(c) \notin \mathcal{Q}_p$ and so $\mathrm{Tr}(cd) \neq s$.

If $p \geq 3$ and if $s \in \mathbb{F}_p^* \setminus \mathcal{Q}_p$, we can take $\mathcal{C} = \left\{x \in \mathbb{F}_q^* : \mathrm{Tr}(x) \in \mathcal{Q}_p\right\}$ and $\mathcal{D} = \mathcal{Q}_p$. Again $|\mathcal{D}| = \frac{p-1}{2}$ and $|\mathcal{C}| = \frac{p-1}{2}\frac{q}{p}$ and thus (V.22) is satisfied. Moreover, if $(c,d) \in \mathcal{C} \times \mathcal{D}$ then $\mathrm{Tr}(cd) = d\,\mathrm{Tr}(c) \in \mathcal{Q}_p$ and so $\mathrm{Tr}(cd) \neq s$.

If $p = 2$ then of course $s = 1$ and we can consider $\mathcal{C} = \left\{x \in \mathbb{F}_q^* : \mathrm{Tr}(x) = 0\right\}$ and $\mathcal{D} = \{1\}$. Then $|\mathcal{C}||\mathcal{D}| = \frac{q}{2} - 1$ and (V.22) is also satisfied. Moreover, if $(c,d) \in \mathcal{C} \times \mathcal{D}$ then $\mathrm{Tr}(cd) = \mathrm{Tr}(c) = 0 \neq s$.

3.3. Proof of Theorem 1.3

We first estimate $|\mathcal{E}_0|$ where

$$\mathcal{E}_0 = \{(c,d) \in \mathcal{C} \times \mathcal{D} : \mathrm{Tr}(cd) = 0\}.$$

Proposition 3.2. *The set $\mathcal{E}_0$ satisfies*

$$|\mathcal{E}_0| = \frac{|\mathcal{C}||\mathcal{D}|}{(q-1)} \left(\frac{q}{p} - 1\right) + R_0$$

with

$$|R_0| \le \frac{p-1}{p}\sqrt{q}\sqrt{|\mathcal{C}||\mathcal{D}|}\left(\frac{1}{p-1}-\Delta_0(\mathcal{C})\right)^{1/2}\left(\frac{1}{p-1}-\Delta_0(\mathcal{D})\right)^{1/2}$$

where $\Delta_0(\mathcal{C})$ *and* $\Delta_0(\mathcal{D})$ *are defined by* (V.6).

It will follow from the proof that the terms between parentheses are non-negative numbers, which is not trivial at first sight.

Proof. We take $\mathcal{A} = \{0\}$. By Lemma 2.1, $|\mathcal{E}_0| = |\mathcal{E}_{\mathcal{A}}| = P_0 + R_0$ where

$$P_0 = \frac{|\mathcal{C}||\mathcal{D}|}{q-1}|\{x \in \mathbb{F}_q^* : \mathrm{Tr}(x) = 0\}|$$

is the main term and R_0 is an error term given by (V.21). The number of elements $x \in \mathbb{F}_q^*$ such that $\mathrm{Tr}(x) = 0$ is $\frac{q}{p} - 1$. Therefore we have

$$P_0 = \frac{|\mathcal{C}||\mathcal{D}|}{(q-1)}\left(\frac{q}{p}-1\right).$$

Moreover, by (V.21),

$$R_0 = \frac{1}{q-1}\sum_{\chi\neq\chi_0}\overline{S_{\mathcal{H}_{\mathcal{A}}}(\chi)}S_{\mathcal{C}}(\chi)S_{\mathcal{D}}(\chi)$$

and by Corollary 2.4, if $\chi \neq \chi_0$,

$$|S_{\mathcal{H}_{\mathcal{A}}}(\chi)| = \frac{p-1}{p}\sqrt{q}\,\mathbb{1}_{\chi_{|\mathbb{F}_p^*}=1}.$$

Thus,

$$|R_0| \le \frac{(p-1)\sqrt{q}}{p(q-1)}\sum_{\substack{\chi\neq\chi_0\\ \chi_{|\mathbb{F}_p^*}=1}}|S_{\mathcal{C}}(\chi)S_{\mathcal{D}}(\chi)|.$$

By the Cauchy–Schwarz inequality,

$$|R_0| \le \frac{(p-1)\sqrt{q}}{p(q-1)}T_{\mathcal{C}}^{1/2}T_{\mathcal{D}}^{1/2} \tag{V.23}$$

where $T_{\mathcal{C}} = \sum_{\substack{\chi\neq\chi_0\\ \chi_{|\mathbb{F}_p^*}=1}}|S_{\mathcal{C}}(\chi)|^2$ and $T_{\mathcal{D}}$ is defined similarly with $\mathcal{D}$ in place of $\mathcal{C}$. Applying Lemma 2.8 with $\lambda = 1$, we get

$$T_{\mathcal{C}} = \frac{q-1}{p-1}\sum_{s\in\mathbb{F}_p^*}|\mathcal{C}\cap s\mathcal{C}| - |\mathcal{C}|^2, \quad T_{\mathcal{D}} = \frac{q-1}{p-1}\sum_{s\in\mathbb{F}_p^*}|\mathcal{D}\cap s\mathcal{D}| - |\mathcal{D}|^2.$$

We conclude by inserting those expressions for $T_{\mathcal{C}}$ and $T_{\mathcal{D}}$ into (V.23). Observe that $T_{\mathcal{C}} \geq 0$ and $T_{\mathcal{D}} \geq 0$ by definition. □

We are now ready to prove Theorem 1.3. It follows from Proposition 3.2 that

$$|\mathcal{E}_0| = \frac{|\mathcal{C}||\mathcal{D}|}{q-1}\left(\frac{q}{p}-1\right) + R_0$$

where by (V.8)

$$|R_0| \leq \frac{\sqrt{q}}{p}\sqrt{|\mathcal{C}||\mathcal{D}|}.$$

In particular, this implies

$$|\mathcal{E}_0| \geq \frac{|\mathcal{C}||\mathcal{D}|}{q-1}\left(\frac{q}{p}-1\right) - \frac{\sqrt{q}}{p}\sqrt{|\mathcal{C}||\mathcal{D}|},$$

thus if $|\mathcal{C}||\mathcal{D}| > q\left(\frac{q-1}{q-p}\right)^2$ then $|\mathcal{E}_0| > 0$ which completes the proof of Theorem 1.3.

Remark 3.3. If we do not assume that condition (V.8) is satisfied then we still obtain an upper bound for $|R_0|$:

$$|R_0| \leq \frac{p-1}{p}\sqrt{q}\sqrt{|\mathcal{C}||\mathcal{D}|}\left(1-\frac{|\mathcal{C}|}{q-1}\right)^{\frac{1}{2}}\left(1-\frac{|\mathcal{D}|}{q-1}\right)^{\frac{1}{2}} \leq \frac{p-1}{p}\sqrt{q}\sqrt{|\mathcal{C}||\mathcal{D}|} \tag{V.24}$$

which is slightly larger but not trivial. Moreover, since $q = p^r \geq p^2$, we have $\frac{1}{q-1}\left(\frac{q}{p}-1\right) > \frac{1}{q}\left(\frac{q}{p}-1\right) = \frac{1}{p}-\frac{1}{q} \geq \frac{p-1}{p^2}$. It follows that

$$|\mathcal{E}_0| > \frac{p-1}{p^2}|\mathcal{C}||\mathcal{D}| - \frac{p-1}{p}\sqrt{q}\sqrt{|\mathcal{C}||\mathcal{D}|}$$

which proves that if $|\mathcal{C}||\mathcal{D}| \geq p^2 q$ then $|\mathcal{E}_0| > 0$.

3.4. Optimality of Theorem 1.3

Conditions (V.7) and (V.9) are optimal up to an absolute constant factor. Indeed, we can construct sets $\mathcal{C}$ and $\mathcal{D}$ satisfying (V.8) such that

$$\frac{q}{32}\left(\frac{q-1}{q-p}\right)^2 < \frac{q}{8} < |\mathcal{C}||\mathcal{D}| \leq q\left(\frac{q-1}{q-p}\right)^2 < 4q \tag{V.25}$$

and for which $\mathcal{E}_0 = \varnothing$. To show this, consider a basis $\{e_1, \ldots, e_r\}$ of $\mathbb{F}_q$ over $\mathbb{F}_p$. For $1 \leq i \leq 2$, we denote by f_i the $\mathbb{F}_p$-linear form on $\mathbb{F}_q$ defined by $f_i(x) = \mathrm{Tr}(e_i x)$ and we choose

$$\mathcal{C} = \{x \in \mathbb{F}_q^* : f_1(x) = 1 \text{ and } f_2(x) \in \mathcal{Q}_p\}$$

and

$$\mathcal{D} = \{c_1 e_1 + e_2 : -c_1 \in \mathbb{F}_p \setminus \mathcal{Q}_p\}.$$

The linear form f_1 is constant on $\mathcal{C}$ and equal to 1. We will show in Section 6.3 that this implies that $\mathcal{C}$ satisfies (V.8). Observing that the coordinates in the base $\{e_1, \dots, e_r\}$ of the elements of $\mathcal{D}$ are $(c_1, 1, 0, \dots, 0)$, one of their coordinates is fixed and distinct from zero. Again we will see in Section 6.3 that this implies that $\mathcal{D}$ satisfies (V.8).

Moreover, since e_1 and e_2 are linearly independent over $\mathbb{F}_p$, the linear forms f_1 and f_2 are also linearly independent and it follows that for each $t \in \mathbb{F}_p$, the number of $x \in \mathbb{F}_q^*$ such that $f_1(x) = 1$ and $f_2(x) = t$ is p^{r-2}. Therefore, if $p \geq 3$ then $|\mathcal{C}| = \frac{p-1}{2} p^{r-2}$ and $|\mathcal{D}| = \frac{p+1}{2}$ and if $p = 2$ then $|\mathcal{C}| = p^{r-2} = q/4$ and $|\mathcal{D}| = 1$. It follows that (V.25) is satisfied.

It remains to show that if $(c, d) \in \mathcal{C} \times \mathcal{D}$ then $\mathrm{Tr}(cd) \neq 0$. If $c \in \mathcal{C}$ and $d = c_1 e_1 + e_2 \in \mathcal{D}$ then, since $\mathrm{Tr}(e_1 c) = 1$,

$$\mathrm{Tr}(cd) = \mathrm{Tr}(c_1 e_1 c + e_2 c) = c_1 + f_2(c)$$

which is not zero because $f_2(c) \in \mathcal{Q}_p$ and $-c_1 \in \mathbb{F}_p \setminus \mathcal{Q}_p$ and therefore $\mathcal{E}_0 = \varnothing$.

3.5. Proof of Theorem 1.1

If $s \in \mathbb{F}_p^*$ then Proposition 3.1 gives

$$\left| |\mathcal{E}_s| - \frac{|\mathcal{C}||\mathcal{D}|}{(q-1)} \frac{q}{p} \right| \leq \frac{\sqrt{q}}{\sqrt{p}} \sqrt{|\mathcal{C}||\mathcal{D}|}$$

thus writing

$$|\mathcal{E}_s| - \frac{|\mathcal{C}||\mathcal{D}|}{p} = |\mathcal{E}_s| - \frac{|\mathcal{C}||\mathcal{D}|}{(q-1)} \frac{q}{p} + \frac{|\mathcal{C}||\mathcal{D}|}{(q-1)p}$$

since $|\mathcal{C}| \leq q-1$ and $|\mathcal{D}| \leq q-1$ and $\frac{1}{p} \leq \sqrt{q}\left(1 - \frac{1}{\sqrt{p}}\right)$, we obtain

$$\left| |\mathcal{E}_s| - \frac{|\mathcal{C}||\mathcal{D}|}{p} \right| \leq \frac{\sqrt{q}}{\sqrt{p}} \sqrt{|\mathcal{C}||\mathcal{D}|} + \frac{\sqrt{|\mathcal{C}||\mathcal{D}|}}{p} \leq \sqrt{q} \sqrt{|\mathcal{C}||\mathcal{D}|}.$$

Similarly, Proposition 3.2 and (V.24) give

$$\left| |\mathcal{E}_0| - \frac{|\mathcal{C}||\mathcal{D}|}{(q-1)} \left(\frac{q}{p} - 1 \right) \right| \leq \frac{p-1}{p} \sqrt{q} \sqrt{|\mathcal{C}||\mathcal{D}|}$$

thus writing

$$|\mathcal{E}_0| - \frac{|\mathcal{C}||\mathcal{D}|}{p} = |\mathcal{E}_0| - \frac{|\mathcal{C}||\mathcal{D}|}{(q-1)} \left(\frac{q}{p} - 1 \right) + \frac{|\mathcal{C}||\mathcal{D}|}{p} \frac{1-p}{q-1}$$

we obtain

$$\left||\mathcal{E}_0| - \frac{|\mathcal{C}||\mathcal{D}|}{p}\right| \leq \frac{p-1}{p}\sqrt{q}\sqrt{|\mathcal{C}||\mathcal{D}|} + \sqrt{|\mathcal{C}||\mathcal{D}|}$$
$$\leq \frac{p-1}{p}\sqrt{q}\sqrt{|\mathcal{C}||\mathcal{D}|} + \frac{1}{p}\sqrt{q}\sqrt{|\mathcal{C}||\mathcal{D}|} = \sqrt{q}\sqrt{|\mathcal{C}||\mathcal{D}|}.$$

This proves that for any $s \in \mathbb{F}_p$,

$$\left||\mathcal{E}_s| - \frac{|\mathcal{C}||\mathcal{D}|}{p}\right| \leq \sqrt{q}\sqrt{|\mathcal{C}||\mathcal{D}|}$$

which completes the proof of Theorem 1.1.

3.6. Optimality of Theorem 1.1

The upper bound given by Theorem 1.1 is optimal up to an absolute constant factor. Indeed, we can construct sets $\mathcal{C}$ and $\mathcal{D}$ such that

$$\left||\mathcal{E}_0| - \frac{|\mathcal{C}||\mathcal{D}|}{p}\right| > \frac{1}{\sqrt{128}}\sqrt{q}\sqrt{|\mathcal{C}||\mathcal{D}|}. \tag{V.26}$$

If $\{e_1, \ldots, e_r\}$ is a basis of $\mathbb{F}_q$ over $\mathbb{F}_p$, we can consider for instance:

$$\mathcal{C} = \{x \in \mathbb{F}_q^* : f_1(x) \in \mathbb{F}_p \setminus \mathcal{Q}_p \text{ and } f_2(x) \in \mathcal{Q}_p\}$$

where f_1 and f_2 are defined as in Section 3.4 and

$$\mathcal{D} = \{c_1e_1 + c_2e_2 : c_1 \in \mathcal{Q}_p \text{ and } -c_2 \in \mathcal{Q}_p\}.$$

If $c \in \mathcal{C}$ and $d = c_1e_1 + c_2e_2 \in \mathcal{D}$ then

$$\mathrm{Tr}(cd) = \mathrm{Tr}(c_1e_1c + c_2e_2c) = c_1f_1(c) + c_2f_2(c)$$

and since $c_1f_1(c) \notin \mathcal{Q}_p$ and $-c_2f_2(c) \in \mathcal{Q}_p$, we deduce that $\mathrm{Tr}(cd) \neq 0$. Therefore $\mathcal{E}_0 = \varnothing$.

Moreover, if $p \geq 3$ then $|\mathcal{C}| = \frac{p-1}{2}\frac{p+1}{2}p^{r-2}$ and $|\mathcal{D}| = \left(\frac{p-1}{2}\right)^2$ and if $p = 2$ then $|\mathcal{C}| = p^{r-2}$ and $|\mathcal{D}| = 1$. It follows that $|\mathcal{C}||\mathcal{D}| > p^{r+2}/128 = p^2q/128$ and thus $\mathcal{C}$ and $\mathcal{D}$ satisfy (V.26).

4. Products cd whose trace belongs to a given subgroup

Let m be a divisor of $p-1$ and let $\mathcal{A}$ be the subgroup of $\mathbb{F}_p^*$ of order m. In order to prove Theorem 1.6, we first estimate $|\mathcal{E}_\mathcal{A}|$ where

$$\mathcal{E}_\mathcal{A} = \{(c,d) \in \mathcal{C} \times \mathcal{D} : \mathrm{Tr}(cd) \in \mathcal{A}\}.$$

4.1. An estimate of $|\mathcal{E}_{\mathcal{A}}|$ for a given subgroup $\mathcal{A}$

Proposition 4.1. *Let m be any divisor of $p-1$ and let $\mathcal{A}$ be the subgroup of $\mathbb{F}_p^*$ of order m. The set $\mathcal{E}_{\mathcal{A}}$ satisfies*

$$|\mathcal{E}_{\mathcal{A}}| = \frac{m}{p}\frac{q}{q-1}|\mathcal{C}||\mathcal{D}| + R_{\mathcal{A}}$$

with

$$|R_{\mathcal{A}}| \leq \frac{m}{\sqrt{p}}\sqrt{q}\sqrt{|\mathcal{C}||\mathcal{D}|}\left(\frac{1}{m} - \Delta_{\mathcal{A}}(\mathcal{C})\right)^{1/2}\left(\frac{1}{m} - \Delta_{\mathcal{A}}(\mathcal{D})\right)^{1/2}$$

where $\Delta_{\mathcal{A}}(\mathcal{C})$ and $\Delta_{\mathcal{A}}(\mathcal{D})$ are defined by (V.11).

It will follow from the proof that the terms between parentheses are non-negative numbers, which is not trivial at first sight.

Proof of Proposition 4.1. Let g_0 be a generator of the cyclic group $\mathbb{F}_p^*$. Then, the subgroup $\mathcal{A}$ can be described in terms of g_0:

$$\mathcal{A} = \left\{ g_0^{k\frac{p-1}{m}} : 1 \leq k \leq m \right\}. \tag{V.27}$$

We introduce the following notations for multiplicative characters of $\mathbb{F}_p$. For $j \in \{1, \dots, p-1\}$, let χ_j be the multiplicative character of $\mathbb{F}_p$ defined by

$$\chi_j(g_0) = \mathrm{e}\left(\frac{j}{p-1}\right). \tag{V.28}$$

The $p-1$ multiplicative characters of $\mathbb{F}_p$ are $\chi_1, \dots, \chi_{p-1}$ (see [38, Theorem 5.8]). The trivial character is χ_{p-1}, it will also be denoted by 1.

The following lemma gives an explicit formula for character sums over all elements of $\mathcal{A}$.

Lemma 4.2. *For any $j \in \{1, \dots, p-1\}$, we have*

$$\sum_{s\in\mathcal{A}} \chi_j(s) = m\,\mathbb{1}_{m|j} = \begin{cases} m & \text{if } m|j, \\ 0 & \text{otherwise.} \end{cases}$$

Proof. By (V.27), we have

$$\sum_{s\in\mathcal{A}} \chi_j(s) = \sum_{k=1}^{m} \chi_j\left(g_0^{k\frac{p-1}{m}}\right) = \sum_{k=1}^{m} \mathrm{e}\left(\frac{kj}{m}\right) = m\,\mathbb{1}_{m|j}. \qquad \square$$

We are now ready to prove Proposition 4.1. By Lemma 2.1, we can write

$$|\mathcal{E}_{\mathcal{A}}| = P_{\mathcal{A}} + R_{\mathcal{A}}$$

where $P_{\mathcal{A}} = \frac{m}{p}\frac{q}{q-1}|\mathcal{C}||\mathcal{D}|$ and $R_{\mathcal{A}}$ is given by (V.21). Filtering the multiplicative characters of $\mathbb{F}_q$ according to their restriction to $\mathbb{F}_p^*$, we obtain

$$R_{\mathcal{A}} = \frac{1}{q-1}\sum_{j=1}^{p-1} \sum_{\substack{\chi \neq \chi_0 \\ \chi_{|\mathbb{F}_p^*} = \chi_j}} \overline{S_{\mathcal{H}_{\mathcal{A}}}(\chi)} S_{\mathcal{C}}(\chi) S_{\mathcal{D}}(\chi). \tag{V.29}$$

By Corollary 2.5 and by Lemma 4.2, for any $j \in \{1, \dots, p-1\}$ and for any character $\chi \neq \chi_0$ with $\chi_{|\mathbb{F}_p^*} = \chi_j$, we have

$$S_{\mathcal{H}_{\mathcal{A}}}(\chi) = \frac{1}{p}\,\overline{\tau(\chi_j)} G(\chi, \psi_1) \sum_{s \in \mathcal{A}} \chi_j(s) = \frac{m}{p}\,\overline{\tau(\chi_j)} G(\chi, \psi_1)\, \mathbb{1}_{m|j},$$

and thus

$$|S_{\mathcal{H}_{\mathcal{A}}}(\chi)| \leq \frac{m}{\sqrt{p}}\sqrt{q}\, \mathbb{1}_{m|j}.$$

It follows from (V.29) that

$$|R_{\mathcal{A}}| \leq \frac{m}{\sqrt{p}}\frac{\sqrt{q}}{q-1} \sum_{\substack{1 \leq j \leq p-1 \\ m|j}} \sum_{\substack{\chi \neq \chi_0 \\ \chi_{|\mathbb{F}_p^*} = \chi_j}} |S_{\mathcal{C}}(\chi) S_{\mathcal{D}}(\chi)|.$$

By the Cauchy–Schwarz inequality, we get

$$|R_{\mathcal{A}}| \leq \frac{m}{\sqrt{p}}\frac{\sqrt{q}}{q-1} T_{\mathcal{C}}^{1/2} T_{\mathcal{D}}^{1/2} \tag{V.30}$$

where

$$T_{\mathcal{C}} = \sum_{\substack{1 \leq j \leq p-1 \\ m|j}} \sum_{\substack{\chi \neq \chi_0 \\ \chi_{|\mathbb{F}_p^*} = \chi_j}} |S_{\mathcal{C}}(\chi)|^2$$

and $T_{\mathcal{D}}$ is defined similarly with $\mathcal{D}$ in place of $\mathcal{C}$. By Lemma 2.8,

$$\begin{aligned} T_{\mathcal{C}} &= \frac{q-1}{p-1} \sum_{s \in \mathbb{F}_p^*} |\mathcal{C} \cap s\mathcal{C}| \sum_{\substack{1 \leq j \leq p-1 \\ m|j}} \chi_j(s) - |\mathcal{C}|^2 \\ &= \frac{q-1}{p-1} \sum_{\ell=1}^{p-1} |\mathcal{C} \cap g_0^{\ell}\mathcal{C}| \sum_{\substack{1 \leq j \leq p-1 \\ m|j}} \chi_j(g_0^{\ell}) - |\mathcal{C}|^2. \end{aligned} \tag{V.31}$$

For each $\ell \in \{1, \dots, p-1\}$, the sum over j with $m|j$ in (V.31) can be computed:

$$\sum_{\substack{1 \leq j \leq p-1 \\ m|j}} \chi_j(g_0^{\ell}) = \sum_{\substack{1 \leq j \leq p-1 \\ m|j}} \mathrm{e}\left(\frac{j\ell}{p-1}\right) = \sum_{u=1}^{\frac{p-1}{m}} \mathrm{e}\left(\frac{u\ell}{\frac{p-1}{m}}\right) = \frac{p-1}{m}\, \mathbb{1}_{\frac{p-1}{m}|\ell}.$$

It follows that

$$T_{\mathcal{C}} = \frac{q-1}{m} \sum_{k=1}^{m} |\mathcal{C} \cap g_0^{k\frac{p-1}{m}} \mathcal{C}| - |\mathcal{C}|^2 = \frac{q-1}{m} \sum_{s \in \mathcal{A}} |\mathcal{C} \cap s\mathcal{C}| - |\mathcal{C}|^2.$$

Similarly, we get

$$T_{\mathcal{D}} = \frac{q-1}{m} \sum_{s \in \mathcal{A}} |\mathcal{D} \cap s\mathcal{D}| - |\mathcal{D}|^2.$$

We conclude by inserting the above expressions for $T_{\mathcal{C}}$ and $T_{\mathcal{D}}$ into (V.30). This completes the proof of Proposition 4.1. Observe that $T_{\mathcal{C}} \geq 0$ and $T_{\mathcal{D}} \geq 0$ by definition. □

4.2. Proof of Theorem 1.6

It follows from Proposition 4.1 that

$$|\mathcal{E}_{\mathcal{A}}| = \frac{m}{p} \frac{q}{q-1} |\mathcal{C}||\mathcal{D}| + R_{\mathcal{A}}$$

where by (V.13)

$$|R_{\mathcal{A}}| \leq \frac{\sqrt{q}}{\sqrt{p}} \sqrt{|\mathcal{C}||\mathcal{D}|}.$$

Thus,

$$|\mathcal{E}_{\mathcal{A}}| > \frac{m}{p} |\mathcal{C}||\mathcal{D}| - \frac{\sqrt{q}}{\sqrt{p}} \sqrt{|\mathcal{C}||\mathcal{D}|}$$

and it follows that if $|\mathcal{C}||\mathcal{D}| \geq \frac{pq}{m^2}$, then $\mathcal{E}_{\mathcal{A}}$ is nonempty. This completes the proof of Theorem 1.6.

4.3. Optimality of Theorem 1.6

Assume $p \geq 3$ and $m \neq p-1$. Then condition (V.12) is optimal up to an absolute constant factor. Indeed, we can construct sets $\mathcal{C}$ and $\mathcal{D}$ satisfying (V.13) such that

$$\frac{pq}{16m^2} < |\mathcal{C}||\mathcal{D}| < \frac{pq}{m^2} \tag{V.32}$$

and for which $\mathcal{E}_{\mathcal{A}} = \varnothing$. To show this, we define $m' = \frac{p-1}{m}$ and we give a construction of such sets $\mathcal{C}$ and $\mathcal{D}$ which depends on the parity of m'.

We first consider the case where m' is even. Since $\mathcal{A} \subset \mathcal{Q}_p$ (by (V.27)), we have $b\mathcal{A} \subset \mathcal{Q}_p$ for $b \in \mathcal{Q}_p$ and $b\mathcal{A} \subset \mathbb{F}_p^* \setminus \mathcal{Q}_p$ for $b \in \mathbb{F}_p^* \setminus \mathcal{Q}_p$. This means that, in the quotient group $\mathbb{F}_p^*/\mathcal{A}$, each equivalence class is either included in $\mathcal{Q}_p$ or included in $\mathbb{F}_p^* \setminus \mathcal{Q}_p$. It follows that a set of representatives of all equivalence classes in $\mathbb{F}_p^*/\mathcal{A}$ has as many elements in $\mathcal{Q}_p$ as elements in $\mathbb{F}_p^* \setminus \mathcal{Q}_p$. Let $\{b_1, \ldots, b_\ell, b_{\ell+1}, \ldots, b_{m'}\}$ be a set of representatives of all equivalence classes in $\mathbb{F}_p^*/\mathcal{A}$ such that $m' = 2\ell$, $b_1, \ldots, b_\ell$ are squares and $b_{\ell+1}, \ldots, b_{m'}$ are not squares. Let $\mathcal{C}$ and $\mathcal{D}$

be the subsets of $\mathbb{F}_q^*$ defined by

$$\mathcal{C} = \{x \in \mathbb{F}_q^* : \mathrm{Tr}(x) \in \{b_1, \ldots, b_\ell\}\} \text{ and } \mathcal{D} = \{b_{\ell+1}, \ldots, b_{m'}\}.$$

Since $\{b_1, \ldots, b_{m'}\}$ is a set of representatives of all equivalence classes in $\mathbb{F}_p^*/\mathcal{A}$, we have $sb_i \neq b_j$ for any $s \in \mathcal{A} \setminus \{1\}$ and any $1 \leq i, j \leq m'$. It follows that for any $s \in \mathcal{A} \setminus \{1\}$, we have $\mathcal{C} \cap s\mathcal{C} = \mathcal{D} \cap s\mathcal{D} = \varnothing$. This implies that $\mathcal{C}$ and $\mathcal{D}$ satisfy (V.13). Moreover, since $|\mathcal{C}| = \ell q/p$ and $|\mathcal{D}| = \ell$, we have

$$\frac{pq}{16m^2} < |\mathcal{C}||\mathcal{D}| = \frac{(p-1)^2}{p}\frac{q}{4m^2} < \frac{pq}{m^2}$$

and so $\mathcal{C}$ and $\mathcal{D}$ satisfy (V.32). Finally, if $(c, d) \in \mathcal{C} \times \mathcal{D}$ then $\mathrm{Tr}(c) \in \mathcal{Q}_p$ and $d \in \mathbb{F}_p^* \setminus \mathcal{Q}_p$ and so $\mathrm{Tr}(cd) = d\,\mathrm{Tr}(c) \in \mathbb{F}_p^* \setminus \mathcal{Q}_p$. Since $\mathcal{A} \subset \mathcal{Q}_p$, this shows that $\mathcal{E}_{\mathcal{A}} = \varnothing$.

We consider now the case where m' is odd and $m' \geq 3$. Let us first prove that if $b \in \mathbb{F}_p^*$ and $b^2 \in \mathcal{A}$ then $b \in \mathcal{A}$. Indeed, if $b^2 \in \mathcal{A}$ then, by (V.27), there exists $1 \leq k \leq m$ such that $b^2 = g_0^{km'}$ and since m' is odd, k is even, therefore $b = g_0^{\frac{k}{2}m'} \in \mathcal{A}$ or $b = g_0^{\frac{k}{2}m' + \frac{p-1}{2}} = g_0^{\frac{k+m}{2}m'} \in \mathcal{A}$. It follows that if $b \in \mathbb{F}_p^* \setminus \mathcal{A}$ then b^{-1} does not belong to the equivalence class of b. We will deduce that there exists a set of representatives of all equivalence classes in $\mathbb{F}_p^*/\mathcal{A}$ which is of the form

$$\{1, b_1, b_1^{-1}, b_2, b_2^{-1}, \ldots, b_\ell, b_\ell^{-1}\}$$

where $\ell = (m'-1)/2$. To show this, consider any element b_1 of $\mathbb{F}_p^* \setminus \mathcal{A}$. Then, 1, b_1 and b_1^{-1} represent three different equivalence classes in $\mathbb{F}_p^*/\mathcal{A}$. For $1 \leq t \leq \ell - 1$, assuming that there exists $b_1, \ldots, b_t \in \mathbb{F}_p^*$ such that $1, b_1, b_1^{-1}, \ldots, b_t, b_t^{-1}$ represent $1 + 2t$ different equivalence classes in $\mathbb{F}_p^*/\mathcal{A}$ and taking an element $b_{t+1} \in \mathbb{F}_p^*$ which belongs to none of these equivalence classes, it is easy to check that $1, b_1, b_1^{-1}, \ldots, b_t, b_t^{-1}, b_{t+1}, b_{t+1}^{-1}$ represent $1 + 2(t+1)$ different equivalence classes in $\mathbb{F}_p^*/\mathcal{A}$ (clearly $b_{t+1}^{-1} \notin \mathcal{A}$, b_{t+1}^{-1} does not belong to the equivalence class of b_{t+1} and for $1 \leq i \leq t$, since b_{t+1} belongs neither to the equivalence class of b_i nor to the equivalence class of b_i^{-1}, b_{t+1}^{-1} belongs neither to the equivalence class of b_i^{-1} nor to the equivalence class of b_i). This proves that there exists $b_1, \ldots, b_\ell \in \mathbb{F}_p^*$ such that $1, b_1, b_1^{-1}, \ldots, b_\ell, b_\ell^{-1}$ represent $1 + 2\ell$ different equivalence classes in $\mathbb{F}_p^*/\mathcal{A}$. Since the number of different equivalence classes in $\mathbb{F}_p^*/\mathcal{A}$ is $m' = 1 + 2\ell$, the set $\{1, b_1, b_1^{-1}, \ldots, b_\ell, b_\ell^{-1}\}$ is a set of representatives of all equivalence classes in $\mathbb{F}_p^*/\mathcal{A}$. Let $\mathcal{C}$ and $\mathcal{D}$ be the subsets of $\mathbb{F}_q^*$ defined by

$$\mathcal{C} = \{x \in \mathbb{F}_q^* : \mathrm{Tr}(x) \in \{1, b_1, b_1^{-1}, \ldots, b_{\ell'}, b_{\ell'}^{-1}\}\}$$

and

$$\mathcal{D} = \{b_{\ell'+1}, b_{\ell'+1}^{-1}, \ldots, b_\ell, b_\ell^{-1}\}$$

where $\ell' = \lfloor \frac{\ell}{2} \rfloor$ is the integral part of $\ell/2$. Again, since $\{1, b_1, b_1^{-1}, \ldots, b_\ell, b_\ell^{-1}\}$ is a set of representatives of all equivalence classes in $\mathbb{F}_p^*/\mathcal{A}$, for any $s \in \mathcal{A} \setminus \{1\}$, we have $\mathcal{C} \cap s\mathcal{C} = \mathcal{D} \cap s\mathcal{D} = \varnothing$, which implies that $\mathcal{C}$ and $\mathcal{D}$ satisfy (V.13). Moreover, since $\|\mathcal{C}| = \frac{(2\ell'+1)q}{p}$ and $|\mathcal{D}| = 2(\ell - \ell')$,

we have $|\mathcal{C}||\mathcal{D}| = \ell(\ell+1)\frac{q}{p}$. Using that $y - 1 \geq 2y/3$ as soon as $y \geq 3$, we obtain

$$\frac{p^2}{16m^2} < \frac{2}{27}\frac{p^2}{m^2} \leq \frac{(p-1)^2}{6m^2} = \frac{m'^2}{6} \leq \frac{m'^2-1}{4} = \ell(\ell+1) < m'^2 < \frac{p^2}{m^2}$$

which shows that $\mathcal{C}$ and $\mathcal{D}$ satisfy (V.32). Finally, since $\{1, b_1, b_1^{-1}, \ldots, b_\ell, b_\ell^{-1}\}$ is a set of representatives of all equivalence classes in $\mathbb{F}_p^*/\mathcal{A}$, for any $\ell'+1 \leq j \leq \ell$ and for any $\varepsilon' \in \{-1, 1\}$ we have $b_j^{\varepsilon'} \notin \mathcal{A}$ and for any $1 \leq i \leq \ell'$ and any $\varepsilon \in \{-1, 1\}$ we have $b_i^{\varepsilon} \neq b_j^{-\varepsilon'}$ which implies that $b_i^{\varepsilon} b_j^{\varepsilon'} \notin \mathcal{A}$. Thus, if $(c, d) \in \mathcal{C} \times \mathcal{D}$ then $\mathrm{Tr}(cd) = d\,\mathrm{Tr}(c) \notin \mathcal{A}$ and it follows that $\mathcal{E}_{\mathcal{A}} = \varnothing$.

For $p \geq 3$ and $m = p - 1$, we will show that condition (V.12) is sharp up to a factor $4p$: we can find explicit sets $\mathcal{C}$ and $\mathcal{D}$ satisfying (V.13) with $\mathcal{A} = \mathbb{F}_p^*$ such that

$$q/(4(p-1)^2) < |\mathcal{C}||\mathcal{D}| = q/p^2 < pq/(p-1)^2 \tag{V.33}$$

and for which $\mathcal{E}_{\mathbb{F}_p^*} = \varnothing$. If $\{e_1, \ldots, e_r\}$ is a basis of $\mathbb{F}_q$ over $\mathbb{F}_p$, we can consider for instance

$$\mathcal{C} = \left\{x \in \mathbb{F}_q^* : f_1(x) = 0 \text{ and } f_2(x) = 1\right\} \text{ and } \mathcal{D} = \{e_1\}$$

where f_1 and f_2 are defined as in Section 3.4. Then, the sets $\mathcal{C}$ and $\mathcal{D}$ satisfy (V.13) with $\mathcal{A} = \mathbb{F}_p^*$ (see Section 6.3). Since $|\mathcal{C}||\mathcal{D}| = q/p^2$, (V.33) is also satisfied. Moreover, if $(c, d) \in \mathcal{C} \times \mathcal{D}$ then $\mathrm{Tr}(cd) = f_1(c) = 0$ and thus $\mathcal{E}_{\mathbb{F}_p^*} = \varnothing$. This shows that condition (V.12) is sharp up to a factor $4p$.

4.4. Proof and optimality of Corollary 1.7

Let $k \geq 1$ be an integer. The set $\mathcal{A}_k$ of k-th powers in $\mathbb{F}_p^*$ is a subgroup of $\mathbb{F}_p^*$ of order $\frac{p-1}{(k,p-1)}$ (see [61, Lemma 2D]). Thus we can apply Theorem 1.6 with $\mathcal{A} = \mathcal{A}_k$ and $m = \frac{p-1}{(k,p-1)}$. This completes the proof of Corollary 1.7.

Let us assume that $p \geq 3$ and $(k, p-1) \neq 1$ which implies $m \neq p - 1$. By Section 4.3, we can construct sets $\mathcal{C}$ and $\mathcal{D}$ satisfying (V.13) with $\mathcal{A} = \mathcal{A}_k$ such that

$$\frac{p(k,p-1)^2}{16(p-1)^2}q < |\mathcal{C}||\mathcal{D}| < \frac{p(k,p-1)^2}{(p-1)^2}q$$

and for which $\mathcal{E}_{\mathcal{A}_k} = \varnothing$. It follows that condition (V.14) is optimal up to an absolute constant factor.

4.5. Proof and optimality of Corollary 1.8

Assume $p \geq 3$. Since $(2, p-1) = 2$, Corollary 1.8 follows immediately from Corollary 1.7.

Moreover, we can find explicit sets $\mathcal{C}$ and $\mathcal{D}$ satisfying (V.13) with $\mathcal{A} = \mathcal{Q}_p$ such that $|\mathcal{C}||\mathcal{D}| = \frac{q}{p}$ and for which $\mathrm{Tr}(cd)$ never belongs to $\mathcal{Q}_p$. Consider for instance $\mathcal{C} = \left\{x \in \mathbb{F}_q^* : \mathrm{Tr}(x) = 1\right\}$ and $\mathcal{D} = \{s_0\}$ where $s_0 \in \mathbb{F}_p^* \setminus \mathcal{Q}_p$. Then, the sets $\mathcal{C}$ and $\mathcal{D}$ satisfy (V.13) with $\mathcal{A} = \mathcal{Q}_p$ (see

Section 6.3), we have $|\mathcal{C}||\mathcal{D}| = \frac{q}{p}$ and if $(c,d) \in \mathcal{C} \times \mathcal{D}$ then $\mathrm{Tr}(cd) = d\,\mathrm{Tr}(c) = s_0 \notin \mathcal{Q}_p$. Since

$$\frac{pq}{4(p-1)^2} < |\mathcal{C}||\mathcal{D}| = \frac{q}{p} < \frac{4pq}{(p-1)^2},$$

this shows that condition (V.15) is optimal up to an absolute constant factor.

It is interesting to notice that the optimality of Corollary 1.8 follows from the optimality of Corollary 1.7 which follows from the optimality of Theorem 1.6 proved in Section 4.3. Note that in the special case where $\mathcal{A} = \mathcal{Q}_p$, the rather technical construction given in Section 4.3 to show the optimality of Theorem 1.6 coincides with the construction given in this section to show directly the optimality of Corollary 1.8.

5. Products cd whose trace is a generator

Let $\mathcal{G}_p$ be the set of all generators of $\mathbb{F}_p^*$. In order to prove Theorem 1.9, we first estimate $|\mathcal{E}_{\mathcal{G}_p}|$ where

$$\mathcal{E}_{\mathcal{G}_p} = \{(c,d) \in \mathcal{C} \times \mathcal{D} : \mathrm{Tr}(cd) \in \mathcal{G}_p\}.$$

5.1. An estimate of $|\mathcal{E}_{\mathcal{G}_p}|$

In order to estimate $|\mathcal{E}_{\mathcal{G}_p}|$, we will need the following lemma.

Lemma 5.1. *The quantity $\Delta_{\mathcal{G}}(g_0, \mathcal{C})$ defined for $g_0 \in \mathcal{G}_p$ and $\mathcal{C} \subset \mathbb{F}_q^*$ by (V.17) does not depend on g_0 and will be simply denoted by $\Delta_{\mathcal{G}}(\mathcal{C})$.*

Proof. It follows immediately from (V.16) that the sequence $(m_k)_{k\geq 1}$ is $p-1$ periodic and that $m_{\ell k} = m_k$ as soon as $k \geq 1$, $\ell \geq 1$ and $(\ell, p-1) = 1$. Therefore, if $g_0 \in \mathcal{G}_p$ and $g_1 \in \mathcal{G}_p$, observing that there exists $\ell \geq 1$ such that $(\ell, p-1) = 1$ and $g_1 = g_0^\ell$, we deduce that for any $\mathcal{C} \subset \mathbb{F}_q^*$

$$\sum_{k=1}^{p-2} \frac{|\mathcal{C} \cap g_1^k \mathcal{C}|}{|\mathcal{C}|} m_k = \sum_{k=1}^{p-2} \frac{|\mathcal{C} \cap g_0^{\ell k} \mathcal{C}|}{|\mathcal{C}|} m_{\ell k} = \sum_{k'=1}^{p-2} \frac{|\mathcal{C} \cap g_0^{k'} \mathcal{C}|}{|\mathcal{C}|} m_{k'},$$

which proves that $\Delta_{\mathcal{G}}(g_0, \mathcal{C}) = \Delta_{\mathcal{G}}(g_1, \mathcal{C})$. □

Proposition 5.2. *The set $\mathcal{E}_{\mathcal{G}_p}$ satisfies*

$$|\mathcal{E}_{\mathcal{G}_p}| = \frac{\varphi(p-1)}{p} \frac{q}{q-1} |\mathcal{C}||\mathcal{D}| + R_{\mathcal{G}_p}$$

with

$$|R_{\mathcal{G}_p}| \leq \frac{\varphi(p-1)}{\sqrt{p}} \sqrt{q} \sqrt{|\mathcal{C}||\mathcal{D}|} \left(\frac{2^{\omega(p-1)}}{p-1} - \Delta_{\mathcal{G}}(\mathcal{C}) \right)^{1/2} \left(\frac{2^{\omega(p-1)}}{p-1} - \Delta_{\mathcal{G}}(\mathcal{D}) \right)^{1/2}$$

where φ is the Euler's totient function and $\Delta_{\mathcal{G}}(\mathcal{C})$ and $\Delta_{\mathcal{G}}(\mathcal{D})$ are defined by (V.17) and Lemma 5.1.

It will follow from the proof that the terms between parentheses are non-negative numbers, which is not trivial at first sight.

Proof of Proposition 5.2. We will need the following classical result on Ramanujan sums.

Lemma 5.3. *For integers $j \geq 1$ and $n \geq 1$, the Ramanujan sum $c_n(j)$ defined by*

$$c_n(j) = \sum_{\substack{1 \leq k \leq n \\ (k,n)=1}} \mathrm{e}\left(\frac{jk}{n}\right),$$

is multiplicative in n and satisfies

$$c_n(j) = \frac{\mu}{\varphi}\left(\frac{n}{(j,n)}\right)\varphi(n)$$

where μ is the Möbius function.

Proof. See [28, Theorem 67 and Theorem 272]. □

As in the previous section, we give an explicit formula for character sums over all generators of $\mathbb{F}_p^*$.

Lemma 5.4. *For any $g_0 \in \mathcal{G}_p$, for any $j \in \{1, \ldots, p-1\}$, the multiplicative character χ_j of $\mathbb{F}_p$ defined by (V.28) satisfies*

$$\sum_{s \in \mathcal{G}_p} \chi_j(s) = \frac{\mu}{\varphi}\left(\frac{p-1}{(j,p-1)}\right)\varphi(p-1).$$

Proof. The set $\mathcal{G}_p$ can be described in terms of g_0:

$$\mathcal{G}_p = \{g_0^k : 1 \leq k \leq p-1 \text{ and } (k, p-1) = 1\}$$

and it follows

$$\sum_{s \in \mathcal{G}_p} \chi_j(s) = \sum_{\substack{1 \leq k \leq p-1 \\ (k,p-1)=1}} \chi_j\left(g_0^k\right) = \sum_{\substack{1 \leq k \leq p-1 \\ (k,p-1)=1}} \mathrm{e}\left(\frac{kj}{p-1}\right).$$

The last sum is the Ramanujan sum $c_{p-1}(j)$ and we conclude by Lemma 5.3. □

The following lemma will enable us to handle the coefficients m_k.

Lemma 5.5. *For $k \geq 1$, the arithmetic function M_k defined for $n \geq 1$ by*

$$M_k(n) = \sum_{j=1}^{n} \frac{\mu^2}{\varphi}\left(\frac{n}{(j,n)}\right)\mathrm{e}\left(\frac{jk}{n}\right)$$

is multiplicative. Moreover, M_k satisfies the following properties for any $n \geq 1$:

(i) $M_k(n) = 2^{\omega((k,n))} \prod_{\substack{p'|n \\ p' \nmid k}} \frac{p'-2}{p'-1} \geq 0,$

(ii) $\frac{1}{n} \sum_{k=1}^{n} M_k(n) = 1.$

Proof. Let $k \geq 1$. For any $n \geq 1$,

$$M_k(n) = \sum_{d|n} \frac{\mu^2}{\varphi}(d) \sum_{\substack{1 \leq j \leq n \\ (j,n)=\frac{n}{d}}} \mathrm{e}\left(\frac{jk}{n}\right) = \sum_{d|n} \frac{\mu^2}{\varphi}(d) \sum_{\substack{1 \leq u \leq d \\ (u,d)=1}} \mathrm{e}\left(\frac{uk}{d}\right) = \sum_{d|n} \frac{\mu^2}{\varphi}(d) c_d(k). \tag{V.34}$$

The function $\frac{\mu^2}{\varphi}$ is multiplicative and by Lemma 5.3, the function $\ell \mapsto c_\ell(k)$ is multiplicative too. Thus, M_k is multiplicative as a convolution of multiplicative functions. By (V.34) and Lemma 5.3, we have for any prime number p' and any integer $\nu \geq 1$:

$$\begin{aligned} M_k(p'^\nu) &= \frac{\mu^2}{\varphi}(1)c_1(k) + \frac{\mu^2}{\varphi}(p')c_{p'}(k) = 1 + \frac{\mu}{\varphi}\left(\frac{p'}{(k,p')}\right) \\ &= \begin{cases} 2 & \text{if } p'|k, \\ 1 - 1/(p'-1) & \text{otherwise.} \end{cases} \end{aligned}$$

Since M_k is multiplicative, we deduce that for any $n \geq 1$,

$$\begin{aligned} M_k(n) &= \prod_{p'^\nu \| n} M_k(p'^\nu) = \prod_{\substack{p'|n \\ p' \nmid k}} (1 - 1/(p'-1)) \prod_{p'|(k,n)} 2 \\ &= 2^{\omega((k,n))} \prod_{\substack{p'|n \\ p' \nmid k}} \frac{p'-2}{p'-1} \geq 0. \end{aligned}$$

This proves (i). To prove (ii), it suffices to notice that

$$\sum_{k=1}^{n} M_k(n) = \sum_{j=1}^{n} \frac{\mu^2}{\varphi}\left(\frac{n}{(j,n)}\right) \sum_{k=1}^{n} \mathrm{e}\left(\frac{jk}{n}\right) = n\,\frac{\mu^2}{\varphi}(1) = n. \qquad \square$$

We are now ready to prove Proposition 5.2. Since $|\mathcal{G}_p| = \varphi(p-1)$, by Lemma 2.1, we can write

$$|\mathcal{E}_{\mathcal{G}_p}| = P_{\mathcal{G}_p} + R_{\mathcal{G}_p}$$

where $P_{\mathcal{G}_p} = \frac{\varphi(p-1)}{p} \frac{q}{q-1} |\mathcal{C}||\mathcal{D}|$ and $R_{\mathcal{G}_p}$ is given by (V.21). In order to study $R_{\mathcal{G}_p}$, consider $g_0 \in \mathcal{G}_p$. Filtering the multiplicative characters of $\mathbb{F}_q$ according to their restriction to $\mathbb{F}_p^*$, we obtain

$$R_{\mathcal{G}_p} = \frac{1}{q-1} \sum_{j=1}^{p-1} \sum_{\substack{\chi \neq \chi_0 \\ \chi_{|\mathbb{F}_p^*} = \chi_j}} \overline{S_{\mathcal{H}_{\mathcal{G}_p}}(\chi)} S_{\mathcal{C}}(\chi) S_{\mathcal{D}}(\chi) \tag{V.35}$$

where χ_j is defined by (V.28). By Corollary 2.5 and by Lemma 5.4, for any $j \in \{1, \dots, p-1\}$ and for any character $\chi \neq \chi_0$ with $\chi_{|\mathbb{F}_p^*} = \chi_j$, we have

$$\begin{aligned} S_{\mathcal{H}_{\mathcal{G}_p}}(\chi) &= \frac{1}{p}\overline{\tau(\chi_j)}G(\chi,\psi_1)\sum_{s\in\mathcal{G}_p}\chi_j(s) \\ &= \frac{1}{p}\overline{\tau(\chi_j)}G(\chi,\psi_1)\frac{\mu}{\varphi}\left(\frac{p-1}{(j,p-1)}\right)\varphi(p-1), \end{aligned}$$

and thus

$$|S_{\mathcal{H}_{\mathcal{G}_p}}(\chi)| \leq \frac{\sqrt{q}}{\sqrt{p}}\frac{\mu^2}{\varphi}\left(\frac{p-1}{(j,p-1)}\right)\varphi(p-1).$$

It follows from (V.35) that

$$|R_{\mathcal{G}_p}| \leq \frac{\varphi(p-1)}{\sqrt{p}}\frac{\sqrt{q}}{q-1}\sum_{j=1}^{p-1}\sum_{\substack{\chi\neq\chi_0\\ \chi_{|\mathbb{F}_p^*}=\chi_j}}\frac{\mu^2}{\varphi}\left(\frac{p-1}{(j,p-1)}\right)|S_{\mathcal{C}}(\chi)S_{\mathcal{D}}(\chi)|.$$

Using the Cauchy–Schwarz inequality, we get

$$|R_{\mathcal{G}_p}| \leq \frac{\varphi(p-1)}{\sqrt{p}}\frac{\sqrt{q}}{q-1}T_{\mathcal{C}}^{1/2}T_{\mathcal{D}}^{1/2} \tag{V.36}$$

where

$$T_{\mathcal{C}} = \sum_{j=1}^{p-1}\sum_{\substack{\chi\neq\chi_0\\ \chi_{|\mathbb{F}_p^*}=\chi_j}}\frac{\mu^2}{\varphi}\left(\frac{p-1}{(j,p-1)}\right)|S_{\mathcal{C}}(\chi)|^2$$

and $T_{\mathcal{D}}$ is defined similarly with $\mathcal{D}$ in place of $\mathcal{C}$. By Lemma 2.8,

$$\begin{aligned} T_{\mathcal{C}} &= \sum_{j=1}^{p-1}\frac{\mu^2}{\varphi}\left(\frac{p-1}{(j,p-1)}\right)\sum_{\substack{\chi\neq\chi_0\\ \chi_{|\mathbb{F}_p^*}=\chi_j}}|S_{\mathcal{C}}(\chi)|^2 \\ &= \sum_{j=1}^{p-1}\frac{\mu^2}{\varphi}\left(\frac{p-1}{(j,p-1)}\right)\left(\frac{q-1}{p-1}\sum_{s\in\mathbb{F}_p^*}\chi_j(s)|\mathcal{C}\cap s\mathcal{C}| - |\mathcal{C}|^2\mathbb{1}_{\chi_j=1}\right) \\ &= \frac{q-1}{p-1}\sum_{s\in\mathbb{F}_p^*}|\mathcal{C}\cap s\mathcal{C}|\sum_{j=1}^{p-1}\frac{\mu^2}{\varphi}\left(\frac{p-1}{(j,p-1)}\right)\chi_j(s) - |\mathcal{C}|^2 \\ &= \frac{q-1}{p-1}\sum_{k=1}^{p-1}|\mathcal{C}\cap g_0^k\mathcal{C}|\sum_{j=1}^{p-1}\frac{\mu^2}{\varphi}\left(\frac{p-1}{(j,p-1)}\right)\chi_j(g_0^k) - |\mathcal{C}|^2. \end{aligned}$$

Since $\chi_j(g_0^k) = \mathrm{e}\left(\frac{jk}{p-1}\right)$, each sum over j in $T_{\mathcal{C}}$ is exactly $M_k(p-1)$ which is equal to m_k by (i)

of Lemma 5.5. It follows that

$$T_{\mathcal{C}} = \frac{q-1}{p-1}\sum_{k=1}^{p-1} |\mathcal{C} \cap g_0^k \mathcal{C}| m_k - |\mathcal{C}|^2.$$

Similarly, we get

$$T_{\mathcal{D}} = \frac{q-1}{p-1}\sum_{k=1}^{p-1} |\mathcal{D} \cap g_0^k \mathcal{D}| m_k - |\mathcal{D}|^2.$$

To conclude, it is enough to insert the above expressions for $T_{\mathcal{C}}$ and $T_{\mathcal{D}}$ into (V.36) and to notice that $m_{p-1} = 2^{\omega(p-1)}$. Observe that $T_{\mathcal{C}} \geq 0$ and $T_{\mathcal{D}} \geq 0$ by definition. □

5.2. Proof of Theorem 1.9

It follows from Proposition 5.2 that

$$|\mathcal{E}_{\mathcal{G}_p}| = \frac{\varphi(p-1)}{p}\frac{q}{q-1}|\mathcal{C}||\mathcal{D}| + R_{\mathcal{G}_p}$$

where by (V.19),

$$|R_{\mathcal{G}_p}| \leq \frac{\varphi(p-1)}{\sqrt{p}}\sqrt{q}\sqrt{|\mathcal{C}||\mathcal{D}|}\,\frac{2^{\omega(p-1)}}{p-1} \leq \frac{2\varphi(p-1)2^{\omega(p-1)}}{p\sqrt{p}}\sqrt{q}\sqrt{|\mathcal{C}||\mathcal{D}|}.$$

Therefore

$$|\mathcal{E}_{\mathcal{G}_p}| > \frac{\varphi(p-1)}{p}|\mathcal{C}||\mathcal{D}| - \frac{2\varphi(p-1)2^{\omega(p-1)}}{p\sqrt{p}}\sqrt{q}\sqrt{|\mathcal{C}||\mathcal{D}|}$$

which proves that if $|\mathcal{C}||\mathcal{D}| \geq 4q\,\frac{2^{2\omega(p-1)}}{p}$ then $\mathcal{E}_{\mathcal{G}_p}$ is nonempty and completes the proof of Theorem 1.9.

If $p \geq 3$, there exists sets $\mathcal{C}$ and $\mathcal{D}$ satisfying (V.19) such that $|\mathcal{C}||\mathcal{D}| = \frac{q}{p}$ and for which $\mathcal{E}_{\mathcal{G}_p} = \varnothing$. Consider for instance $\mathcal{C} = \left\{x \in \mathbb{F}_q^* : \mathrm{Tr}(x) = s_0\right\}$ where $s_0 \in \mathbb{F}_p^* \setminus \mathcal{G}_p$ and $\mathcal{D} = \{1\}$. The sets $\mathcal{C}$ and $\mathcal{D}$ satisfy (V.19) (see Section 6.3) and $|\mathcal{C}||\mathcal{D}| = \frac{q}{p}$. Moreover, if $(c,d) \in \mathcal{C} \times \mathcal{D}$ then $\mathrm{Tr}(cd) = \mathrm{Tr}(c) = s_0 \notin \mathcal{G}_p$ and so $\mathcal{E}_{\mathcal{G}_p} = \varnothing$.

6. Study of $|\mathcal{C} \cap s\mathcal{C}|$ for $\mathcal{C} \subset \mathbb{F}_q^*$

The quantity $|\mathcal{C} \cap s\mathcal{C}|$ where $\mathcal{C} \subset \mathbb{F}_q^*$ arises naturally from the proofs of Theorems 1.3, 1.6 and 1.9. We will first study this quantity on average over all subsets $\mathcal{C}$ of $\mathbb{F}_q^*$ with fixed cardinality (see Section 6.1). This will enable us to show that conditions (V.8), (V.13) and (V.19) in Theorems 1.3, 1.6 and 1.9 respectively are true "on average" (see Section 6.2). In Section 6.3, we will give explicit examples of sets $\mathcal{C}$ satisfying these conditions.

6.1. An exact formula for the average of $|\mathcal{C} \cap s\mathcal{C}|$ over $\mathcal{C} \subset \mathbb{F}_q^*$ with $|\mathcal{C}|$ fixed

We will show the following result.

Proposition 6.1. *If $x \in \mathbb{F}_q^* \setminus \{1\}$ then for any $1 \leq d \leq q-1$, the sum $T(d,x)$ defined by*

$$T(d,x) = \sum_{\substack{\mathcal{C} \subset \mathbb{F}_q^* \\ |\mathcal{C}|=d}} |\mathcal{C} \cap x\mathcal{C}|$$

is independent of x and satisfies

$$T(d,x) = \frac{d(d-1)}{q-2}\binom{q-1}{d}.$$

It follows that if $x \in \mathbb{F}_q^* \setminus \{1\}$ then the average of $|\mathcal{C} \cap x\mathcal{C}|$ over all subsets $\mathcal{C}$ of $\mathbb{F}_q^*$ with d elements is $\frac{d(d-1)}{q-2}$. We will see in Section 6.3 that the quantity $|\mathcal{C} \cap x\mathcal{C}|$ can be "far" from $\frac{|\mathcal{C}|(|\mathcal{C}|-1)}{q-2}$ (for example, it can be equal to 0 even for "large sets" $\mathcal{C}$). This leads us to ask the following question.

Question 6.2. For $x \in \mathbb{F}_q^* \setminus \{1\}$, give natural conditions on $\mathcal{C}$ so that $|\mathcal{C} \cap x\mathcal{C}|$ is "close" to $\frac{|\mathcal{C}|(|\mathcal{C}|-1)}{q-2}$.

Proposition 6.1 is an immediate consequence of the following result.

Lemma 6.3. *If G is a finite group of order $N \geq 2$ then for any $x \in G$, $x \neq 1$ and for any $1 \leq d \leq N$, the sum $U_G(d,x)$ defined by*

$$U_G(d,x) = \sum_{\substack{\mathcal{C} \subset G \\ |\mathcal{C}|=d}} |\mathcal{C} \cap x\mathcal{C}|$$

is independent of x and satisfies

$$U_G(d,x) = \frac{d(d-1)}{N-1}\binom{N}{d}.$$

Proof. (Lemma 6.3) It suffices to write for any $x \in G$ and any $1 \leq d \leq N$,

$$U_G(d,x) = \sum_{\substack{\mathcal{C} \subset G \\ |\mathcal{C}|=d}} \sum_{\substack{y \in \mathcal{C} \\ xy \in \mathcal{C}}} 1 = \sum_{y \in G} \sum_{\substack{\mathcal{C} \subset G \\ |\mathcal{C}|=d \\ y \in \mathcal{C} \\ xy \in \mathcal{C}}} 1.$$

If $x \neq 1$ and $d \geq 2$ then the number of subsets $\mathcal{C} \subset G$ with $|\mathcal{C}| = d$ containing the two distinct

elements y and xy is $\binom{N-2}{d-2}$, hence

$$U_G(d,x) = N\binom{N-2}{d-2} = \frac{d(d-1)}{N-1}\binom{N}{d}.$$

If $x \neq 1$ and $d = 1$ then it is clear that $U_G(d,x) = 0$ which completes the proof of Lemma 6.3. □

6.2. Conditions (V.8), (V.13) and (V.19) are true "on average"

Let us recall these conditions:

(i) $\dfrac{1}{p-1}\displaystyle\sum_{s\in\mathbb{F}_p^*\setminus\{1\}} \frac{|\mathcal{C}\cap s\mathcal{C}|}{|\mathcal{C}|} \le \frac{|\mathcal{C}|}{q-1}$ (condition (V.8) in Theorem 1.3),

(ii) $\dfrac{1}{m}\displaystyle\sum_{s\in\mathcal{A}\setminus\{1\}} \frac{|\mathcal{C}\cap s\mathcal{C}|}{|\mathcal{C}|} \le \frac{|\mathcal{C}|}{q-1}$ (condition (V.13) in Theorem 1.6),

(iii) $\dfrac{1}{p-1}\displaystyle\sum_{k=1}^{p-2} \frac{|\mathcal{C}\cap g_0^k\mathcal{C}|}{|\mathcal{C}|} m_k \le \frac{|\mathcal{C}|}{q-1}$ (condition (V.19) in Theorem 1.9).

Let $1 \le d \le q-1$. Consider all the subsets $\mathcal{C}$ of $\mathbb{F}_q^*$ with $|\mathcal{C}| = d$. It follows from Proposition 6.1 that the sum

$$\frac{1}{p-1}\sum_{s\in\mathbb{F}_p^*\setminus\{1\}} \frac{|\mathcal{C}\cap s\mathcal{C}|}{|\mathcal{C}|}$$

is on average equal to

$$\frac{1}{\binom{q-1}{d}}\sum_{\substack{\mathcal{C}\subset\mathbb{F}_q^*\\ |\mathcal{C}|=d}} \frac{1}{p-1}\sum_{s\in\mathbb{F}_p^*\setminus\{1\}} \frac{|\mathcal{C}\cap s\mathcal{C}|}{|\mathcal{C}|} = \frac{p-2}{p-1}\,\frac{d-1}{q-2} < \frac{d}{q-1}.$$

Thus, (i) is true "on average". The average of the sums

$$\frac{1}{m}\sum_{s\in\mathcal{A}\setminus\{1\}} \frac{|\mathcal{C}\cap s\mathcal{C}|}{|\mathcal{C}|}$$

is equal to $\frac{m-1}{m}\frac{d-1}{q-2} < \frac{d}{q-1}$. Thus, (ii) is true "on average". This is also the case for (iii). Indeed, by Lemma 5.5, since $m_k = M_k(p-1)$ for any $1 \le k \le p-1$ and since $m_{p-1} = 2^{\omega(p-1)}$ we obtain

$$\frac{2^{\omega(p-1)}}{p-1} + \frac{1}{p-1}\sum_{k=1}^{p-2} m_k = 1.$$

Thus the average of the sums

$$\frac{1}{p-1}\sum_{k=1}^{p-2} \frac{|\mathcal{C}\cap g_0^k\mathcal{C}|}{|\mathcal{C}|} m_k$$

is equal to $\frac{d-1}{q-2}\left(1 - \frac{2^{\omega(p-1)}}{p-1}\right) < \frac{d}{q-1}$ which shows that (iii) is true "on average".

To go further in the study of conditions (V.8), (V.13) and (V.19), it would be interesting to answer the following question.

Question 6.4. For each of the conditions (V.8), (V.13) and (V.19), find an estimate of the number of sets $\mathcal{C}$ satisfying the condition and such that $|\mathcal{C}| = d$.

6.3. Explicit examples of sets satisfying conditions (V.8), (V.13) and (V.19)

6.3.1. Subsets $\mathcal{C}$ contained in an affine hyperplane H such that $0 \notin H$

If $f : \mathbb{F}_q \to \mathbb{F}_p$ is an $\mathbb{F}_p$-linear form and if $s \in \mathbb{F}_p$, we denote by $H(f, s)$ the affine hyperplane defined by

$$H(f, s) = \{x \in \mathbb{F}_q : f(x) = s\}$$

and we will show

Lemma 6.5. *If $\mathcal{C}$ is a subset of $\mathbb{F}_q^*$ such that $\mathcal{C} \subset H(f, s)$ for some linear form $f : \mathbb{F}_q \to \mathbb{F}_p$ and some $s \in \mathbb{F}_p^*$ then $\mathcal{C}$ satisfies the three conditions (V.8), (V.13) and (V.19).*

In particular, the following sets $\mathcal{C}$ satisfy the three conditions (V.8), (V.13) and (V.19):

- any subset $\mathcal{C}$ on which Tr is constant and not equal to 0 (take $f = \mathrm{Tr}$),
- any subset $\mathcal{C}$ for which there exists a basis $\mathcal{B}$ of $\mathbb{F}_q$ over $\mathbb{F}_p$ and $1 \leq j \leq r$ such that all the j-th coordinates in base $\mathcal{B}$ of the elements of $\mathcal{C}$ are equal to the same $c_j \neq 0$ (take $f = \varepsilon_j$ where ε_j is the linear form which maps each $x \in \mathbb{F}_q$ to its j-th coordinate in base $\mathcal{B}$).

Remark 6.6. Lemma 6.5 provides sets $\mathcal{C}$ satisfying the three conditions (V.8), (V.13) and (V.19) of any cardinality less than q/p.

Proof. (Lemma 6.5) If $f : \mathbb{F}_q \to \mathbb{F}_p$ is a linear form, if $s \in \mathbb{F}_p^*$ and if $\mathcal{C} \subset H(f, s)$ then for any $t \in \mathbb{F}_p^* \setminus \{1\}$ and any $c \in \mathcal{C}$, we have $f(tc) = ts \neq s$ thus $\mathcal{C} \cap t\mathcal{C} = \varnothing$ which implies that $\mathcal{C}$ satisfies the three conditions (V.8), (V.13) and (V.19). □

6.3.2. Subgroups $\mathcal{C}$ of $\mathbb{F}_q^*$ satisfying condition (V.8), (V.13) or (V.19)

In this section, our purpose is to determine which subgroups $\mathcal{C}$ of $\mathbb{F}_q^*$ satisfy condition (V.8), (V.13) or (V.19). The following lemma will enable us to answer this question.

Lemma 6.7. *If d is a divisor of $q - 1$, if $\mathcal{C}$ is the subgroup of $\mathbb{F}_q^*$ with $|\mathcal{C}| = d$ and if g_0 is a generator of $\mathbb{F}_p^*$ then for any $1 \leq \ell \leq p - 1$,*

$$\mathcal{C} \cap g_0^\ell \mathcal{C} = \begin{cases} \mathcal{C} & \text{if } p - 1 \mid \ell d, \\ \varnothing & \text{otherwise.} \end{cases} \tag{V.37}$$

Proof. Let $1 \leq \ell \leq p-1$. Since $\mathcal{C}$ is a subgroup, $\mathcal{C} \cap g_0^\ell \mathcal{C} = \mathcal{C}$ if $g_0^\ell \in \mathcal{C}$ and $\mathcal{C} \cap g_0^\ell \mathcal{C} = \varnothing$ otherwise. Moreover, since the order of $\mathcal{C}$ is d, $g_0^\ell \in \mathcal{C}$ if and only if $g_0^{\ell d} = 1$ i.e. $p - 1$ divides ℓd. □

Corollary 6.8. *Let d be a divisor of $q-1$. The subgroup $\mathcal{C}$ of $\mathbb{F}_q^*$ of order d satisfies*

(i) condition (V.8) if and only if $(q-1)((p-1,d)-1) \leq d(p-1)$,

(ii) condition (V.13) if and only if $(q-1)((m,d)-1) \leq dm$,

(iii) condition (V.19) if and only if $(q-1)\left((p-1,d)2^{\omega\left(\frac{p-1}{(p-1,d)}\right)} - 2^{\omega(p-1)}\right) \leq d(p-1)$.

In particular:

a) if $(p-1,d)=1$ then $\mathcal{C}$ satisfies the three conditions (V.8), (V.13) or (V.19),

b) if $(m,d)=1$ then $\mathcal{C}$ satisfies (V.13),

c) if $p \geq 3$, r is odd and $d=\frac{q-1}{2}$ then $\mathcal{C}$ satisfies condition (V.8) and if $\frac{p-1}{m}$ is odd, $\mathcal{C}$ satisfies also (V.13).

Remark 6.9. If $p \geq 3$ and r is odd, Corollary 6.8 provides a nontrivial example of a set $\mathcal{C}$ satisfying condition (V.8) such that $\mathcal{C} \cap s\mathcal{C} \neq \varnothing$ for several values of s. Indeed, the subgroup $\mathcal{C}$ considered in c) satisfies $\mathcal{C} \cap s\mathcal{C} = \mathcal{C}$ for $\frac{p-1}{2}$ values of $s \in \mathbb{F}_p^*$ (it will follow from the proof of c) that $(p-1,d)=\frac{p-1}{2}$ and thus, by Lemma 6.7, $\mathcal{C} \cap g_0^\ell \mathcal{C} = \mathcal{C}$ as soon as ℓ is even).

Proof. (Corollary 6.8) We start by proving (ii). Let us recall that m is a divisor of $p-1$ and that $\mathcal{A}$ is the subgroup of $\mathbb{F}_p^*$ of order m. By (V.37) and (V.27),

$$\sum_{s \in \mathcal{A}\setminus\{1\}} |\mathcal{C} \cap s\mathcal{C}| = |\mathcal{C}| \left| \left\{ 1 \leq k < m : p-1 \,\middle|\, kd\frac{p-1}{m} \right\} \right| = d((m,d)-1)$$

which proves (ii). Taking $m=p-1$, (i) follows immediately from (ii). We now prove (iii). By (V.37) and by Lemma 5.5,

$$\begin{aligned}
\sum_{k=1}^{p-1} |\mathcal{C} \cap g_0^k \mathcal{C}| m_k = |\mathcal{C}| \sum_{h=1}^{(p-1,d)} m_{h\frac{p-1}{(p-1,d)}} &= d \sum_{h=1}^{(p-1,d)} M_{h\frac{p-1}{(p-1,d)}}(p-1) \\
&= d \sum_{j=1}^{p-1} \frac{\mu^2}{\varphi}\left(\frac{p-1}{(p-1,j)}\right) \sum_{h=1}^{(p-1,d)} \mathrm{e}\left(\frac{jh}{(p-1,d)}\right) \\
&= d(p-1,d) \sum_{\substack{j=1 \\ (p-1,d)|j}}^{p-1} \frac{\mu^2}{\varphi}\left(\frac{p-1}{(p-1,j)}\right) \\
&= d(p-1,d) \sum_{u=1}^{d'} \frac{\mu^2}{\varphi}\left(\frac{d'}{(d',u)}\right) = d(p-1,d) M_{d'}(d')
\end{aligned}$$

where $d'=\frac{p-1}{(p-1,d)}$. Moreover, $m_{p-1}=2^{\omega(p-1)}$ and by Lemma 5.5, $M_{d'}(d')=2^{\omega(d')}$. We deduce that

$$\sum_{k=1}^{p-2} |\mathcal{C} \cap g_0^k \mathcal{C}| m_k = d\left((p-1,d)2^{\omega(d')} - 2^{\omega(p-1)}\right)$$

which completes the proof of (iii). a) and b) follow immediately from (i), (ii) and (iii). It remains to prove c). Since r is odd and $p \equiv 1 \bmod 2$, $\frac{q-1}{p-1} = p^{r-1} + \cdots + p + 1 \equiv 1 \bmod 2$ and

thus $(p-1,d) = \frac{p-1}{2}\left(2, \frac{q-1}{p-1}\right) = \frac{p-1}{2}$. It follows from (i) that $\mathcal{C}$ satisfies (V.8). If $\frac{p-1}{m}$ is odd then m is even and $\frac{q-1}{m} = \frac{p-1}{m}\frac{q-1}{p-1}$ is odd, thus $(m,d) = \frac{m}{2}\left(2, \frac{q-1}{m}\right) = \frac{m}{2}$ which implies, by (ii), that $\mathcal{C}$ satisfies (V.13). □

7. Further properties of $|\mathcal{C} \cap s\mathcal{C}|$ for $\mathcal{C} \subset \mathbb{F}_q^*$ and consequences

For any $\mathcal{A} \subset \mathbb{F}_q^*$ such that $1 \in \mathcal{A}$ and for any nonempty $\mathcal{C} \subset \mathbb{F}_q^*$, we define

$$T_{\mathcal{A}}(\mathcal{C}) = \frac{1}{m} \sum_{s \in \mathcal{A} \setminus \{1\}} \frac{|\mathcal{C} \cap s\mathcal{C}|}{|\mathcal{C}|} \qquad \text{where } m = |\mathcal{A}|.$$

This quantity arised naturally from the proof of Theorem 1.3 (with $\mathcal{A} = \mathbb{F}_p^*$) and Theorem 1.6 (with $\mathcal{A}$ a subgroup of $\mathbb{F}_p^*$). We proved in Section 6 that for any $1 \le d \le q-1$, the average of $T_{\mathcal{A}}(\mathcal{C})$ over all subsets $\mathcal{C}$ of $\mathbb{F}_q^*$ with $|\mathcal{C}| = d$ is

$$\mathbb{E}_{\mathcal{A},d} := \frac{1}{\binom{q-1}{d}} \sum_{\substack{\mathcal{C} \subset \mathbb{F}_q^* \\ |\mathcal{C}|=d}} T_{\mathcal{A}}(\mathcal{C}) = \frac{m-1}{m}\frac{d-1}{q-2}.$$

In Section 7.1, we will go further by studying the variance of $T_{\mathcal{A}}(\mathcal{C})$. This will allow us to obtain in Section 7.2 some improvements of Theorems 1.3 and 1.6.

7.1. An exact formula for the variance of $T_{\mathcal{A}}(\mathcal{C})$ over $\mathcal{C} \subset \mathbb{F}_q^*$ with $|\mathcal{C}|$ fixed

We will prove the following result.

Proposition 7.1. *If $q \ge 5$ and if $\mathcal{A}$ is a subset of $\mathbb{F}_q^*$ such that $1 \in \mathcal{A}$ and $\mathcal{A}$ is closed under inversion then for any $1 \le d \le q-1$, denoting $m = |\mathcal{A}|$, we have*

$$\begin{aligned} \mathbb{V}_{\mathcal{A},d} &:= \frac{1}{\binom{q-1}{d}} \sum_{\substack{\mathcal{C} \subset \mathbb{F}_q^* \\ |\mathcal{C}|=d}} \left(T_{\mathcal{A}}(\mathcal{C}) - \mathbb{E}_{\mathcal{A},d}\right)^2 \qquad \text{(V.38)} \\ &= \frac{2(m-1)}{m^2}\frac{(d-1)}{d}\frac{(q-1-d)(q-2-d)(q-m-1)}{(q-2)^2(q-3)(q-4)}. \end{aligned}$$

It follows that, under the conditions of Proposition 7.1, the variance $\mathbb{V}_{\mathcal{A},d}$ of $T_{\mathcal{A}}(\mathcal{C})$ over all subsets $\mathcal{C}$ of $\mathbb{F}_q^*$ with $|\mathcal{C}| = d$ satisfies

$$\mathbb{V}_{\mathcal{A},d} \le \frac{2}{m(q-2)}. \qquad \text{(V.39)}$$

Proposition 7.1 is a consequence of the following more general result.

Lemma 7.2. *If G is a finite group of order $N \geq 4$ and if H is a subset of $G \setminus \{1\}$ which is closed under inversion then for any $1 \leq d \leq N$, denoting $h = |H|$, we have*

$$\frac{1}{\binom{N}{d}} \sum_{\substack{\mathcal{C} \subset G \\ |\mathcal{C}|=d}} \left(\left(\sum_{x \in H} |\mathcal{C} \cap x\mathcal{C}| \right) - \frac{hd(d-1)}{N-1} \right)^2 \tag{V.40}$$
$$= 2hd(d-1) \frac{(N-d)(N-d-1)(N-h-1)}{(N-1)^2(N-2)(N-3)}.$$

By applying Lemma 7.2 with $G = \mathbb{F}_q^*$, $N = q-1$, $H = \mathcal{A} \setminus \{1\}$ and $h = m-1$, we obtain (V.38).

In order to prove Lemma 7.2, we first establish an exact formula for the average of

$$|\mathcal{C} \cap x_1\mathcal{C}||\mathcal{C} \cap x_2\mathcal{C}|$$

over $\mathcal{C} \subset G$ with $|\mathcal{C}|$ fixed.

Lemma 7.3. *If G is a finite group of order $N \geq 4$ then for any $(x_1, x_2) \in G^2$, $x_1 \neq 1$, $x_2 \neq 1$ and for any $1 \leq d \leq N$, the sum $V_G(d, x_1, x_2)$ defined by*

$$V_G(d, x_1, x_2) = \sum_{\substack{\mathcal{C} \subset G \\ |\mathcal{C}|=d}} |\mathcal{C} \cap x_1\mathcal{C}||\mathcal{C} \cap x_2\mathcal{C}|$$

satisfies

$$V_G(d, x_1, x_2) = \binom{N}{d} \frac{d(d-1)}{N-1} \left(Q_2(x_1, x_2) + \frac{d-2}{N-2} Q_3(x_1, x_2) + \frac{(d-2)(d-3)}{(N-2)(N-3)} Q_4(x_1, x_2) \right)$$

where

$$(Q_2(x_1, x_2), Q_3(x_1, x_2), Q_4(x_1, x_2)) = \begin{cases} (0, 4, N-4) & \text{if } x_2 \notin \{x_1, x_1^{-1}\}, \\ (1, 2, N-3) & \text{if } x_2 \in \{x_1, x_1^{-1}\} \text{ and } x_1 \neq x_1^{-1}, \\ (2, 0, N-2) & \text{if } x_2 = x_1 = x_1^{-1}. \end{cases}$$

Proof. Since $|\mathcal{C} \cap x\mathcal{C}| = \sum_{y \in G} \mathbb{1}_{(y,xy) \in \mathcal{C}^2}$ for any $x \in G$, we can write

$$V_G(d, x_1, x_2) = \sum_{(y_1, y_2) \in G^2} \sum_{\substack{\mathcal{C} \subset G \\ |\mathcal{C}|=d}} \mathbb{1}_{(y_1, x_1y_1, y_2, x_2y_2) \in \mathcal{C}^4}$$

and then, putting $y_2 = yy_1$,

$$V_G(d, x_1, x_2) = \sum_{(y_1, y) \in G^2} \sum_{\substack{\mathcal{C} \subset G \\ |\mathcal{C}|=d}} \mathbb{1}_{(1, x_1, y, x_2y) \in (\mathcal{C}y_1^{-1})^4} = N \sum_{y \in G} \sum_{\substack{\mathcal{D} \subset G \\ |\mathcal{D}|=d}} \mathbb{1}_{(1, x_1, y, x_2y) \in \mathcal{D}^4}.$$

Observing that

$$|\{1, x_1, y, x_2y\}| = \begin{cases} 2 \text{ if } (y = 1 \text{ and } x_2 = x_1) \text{ or } (y = x_1 \text{ and } x_2 = x_1^{-1}), \\ 4 \text{ if } y \notin \{1, x_1, x_2^{-1}, x_2^{-1}x_1\}, \\ 3 \text{ otherwise,} \end{cases} \tag{V.41}$$

and denoting $Q_i(x_1, x_2) = |\{y \in G : |\{1, x_1, y, x_2y\}| = i\}|$ for $2 \leq i \leq 4$, we obtain

$$\begin{aligned} V_G(d, x_1, x_2) &= N \sum_{\substack{i=2 \\ i \leq d}}^{4} \binom{N-i}{d-i} Q_i(x_1, x_2) \\ &= \binom{N}{d} \frac{d(d-1)}{N-1} \left(Q_2(x_1, x_2) + \frac{d-2}{N-2} Q_3(x_1, x_2) + \frac{(d-2)(d-3)}{(N-2)(N-3)} Q_4(x_1, x_2) \right). \end{aligned}$$

Moreover, by (V.41),

$$Q_2(x_1, x_2) = \begin{cases} 0 & \text{if } x_2 \notin \{x_1, x_1^{-1}\}, \\ 1 & \text{if } x_2 \in \{x_1, x_1^{-1}\} \text{ and } x_1 \neq x_1^{-1}, \\ 2 & \text{if } x_2 = x_1 = x_1^{-1}, \end{cases}$$

$$Q_4(x_1, x_2) = \begin{cases} N-4 & \text{if } x_2 \notin \{x_1, x_1^{-1}\}, \\ N-3 & \text{if } x_2 \in \{x_1, x_1^{-1}\} \text{ and } x_1 \neq x_1^{-1}, \\ N-2 & \text{if } x_2 = x_1 = x_1^{-1}, \end{cases}$$

and thus

$$Q_3(x_1, x_2) = N - Q_2(x_1, x_2) - Q_4(x_1, x_2) = \begin{cases} 4 & \text{if } x_2 \notin \{x_1, x_1^{-1}\}, \\ 2 & \text{if } x_2 \in \{x_1, x_1^{-1}\} \text{ and } x_1 \neq x_1^{-1}, \\ 0 & \text{if } x_2 = x_1 = x_1^{-1}, \end{cases}$$

which completes the proof of Lemma 7.3. □

We are now ready to prove Lemma 7.2. Using the same notations as in Lemma 7.3, we can write

$$\begin{aligned} \sum_{\substack{\mathcal{C} \subset G \\ |\mathcal{C}| = d}} \left(\sum_{x \in H} |\mathcal{C} \cap x\mathcal{C}| \right)^2 &= \sum_{(x_1, x_2) \in H^2} V_G(d, x_1, x_2) \\ &= \sum_{x_1 \in H} \sum_{\substack{x_2 \in H \\ x_2 \notin \{x_1, x_1^{-1}\}}} V_G(d, x_1, x_2) + \sum_{\substack{x_1 \in H \\ x_1^2 \neq 1}} \sum_{x_2 \in \{x_1, x_1^{-1}\}} V_G(d, x_1, x_2) + \sum_{\substack{x_1 \in H \\ x_1^2 = 1}} V_G(d, x_1, x_1). \end{aligned}$$

Since H is a subset of $G \setminus \{1\}$ which is closed under inversion, we have by denoting

$e = |\{x \in H : x^2 = 1\}|$ and $h = |H|$,

$$\sum_{\substack{x_1 \in H \\ x_1^2 = 1}} 1 = e,$$

$$\sum_{\substack{x_1 \in H \\ x_1^2 \neq 1}} \sum_{\substack{x_2 \in H \\ x_2 \in \{x_1, x_1^{-1}\}}} 1 = 2(h-e),$$

$$\sum_{x_1 \in H} \sum_{\substack{x_2 \in H \\ x_2 \notin \{x_1, x_1^{-1}\}}} 1 = e(h-1) + (h-e)(h-2),$$

and it follows from Lemma 7.3 that

$$\sum_{\substack{\mathcal{C} \subset G \\ |\mathcal{C}| = d}} \left(\sum_{x \in H} |\mathcal{C} \cap x\mathcal{C}| \right)^2 \tag{V.42}$$
$$= \binom{N}{d} \frac{hd(d-1)}{N-1} \left(2 + \frac{d-2}{N-2}(4(h-1)) + \frac{(d-2)(d-3)}{(N-2)(N-3)}(Nh - 4h + 2) \right).$$

Moreover, by Lemma 6.3,

$$\sum_{\substack{\mathcal{C} \subset G \\ |\mathcal{C}| = d}} \sum_{x \in H} |\mathcal{C} \cap x\mathcal{C}| = \binom{N}{d} \frac{hd(d-1)}{N-1}. \tag{V.43}$$

By combining (V.42) and (V.43), we obtain (V.40).

7.2. Improvements of Theorems 1.3 and 1.6

For any $\mathcal{A} \subset \mathbb{F}_q^*$ such that $1 \in \mathcal{A}$ and for any nonempty $\mathcal{C} \subset \mathbb{F}_q^*$, we define

$$\Delta_{\mathcal{A}}(\mathcal{C}) = \frac{|\mathcal{C}|}{q-1} - \frac{1}{m} \sum_{s \in \mathcal{A} \setminus \{1\}} \frac{|\mathcal{C} \cap s\mathcal{C}|}{|\mathcal{C}|} \qquad \text{where } m = |\mathcal{A}|.$$

By the same arguments as in the proof of Theorem 1.3, it follows from Proposition 3.2 that

Theorem 7.4. *If $\mathcal{C}$ and $\mathcal{D}$ are nonempty subsets of $\mathbb{F}_q^*$ satisfying*

$$|\mathcal{C}||\mathcal{D}| > 4q \left(\frac{q-1}{q-p} \right)^2 \tag{V.44}$$

and

$$\Delta_{\mathbb{F}_p^*}(\mathcal{C}) \geq -\frac{1}{p-1} \quad \text{and} \quad \Delta_{\mathbb{F}_p^*}(\mathcal{D}) \geq -\frac{1}{p-1} \tag{V.45}$$

then there exists $(c,d) \in \mathcal{C} \times \mathcal{D}$ such that $\mathrm{Tr}(cd) = 0$.

The condition (V.44) is slightly more restrictive than the condition (V.7) in Theorem 1.3 but it is still optimal up to an absolute constant factor : we constructed in Section 3.4 sets $\mathcal{C}$ and $\mathcal{D}$ satisfying (V.8) and thus (V.45) (note that in (V.8), $\Delta_0(\mathcal{C}) = \Delta_{\mathbb{F}_p^*}(\mathcal{C})$), such that

$$|\mathcal{C}||\mathcal{D}| > \frac{q}{32}\left(\frac{q-1}{q-p}\right)^2$$

and for which there is no $(c,d) \in \mathcal{C}\times\mathcal{D}$ such that $\mathrm{Tr}(cd) = 0$. The advantage of Theorem 7.4 over Theorem 1.3 is that the technical condition (V.45) is less restrictive than the condition (V.8) in Theorem 1.3 and is actually true with a probability close to 1 for large values of q (see Lemma 7.6 below).

Using the same idea, we obtain an improvement of Theorem 1.6 : by the same arguments as in the proof of Theorem 1.6, it follows from Proposition 4.1 that

Theorem 7.5. *If $\mathcal{A}$ is a nontrivial subgroup of $\mathbb{F}_p^*$ of order m and if $\mathcal{C}$ and $\mathcal{D}$ are nonempty subsets of $\mathbb{F}_q^*$ satisfying*

$$|\mathcal{C}||\mathcal{D}| \geq \frac{4pq}{m^2} \tag{V.46}$$

and

$$\Delta_{\mathcal{A}}(\mathcal{C}) \geq -\frac{1}{m} \quad \text{and} \quad \Delta_{\mathcal{A}}(\mathcal{D}) \geq -\frac{1}{m} \tag{V.47}$$

then there exists $(c,d) \in \mathcal{C}\times\mathcal{D}$ such that $\mathrm{Tr}(cd) \in \mathcal{A}$.

The condition (V.46) is slightly more restrictive than the condition (V.12) in Theorem 1.6 but it is still optimal up to an absolute constant factor : we constructed in Section 4.3 sets $\mathcal{C}$ and $\mathcal{D}$ satisfying (V.13) and thus (V.47), such that

$$|\mathcal{C}||\mathcal{D}| > \frac{pq}{16m^2}$$

and for which $\mathrm{Tr}(cd)$ never belongs to $\mathcal{A}$. Again, the advantage of Theorem 7.5 over Theorem 1.6 is that the technical condition (V.47) is less restrictive than the condition (V.13) in Theorem 1.6 and is actually true with a probability close to 1 for large values of q (see Lemma 7.6 below).

Lemma 7.6. *Assume that $q \geq 5$. Let $\mathcal{A}$ be a subset of $\mathbb{F}_q^*$ such that $1 \in \mathcal{A}$ and $\mathcal{A}$ is closed under inversion and denote $m = |\mathcal{A}|$. Let $1 \leq d \leq q-1$. If $\mathcal{C}$ is chosen at random among subsets of $\mathbb{F}_q^*$ with d elements then the probability that $\Delta_{\mathcal{A}}(\mathcal{C}) \geq -\frac{1}{m}$ is defined by*

$$\mathbb{P}\left(\Delta_{\mathcal{A}}(\mathcal{C}) \geq -\frac{1}{m}\right) = \frac{1}{\binom{q-1}{d}} \sum_{\substack{\mathcal{C}\subset\mathbb{F}_q^* \\ |\mathcal{C}|=d}} \mathbb{1}_{\Delta_{\mathcal{A}}(\mathcal{C})\geq -\frac{1}{m}}$$

and satisfies

$$\mathbb{P}\left(\Delta_{\mathcal{A}}(\mathcal{C}) \geq -\frac{1}{m}\right) \geq 1 - \frac{2m}{q-2}.$$

In particular, if $\mathcal{A}$ is $\mathbb{F}_p^*$ or any nontrivial subgroup of $\mathbb{F}_p^*$ then, since $m \leq p \leq \sqrt{q}$,

$$\lim_{q \to +\infty} \mathbb{P}\left(\Delta_{\mathcal{A}}(\mathcal{C}) \geq -\frac{1}{m}\right) = 1$$

which shows that the conditions (V.45) and (V.47) are true with a probability close to 1 for large values of q.

Proof. If $|\mathcal{C}| = d$ then $\Delta_{\mathcal{A}}(\mathcal{C}) = \frac{|\mathcal{C}|}{q-1} - T_{\mathcal{A}}(\mathcal{C}) \geq \mathbb{E}_{\mathcal{A},d} - T_{\mathcal{A}}(\mathcal{C})$ and thus

$$\mathbb{P}\left(\Delta_{\mathcal{A}}(\mathcal{C}) < -\frac{1}{m}\right) \leq \mathbb{P}\left(T_{\mathcal{A}}(\mathcal{C}) - \mathbb{E}_{\mathcal{A},d} > \frac{1}{m}\right) \leq \mathbb{P}\left(|T_{\mathcal{A}}(\mathcal{C}) - \mathbb{E}_{\mathcal{A},d}| \geq \frac{1}{m}\right).$$

Moreover, by applying the Bienaymé–Chebyshev inequality and the inequality (V.39), we obtain

$$\mathbb{P}\left(|T_{\mathcal{A}}(\mathcal{C}) - \mathbb{E}_{\mathcal{A},d}| \geq \frac{1}{m}\right) \leq \frac{\mathbb{V}_{\mathcal{A},d}}{(1/m)^2} \leq \frac{2m}{q-2}.$$

This completes the proof of Lemma 7.6. □

Annexe

Fonctions à support compact dont la transformée de Fourier est « très petite » à l'infini

Soit f une fonction intégrable sur $\mathbb{R}$, à support compact et qui n'est pas nulle presque partout. À quel point la transformée de Fourier

$$\widehat{f}(x) = \int_{\mathbb{R}} f(t)\,\mathrm{e}(-tx)dt$$

peut-elle être « petite » lorsque $|x| \to +\infty$?

Ingham remarque dans [33] que $\widehat{f}$ ne peut pas vérifier une condition du type

$$\widehat{f}(x) = O\left(e^{-|x|\varepsilon}\right) \qquad (|x| \to +\infty), \tag{A.1}$$

où $\varepsilon > 0$ est un réel fixé. En effet, sinon la transformée de Fourier h de $\widehat{f}$ serait holomorphe dans la bande $|\mathrm{Im}(z)| < \varepsilon/(2\pi)$. Alors, comme f est à support compact et $h(x) = f(-x)$ pour presque tout $x \in \mathbb{R}$, h serait identiquement nulle sur $\mathbb{R}$ et donc f serait nulle presque partout.

Il est alors naturel de se demander si $\widehat{f}$ peut vérifier une condition du type (A.1) où le réel ε est remplacé par $\varepsilon(|x|)$ avec ε une fonction telle que $\lim\limits_{x\to+\infty} \varepsilon(x) = 0$.

Dans [33], Ingham apporte une réponse complète à cette question : si ε est une fonction décroissante telle que $\lim\limits_{x\to+\infty} \varepsilon(x) = 0$ alors il existe une fonction f intégrable sur $\mathbb{R}$, à support compact, non nulle presque partout et telle que

$$\widehat{f}(x) = O\left(e^{-|x|\varepsilon(|x|)}\right) \qquad (|x| \to +\infty)$$

si et seulement si $x \mapsto \frac{\varepsilon(x)}{x}$ est intégrable en $+\infty$.

Nous présentons ici la construction d'Ingham [33] d'une telle fonction f pour laquelle nous étudions quelques propriétés utiles en pratique.

Soit $(\rho_n)_{n\geq 1}$ une suite de réels strictement positifs et posons pour tout $n \geq 1$,

$$\varphi_n(x) = \begin{cases} \frac{\sin(\pi\rho_n x)}{\pi\rho_n x} & \text{si } x \in \mathbb{R}^*, \\ 1 & \text{si } x = 0. \end{cases}$$

Afin de construire une fonction f convenable, Ingham considère le produit infini

$$\prod_{n=1}^{+\infty} \varphi_n(x).$$

Lemme A.1. *Si $(\rho_n)_{n\geq 1}$ est une suite de réels strictement positifs telle que $\sum_{n=1}^{+\infty} \rho_n$ converge alors le produit infini $\prod_{n=1}^{+\infty} \varphi_n(x)$ converge uniformément sur tout compact de $\mathbb{R}$.*

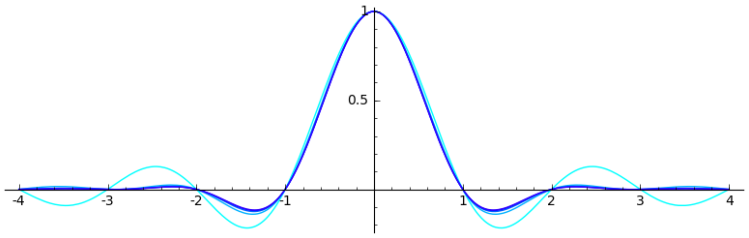

FIGURE A.1. – Courbes de $\prod_{n=1}^{N} \varphi_n$ pour $N \in \{1,2,3,4,5\}$ lorsque $\rho_n = n^{-3/2}$.

Démonstration. Pour tout $n \geq 1$, posons $h_n = \varphi_n - 1$. Comme $\sin x = x + O(x^2)$ pour tout $x \in \mathbb{R}$, on a $h_n(x) = O(\rho_n|x|)$ pour tout $x \in \mathbb{R}$ et tout $n \geq 1$. Ainsi, comme $\sum_{n=1}^{+\infty} \rho_n$ converge, la série $\sum_{n=1}^{+\infty} |h_n(x)|$ converge normalement (et donc uniformément) sur tout compact. De plus, $(h_n)_{n\geq 1}$ est une suite de fonctions bornées sur $\mathbb{R}$. On en déduit que le produit $\prod_{n=1}^{+\infty}(1 + h_n(x))$ converge uniformément sur tout compact (voir par exemple [60, Theorem 15.4]). □

La convolution de deux fonctions u et v de $\mathbb{R}$ dans $\mathbb{C}$ est définie formellement par

$$u * v(x) = \int_{\mathbb{R}} u(t)v(x-t)dt.$$

Cette notion va nous permettre de construire une suite de fonctions dont la limite f est à support compact et vérifie $\widehat{f} = \prod_{n=1}^{+\infty} \varphi_n$.

Lemme A.2. *Soit $(\rho_n)_{n\geq 1}$ une suite de réels strictement positifs telle que $\sum_{n=1}^{+\infty} \rho_n$ converge. Si*

$$u_n = \frac{1}{\rho_n} \mathbb{1}_{[-\frac{\rho_n}{2}, \frac{\rho_n}{2}]} \quad \text{et} \quad f_n = u_1 * \cdots * u_n \tag{A.2}$$

alors, pour tout $n \geq 1$, f_n est bien définie sur $\mathbb{R}$ et $(f_n)_{n\geq 1}$ converge uniformément sur $\mathbb{R}$ vers $f : \mathbb{R} \to \mathbb{R}$ qui satisfait

- $f \geq 0$,
- $\operatorname{supp} f \subset [-\ell/2, \ell/2]$ *où* $\ell = \sum_{n=1}^{+\infty} \rho_n$,
- $\int_{\mathbb{R}} f = 1$,
- $f \in \mathcal{C}^\infty(\mathbb{R})$,
- *pour tout* $x \in \mathbb{R}$, $\widehat{f}(x) = \prod_{n=1}^{+\infty} \varphi_n(x)$.

Si de plus on a $\rho_{2k-1} = \rho_{2k}$ pour tout $k \geq 1$, alors $\widehat{f} \geq 0$.

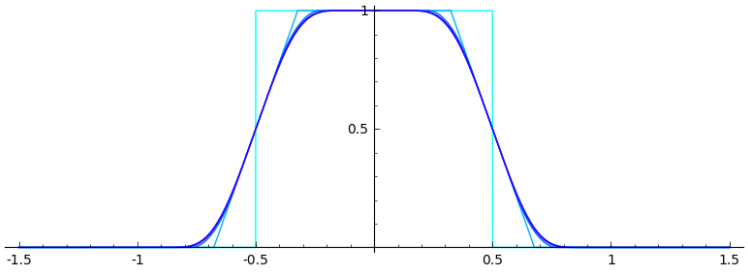

FIGURE A.2. – Courbes de f_1, f_2, f_3, f_4 et f_5 lorsque $\rho_n = n^{-3/2}$.

Démonstration. Pour tout $n \geq 2$, f_n est (uniformément) continue sur $\mathbb{R}$ car $u_1 \in L^\infty(\mathbb{R})$ et $u_2, \ldots, u_n \in L^1(\mathbb{R})$. De plus, pour tout $n \geq 1$, comme $u_1, \ldots, u_n \in L^1(\mathbb{R})$, on a $f_n \in L^1(\mathbb{R})$ et en posant $P_n = \widehat{f_n}$, on a pour tout $x \in \mathbb{R}$,

$$P_n(x) = \prod_{k=1}^{n} \widehat{u_k}(x) = \prod_{k=1}^{n} \varphi_k(x).$$

D'après le lemme A.1, $(P_n)_{n\geq 1}$ converge uniformément sur tout compact vers $P = \prod_{k=1}^{+\infty} \varphi_k$. De plus, pour tout $n \geq 2$, $|P_n| \leq |P_2|$ et $P_2 \in L^1(\mathbb{R})$, donc $P \in L^1(\mathbb{R})$ et d'après le théorème de convergence dominée, $(\|P_n - P\|_1)_{n\geq 2}$ converge vers 0. On en déduit que $(\widehat{P_n})_{n\geq 2}$ converge uniformément vers $\widehat{P}$ sur $\mathbb{R}$. Par ailleurs, pour tout $n \geq 2$, $f_n \in L^1(\mathbb{R})$, f_n est continue sur $\mathbb{R}$, $P_n = \widehat{f_n} \in L^1(\mathbb{R})$ et $\widehat{P_n}$ est paire. Par inversion de Fourier, on obtient donc : pour tout $x \in \mathbb{R}$, $\widehat{P_n}(x) = f_n(x)$. Ainsi, en posant $f = \widehat{P}$, $(f_n)_{n\geq 1}$ converge uniformément vers f sur $\mathbb{R}$.

Pour tout $n \geq 1$, $f_n \geq 0$ en tant que convolution de fonctions positives, d'où $f \geq 0$. De plus, en posant $\ell = \sum_{k=1}^{+\infty} \rho_k$, on a pour tout $n \geq 1$,

$$\operatorname{supp} f_n \subset \overline{\sum_{k=1}^{n} \operatorname{supp} u_n} = \left[-\frac{1}{2}\sum_{k=1}^{n}\rho_k, \frac{1}{2}\sum_{k=1}^{n}\rho_k\right] \subset \left[-\frac{\ell}{2}, \frac{\ell}{2}\right],$$

d'où $\operatorname{supp} f \subset [-\ell/2, \ell/2]$. Par ailleurs, comme P est paire et continue sur $\mathbb{R}$ (en tant que limite uniforme sur tout compact de fonctions paires et continues), comme $P \in L^1(\mathbb{R})$ et $\widehat{P} \in L^1(\mathbb{R})$ (car $\widehat{P} = f$ est à support compact et $\widehat{P}$ est bornée sur $\mathbb{R}$), on obtient par inversion de Fourier : pour tout $x \in \mathbb{R}$, $\widehat{f}(x) = P(x)$. Ainsi, $\int_{\mathbb{R}} f = \widehat{f}(0) = P(0) = 1$. Enfin, pour tout $n \geq 0$ et pour tout $x \in \mathbb{R}^*$, $|P(x)| \leq |P_{n+2}(x)| \leq \frac{1}{|x|^{n+2}} \prod_{k=1}^{n+2} \frac{1}{\pi\rho_k}$, d'où $x \mapsto x^n P(x) \in L^1(\mathbb{R})$ et donc $f = \widehat{P} \in C^\infty(\mathbb{R})$.

Si pour tout $k \geq 1$, $\rho_{2k-1} = \rho_{2k}$ alors pour tout $x \in \mathbb{R}$ et tout $m \geq 1$,

$$P_{2m}(x) = \prod_{k=1}^{m} \left(\varphi_{2k}(x)\right)^2 \geq 0$$

d'où $\widehat{f}(x) = P(x) \geq 0$. □

Dans [33], Ingham choisit la suite $(\rho_n)_{n\geq 1}$ convenablement de sorte que $\widehat{f} = \prod_{n=1}^{+\infty} \varphi_n$ soit « très petit » à l'infini. Ce choix de la suite $(\rho_n)_{n\geq 1}$ permet d'obtenir :

Théorème A.3. *Pour toute fonction $\varepsilon : [1, +\infty[\to \mathbb{R}_+^*$ décroissante telle que*

$$\lim_{x\to+\infty} \varepsilon(x) = 0 \qquad et \qquad \sum_{n=1}^{+\infty} \frac{\varepsilon(n)}{n} < +\infty,$$

il existe une fonction explicite $f : \mathbb{R} \to \mathbb{R}$ telle que

(i) $f \geq 0$,
(ii) $\operatorname{supp} f \subset [-1,1]$,
(iii) $\int_{\mathbb{R}} f = 1$,
(iv) $f \in \mathcal{C}^\infty(\mathbb{R})$,
(v) $\widehat{f} \geq 0$,
(vi) il existe $x_0(\varepsilon) \geq 1$ ne dépendant que de la fonction ε tel que pour tout $|x| \geq x_0(\varepsilon)$,

$$0 \leq \widehat{f}(x) \leq e^{-\lfloor |x|\varepsilon(|x|)\rfloor}.$$

Démonstration. Supposons tout d'abord que $\lim_{x\to+\infty} x\varepsilon(x) = +\infty$. Soit $n_0 = n_0(\varepsilon) \geq 1$ un nombre entier pair tel que $e\varepsilon(n_0) + 2e\sum_{\substack{n>n_0\\ n \text{ impair}}} \frac{\varepsilon(n)}{n} \leq 2$ et posons

$$\rho_n = \begin{cases} e\,\varepsilon(n_0)/n_0 & \text{si } 1 \leq n \leq n_0, \\ e\,\varepsilon(n)/n & \text{si } n > n_0 \text{ et } n \text{ est impair}, \\ e\,\varepsilon(n-1)/(n-1) & \text{si } n > n_0 \text{ et } n \text{ est pair}. \end{cases}$$

Alors

$$\ell := \sum_{n=1}^{+\infty} \rho_n = e\varepsilon(n_0) + 2e \sum_{\substack{n>n_0\\ n \text{ impair}}} \frac{\varepsilon(n)}{n} \leq 2$$

et pour tout $k \geq 1$, $\rho_{2k-1} = \rho_{2k}$. D'après le lemme A.2, la suite de fonctions $(f_n)_{n\geq 1}$ définie par (A.2) converge uniformément sur $\mathbb{R}$ et sa limite $f : \mathbb{R} \to \mathbb{R}$ vérifie (i), $\operatorname{supp} f \subset \left[-\frac{\ell}{2}, \frac{\ell}{2}\right] \subset [-1,1]$ d'où (ii), (iii), (iv) et (v). De plus, d'après le lemme A.2, pour tout $x \in \mathbb{R}_+^*$ et tout $n \geq 1$,

$$|\widehat{f}(x)| = \prod_{k=1}^{+\infty} |\varphi_k(x)| \leq \prod_{k=1}^{n} |\varphi_k(x)| \leq \prod_{k=1}^{n} \frac{1}{\rho_k x} \leq \left(\frac{1}{\rho_n x}\right)^n \tag{A.3}$$

en observant que $(\rho_n)_{n\geq 1}$ est décroissante (car ε est décroissante). Comme $\lim_{x\to+\infty} \varepsilon(x) = 0$ et $\lim_{x\to+\infty} x\varepsilon(x) = +\infty$, il existe $x_0 = x_0(\varepsilon) \geq 1$ tel que pour tout $x \geq x_0$,

$$n_0 < \lfloor x\varepsilon(x)\rfloor \qquad \text{et} \qquad \varepsilon(x) \leq 1.$$

Soit $x \geq x_0$ et posons $n = \lfloor x\varepsilon(x) \rfloor$. Comme $n > n_0$, on a $\rho_n \geq e^{\frac{\varepsilon(n)}{n}}$ et comme $n \leq x\varepsilon(x) \leq x$ et ε est décroissante, on obtient

$$\rho_n x \geq e\,\frac{\varepsilon(n)}{\varepsilon(x)} \geq e$$

et donc, d'après (A.3),

$$|\widehat{f}(x)| \leq e^{-n} = e^{-\lfloor x\varepsilon(x) \rfloor}.$$

En remarquant que $\widehat{f}$ est paire, on obtient finalement (vi), ce qui termine la preuve du théorème dans le cas où $\lim_{x\to+\infty} x\varepsilon(x) = +\infty$.

Si $x\varepsilon(x)$ ne tend pas vers $+\infty$ quand $x \to +\infty$ alors il suffit d'appliquer ce qui précède à $\varepsilon_1(x) = \varepsilon(x) + x^{-1/2}$. □

Corollaire A.4. *Pour tout $\alpha \in]0,1[$, il existe une fonction explicite $f : \mathbb{R} \to \mathbb{R}$ vérifiant les propriétés (i) à (v) et telle que pour tout $x \in \mathbb{R}$,*

$$\widehat{f}(x) = O_\alpha\left(e^{-|x|^\alpha}\right).$$

Démonstration. Cela découle immédiatement du théorème A.3 avec $\varepsilon(x) = x^{\alpha-1}$. □

La construction d'Ingham est mentionnée dans de nombreux articles. Elle a été utilisée par exemple dans [4, 5] sous la forme du corollaire A.4 et aussi dans [64] sous une forme plus précise (avec $|x|/(\log|x|)^2$ au lieu de $|x|^\alpha$). Nous notons qu'elle permet d'obtenir le résultat encore plus précis suivant.

Corollaire A.5. *Il existe une fonction explicite $f : \mathbb{R} \to \mathbb{R}$ vérifiant les propriétés (i) à (v) et telle que pour tout $|x| \geq 3$,*

$$\widehat{f}(x) = O\left(e^{-\frac{|x|}{(\log|x|)(\log\log|x|)^2}}\right).$$

Démonstration. Cela découle immédiatement du théorème A.3 avec $\varepsilon(x) = \frac{1}{(\log x)(\log\log x)^2}$ pour $x \geq 3$ (et $\varepsilon(x) = \varepsilon(3)$ pour $1 \leq x \leq 3$) qui vérifie bien $\sum_{n=1}^{+\infty} \frac{\varepsilon(n)}{n} < +\infty$ puisqu'une primitive sur $[3, +\infty[$ de $x \mapsto \frac{\varepsilon(x)}{x}$ est $x \mapsto \frac{-1}{\log\log x}$ et donc $\int_1^{+\infty} \frac{\varepsilon(x)}{x} dx < +\infty$. □

Bibliographie

[1] R. C. Baker et L. Zhao. « Gaps of smallest possible order between primes in an arithmetic progression ». *Int. Math. Res. Not. IMRN* 23 (2016), p. 7341–7368.

[2] B. C. Berndt, R. J. Evans et K. S. Williams. *Gauss and Jacobi sums*. Canadian Mathematical Society Series of Monographs and Advanced Texts. A Wiley-Interscience Publication. John Wiley & Sons, Inc., New York, 1998, p. xii+583.

[3] E. Bombieri. *Le grand crible dans la théorie analytique des nombres*. Astérisque 18. Société mathématique de France, 1974.

[4] J. Bourgain. « Prescribing the binary digits of primes ». *Israel J. Math.* 194.2 (2013), p. 935–955.

[5] J. Bourgain. « Prescribing the binary digits of primes, II ». *Israel J. Math.* 206.1 (2015), p. 165–182.

[6] M. Car et C. Mauduit. « Sur les puissances des polynômes sur un corps fini ». *Unif. Distrib. Theory* 8.2 (2013), p. 171–182.

[7] M. Car et C. Mauduit. « Répartition des fonctions complètement Q-additives le long des carrés de polynômes sur un corps fini ». *Bull. Soc. Math. France* 144.4 (2016), p. 775–817.

[8] M. Car et C. Mauduit. « Le poids des polynômes irréductibles à coefficients dans un corps fini » (2019). hal : hal-02088354.

[9] C. Dartyge et C. Mauduit. « Nombres presque premiers dont l'écriture en base r ne comporte pas certains chiffres ». *J. Number Theory* 81.2 (2000), p. 270–291.

[10] C. Dartyge et C. Mauduit. « Ensembles de densité nulle contenant des entiers possédant au plus deux facteurs premiers ». *J. Number Theory* 91.2 (2001), p. 230–255.

[11] C. Dartyge, C. Mauduit et A. Sárközy. « Polynomial values and generators with missing digits in finite fields ». *Funct. Approx. Comment. Math.* 52.1 (2015), p. 65–74.

[12] C. Dartyge et A. Sárközy. « The sum of digits function in finite fields ». *Proc. Amer. Math. Soc.* 141.12 (2013), p. 4119–4124.

[13] C. Dartyge et G. Tenenbaum. « Sommes des chiffres de multiples d'entiers ». *Ann. Inst. Fourier* 55.7 (2005), p. 2423–2474.

[14] C. Dartyge et G. Tenenbaum. « Congruences de sommes de chiffres de valeurs polynomiales ». *Bull. London Math. Soc.* 38.1 (2006), p. 61–69.

[15] H. Davenport. *Multiplicative number theory*. Third. T. 74. Graduate Texts in Mathematics. Revised and with a preface by Hugh L. Montgomery. New York : Springer-Verlag, 2000, p. xiv+177.

[16] R. Dietmann, C. Elsholtz et I. E. Shparlinski. « Prescribing the binary digits of squarefree numbers and quadratic residues ». *Trans. Amer. Math. Soc.* 369.12 (2017), p. 8369–8388.

[17] M. Drmota et G. Gutenbrunner. « The joint distribution of Q-additive functions on polynomials over finite fields ». *J. Théor. Nombres Bordeaux* 17.1 (2005), p. 125–150.

[18] M. Drmota, C. Mauduit et J. Rivat. « Primes with an average sum of digits ». *Compos. Math.* 145.2 (2009), p. 271–292.

[19] P. Erdős, C. Mauduit et A. Sárközy. « On arithmetic properties of integers with missing digits. I. Distribution in residue classes ». *J. Number Theory* 70.2 (1998), p. 99–120.

[20] P. Erdős, C. Mauduit et A. Sárközy. « On arithmetic properties of integers with missing digits. II. Prime factors ». *Discrete Math.* 200.1-3 (1999). Paul Erdős memorial collection, p. 149–164.

[21] E. Fouvry et C. Mauduit. « Sommes des chiffres et nombres presque premiers ». *Mathematische Annalen* 305 (1996), p. 571–599.

[22] J. Friedlander et H. Iwaniec. « The polynomial $X^2 + Y^4$ captures its primes ». *Ann. of Math. (2)* 148.3 (1998), p. 945–1040.

[23] M. R. Gabdullin. « On the squares in the set of elements of a finite field with constraints on the coefficients of its basis expansion ». *Mat. Zametki* 100.6 (2016), p. 807–824.

[24] P. X. Gallagher. « Primes in progressions to prime-power modulus ». *Invent. Math.* 16 (1972), p. 191–201.

[25] A. O. Gelfond. « Sur les nombres qui ont des propriétés additives et multiplicatives données ». *Acta Arith.* 13 (1967/1968), p. 259–265.

[26] B. Green et S. Konyagin. « On the Littlewood problem modulo a prime ». *Canad. J. Math.* 61.1 (2009), p. 141–164.

[27] J. Ha. « Irreducible polynomials with several prescribed coefficients ». *Finite Fields Appl.* 40 (2016), p. 10–25.

[28] G. H. Hardy et E. M. Wright. *An Introduction to the Theory of Numbers*. fifth. Oxford Science Publications, 1979.

[29] G. Harman. « Primes with preassigned digits ». *Acta Arith.* 125.2 (2006), p. 179–185.

[30] G. Harman et I. Kátai. « Primes with preassigned digits. II ». *Acta Arith.* 133.2 (2008), p. 171–184.

[31] D. R. Heath-Brown. « Primes represented by $x^3 + 2y^3$ ». *Acta Math.* 186.1 (2001), p. 1–84.

[32] M. N. Huxley. *The distribution of prime numbers*. Large sieves and zero-density theorems, Oxford Mathematical Monographs. Clarendon Press, Oxford, 1972, p. x+128.

[33] A. E. Ingham. « A Note on Fourier Transforms ». *J. London Math. Soc.* S1-9.1 (1934), p. 29–32.

[34] H. Iwaniec. « On zeros of Dirichlet's L series ». *Invent. Math.* 23 (1974), p. 97–104.

[35] H. Iwaniec et E. Kowalski. *Analytic number theory*. T. 53. American Mathematical Society Colloquium Publications. Providence, RI : American Mathematical Society, 2004, p. xii+615.

[36] A. A. Karatsuba. *Basic analytic number theory*. Translated from the second (1983) Russian edition and with a preface by Melvyn B. Nathanson. Springer-Verlag, Berlin, 1993, p. xiv+222.

[37] I. Kátai. « Distribution of digits of primes in q-ary canonical form ». *Acta Math. Hungar.* 47.3-4 (1986), p. 341–359.

[38] R. Lidl et H. Niederreiter. *Finite fields*. Second. T. 20. Encyclopedia of Mathematics and its Applications. With a foreword by P. M. Cohn. Cambridge University Press, Cambridge, 1997, p. xiv+755.

[39] B. Martin, C. Mauduit et J. Rivat. « Théorème des nombres premiers pour les fonctions digitales ». *Acta Arith.* 165.1 (2014), p. 11–45.

[40] B. Martin, C. Mauduit et J. Rivat. « Fonctions digitales le long des nombres premiers ». *Acta Arith.* 170.2 (2015), p. 175–197.

[41] B. Martin, C. Mauduit et J. Rivat. « Propriétés locales des chiffres des nombres premiers ». *J. Inst. Math. Jussieu* 18.1 (2019), p. 189–224.

[42] B. Martin, C. Mauduit et J. Rivat. « Nombres premiers avec contraintes digitales multiples ». *Bull. Soc. Math. France* (à paraître).

[43] C. Mauduit et J. Rivat. « La somme des chiffres des carrés ». *Acta Math.* 203.1 (2009), p. 107–148.

[44] C. Mauduit et J. Rivat. « Sur un problème de Gelfond : la somme des chiffres des nombres premiers ». *Ann. of Math. (2)* 171.3 (2010), p. 1591–1646.

[45] C. Mauduit et J. Rivat. « Prime numbers along Rudin-Shapiro sequences ». *J. Eur. Math. Soc. (JEMS)* 17.10 (2015), p. 2595–2642.

[46] J. Maynard. « Primes and polynomials with restricted digits » (2015). arXiv : 1510.07711v1.

[47] J. Maynard. « Digits of primes. » *European congress of mathematics. Proceedings of the 7th ECM (7ECM) congress, Berlin, Germany, July 18–22, 2016*. Zürich: European Mathematical Society (EMS), 2018, p. 641–661.

[48] J. Maynard. « Primes with restricted digits ». *Inventiones mathematicae* (2019).

[49] H. L. Montgomery. « The analytic principle of the large sieve ». *Bull. Amer. Math. Soc.* 84.4 (1978), p. 547–567.

[50] H. L. Montgomery et R. C. Vaughan. *Multiplicative number theory. I. Classical theory*. T. 97. Cambridge Studies in Advanced Mathematics. Cambridge University Press, Cambridge, 2007, p. xviii+552.

[51] C. Moreno et O. Moreno. « Exponential sums and Goppa codes: I ». *Proceedings of the American Mathematical Society* 111 (1991), p. 523–531.

[52] G. L. Mullen et D. Panario. *Handbook of Finite Fields*. 1st. Chapman & Hall/CRC, 2013.

[53] H. Niederreiter et A. Winterhof. « Incomplete exponential sums over finite fields and their applications to new inversive pseudorandom number generators ». *Acta Arith.* 93.4 (2000), p. 387–399.

[54] A. Ostafe. « Polynomial values in affine subspaces of finite fields ». *J. Anal. Math.* (2019).

[55] J. Pintz. « Some new density theorems for Dirichlet L-functions » (2018). arXiv : 1804.05552v1.

[56] P. Pollack. « Irreducible polynomials with several prescribed coefficients ». *Finite Fields Appl.* 22 (2013), p. 70–78.

[57] S. Porritt. « Irreducible Polynomials Over a Finite Field with Restricted Coefficients ». *Canadian Mathematical Bulletin* (2018), p. 1–11.

[58] J. Rivat et P. Sargos. « Nombres premiers de la forme $\lfloor n^c \rfloor$ ». *Canad. J. Math.* 53.2 (2001), p. 414–433.

[59] J. Rivat et A. Sárközy. « On arithmetic properties of products and shifted products ». *Analytic number theory*. Springer, Cham, 2015, p. 345–355.

[60] W. Rudin. *Real and complex analysis*. Third. New York : McGraw-Hill Book Co., 1987, p. xiv+416.

[61] W. Schmidt. *Equations over Finite Fields. An elementary approach*. T. 536. Lecture Notes in Math. Springer Verlag, New-York – Berlin, 1976.

[62] A. Selberg. *Collected papers. Vol. I*. With a foreword by K. Chandrasekharan. Berlin : Springer-Verlag, 1989, p. vi+711.

[63] W. Sierpiński. « Sur les nombres premiers ayant des chiffres initiaux et finals donnés ». *Acta Arith.* 5 (1959), p. 265–266.

[64] K. Soundararajan. « Strong multiplicity one for the Selberg class ». *Canad. Math. Bull.* 47.3 (2004), p. 468–474.

[65] C. Swaenepoel. « On the sum of digits of special sequences in finite fields ». *Monatsh. Math.* 187.4 (2018), p. 705–728.

[66] C. Swaenepoel. « Prescribing digits in finite fields ». *J. Number Theory* 189 (2018), p. 97–114.

[67] C. Swaenepoel. « Trace of products in finite fields ». *Finite Fields and Their Applications* 51 (2018), p. 93–129.

[68] G. Tenenbaum. *Introduction à la théorie analytique et probabiliste des nombres*. Belin, 2008.

[69] C. J. de la Vallée Poussin. « Recherches analytiques sur la théorie des nombres premiers ». French. *Brux. S. sc.* B 21 (1896), p. 183–256, 281–362, 363–397.

[70] D. Wolke. « Primes with preassigned digits ». *Acta Arith.* 119.2 (2005), p. 201–209.

[71] P. Zimmermann, L. Fousse, F. Maltey et al. *Calcul mathématique avec Sage (French Edition)*. CreateSpace Independent Publishing Platform, 2013.