Équidistribution découlant du théorème des restes chinois

E. Kowalski
K. Soundararajan

Résumé : On prouve l'équidistribution des sous-ensembles de $(\mathbf{R}/\mathbf{Z})^n$ définis par parties fractionnées des sous-ensembles de $(\mathbf{Z}/q\mathbf{Z})^n$ qui sont construits en utilisant le théorème des restes chinois.

Dédié à la mémoire de Hédi Daboussi

1. Introduction

Étant donné un polynôme quadratique irréductible $f \in \mathbf{Z}[\mathrm{X}]$, un célèbre travail de Duke, Friedlander, et Iwaniec [4] (voir aussi Toth [16]) montre que les racines de la congruence $f(x) \equiv 0 \pmod p$ deviennent équidistribuées quand on les prend sur tous les nombres premiers $p \leqslant \mathrm{P}$. Précisément, leur résultat établit l'équidistribution dans $\mathbf{R}/\mathbf{Z}$ des points x_p/p pris sur tout $p \leqslant \mathrm{P}$ et des racines x_p de $f(x_p) \equiv 0 \pmod p$. On attend un résultat similaire pour les racines des polynômes de degré supérieur, mais cela reste un problème remarquable ouvert. Dans [10], Hooley a établi que si l'on considère plutôt les racines d'une congruence polynomiale $\pmod n$ sur tous les modules n entiers, alors le résultat d'équidistribution qui convient est vérifié. Dans cette note, on montre que le résultat de Hooley peut être refondu en un fait général concernant l'équidistribution d'ensembles découlant du théorème des restes chinois. Notre travail était en partie motivé par l'article [7] de Granville et Kurlberg (qui considèrent l'espace entre éléments de "grands" ensembles définis par le théorème des restes chinois). Certaines applications ont aussi été suggérées par le travail récent de Hrushovski [11].

Pour simplifier, on commence par considérer l'équidistribution dans $\mathbf{R}/\mathbf{Z}$; on discutera ultérieurement le cas de dimension plus élevée de points dans $(\mathbf{R}/\mathbf{Z})^n$. Supposons que pour toute puissance de nombre premier p^v, soit donné un ensemble A_{p^v} de classes de congruences modulo p^v (où dans toute la suite, on inclut les nombres premiers dans les puissances de nombres premiers, en excluant 1). Soit $\varrho(p^v) = |\mathrm{A}_{p^v}|$. On autorise la possibilité que $\varrho(p^v) = 0$, de telle façon que A_{p^v} est vide, pour certaines puissances de premiers p^v, et aucune supposition n'est faite concernant les relations entre les ensembles $\mathrm{A}_{p^{v_1}}$ et $\mathrm{A}_{p^{v_2}}$ correspondant à différentes puissances du nombre premier p. Pour un entier positif q, dénotons par $\mathrm{A}_q \subset$

ETH Zürich – D-MATH
Rämistrasse 101
8092 Zürich
Suisse
email : kowalski@math.ethz.ch

Département de mathématiques,
Université Stanford,
Stanford, CA 94305
email : ksound@stanford.edu

Traduction par Denise Vella-Chemla de l'article arxiv https://arxiv.org/pdf/2003.12965.pdf, janvier 2023.

$\mathbf{Z}/q\mathbf{Z}$ l'ensemble des classes de restes $x \pmod q$ de telle façon que $x \pmod{p^v} \in \mathrm{A}_{p^v}$ pour toutes les puissances de premiers p^v divisant exactement q (c'est-à-dire que $p^v | q$ mais que $p^{v+1} \nmid q$; on dénotera cela par $p^v \| q$ à partir de maintenant). Ce sont les "ensembles définis en utilisant le théorème des restes chinois". Soit $\varrho(q) = |\mathrm{A}_q|$, de telle façon que (en posant $\varrho(1) = 1$) la fonction $\varrho(q)$ soit multiplicative :

$$\varrho(q) = \prod_{p^v \| q} \varrho(p^v).$$

Dénotons par $\mathcal{Q}$ l'ensemble de tous les q avec $\varrho(q) \geqslant 1$, et pour tout entier $k \geqslant 1$, dénotons par $\mathcal{Q}_k$ les éléments de $\mathcal{Q}$ avec exactement k facteurs premiers distincts. De plus, pour $x \geqslant 1$, dénotons par $\mathcal{Q}(x)$ (resp. $\mathcal{Q}_k(x)$) le sous-ensemble d'éléments de $\mathcal{Q}$ (resp. de $\mathcal{Q}_k$) qui sont $\leqslant x$. Pour assurer que les ensembles $\mathcal{Q}$ et $\mathcal{Q}_k$ se comportent correctement et ont de nombreux éléments, on fera la supposition suivante.

Supposition 1.1. *Il existe des constantes $\alpha > 0$ et $x_0 \geqslant 2$ telles que pour tout $x \geqslant x_0$*

$$\sum_{\substack{p \leqslant x \\ \varrho(p) \geqslant 1}} \log p \geqslant \alpha x.$$

Dans la suite, on travaille en supposant 1.1, et le paramètre x sera considéré comme étant grand en fonction de α et x_0, de telle façon que par exemple, on aurait $\alpha \log\log x \geqslant \sqrt{\log\log x}$.

Étant donné $q \in \mathcal{Q}$, on définit une mesure de probabilité Δ_q sur $\mathbf{R}/\mathbf{Z}$ par

$$\Delta_q = \frac{1}{\varrho(q)} \sum_{a \in \mathrm{A}_q} \delta_{\{\frac{a}{q}\}}$$

où δ_t dénote une masse de Dirac au point t, et $\{\cdot\}$ dénote la partie fractionnaire d'un nombre réel. Le comportement limite de telles mesures est l'objet de notre étude. Par exemple, on s'intéresse à savoir si Δ_q tend vers une mesure uniforme pour la plupart des $q \in \mathcal{Q}$. Pour quantifier si Δ_q est près d'être uniforme, on utilise la divergence

$$\mathrm{disc}(\Delta_q) = \sup_{\mathrm{I} \subset \mathbf{R}/\mathbf{Z}} |\Delta_q(\mathrm{I}) - |\mathrm{I}||,$$

où le supremum est pris sur tous les intervalles fermés I dans $\mathbf{R}/\mathbf{Z}$, et $|\mathrm{I}|$ dénote la longueur de l'intervalle I. Par intervalle (fermé) dans $\mathbf{R}/\mathbf{Z}$, on désigne l'image dans $\mathbf{R}/\mathbf{Z}$ d'un intervalle (fermé) dans $\mathbf{R}$ de longueur au plus 1. On a $0 \leqslant \mathrm{disc}(\Delta_q) \leqslant 1$ pour tout q, et une petite valeur de $\mathrm{disc}(\Delta_q)$ indique que Δ_q est proche d'être uniforme.

Théorème 1.2. *Prenons comme hypothèse que la* Supposition 1.1 *est vérifiée, et que x est grand en fonction de α et x_0. Alors, il y a une constante absolue* C *telle que*

$$\frac{1}{|\mathcal{Q}(x)|} \sum_{q \in \mathcal{Q}(x)} \mathrm{disc}(\Delta_q) \leqslant \frac{\mathrm{C}}{\alpha} \exp\Big(-\frac{1}{6} \sum_{\substack{p \leqslant x \\ \varrho(p) \geqslant 2}} \frac{1}{p} \Big).$$

Remarque 1.3. *(1) Si on écrit*

$$\sum_{\substack{p \leqslant x \\ \varrho(p) \geqslant 2}} \frac{1}{p} = \mathrm{P},$$

alors le théorème 1.2 garantit qu'à part au plus $C\alpha^{-1}|\mathcal{Q}(x)|e^{-P/12}$ *valeurs de* q*, on a* $\mathrm{disc}(\Delta_q) \leqslant e^{-P/12}$*. Ainsi si* P *est grand alors pour presque tous les* $q \leqslant x$ *avec* $q \in \mathcal{Q}$*, on a équidistribution des ensembles* A_q *(ce par quoi on souhaite signifier l'équidistribution des mesures* Δ_q*). À part les constantes, ce résultat est le meilleur possible, car on pourrait s'attendre à ce qu'environ* $e^{-P}|\mathcal{Q}(x)|$ *éléments sans facteur carré* $q \in \mathcal{Q}(x)$ *ne soient divisibles par aucun nombre premier* p *avec* $\varrho(p) \geqslant 2$*, et pour de tels* q*, on aurait* $|A_q| = 1$ *et* $\mathrm{disc}(\Delta_q) = 1$*.*

(2) En particulier, pour presque tous les $q \in \mathcal{Q}$*, la limite de la divergence implique que le plus petit élément de* A_q *est* $\ll qe^{-P/12}$ *(si on identifie* $\mathbf{Z}/q\mathbf{Z}$ *avec* $\{0, \dots, q-1\}$*). Dans le cas des racines des congruences polynomiales, un tel résultat a été démontré récemment par Crişan et Pollack* [1].

Le théorème 1.2 s'applique au résultat de Hooley sur les racines d'un polynôme modulo tous les entiers. Par le théorème de densité de Chebotarev, tout polynôme irréductible de degré $d \geqslant 2$ a d racines modulo p pour une densité positive de nombres premliers, de telle façon que la supposition 1.1 est vérifiée, et de plus

$$\sum_{\substack{p \leqslant x \\ \varrho(p) \geqslant 2}} \frac{1}{p} \geqslant c(d) \log\log x$$

pour une certaine constante $c(d) \geqslant \frac{1}{d!}$ (de telle façon que le côté droit de l'estimée dans le théorème 1.2 est de l'ordre de $(\log x)^{-c}$ pour une certaine $c > 0$). Nous donnerons des applications plus avancées selon ces lignes dans la section 2. Notre version est quelque peu différente de celle de Hooley, et nous les comparerons et les mettrons en contraste dans la section 2.2. La généralité du théorème 1.2 indique que l'équidistribution de Hooley [10] est une manifestation des propriétés de mélange du théorème des restes chinois plutôt que la structure arithmétique des racines des congruences polynomiales.

On va généraliser et renforcer le théorème 1.2 de quelques façons différentes. D'abord, on considère des sous-ensembles de $(\mathbf{Z}/p^v\mathbf{Z})^n$ pour un $n \geqslant 1$ fixé. Ici un problème-clef est de trouver la généralisation correcte de la condition que $\varrho(p) \geqslant 2$ pour de nombreux nombres premiers qui advient naturellement dans le cas à une dimension. Deuxièmement, on considèrera l'équidistribution des mesures Δ_q quand q est restreint aux entiers dans $\mathcal{Q}$ avec exactement k facteurs premiers distincts. Sous de légères hypothèses sur $\varrho(p)$, on montrera que dans un large domaine de k, la divergence des mesures Δ_q est typiquement petite. Sous des hypothèses plus restrictives (quand $\varrho(p)$ est grand pour $p \in \mathcal{Q}$), on montre que $\mathrm{disc}(\Delta_q)$ est typiquement petit déjà pour les nombres qui ont deux facteurs premiers.

On commence par introduire le réglage de plus grande dimension, et on formule un analogue du théorème 1.2. Dans la suite, la dimension n sera considérée fixée, de telle façon que les constantes implicites seront autorisées à dépendre de n, mais on montrera les dépendances des autres paramètres. Pour chaque puissance de nombre premier p^v, soit $A_{p^v} \subset (\mathbf{Z}/p^v\mathbf{Z})^n$ un ensemble de n-uplets de classes de restes modulo p^v. Comme précédemment, on pose $\varrho(p^v) = |A_{p^v}|$ et on autorise A_{p^v} à être l'ensemble vide (de telle façon que $\varrho(p^v) = 0$) pour certaines puissances de nombres premiers. Pour un entier positif q, on dénote par $A_q \subset (\mathbf{Z}/q\mathbf{Z})^n$ l'ensemble des classes des restes $x \pmod q$ telles que $x \pmod{p^v} \in A_{p^v}$ pour toutes les puissances de nombres premiers $p^v \| q$. Dénotons par $\varrho(q)$ la taille de A_q, qui est à nouveau une fonction multiplicative. Les variables $\mathcal{Q}$, $\mathcal{Q}(x)$, $\mathcal{Q}_k$, et $\mathcal{Q}_k(x)$ gardent leur signification précédente, et on travaillera comme avant sous la supposition 1.1.

Pour $a = (a_1, \dots, a_n) \in \mathbf{R}^n$, on écrit

$$\{a\} = (\{a_1\}, \dots, \{a_n\}) \in (\mathbf{R}/\mathbf{Z})^n.$$

On définit une mesure de probabilité Δ_q sur $(\mathbf{R}/\mathbf{Z})^n$ par

$$\Delta_q = \frac{1}{\varrho(q)} \sum_{a \in \mathrm{A}_q} \delta_{\{\frac{a}{q}\}}.$$

La proximité de Δ_q et de la mesure uniforme est quantifiée au moyen de la *boîte de divergence*

$$\mathrm{disc}(\Delta_q) = \sup_{\mathrm{B} \subset (\mathbf{R}/\mathbf{Z})^n} |\Delta_q(\mathrm{B}) - \mathrm{Vol}(\mathrm{B})|$$

où le supremum est pris sur toutes les boîtes B dans $(\mathbf{R}/\mathbf{Z})^n$, et où Vol(B) dénote le volume usuel (mesure de Lebesgue) de la boîte. Ici, par le terme boîte dans $(\mathbf{R}/\mathbf{Z})^n$, on veut dire la projection modulo $\mathbf{Z}^n$ d'une boîte fermée (c'est-à-dire un produit d'intervalles fermés) dans $\mathbf{R}^n$ avec toutes les tailles des côtés $\leqslant 1$.

Supposons qu'il y ait un hyperplan affine fixé H défini sur $\mathbf{Z}$ tels que les éléments dans A_{p^v} vivent tous dans la réduction de H modulo p^v pour tout $p \in \mathcal{Q}$. Alors pour $q \in \mathcal{Q}$, les éléments dans A_q vivront aussi dans cet hyperplan, de telle façon que les mesures Δ_q auront pour support une translation d'un sous-tore propre de $(\mathbf{R}/\mathbf{Z})^n$. Cette situation empêche l'équidistribution ; elle généralise le cas $n = 1$, où un hyperplan affine est un point unique, de telle façon que la concentration dans un hyperplan unique correspond au cas où $\varrho(p) \leqslant 1$ pour la plupart des nombres premiers p. Notre généralisation du théorème 1.2 établit que si les ensembles A_p ne se concentrent pas sur des hyperplans pour une densité positive de nombres premiers p, alors Δ_q est proche de la mesure uniforme (i.e., a une petite divergence) pour la plupart des modules q.

Pour établir cela précisément, on a besoin d'une définition supplémentaire. Étant donné un nombre premier p dans $\mathcal{Q}$, définissons

$$\lambda(p) = \max_{\substack{\mathrm{H} \subset (\mathbf{Z}/p\mathbf{Z})^n \\ \mathrm{H}\text{hyperplan affine}}} |\mathrm{H} \cap \mathrm{A}_p|,$$

où l'hyperplan affine $\mathrm{H} \subset (\mathbf{Z}/p\mathbf{Z})^n$ est un sous-ensemble de la forme

$$\mathrm{H} = \{x \in (\mathbf{Z}/p\mathbf{Z})^n \mid h_1 x_1 + \cdots + h_n x_n = a\}$$

pour un certain $a \in \mathbf{Z}/p\mathbf{Z}$ et $(h_i) \in (\mathbf{Z}/q\mathbf{Z})^n \setminus \{(0, \dots, 0)\}$.

Théorème 1.4. *Supposons que la* supposition 1.1 *est vérifiée, et que x est grand en fonction de α et x_0. Alors, il y a une constante $\mathrm{C}(n)$ dépendant seulement de n telle que*

$$\frac{1}{|\mathcal{Q}(x)|} \sum_{q \in \mathcal{Q}(x)} \mathrm{disc}(\Delta_q) \leqslant \frac{\mathrm{C}(n)}{\alpha} \exp\Big(-\frac{1}{3} \sum_{\substack{p \leqslant x \\ \varrho(p) \geqslant 1}} \Big(1 - \frac{\lambda(p)}{\varrho(p)}\Big) \frac{1}{p} \Big).$$

Remarque 1.5. *Considérons le cas $n = 1$. Alors on a $\lambda(p) = 1$ à chaque fois que $\varrho(p) \geqslant 1$, et ainsi*

$$\sum_{\substack{p \leqslant x \\ \varrho(p) \geqslant 1}} \Big(1 - \frac{\lambda(p)}{\varrho(p)}\Big) \frac{1}{p} \geqslant \frac{1}{2} \sum_{\substack{p \leqslant x \\ \varrho(p) \geqslant 2}} \frac{1}{p},$$

et le théorème 1.2 est vu comme un cas particulier du théorème 1.4.

Pour tout n, étant donnés au plus n points dans $(\mathbf{Z}/p\mathbf{Z})^n$, on peut toujours trouver un hyperplan affine les contenant tous. Mais étant donnés $n+1$ points, on peut s'attendre à ce qu'ils soient "dans une position générale", au sens où il n'y a pas d'hyperplan affine qui les contient tous. Ainsi, pour le dire rapidement, le théorème 1.4 dit que s'il y a beaucoup de nombres premiers p avec A_p en position générale, et contenant au moins $n+1$ éléments, alors pour presque tous les $q \in \mathcal{Q}$, les mesures Δ_q sont proches de l'équidistribution.

En imposant une hypothèse plus forte (mais toujours bénigne), on peut obtenir l'équidistribution de Δ_q en moyenne, quand q est restreint aux entiers avec un nombre donné de facteurs premiers.

Théorème 1.6. *Supposons que la* Supposition 1.1 *est vérifiée, et que x est grand en fonction de x_0 et de α. Supposons que $0 < \delta \leqslant 1$ est tel que*

$$\sum_{\substack{p \leqslant x \\ p \in \mathcal{Q}}} \Big(1 - \frac{\lambda(p)}{\varrho(p)}\Big)\frac{1}{p} \geqslant \delta \log\log x. \tag{1}$$

Alors uniformément dans le domaine

$$\frac{20(6+n)}{\delta}\log\Big(\frac{20(6+n)}{\delta}\Big) \leqslant k \leqslant \exp\Big(\sqrt{\frac{\alpha\delta\log\log x}{20(6+n)}}\Big)$$

on a

$$\frac{1}{|\mathcal{Q}_k(x)|}\sum_{\substack{q \leqslant x \\ q \in \mathcal{Q}_k}} \mathrm{disc}(\Delta_q) \ll \frac{1}{\alpha}\Big(e^{-\delta k/18} + (\log x)^{-\alpha\delta/18}\Big).$$

Remarque 1.7. *(1) si on pense à δ comme à une constante positive fixée, alors le théorème 1.6 montre que pour la plupart des $q \in \mathcal{Q}_k(x)$, on a équidistribution de Δ_q tant que $k \to \infty$ (arbitrairement lentement en fonction de x) et sous l'hypothèse que $k \leqslant \exp(c\sqrt{\log\log x})$ pour un certain $c > 0$. Une condition telle que $k \to \infty$ est nécessaire pour garantir que A_q a de nombreux points, ce qui est essentiel pour l'équidistribution.*

(2) Bien que des entiers "typiques" dans $\mathcal{Q}$ aient de l'ordre de $\log\log x$ facteurs premiers, et que les plus grandes valeurs de k n'adviennent que rarement, il serait intéressant d'étendre le résultat aux valeurs plus grandes de k, spécialement à celles jusqu'à ce que $k \leqslant (\log x)^c$ pour un certain $c > 0$.

Notre dernier résultat fournit l'équidistribution pour Δ_q pour la plupart des q dans $\mathcal{Q}_k$, pour n'importe quel $k \geqslant 2$ *fixé*, en supposant qu'on sait que les ensembles A_p sont grands pour la plupart des $p \in \mathcal{Q}$.

Théorème 1.8. *Supposons que la* Supposition 1.1 *est vérifiée, et que x est grand en fonction de x_0 et α. Supposons que $\delta > 0$ soit tel que $1/\log\log x \leqslant \delta \leqslant 1/e$ et*

$$\sum_{p \in \mathcal{Q}(x)} \frac{1}{p}\frac{\lambda(p)}{\varrho(p)} \leqslant \delta \sum_{p \in \mathcal{Q}(x)} \frac{1}{p}. \tag{2}$$

Alors, uniformément dans le domaine $2 \leqslant k \leqslant \alpha\delta\log\log x$,

$$\frac{1}{|\mathcal{Q}_k(x)|}\sum_{q \in \mathcal{Q}_k(x)} \mathrm{disc}(\Delta_q) \ll \frac{1}{\alpha}\delta^{(k-1)/10}.$$

L'intérêt du théorème 1.8 est vraiment pour les petites valeurs de k, puisque quand k est grand, on peut simplement utiliser les limites dans le théorème 1.6. Si δ dans le théorème 1.8 est proche de 0, alors on obtient l'équidistribution pour la plupart des Δ_q déjà pour les entiers q avec 2 facteurs premiers. Par exemple, cela s'applique, dans le cas $n = 1$, à chaque fois que $\varrho(p)$ tend vers l'infini pour $p \in \mathcal{Q}$.

La dernière remarque avant de fermer la section Introduction est que la supposition 1.1, ainsi que les estimées dans les théorèmes 1.2, 1.4, 1.6 et 1.8 ne concerne que les ensembles A_p et leur taille. En d'autres termes, *il n'y a aucune restriction quelle qu'elle soit* sur le choix des ensembles A_{p^v} pour $v \geqslant 2$. Cela ne devrait pas être surprenant parce que la plupart des nombres naturels ne sont pas divisibles par de nombreuses puissances de nombres premiers p^v avec $v \geqslant 2$.

Survol de l'article. La prochaine section fournit une sélection d'applications du théorème 1.4, et compare les résultats avec ceux de [10]. La section 3 discute de quelques préliminaires, et la preuve du théorème 1.4 (qui contient le théorème 1.2 comme cas particulier) est établie dans la section 4. Dans la section 5, on développe un estimée technique (proposition 5.1) qui est plus précise (mais moins compliquée à établir) que les théorèmes 1.6 et 1.8, et dans la section 6, on les démontre à partir d'un résultat technique. Finalement, la section 7 discute brièvement d'une autre généralisation possible de notre méthode, qui sera le sujet d'un travail ultérieur [13], et un appendice considère brièvement des analogues pour les corps de fonctions des conjectures à propos des racines de congruences polynomiales modulo des nombres premiers.

Remerciements. E.K. a été partiellement financé par une subvention du programme DFG-SNF (subvention numéro 200020L_175755). K.S. est partiellement financé par une subvention de la Fondation nationale pour la Science, et une subvention pour la recherche de la Fondation Simons. Ce travail a été mené lorsque K.S. était invité senior à l'ETH Institut des études théoriques, qu'il remercie pour leur gentillesse et leur hospitalité généreuse.

Nous remercions D.R. Heath–Brown et J-P. Serre pour d'utiles commentaires, P. Pollack pour avoir cité son article [1] avec V. Crişan et V. Kuperberg pour nous avoir envoyé son article [14].

2. Exemples et contre-exemples

Dans cette section, nous présentons quelques exemples d'applications du théorème 1.4, et nous discutons de la relation de notre travail avec [10].

Les applications du théorème 1.4 sont peut-être plus intéressantes quand les ensembles A_q peuvent être décrits globalement sans référence au théorème des restes chinois ou à la factorisation en nombres premiers de q. Par exemple, A_q pourrait être l'ensemble des solutions de certaines équations (e.g., les racines d'un certain polynôme fixé à coefficients entiers), ou l'ensemble de paramètres où une famille d'équations a une solution (e.g, l'ensemble des carrés modulo q), ou des combinaisons de ceux-ci. Ou, par exemple, on peut restreindre les valeurs q à être les normes d'idéaux dans un certain corps de nombres donné K.

2.1. Variations sur les racines de congruences polynomiales.

On commence par une application du théorème 1.4 aux racines des polynômes. Cela donne une version en plus grande dimension du résultat de Hooley, et c'est motivé par une question de Hrushovski [11, Conjecture 4.1].

Théorème 2.1. *Soit $d \geqslant 1$. Soit $f \in \mathbf{Z}[\mathrm{X}]$ un polynôme avec d racines complexes distinctes. Pour chaque puissance de nombre premier p^v, dénotons par A_{p^v} le sous-ensemble de $(\mathbf{Z}/p^v\mathbf{Z})^{d-1}$ constitué des points $(a, a^2, \dots, a^{d-1})$ où a parcourt les racines de $f(x) \equiv 0 \pmod{p^v}$. Alors, avec les définitions correspondantes de $\mathcal{Q}$ et Δ_q, pour de grandes valeurs de x on a*

$$\frac{1}{|\mathcal{Q}(x)|} \sum_{q \in \mathcal{Q}(x)} \mathrm{disc}(\Delta_q) \ll_d (\log x)^{-\frac{1}{(4d)d!}}.$$

***Preuve* 1.** *Dénotons par K_f le corps de décomposition de f sur $\mathbf{Q}$, qui a pour degré $[\mathrm{K}_f : \mathbf{Q}] \leqslant d!$. Si un grand nombre premier p décompose complètement dans K_f, alors il y a d solutions distinctes pour la congruence $f(x) \equiv 0 \pmod{p}$, de telle façon que $\varrho(p) = d$ pour de tels nombres premiers. De plus, par le théorème de densité de Chebotarev, la proportion de nombres premiers qui décomposent complètement dans K_f est $1/[\mathrm{K}_f : \mathbf{Q}] \geqslant 1/d!$, de telle façon que la supposition 1.1 est vérifiée. Finalement, n'importe quel hyperplan affine dans $(\mathbf{Z}/p\mathbf{Z})^{d-1}$ peut intersecter la courbe $(t, t^2, \dots, t^{d-1})$ en au plus $d-1$ points. Ainsi, $\lambda(p) \leqslant d-1$, et on conclut que*

$$\sum_{\substack{p \leqslant x \\ \varrho(p) \geqslant 1}} \Big(1 - \frac{\lambda(p)}{\varrho(p)}\Big)\frac{1}{p} \geqslant \sum_{\substack{p \leqslant x \\ \varrho(p) = d}} \Big(1 - \frac{d-1}{d}\Big)\frac{1}{p} \geqslant \frac{1}{d}\Big(\frac{1}{d!} + o(1)\Big) \log\log x.$$

Le résultat découle maintenant du théorème 1.4.

Énoncé qualitativement, le théorème 2.1 implique que les mesures

$$\frac{1}{|\mathcal{Q}(x)|} \sum_{q \in \mathcal{Q}(x)} \frac{1}{\varrho(q)} \sum_{\substack{a \pmod q \\ f(a) \equiv 0 \pmod q}} \delta_{\{\frac{a}{q}, \frac{a^2}{q}, \dots, \frac{a^{d-1}}{q}\}}$$

convergent vers la mesure uniforme lorsque $x \to \infty$. En effet, le théorème 2.1 implique une version quantitative "mod q" de [11, Conjecture 4.1] ; cette conjecture est reliée à l'axiomatisation (dans le paradigme de la logique continue du premier ordre) de la théorie des corps premiers finis avec un caractère additif. Dans les remarques ci-dessous, on mentionne quelques autres applications reliées qui peuvent être plutôt déduites qualitativement du théorème 2.1, ou bien établies sous une forme quantitative en adaptant le même argument.

Exemple 1. *Si $d \geqslant 2$, alors en ignorant toutes les coordonnées sauf la première, l'équidistribution de $\{\frac{a}{q}, \frac{a^2}{q}, \dots, \frac{a^{d-1}}{q}\}$ implique l'équidistribution de la première coordonnée $\{\frac{a}{q}\}$. Soit $f \in \mathbf{Z}[\mathrm{X}]$ un polynôme avec $d \geqslant 2$ racines complexes distinctes, et dénotons par A_{p^v} le sous-ensemble de $\mathbf{Z}/p^v\mathbf{Z}$ constitué des points a avec $f(a) \equiv 0 \pmod{p^v}$. Dans ce cas à 1 dimension, on peut prendre $\lambda(p) = 1$. Alors, avec les significations habituelles de $\mathcal{Q}$, Δ_q, on a pour de grandes valeurs de x*

$$\frac{1}{|\mathcal{Q}(x)|} \sum_{q \in \mathcal{Q}(x)} \mathrm{disc}(\Delta_q) \ll_d (\log x)^{-\frac{1}{8(d!)}}.$$

Ceci est une version du résultat de Hooley, et nous allons discuter des différences entre sa formulation et la nôtre dans la prochaine sous-section. Notons que f n'a pas besoin d'être irréductible, mais devrait plutôt avoir au moins deux racines complexes distinctes. Le cas des polynômes quadratiques réductibles a été discuté précédemment par Martin et Sitar [15].

Exemple 2. *Soit $f \in \mathbf{Z}[\mathrm{X}]$ qui a $d \geqslant 2$ racines complexes distinctes, et soit $g \in \mathbf{Z}[\mathrm{X}]$ un polynôme non-constant de degré $< d$. Pour chaque puissance de nombre premier p^v, dénotons par A_{p^v} l'ensemble des classes de restes $g(a) \pmod{p^v}$ où a est une racine de $f(x) \equiv 0 \pmod{p^v}$. Soient A_q, $\mathcal{Q}$, Δ_q avec leur signification habituelle. Comme on l'a vu dans la preuve du théorème 2.1 pour une densité de nombres premiers au moins égale à $1/d!$, la congruence $f(x) \equiv 0 \pmod{p}$ a d racines. Puisque g est non-constant et a un degré $\leqslant d-1$, pour de tels nombres premiers p, on voit que A_p a au moins 2 éléments. Par conséquent, on obtient en utilisant le théorème 1.2 que*

$$\frac{1}{|\mathcal{Q}(x)|} \sum_{q \in \mathcal{Q}(x)} \mathrm{disc}(\Delta_q) \ll_d (\log x)^{-\frac{1}{7(d!)}}.$$

En d'autres termes, pour la plupart des $q \in \mathcal{Q}$, les points $g(a) \pmod{q}$ sont équidistribués.

Pour donner une autre variante, supposons maintenant que $g \in \mathbf{Z}[\mathrm{X}]$ est de degré au moins 2 mais au plus $d-1$, et dénotons alors maintenant par A_{p^v} l'ensemble des points $(a, g(a)) \in (\mathbf{Z}/p^v\mathbf{Z})^2$ où $f(a) \equiv 0 \pmod{p^v}$. L'intersection de A_p avec n'importe quel hyperplan affine a au plus $d-1$ points, et ainsi l'application du théorème 1.4 montre que

$$\frac{1}{|\mathcal{Q}(x)|} \sum_{q \in \mathcal{Q}(x)} \mathrm{disc}(\Delta_q) \ll_d (\log x)^{-\frac{1}{4d(d!)}}.$$

Exemple 3. *Voici (essentiellement) une reformulation de l'exemple précédent. Soient f et g deux polynômes dans $\mathbf{Z}[\mathrm{X}]$ de degrés respectifs d_1 et d_2. Supposons que $f \circ g$ a d racines complexes distinctes avec $d > d_2$. Prenons A_{p^v} comme étant l'ensemble des classes de restes $a \pmod{p^v}$ telles que $f(a) \equiv 0 \pmod{p^v}$, et telles que $a \equiv g(b) \pmod{p^v}$ est une valeur du polynôme g. Cela correspond au modèle de l'exemple 2, en notant que b est une racine de $f \circ g \pmod{p^v}$ et alors a est juste la valeur $g(b)$. Ainsi, on obtient l'équidistribution des $\{a/q\}$ pour ces racines a d'un polynôme f qui est contraint à être l'image d'un polynôme g.*

Exemple 4. *On considère maintenant des extensions du théorème 2.1, lorsque les modules q sont restreints aux entiers dont les facteurs premiers appartiennent à un ensemble prescrit $\mathcal{P}$. C'est-à-dire, étant donné $f \in \mathbf{Z}[\mathrm{X}]$ avec au moins 2 racines complexes distinctes, on prend $\mathrm{A}_{p^v} = \varnothing$ si $p \notin \mathcal{P}$ et quand $p \in \mathcal{P}$, on prend pour A_{p^v} les points $(a, a^2, \dots, a^{d-1}) \in (\mathbf{Z}/p^v\mathbf{Z})^{d-1}$ où a est une racine de $f \pmod{p^v}$. Ou, comme dans l'exemple 1, nous pourrions considérer la situation à une dimension où A_{p^v} contient les racines de $f \pmod{p^v}$ pour $p \in \mathcal{P}$. On donne maintenant deux exemples de tels analogues du théorème 2.1.*

Soit $\mathrm{K}/\mathbf{Q}$ une extension galoisienne, et dénotons par $\mathcal{P}$ l'ensemble des nombres premiers qui sont la norme d'un idéal principal dans K. Cela signifie que les nombres premiers dans $\mathcal{P}$ sont ceux qui se décomposent complètement dans H_K, le corps de classe de Hilbert de K. L'ensemble $\mathcal{P}'$ des nombres premiers qui se décomposent complètement dans le composé $\mathrm{H}_\mathrm{K}\mathrm{K}_f$ (avec K_f le corps de décomposition de f) forme un sous-ensemble de $\mathcal{P}$ et si $p \in \mathcal{P}'$ alors $f \equiv 0 \pmod{p}$ a d racines. Le théorème de densité de Chebotarev montre que $\mathcal{P}'$ a une densité positive. Ainsi

$$\sum_{\substack{p \in \mathcal{P} \\ \varrho(p) \geqslant 1 \\ p \leqslant x}} \Big(1 - \frac{\lambda(p)}{\varrho(p)}\Big)\frac{1}{p} \geqslant \sum_{\substack{p \in \mathcal{P}' \\ p \leqslant x}} \Big(1 - \frac{d-1}{d}\Big)\frac{1}{p} \geqslant \delta(\mathrm{K}, f) \log\log x,$$

pour une certaine constante $\delta(\mathrm{K}, f) > 0$ *et pour toutes les grandes valeurs de* x. *Le théorème 1.4 fournit maintenant l'équidistribution de* A_q *pour la plupart des modules* q *pour lesquels* $f \equiv 0 \pmod q$ *a une racine, et quand les facteurs premiers de* q *sont contraints dans l'ensemble* $\mathcal{P}$. *Par exemple, si* $m \geqslant 1$ *est un entier fixé, ceci s'applique à* $\mathcal{P}$ *qui est alors l'ensemble des nombres premiers de la forme* $x^2 + my^2$.

Pour donner un exemple complémentaire, supposons que $\mathrm{K}/\mathbf{Q}$ *est une extension de Galois, avec* $\mathrm{K} \neq \mathbf{Q}$, *qui est linéairement disjointe de* K_f, *et prenons* $\mathcal{P}$ *comme étant l'ensemble des nombres premiers qui* ne sont pas *les normes d'idéaux dans* K. *Puisque* K *et* K_f *sont linéairement disjoints, le groupe de Galois du composé* KK_f *est isomorphe à* $\mathrm{G} \times \mathrm{G}_f$. *Il y a une densité positive de nombres premiers* p *tels que le Frobenius en* p *est trivial dans* G_f, *de telle façon que* $\varrho_f(p) = d \geqslant 2$ *(si* $p \nmid \mathrm{D}$*), mais non-trivial dans* G *(puisque* $|\mathrm{G}| \geqslant 2$*). Alors* p *n'est pas la norme d'un idéal de* $\mathbf{Z}_\mathrm{K}$, *ainsi* $p \in \mathcal{P}$. *Maintenant on peut appliquer le théorème 1.4 comme d'habitude.*

Remarque 2.2. *D.R. Heath-Brown nous a informés d'une autre variante possible de ces résultats. Si* $\mathrm{F}(x, y)$ *est une forme intégrale irréductible de degré* > 1, *alors on peut obtenir l'équidistribution (pour les modules pertinents* q*) des parties fractionnaires des solutions* (x, y) *de la congruence* $\mathrm{F}(x, y) \equiv 0 \pmod q$. *Un tel résultat peut potentiellement être utilisé pour compter le nombre de points de hauteur limitée sur les surfaces de Châtelet* $\mathrm{Z}^2 + \mathrm{W}^2 = \mathrm{F}(\mathrm{X}, \mathrm{Y})$ *où* F *est un polynôme quartique (voir* [3]*).*

2.2. **Mesures de Hooley.** Comparons maintenant nos résultats avec l'assertion précise de [10]. Si f est un polynôme irréductible primitif fixé dans $\mathbf{Z}[\mathrm{X}]$ de degré au moins 2, alors Hooley [10] a montré que les mesures de probabilité

$$\mu_x = \frac{1}{\mathrm{M}_x} \sum_{q \in \mathcal{Q}(x)} \varrho_f(q) \Delta_q = \frac{1}{\mathrm{M}_x} \sum_{q \in \mathcal{Q}(x)} \sum_{a \in \mathrm{Z}_q} \delta_{\{\frac{a}{q}\}}$$

convergent, lorsque $x \to +\infty$, vers la mesure uniforme sur $\mathbf{R}/\mathbf{Z}$. Ici

$$\mathrm{M}_x = \sum_{q \leqslant x} \varrho_f(q)$$

dénote un facteur de normalisation, qui est asymptotiquement $\mathrm{C}_f x$ pour une constante positive C_f. Les mesures de Hooley ne sont pas les mêmes que les mesures

$$\frac{1}{|\mathcal{Q}(x)|} \sum_{q \in \mathcal{Q}(x)} \Delta_q = \frac{1}{|\mathcal{Q}(x)|} \sum_{q \in \mathcal{Q}(x)} \frac{1}{\varrho_f(q)} \sum_{a \in \mathrm{Z}_q} \delta_{\{\frac{a}{q}\}}$$

qui interviennent implicitement dans le théorème 1.2. Dans le contexte de l'équidistribution découlant du théorème des restes chinois, les mesures que nous introduisons semblent plus naturelles, et un analogue du théorème 1.2 pour les mesures μ_x est faux en général.

Proposition 2.3. *Existent des ensembles* $\mathrm{A}_p \subset \mathbf{Z}/p\mathbf{Z}$ *définis pour tous les nombres premiers* p, *avec* $|\mathrm{A}_p| \geqslant 2$ *pour tout* p *suffisamment grand, tels que les mesures*

$$\mu_x = \frac{1}{\mathrm{M}_x} \sum_{q \in \mathcal{Q}(x)} \varrho(q) \Delta_q = \frac{1}{\mathrm{M}_x} \sum_{q \in \mathcal{Q}(x)} \sum_{a \in \mathrm{Z}_q} \delta_{\{\frac{a}{q}\}}, \qquad \textit{avec} \qquad \mathrm{M}_x = \sum_{q \leqslant x} \varrho(q),$$

ne convergent pas vers la mesure uniforme lorsque $x \to +\infty$. *Ici on prend* $\mathrm{A}_{p^v} = \varnothing$ *pour tout* $v \geqslant 2$.

Lemme 2.4. *Dénotons par g la fonction multiplicative définie sur les entiers sans facteur carré q en posant $g(p) = 0$ pour $p \leqslant e^2$, et $g(p) = \lfloor p/\log p \rfloor$ for $p > e^2$. Alors il existe une constante absolue C telle que pour toute grande valeur de x*

$$\sum_{q \leqslant x} g(q) \leqslant \mathrm{C} \sum_{p \leqslant x} g(p). \tag{3}$$

***Preuve* 2.** *Puisque $\sum_{p\leqslant x} g(p) \gg x^2/(\log x)^2$, le lemme revient à prouver la borne*

$$\sum_{q \leqslant x} g(q) \ll \frac{x^2}{(\log x)^2}. \tag{4}$$

Si q est un entier sans facteur carré seulement divisible par des nombres premiers $> e^2$, alors une simple induction sur le nombre de facteurs premiers de q montre que

$$\prod_{p|q} \log p \geqslant \log q.$$

Par conséquent, si q peut être factorisé $q = q_1 q_2$ avec $q_i > q^{1/10}$, alors

$$\prod_{p|q} \log p = \prod_{p|q_1} \log p \prod_{p|q_2} \log p \geqslant (\log q_1)(\log q_2) \geqslant \frac{1}{100}(\log q)^2.$$

Ainsi, la contribution de tels entiers $q \leqslant x$ au côté gauche de (4) est

$$\leqslant 100 \sum_{q \leqslant x} \frac{q}{(\log q)^2} \ll \frac{x^2}{(\log x)^2}.$$

La contribution de q avec $q \leqslant x^{9/10}$ est aussi d'un ordre de grandeur plus petit.

Il reste à considérer la contribution des entiers $x^{9/10} \leqslant q \leqslant x$ qui ne peuvent pas être factorisés en $q_1 q_2$ avec $x^{1/5} \leqslant q_i \leqslant x^{4/5}$. Notons que de tels q doivent avoir un facteur premier au moins plus grand que $x^{1/20}$, puisqu'une procédure gloutonne produirait une factorisation de q avec deux facteurs grands. Ainsi les entiers restant $x^{9/10} \leqslant q \leqslant x$ peuvent s'écrire pq_1 avec $p > x^{1/20}$ et leur contribution est

$$\ll \sum_{q_1 \leqslant x^{19/20}} g(q_1) \sum_{x^{1/20} \leqslant p \leqslant x/q_1} \frac{p}{\log p} \ll \sum_{q_1 \leqslant x^{19/20}} g(q_1) \frac{x^2}{q_1^2 (\log x)^2} \ll \frac{x^2}{\log x^2} \prod_{p \leqslant x^{19/20}} \Big(1 + \frac{g(p)}{p^2}\Big)$$
$$\ll \frac{x^2}{(\log x)^2},$$

puisque le produit eulérien sur tous les nombres premiers converge. Cela conclut la preuve de (4), et du lemme.

***Preuve* 3** (Preuve de la Proposition 2.3)**.** *Pour $p > e^2$, désignons par A_p l'ensemble des classes de restes $k \pmod p$ avec $1 \leqslant k \leqslant g(p)$, avec g comme dans le lemme 2.4. Prenons $\mathrm{A}_{p^v} = \varnothing$ pour tout $v \geqslant 2$. Ici $\mathrm{M}_x = \sum_{q\leqslant x} g(q)$, et notons que pour tout $\varepsilon > 0$ si $p > e^{1/\varepsilon}$ alors tous les $g(p)$ points k/p avec $k \in \mathrm{A}_p$ sont dans l'intervalle $[0, \varepsilon]$. Par conséquent, en utilisant le lemme 2.4, pour de grandes valeurs de x*

$$\mu_x([0,\varepsilon]) \geqslant \frac{1}{\mathrm{M}_x} \sum_{e^{1/\varepsilon} < p \leqslant x} g(p) \geqslant \frac{1}{2\mathrm{C}}.$$

En choisissant $\varepsilon = 1/(4\mathrm{C})$, on voit que μ_x ne converge pas vers la mesure uniforme.

Remarque 2.5. *(1) On peut prouver des généralisations du résultat de* [10] *à des ensembles arbitraires définis par le théorème des restes chinois en supposant de plus que les ensembles A_{p^v} ne sont pas trop grands. Par exemple, on peut montrer que si les estimées*

$$\sum_{\substack{p\leqslant x\\ \varrho(p)\geqslant 2}} \log p \gg x, \qquad \sum_{p^v\leqslant x} \varrho(p^v)^2 \log p^v \ll x$$

sont respectées pour x suffisamment grand, alors les mesures

$$\mu_x = \frac{1}{\mathrm{M}_x}\sum_{q\in\mathcal{Q}(x)} \varrho(q)\Delta_q, \qquad \mathrm{M}_x = \sum_{q\in\mathcal{Q}(x)} \varrho(q),$$

convergent vers la mesure uniforme sur $\mathbf{R}/\mathbf{Z}$.

Puisque ces conditions sont vérifiées par l'ensemble des racines modulo p d'un monôme fixé f (où $\varrho_f(q) \leqslant \deg(f)$), cela devrait permettre de retrouver [10, Th. 2].

(2) Pour des calculs précis des sommes de Weyl (relatives aux mesures de Hooley) pour certains polynômes réductbles, voir le travail de Dartyge et Martin [2].

2.3. **Équidistribution de points de Bézout.** Soit $n \geqslant 2$ fixé, et soient X_1 et X_2 deux sous-schémas réduits fermés de $\mathbf{A}^n/\mathbf{Z}$. Supposons que la fibre générique de X_1 est une courbe géométriquement connexe sur $\mathbf{Q}$, de degré d_1, et que la fibre générique de X_2 est une hypersurface géométriquement connexe de degré d_2. (Concrètement, X_2 est l'ensemble nul d'un polynôme entier absolument irréductible à n variables, et X_1 pourrait être donné par $n-1$ telles équations "génériquement transverses".)

Supposons que les fermetures des fibres génériques de X_1 et X_2 dans $\mathbf{P}^n/\mathbf{Q}$ s'intersectent transversalement. L'intersection est alors finie par le théorème de Bézout, et a d_1d_2 points géométriques (notons qu'on suppose l'intersection transverse également à l'infini). Soit $k \leqslant d_1d_2$ le onmbre de points d'intersection géométrique appartenant à l'hyperplan à l'infini.

Pour n'importe quelle puissance de nombre premier p^v, soit $\mathrm{A}_{p^v} = (\mathrm{X}_1 \cap \mathrm{X}_2)(\mathbf{Z}/p^v\mathbf{Z})$ l'ensemble des points d'intersection $\mathbf{Z}/p^v\mathbf{Z}$-rationnels de la courbe et de l'hypersurface. Alors, pour tout q, l'ensemble A_q est l'ensemble des points d'intersection avec coordonnées dans $\mathbf{Z}/q\mathbf{Z}$.

La fibre générique de la variété intersection $\mathrm{X}_1 \cap \mathrm{X}_2$ est définie sur $\mathbf{Q}$, et a un nombre fini de points géométriques. Soit γ l'action de Galois du groupe de Galois de $\mathbf{Q}$ sur $\mathrm{X}_1 \cap \mathrm{X}_2$. Le corps fixé K du noyau de cette action est une extension finie de Galois $\mathrm{K}/\mathbf{Q}$. Si p est totalement décomposé dans K, alors tous les points d'intersection sont fixés par la classe de conjugaison de Frobenius de K en p, ce qui signifie que leurs coordonnées appartiennent à $\mathbf{Z}/p\mathbf{Z}$. En combinant cela avec le théorème de Bézout, il en découle qu'il existe un ensemble de nombres premiers p de densité positive tel que $|\mathrm{A}_p| = d_1d_2 - k$.

On suppose ensuite que $d_2 \geqslant 2$ et que la courbe X_1 n'est pas contenue dans l'hyperplan affine H (cela implique que $d_1 \geqslant 2$, mais c'est une supposition plus forte si $n \geqslant 3$). Alors pour tout hyperplan affine $\mathrm{H} \subset (\mathbf{Z}/p\mathbf{Z})^n$, on a

$$|\mathrm{A}_p \cap \mathrm{H}| \leqslant \min(d_1, d_2)$$

de telle façon que $\lambda(p) \leqslant \min(d_1, d_2)$. Par conséquent, on conclut du théorème 1.4 que pour la plupart des q, les parties fractionnaires des points d'intersection modulo q deviennent

équidistribuées dans $(\mathbf{R}/\mathbf{Z})^n$, en supposant que $\min(d_1, d_2) < d_1 d_2 - k$. Comme dans le cas des congruences polynomiales, il est naturel de se demander si l'équidistribution des parties fractionnaires des points d'intersection est vérifiée pour des modules premiers.

Comme exemple concret, supposons que X_1 et X_2 sont des courbes planes données par les équations

$$\mathrm{X}_1 \colon \mathrm{X}^3 + \mathrm{Y}^3 = 1, \qquad \mathrm{X}_2 \colon \mathrm{Y}^2 = \mathrm{X}^3 - 2.$$

Ces courbes s'intersectent transversalement (en incluant la ligne à l'infini dans $\mathbf{P}^2$, puisqu'elles n'ont aucun point en commun là), et par conséquent, la condition est vérifiée puisque $3 < 9$.

2.4. **Pseudo-polynômes.** Un *pseudo-polynôme*, au sens de Hall [9], est une fonction arithmétique $f \colon \mathbf{Z} \to \mathbf{Z}$ telle que $m - n$ divise $f(m) - f(n)$ pour tous les entiers $m \neq n$. En d'autres termes, pour tout $q \geqslant 1$, la réduction de f modulo q est q-périodique. Des exemples de telles fonctions sont donnés par les polynômes $f \in \mathbf{Z}[\mathrm{X}]$, mais il y a un nombre non dénombrable de pseudo-polynômes qui ne sont pas des polynômes (voir [9, Th. 1]). Parmi les exemples explicites les plus simples, on a $f_1(n) = \lfloor en! \rfloor$ ([9, Cor. 2]), et

$$f_2(n) = 1 - n + \frac{n(n-1)}{2} + \cdots + (-1)^n \frac{n!}{2} = (-1)^n \mathrm{D}(n),$$

où $\mathrm{D}(n)$ est le nombre de *dérangements* (permutations sans points fixes) dans le groupe symétrique sur n lettres. La formule pour $\mathrm{D}(n)$ est une application classique du principe d'inclusion–exclusion, et le fait que f_2 soit un pseudo-polynôme découle alors de [9, Th. 1]).

Pour un pseudo-polynôme f, et un entier positif q, désignons par A_q les zéros de $f \pmod q$; c'est-à-dire que A_q est l'ensemble des classes de restes $n \pmod q$ avec $f(n) \equiv 0 \pmod q$. Ces ensembles A_q sont construits à partir des ensembles A_{p^v} pour les puissances de nombres premiers p^v en utilisant le théorème des restes chinois. Comme cela a été discuté, les ensembles A_q sont équidistribués pour la plupart des q, quand f est un polynôme effectif. Le théorème 1.2 s'applique-t-il aussi généralement aux pseudo-polynômes ? Vivian Kuperberg [14] nous a fait remarquer qu'il y a des pseudo-polynômes dont les valeurs sont seulement divisibles par une séquence de nombres premiers très clairsemée (en effet, on peut remarquer que cette séquence augmente arbitrairement rapidement). Ainsi, il n'y a pas d'espoir d'appliquer le théorème 1.2 à un pseudo-polynôme général, mais les exemples f_1 et f_2 semblent bien se comporter, et on présente des expérimentations numériques concernant ces exemples. Pour des calculs avec f_1 et f_2, il est efficace d'utiliser les définitions récursive

$$f_1(1) = 2, \qquad f_1(n+1) = 1 + (n+1) f_1(n),$$
$$f_2(0) = 1, \qquad f_2(n+1) = 1 - (n+1) f_2(n).$$

Les expérimentations numériques suggèrent que les valeurs $f_1(n) = \lfloor en! \rfloor \pmod p$ pour $1 \leqslant n \leqslant p$ se comportent comme p classes résiduelles indépendantes prises au hasard dans $\mathbf{Z}/p\mathbf{Z}$. S'il en est ainsi, cela suggère qu'il y a k solutions à $f_1(n) \equiv 0 \pmod p$ pour une proportion $e^{-1}/k!$ des nombres premiers p inférieurs à x : c'est-à-dire, pour tout $k \geqslant 0$

$$\lim_{x \to +\infty} \frac{1}{\pi(x)} |\{p \leqslant x \mid \varrho(p) = k\}| = \frac{1}{e} \frac{1}{k!}.$$

En d'autres termes, la quantité $\varrho(p)$ est distribuée comme une variable aléatoire de Poisson de paramètre 1. Si tel est le cas, cela devrait impliquer que le théorème 1.2 s'applique aux zéros des nombres premiers modulo f_1. Pourtant, on ne sait pas démontrer que $\varrho(p) \geqslant 2$ pour un ensemble infini de nombres premiers.

La table suivante donne la distribution empirique et théorique de la distribution de Poisson pour les 78498 nombres premiers $p \leqslant x = 10^6$ (normalisée en multipliant les probabilités de Poisson par $\pi(x)$; aucune valeur empirique n'est supérieure à 8 dans ce domaine), ainsi que les moments empirique et théorique d'ordre $1 \leqslant n \leqslant 4$.

Distribution de probabilité empirique et théorique

k	0	1	2	3	4	5	6	7	8
Empirique	29054	28822	14314	4777	1250	236	38	5	2
Poisson	28877.8	28877.8	14438.9	4813	1203.2	240.6	40.17	5.7	0.7

Moments empiriques et théoriques

n	1	2	3	4
Empirique	0.99671	1.9964	5.0034	15.054
Poisson	1	2	5	15

Notons que si $g \in \mathbf{Z}[\mathrm{X}]$ est un polynôme irréductible de degré n ayant pour groupe de Galois S_n (le cas générique), alors le théorème de densité de Chebotarev implique que

$$\lim_{x\to+\infty} \frac{1}{\pi(x)} |\{p \leqslant x \mid \varrho_g(p) = k\}| = \frac{1}{n!} |\{\pi \in \mathrm{S}_n \text{ avec } k \text{ points fixes}\}|.$$

Maintenant pour de grandes valeurs de n, le nombre de points fixes d'une permutation piochée uniformément au hasard dans S_n est approximativement distribué comme une variable aléatoire de Poisson de paramètre 1. Ainsi notre conjecture sur le nombre de zéros du pseudo-polynôme $f_1 \pmod p$ semble être vérifiée pour un polynôme irréductible générique de grand degré.

Pour la fonction $f_2(n) = (-1)^n \mathrm{D}(n)$, les expérimentations numériques suggèrent également qu'il y a une densité positive de nombres premiers avec $\varrho(p) \geqslant 2$, de telle façon que le théorème 1.2 devrait s'appliquer. Une fois encore, nous sommes incapables de démontrer une telle assertion.

Mais, si on pose $f_3(n) = f_2(n) - 1$, alors à partir de la définition récursive pour f_2 donnée ci-dessus, on peut voir que $f_3(0) = 0$, et $f_3(p-1) \equiv 0 \pmod p$ pour tout nombre premier p. Par conséquent, dans ce cas, $\varrho(p) \geqslant 2$ pour tout nombre premier p, et le théorème 1.2 s'applique. Notons que $|f_3(n)|$ a une signification combinatoire : il est égal au nombre de permutations dans S_n avec exactement un point fixe. Puisque $|f_3|$ et f_3 ont les mêmes zéros $\pmod q$ pour tout q, on voit que le théorème 1.2 s'applique à la séquence combinatoire $|f_3(n)|$.

3. Préliminaires

Dans la suite, on travaille dans le cadre de plus haute dimension des théorèmes 1.4, 1.6, 1.8, de telle façon que A_q est un sous-ensemble de $(\mathbf{Z}/q\mathbf{Z})^n$, et $\varrho(q)$ est sa cardinalité. On garde la supposition 1.1, et on a à l'esprit que x est grand comparativement à α et x_0.

3.1. **Les ensembles Ω et Ω_k.** On commence par acquérir une compréhension de la taille des ensembles $\Omega(x)$ et $\Omega_k(x)$ (d'éléments dans Ω avec exactement k facteurs premiers distincts).

Lemme 3.1. *Pour x suffisamment grand en fonction de α et x_0*

$$|\mathcal{Q}(x)| \gg \frac{\alpha x}{\log x} \prod_{\substack{p \leqslant x \\ p \in \mathcal{Q}}} \Big(1 + \frac{1}{p}\Big).$$

***Preuve* 4.** *Observons que*

$$|\mathcal{Q}(x)| \geqslant \frac{1}{\log x} \sum_{q \in \mathcal{Q}(x)} \log q \geqslant \frac{1}{\log x} \sum_{q \in \mathcal{Q}(x)} \sum_{pd = q} \log p \geqslant \frac{1}{\log x} \sum_{\substack{d < x^{1/3} \\ d \in \mathcal{Q}}} \sum_{\substack{x^{1/3} < p \leqslant x/d \\ p \in \mathcal{Q}}} \log p.$$

En utilisant la supposition 1.1, il découle pour les grandes valeurs de x que

$$|\mathcal{Q}(x)| \geqslant \frac{\alpha x}{2 \log x} \sum_{\substack{d < x^{1/3} \\ d \in \mathcal{Q}}} \frac{1}{d}.$$

Maintenant posons $z = x^{1/9}$ et $\tau = 1/\log z$, et notons que (en restreignant l'attention à d sans facteur carré)

$$\sum_{\substack{d < x^{1/3} \\ d \in \mathcal{Q}}} \frac{1}{d} \geqslant \sum_{\substack{d < x^{1/3} \\ d \in \mathcal{Q} \\ p \mid d \Longrightarrow p \leqslant z}} \frac{\mu(d)^2}{d} = \prod_{\substack{p \leqslant z \\ p \in \mathcal{Q}}} \Big(1 + \frac{1}{p}\Big) - \sum_{\substack{d > x^{1/3} \\ d \in \mathcal{Q} \\ p \mid d \Longrightarrow p \leqslant z}} \frac{\mu(d)^2}{d},$$

et de plus

$$\sum_{\substack{d > x^{1/3} \\ d \in \mathcal{Q} \\ p \mid d \Longrightarrow p \leqslant z}} \frac{\mu(d)^2}{d} \leqslant \sum_{\substack{d \in \mathcal{Q} \\ p \mid d \Longrightarrow p \leqslant z}} \frac{\mu(d)^2}{d} \Big(\frac{d}{x^{1/3}}\Big)^{\tau} = e^{-3} \prod_{\substack{p \leqslant z \\ p \in \mathcal{Q}}} \Big(1 + \frac{p^{\tau}}{p}\Big).$$

Par conséquent

$$\sum_{\substack{d < x^{1/3} \\ d \in \mathcal{Q}}} \frac{1}{d} \geqslant \prod_{\substack{p \leqslant z \\ p \in \mathcal{Q}}} \Big(1 + \frac{1}{p}\Big) \Big(1 - e^{-3} \prod_{\substack{p \leqslant z \\ p \in \mathcal{Q}}} \frac{1 + p^{\tau}/p}{1 + 1/p}\Big).$$

Maintenant, pour de grandes valeurs de x (et donc de grandes valeurs de z),

$$\prod_{\substack{p \leqslant z \\ p \in \mathcal{Q}}} \frac{1 + p^{\tau}/p}{1 + 1/p} \leqslant \prod_{p \leqslant z} \Big(1 + \frac{p^{\tau} - 1}{p}\Big) \leqslant \exp\Big(\sum_{p \leqslant z} \frac{p^{\tau} - 1}{p}\Big) \leqslant \exp\Big(\sum_{p \leqslant z} \frac{(e-1)\tau \log p}{p}\Big) \leqslant e^2.$$

En assemblant les observations ci-dessus, on conclut que

$$|\mathcal{Q}(x)| \geqslant \frac{\alpha x}{2 \log x} \Big(1 - \frac{1}{e}\Big) \prod_{\substack{p \leqslant z \\ p \in \mathcal{Q}}} \Big(1 + \frac{1}{p}\Big).$$

Le lemme s'ensuit puisque

$$\prod_{x^{1/9} < p \leqslant x} (1 + 1/p) \ll 1.$$

On peut également démontrer une borne supérieure correcte pour $|\mathcal{Q}(x)|$, et en fait, on aura besoin d'une telle borne pour les éléments lisses (ou friables) dans $\mathcal{Q}(x)$.

Lemme 3.2. *Soit x grand, et z un paramètre avec $\log x \leqslant z \leqslant x$. Alors*

$$\sum_{\substack{q\in\mathcal{Q}(x)\\ p|q\Longrightarrow p\leqslant z}} 1 \ll \frac{x}{\log x}\exp\Big(-\frac{\log x}{\log z}\Big)\prod_{\substack{p\leqslant z\\ p\in\mathcal{Q}}}\Big(1+\frac{1}{p}\Big).$$

***Preuve* 5.** *On commence par noter que*

$$\sum_{\substack{q\in\mathcal{Q}(x)\\ p|q\Longrightarrow p\leqslant z}} 1 \leqslant \sqrt{x}+\frac{2}{\log x}\sum_{\substack{\sqrt{x}<q\leqslant x\\ q\in\mathcal{Q}\\ p|q\Longrightarrow p\leqslant z}}\log q \leqslant \sqrt{x}+\frac{2}{\log x}\sum_{\substack{q\in\mathcal{Q}(x)\\ p|q\Longrightarrow p\leqslant z}}\sum_{\substack{q=d\ell\\ (d,\ell)=1}}\log \ell,$$

où ℓ dénote une puissance de nombre premier. Le terme $\sqrt{x}$ est beaucoup plus petit que l'estimation désirée, et donc, on peut l'ignorer et se concentrer sur le second terme ci-dessus.

Pour estimer la seconde somme, on va d'abord sommer sur d (qui doit être dans $\mathcal{Q}$), et ensuite sur ℓ. Notons que ℓ doit être $\leqslant x/d$, et si ℓ est un nombre premier, il est aussi contraint à être $\leqslant z$. Ainsi, pour un d donné, la somme sur ℓ est

$$\leqslant \sum_{\substack{p^v\leqslant x/d\\ v\geqslant 2}}\log(p^v)+\sum_{p\leqslant\min(x/d,z)}\log p \ll \frac{\sqrt{x}}{\sqrt{d}}+\min\Big(\frac{x}{d},z\Big)\ll\Big(\frac{x}{d}\Big)^{1-\tau}z^{\tau},$$

pour tout $\tau\in[0,\frac{1}{2}]$. En utilisant cette observation avec $\tau=1/\log z$, on obtient

$$\begin{aligned}\sum_{\substack{q\in\mathcal{Q}(x)\\ p|q\Longrightarrow p\leqslant z}}\sum_{\substack{q=d\ell\\ (d,\ell)=1}}\log\ell \ll \sum_{\substack{d\in\mathcal{Q}(x)\\ p|d\Longrightarrow p\leqslant z}}\Big(\frac{x}{d}\Big)^{1-\tau}z^{\tau} &= x\exp\Big(-\frac{\log x}{\log z}\Big)\sum_{\substack{d\in\mathcal{Q}(x)\\ p|d\Longrightarrow p\leqslant z}}\frac{1}{d^{1-1/\log z}}\\ &\leqslant x\exp\Big(-\frac{\log x}{\log z}\Big)\prod_{\substack{p\leqslant z\\ p\in\mathcal{Q}}}\Big(1-\frac{p^{1/\log z}}{p}\Big)^{-1}\\ &\ll x\exp\Big(-\frac{\log x}{\log z}\Big)\prod_{\substack{p\leqslant z\\ p\in\mathcal{Q}}}\Big(1+\frac{p^{1/\log z}}{p}\Big).\end{aligned}$$

Le lemme en découle en notant que

$$\begin{aligned}\prod_{\substack{p\leqslant z\\ p\in\mathcal{Q}}}\Big(1+\frac{p^{1/\log z}}{p}\Big) &\leqslant \prod_{\substack{p\leqslant z\\ p\in\mathcal{Q}}}\Big(1+\frac{1}{p}\Big)\prod_{p\leqslant z}\Big(\frac{1+p^{1/\log z}/p}{1+1/p}\Big)\\ &\leqslant \prod_{\substack{p\leqslant z\\ p\in\mathcal{Q}}}\Big(1+\frac{1}{p}\Big)\exp\Big(\sum_{p\leqslant z}\frac{p^{1/\log z}-1}{p}\Big)\ll\prod_{\substack{p\leqslant z\\ p\in\mathcal{Q}}}\Big(1+\frac{1}{p}\Big).\end{aligned}$$

Les deux prochains lemmes seront analogues à celui ci-dessus pour les ensembles $\mathcal{Q}_k(x)$ pour un entier donné $k\geqslant 1$. Les lecteurs qui sont essentiellement intéressés par les théorèmes 1.2 et 1.4 peuvent sauter à ce point de la section 3.2

Définissons

$$\mathcal{P}(x) = \sum_{\substack{p \leqslant x \\ p \in \mathcal{Q}}} \frac{1}{p} + 3, \tag{5}$$

de telle façon que pour de grandes valeurs de x, la supposition 1.1 donne

$$\alpha \log\log x + \mathrm{O}(1) \leqslant \mathcal{P}(x) \leqslant \log\log x + \mathrm{O}(1). \tag{6}$$

La constante ajoutée 3 dans (5) est sans importance, mais elle sera pratique plus tard.

Lemme 3.3. *Soit x grand, et soit k un entier avec $1 \leqslant k \leqslant \exp(\mathcal{P}(x)/4)$. Alors*

$$|\mathcal{Q}_k(x)| \gg \frac{\alpha x}{\log x} \frac{\mathcal{P}(x)^{k-1}}{(k-1)!} \exp\Big(-\frac{4k\log k}{\mathcal{P}(x)}\Big),$$

où la constante qui intervient est absolue.

***Preuve* 6.** *On obtient une borne inférieure en comptant seulement les éléments de $\mathcal{Q}_k(x)$ qui sont de la forme $p_1 \cdots p_k$, où les nombres premiers p_j sont en ordre strictement croissant et satisfont $p_1, \ldots, p_{k-1} \leqslant x^{1/(2k)}$. En fixant ces nombres premiers $p_1, \ldots, p_{k-1}$, on voit en utilisant la supposition 1.1 qu'il y a au moins*

$$\geqslant \frac{\alpha x}{4p_1 \cdots p_{k-1} \log x}$$

choix possibles pour le grand nombre premier p_k. Par conséquent

$$\begin{aligned} |\mathcal{Q}_k(x)| &\geqslant \frac{\alpha x}{4\log x} \sum_{\substack{p_1 < \cdots < p_{k-1} \leqslant x^{1/(2k)} \\ p_j \in \mathcal{Q}}} \frac{1}{p_1 \cdots p_{k-1}} \\ &= \frac{\alpha x}{4\log x} \frac{1}{(k-1)!} \sum_{\substack{p_1, \ldots, p_{k-1} \leqslant x^{1/(2k)} \\ p_j \in \mathcal{Q} \\ p_j \text{ distincts}}} \frac{1}{p_1 \cdots p_{k-1}}. \end{aligned}$$

Soient $p_1, \ldots, p_{k-2}$ des nombres premiers distincts dans $\mathcal{Q}$ tous inférieurs à $x^{1/(2k)}$. Alors

$$\sum_{\substack{p_{k-1} \leqslant x^{1/(2k)} \\ p_{k-1} \neq p_1, \ldots, p_{k-2} \\ p_{k-1} \in \mathcal{Q}}} \frac{1}{p_{k-1}} = \big(\mathcal{P}(x^{\frac{1}{2k}}) - 2\big) - \frac{1}{p_1} - \cdots - \frac{1}{p_{k-2}}.$$

La quantité $1/p_1 + \ldots + 1/p_{k-2}$ est au plus égale à la somme correspondante quand les nombres premiers p_i sont égaux aux $k-2$ premiers nombres premiers, et par conséquent elle est $\leqslant \log\log(k+1) + \mathrm{O}(1)$, de telle façon que

$$\sum_{\substack{p_{k-1} \leqslant x^{1/(2k)} \\ p_{k-1} \neq p_1, \ldots, p_{k-2} \\ p_{k-1} \in \mathcal{Q}}} \frac{1}{p_{k-1}} \geqslant \mathcal{P}(x^{\frac{1}{2k}}) - \log\log(k+1) - \mathrm{C}$$

pour une certaine constante absolue $\mathrm{C} \geqslant 0$. En répétant cet argument, on trouve la même borne inférieure pour chaque somme sur $p_{k-2}, \ldots, p_1$, et par conséquent on obtient la borne

inférieure

$$|\Omega_k(x)| \gg \frac{\alpha x}{\log x}\frac{(\mathcal{P}(x^{\frac{1}{2k}}) - \log\log(k+1) - \mathrm{C})^{k-1}}{(k-1)!}$$

pour $x \geqslant x_0$, où la constante qui intervient est absolue. Puisque

$$\mathcal{P}(x^{\frac{1}{2k}}) \geqslant \mathcal{P}(x) - \sum_{x^{\frac{1}{2k}} < p \leqslant x} \frac{1}{p} = \mathcal{P}(x) - \log k + \mathrm{O}(1),$$

et $\log k \leqslant \mathcal{P}(x)/4$, le lemme s'ensuit.

Lemme 3.4. *Soit x grand. Soit $k \leqslant (\log x)^{\frac{1}{2}}$ un entier positif, et κ un entier négatif avec $\kappa \leqslant k$. Le nombre d'entiers dans $\Omega_k(x)$ ayant au moins κ facteurs premiers distincts qui sont plus grands que $x^{1/(4k)}$ est*

$$\ll \frac{kx}{\log x}\frac{\mathcal{P}(x)^{k-1}}{(k-1)!}\exp\Big(\frac{2k\log k}{\mathcal{P}(x)} - \kappa\Big),$$

où la constante qui intervient est absolue.

***Preuve* 7.** *Dénotons par* N *ce nombre. Écrivons $q \in \Omega_k$ comme $q = p_1^{v_1}\cdots p_k^{v_k}$ avec les nombres premiers p_j dans l'ordre strictement croissant.*

D'abord, si $p_k < x^{1/(4k)}$, alors $p_1\cdots p_k \leqslant x^{1/4}$, et le nombre de choix pour les exposants $(v_1,\dots,v_k)$ est $\ll (\log x)^k \ll x^{\varepsilon}$ pour tout $\varepsilon > 0$. Par conséquent, dans ce cas (qui est seulement pertinent pour $\kappa = 0$), on a

$$\mathrm{N} \ll x^{1/4+\epsilon} \leqslant x^{1/3}$$

puisque x est grand.

Supposons maintenant que $p_k > x^{1/(4k)}$. Soient $p_1^{v_1}$, …, $p_{k-1}^{v_{k-1}}$ fixés. Notons que $p_1^{v_1}\cdots p_{k-1}^{v_{k-1}} \leqslant x^{1-1/(4k)}$, donc par l'inégalité de Brun–Titchmarsh, le nombre de choix possibles pour $p_k^{v_k}$ est

$$\leqslant \frac{3x}{p_1^{v_1}\cdots p_{k-1}^{v_{k-1}}\log(x/p_1^{v_1}\cdots p_{k-1}^{v_{k-1}})} \leqslant \frac{12kx}{p_1^{v_1}\cdots p_{k-1}^{v_{k-1}}\log x}.$$

Par conséquent

$$\begin{aligned}\mathrm{N} &\leqslant x^{\frac{1}{3}} + \frac{12kx}{\log x}\sum_{\substack{p_1<\cdots<p_{k-1}\leqslant x\\ p_j^{v_j}\in\mathcal{Q}\\ p_{k-\kappa+1}>x^{1/(4k)}}}\frac{1}{p_1^{v_1}\cdots p_{k-1}^{v_{k-1}}}\\ &\leqslant x^{\frac{1}{3}} + \frac{12kx}{\log x}\sum_{\kappa-1\leqslant j\leqslant k-1}\frac{1}{j!}\Big(\sum_{\substack{x\geqslant p>x^{1/(4k)}\\ p^v\in\mathcal{Q}}}\frac{1}{p^v}\Big)^j\frac{1}{(k-1-j)!}\Big(\sum_{\substack{p\leqslant x^{1/(4k)}\\ p^v\in\mathcal{Q}}}\frac{1}{p^v}\Big)^{k-1-j},\end{aligned}$$

où la variable j représente le nombre de nombres premiers parmi p_1, …, p_{k-1} qui sont plus grands que $x^{1/(4k)}$, et pour chaque p, on calcule la somme sur tous les v tels que $p^v \in \mathcal{Q}$.

Maintenant la somme sur j ci-dessus peut être bornée par

$$e^{-(\kappa-1)}\sum_{0\leqslant j\leqslant k-1}\frac{1}{j!}\Big(\sum_{\substack{x\geqslant p>x^{1/(4k)}\\ p^v\in\mathcal{Q}}}\frac{e}{p^v}\Big)^j\frac{1}{(k-1-j)!}\Big(\sum_{\substack{p\leqslant x^{1/(4k)}\\ p^v\in\mathcal{Q}}}\frac{1}{p^v}\Big)^{k-1-j}$$
$$=\frac{e^{-(\kappa-1)}}{(k-1)!}\Big(\sum_{\substack{x\geqslant p>x^{1/(4k)}\\ p^v\in\mathcal{Q}}}\frac{e}{p^v}+\sum_{\substack{p\leqslant x^{1/(4k)}\\ p^v\in\mathcal{Q}}}\frac{1}{p^v}\Big)^{k-1}$$
$$\ll\frac{e^{-(\kappa-1)}}{(k-1)!}(\mathcal{P}(x)+(e-1)\log k+\mathrm{O}(1))^{k-1},$$

ce qui établit le lemme.

3.2. **Sommes de Weyl.** Pour un module $q\in\mathcal{Q}$ et $h\in\mathbf{Z}^n$, définissons la somme de Weyl normalisée

$$\mathrm{W}(h;q)=\frac{1}{\varrho(q)}\sum_{x\in\mathrm{A}_q}e\Big(\frac{h\cdot x}{q}\Big) \tag{7}$$

où

$$h\cdot x=h_1x_1+\cdots+h_nx_n.$$

On étend la définition de $\lambda(p)$ (donnée juste avant le théorème 1.4) à tous les entiers positifs. Étant donné une puissance de nombre premlier p^v dans $\mathcal{Q}$, notons

$$\lambda(p^v)=\max_{\substack{\mathrm{H}\subset(\mathbf{Z}/p^v\mathbf{Z})^n\\ \text{Hhyperplan affine}}}|\mathrm{H}\cap\mathrm{A}_{p^v}|,$$

et étendons λ à $\mathcal{Q}$ par multiplicativité. Par le théorème des restes chinois, on a

$$\lambda(q)=\max_{\substack{\mathrm{H}\subset(\mathbf{Z}/q\mathbf{Z})^n\\ \text{Hhyperplan affine}}}|\mathrm{H}\cap\mathrm{A}_q|$$

pour $q\in\mathcal{Q}$, où un hyperplan affine $\mathrm{H}\subset(\mathbf{Z}/q\mathbf{Z})^n$ est un sous-ensemble de la forme

$$\mathrm{H}=\{x\in(\mathbf{Z}/q\mathbf{Z})^n\mid h_1x_1+\cdots+h_nx_n=a\}$$

pour un certain $a\in\mathbf{Z}/q\mathbf{Z}$ et $(h_i)\in(\mathbf{Z}/q\mathbf{Z})^n\setminus\{(0,\dots,0)\}$.

Pour un $h\in\mathbf{Z}^n$ non nul donné et une puissance de nombre premier p^v, on pose

$$\{h,p^v\}=\begin{cases}1 & \text{if } h\equiv 0\,(\mathrm{mod}\,p^v)\\ p^v & \text{sinon,}\end{cases}$$

et alors on étend cette définition multiplicativement pour définir $\{h,q\}$.

Lemme 3.5. (1) *Si q_1 et q_2 sont des éléments premiers entre eux de $\mathcal{Q}$, alors*

$$\mathrm{W}(h;q_1q_2)=\mathrm{W}(\bar{q}_1h;q_2)\mathrm{W}(\bar{q}_2h;q_1),$$

où $q_1\bar{q}_1\equiv 1\,(\mathrm{mod}\,q_2)$ et $q_2\bar{q}_2\equiv 1\,(\mathrm{mod}\,q_1)$.

(2) *Soit $h\in\mathbf{Z}^n$, avec $h\neq(0,\dots,0)$. Pour $q\in\mathcal{Q}$, on a*

$$\frac{1}{q}\sum_{a\,(\mathrm{mod}\,q)}|\mathrm{W}(ah;q)|^2\leqslant\frac{\lambda(\{h,q\})}{\varrho(\{h,q\})}. \tag{8}$$

***Preuve* 8.** *Ces assertions sont élémentaires (voir* [10, Lemmes 1 et 3] *pour $n = 1$).*

(1) Pour $x_1 \in \mathbf{Z}^n$ et $x_2 \in \mathbf{Z}^n$, l'élément de $(\mathbf{Z}/q_1q_2\mathbf{Z})^n$ qui est congruent à x_i modulo q_i est la classe de reste du vecteur

$$x = q_1\bar{q}_1x_2 + q_2\bar{q}_2x_1 \in \mathbf{Z}^n.$$

Par conséquent

$$\begin{aligned}\mathrm{W}(h; q_1q_2) &= \frac{1}{\varrho(q_1q_2)} \sum_{x \in \mathrm{A}_{q_1q_2}} e\Big(\frac{h \cdot x}{q_1q_2}\Big) \\ &= \frac{1}{\varrho(q_1)\varrho(q_2)} \sum_{x_1 \in \mathrm{A}_{q_1}} \sum_{x_2 \in \mathrm{A}_{q_2}} e\Big(\frac{h \cdot (q_1\bar{q}_1x_2 + q_2\bar{q}_2x_2)}{q_1q_2}\Big) = \mathrm{W}(\bar{q}_1h; q_2)\mathrm{W}(\bar{q}_2h; q_1).\end{aligned}$$

(2) En ouvrant le carré et en échangeant l'ordre des sommations, on trouve que

$$\sum_{a \,(\mathrm{mod}\, q)} |\mathrm{W}(ah; q)|^2 = \frac{1}{\varrho(q)^2} \sum_{x,y \in \mathrm{A}_q} \sum_{a \,(\mathrm{mod}\, q)} e\Big(\frac{ah \cdot (x-y)}{q}\Big).$$

Par orthogonalité des caractères modulo q, cela implique que

$$\sum_{a \,(\mathrm{mod}\, q)} |\mathrm{W}(ah; q)|^2 = \frac{q}{\varrho(q)^2} \sum_{\substack{x,y \in \mathrm{A}_q \\ h\cdot(x-y) = 0 \,(\mathrm{mod}\, q)}} 1.$$

En sommant sur x d'abord, cela donne

$$\sum_{a \,(\mathrm{mod}\, q)} |\mathrm{W}(ah; q)|^2 \leqslant \frac{q}{\varrho(q)^2} \sum_{x \in \mathrm{A}_q} \alpha(x)$$

où $\alpha(x)$ est le nombre de $y \in \mathrm{A}_q$ tels que $h \cdot y = h \cdot x \,(\mathrm{mod}\, q)$. Par le théorème des restes chinois, $\alpha(x)$ est borné par le produit sur $p^v \| q$ du nombre de solutions de $h \cdot x = h \cdot y \,(\mathrm{mod}\, p^v)$, et ce nombre peut être borné par $\varrho(p^v)$ si $h \equiv 0 \,(\mathrm{mod}\, p^v)$ et l'hyperplan résultant est dégénéré, ou par $\lambda(p^v)$ sinon. Par conséquent

$$\alpha(x) \leqslant \varrho(q/\{h, q\})\lambda(\{h, q\})$$

pour tout x, et le résultat s'ensuit.

Remarque 3.6. *La partie (1) est l'endroit crucial où on utilise le fait que A_q est défini par le théorème des restes chinois, alors que (2) est le seul point où on détecte une annulation dans les sommes de Weyl $\mathrm{W}(h; q)$.*

3.3. **L'inégalité de Erdős–Turán.** On rappelle l'inégalité de Erdős–Turán n-dimensionnelle pour la divergece de Δ_q (voir, e.g., [8, Lemme 2] pour des références) : pour tout entier $\mathrm{H} \geqslant 1$, on a

$$\mathrm{disc}(\Delta_q) \ll \frac{1}{\mathrm{H}} + \sum_{0 < \|h\| \leqslant \mathrm{H}} \frac{1}{\mathrm{M}(h)} |\mathrm{W}(h; q)|, \tag{9}$$

où $\|h\| = \max(|h_i|)$ et $\mathrm{M}(h) = \prod_i \max(1, |h_i|)$ et où la constante impliquée dépend seulement de n. On enregistre maintenant une conséquence du lemme 3.5 pour les termes apparaissant dans (9), et on l'utilise alors pour borner certaines moyennes utiles de $\mathrm{disc}(\Delta_q)$.

Lemme 3.7. *Soit $q \in \mathcal{Q}$ et $\mathrm{H} \geqslant 2$ donnés. Alors*

$$\frac{1}{q}\sum_{a \,(\mathrm{mod}\, q)}\sum_{0<\|h\|\leqslant \mathrm{H}}\frac{1}{\mathrm{M}(h)}|\mathrm{W}(ah;q)| \ll (\log \mathrm{H})^n \prod_{p^v \| q}\Big(\frac{\sqrt{\lambda(p^v)}}{\sqrt{\varrho(p^v)}}+\frac{1}{p^v}\Big),$$

où la constante impliquée ne dépend que de n.

***Preuve* 9.** *En appliquant l'inégalité de Cauchy–Schwarz et (8), on a*

$$\begin{aligned}\frac{1}{q}\sum_{a \,(\mathrm{mod}\, q)}\sum_{0<\|h\|\leqslant \mathrm{H}}\frac{1}{\mathrm{M}(h)}|\mathrm{W}(ah;q)| &\leqslant \sum_{0<\|h\|\leqslant \mathrm{H}}\frac{1}{\mathrm{M}(h)}\Big(\frac{\lambda(\{h,q\})}{\varrho(\{h,q\})}\Big)^{\frac12}\\ &= \sum_{\substack{d\mid q\\(d,q/d)=1}}\Big(\frac{\lambda(d)}{\varrho(d)}\Big)^{\frac12}\sum_{\substack{0<\|h\|\leqslant \mathrm{H}\\ \{q,h\}=d}}\frac{1}{\mathrm{M}(h)},\end{aligned}$$

puisque $\{h,q\}=d$ est possible seulement pour ces diviseurs de d qui sont premiers à q/d. Observons que si $1 \leqslant \|h\| \leqslant \mathrm{H}$ et $\{h,q\}=d$, alors au moins l'une des coordonnées h_i est un multiple non nul de q/d. Par conséquent

$$\sum_{\substack{0<\|h\|\leqslant \mathrm{H}\\ \{q,h\}=d}}\frac{1}{\mathrm{M}(h)} \leqslant \frac{d}{q}\sum_{0<\|h\|\leqslant \mathrm{H}}\frac{1}{\mathrm{M}(h)} \ll \frac{d}{q}(\log \mathrm{H})^n,$$

et le lemme en découle par multiplicativité.

Lemme 3.8. *Soit x grand, et z un nombre réel dans le domaine $e \leqslant z \leqslant x^{1/3}$. Soit $s \leqslant x^{\frac13}$ un entier avec $s \in \mathcal{Q}$ et tel que tous les facteurs premiers de s sont inférieurs à z. Alors, pour tout $\mathrm{H} \geqslant 2$, on a*

$$\sum_{\substack{r\leqslant x/s\\ rs\in\mathcal{Q}\\ p\mid r\Longrightarrow p>z}}\mathrm{disc}(\Delta_{rs}) \ll \frac{x}{\varphi(s)\log z}\Big(\frac{1}{\mathrm{H}}+(\log \mathrm{H})^n\prod_{p^v\| s}\Big(\frac{\sqrt{\lambda(p^v)}}{\sqrt{\varrho(p^v)}}+\frac{1}{p^v}\Big)\Big).$$

***Preuve* 10.** *On applique l'inégalité de Erdős-Turán (9). En utilisant la multiplicativité twistée du lemme 3.5, (1), qui s'applique puisque r et s sont premiers entre eux, on obtient*

$$\sum_{\substack{r\leqslant x/s\\ rs\in\mathcal{Q}\\ p\mid r\Longrightarrow p>z}}\mathrm{disc}(\Delta_{rs}) \ll \sum_{\substack{r\leqslant x/s\\ rs\in\mathcal{Q}\\ p\mid r\Longrightarrow p>z}}\Big(\frac{1}{\mathrm{H}}+\sum_{0<\|h\|\leqslant \mathrm{H}}\frac{1}{\mathrm{M}(h)}|\mathrm{W}(\overline{r}h;s)\mathrm{W}(\overline{s}h;r)|\Big).$$

On bornee $|\mathrm{W}(\overline{s}h;r)|$ trivialement par 1, et on décompose la somme sur r en classes de restes (réduites) $r \equiv \bar{a} \,(\mathrm{mod}\, s)$. Si $r \equiv \bar{a} \,(\mathrm{mod}\, s)$ alors $\mathrm{W}(\bar{r}h;s)=\mathrm{W}(ah;s)$, de telle façon que

$$\sum_{\substack{r\leqslant x/s\\ rs\in\mathcal{Q}\\ p\mid r\Longrightarrow p>z}}\mathrm{disc}(\Delta_{rs}) \ll \sum_{\substack{a \,(\mathrm{mod}\, s)\\ (a,s)=1}}\Big(\frac{1}{\mathrm{H}}+\sum_{0<\|h\|\leqslant \mathrm{H}}\frac{1}{\mathrm{M}(h)}|\mathrm{W}(ah;s)|\Big)\sum_{\substack{r\leqslant x/s\\ rs\in\mathcal{Q}\\ p\mid r\Longrightarrow p>z\\ r\equiv\bar{a}\,(\mathrm{mod}\, s)}}1.$$

Puisque $s \leqslant x^{\frac{1}{3}}$, il s'ensuit que $x/s \geqslant x^{\frac{2}{3}}$. En ignorant la condition que $rs \in \mathcal{Q}$, et en utilisant le crible, on trouve que

$$\sum_{\substack{r\leqslant x/s\\ rs\in\mathcal{Q}\\ p|r\Longrightarrow p>z\\ r\equiv\overline{a}\,(\mathrm{mod}\,s)}} 1 \leqslant \sum_{\substack{r\leqslant x/s\\ p|r\Longrightarrow p>z\\ r\equiv\overline{a}\,(\mathrm{mod}\,s)}} 1 \ll \frac{x/s}{\varphi(s)\log z}$$

avec une constante appliquée absolue. Par conséquent

$$\sum_{\substack{r\leqslant x/s\\ rs\in\mathcal{Q}\\ p|r\Longrightarrow p>z}} \mathrm{disc}(\Delta_{rs}) \ll \frac{x}{\varphi(s)\log z}\frac{1}{s}\sum_{\substack{a\,(\mathrm{mod}\,s)\\ (a,s)=1}}\Big(\frac{1}{\mathrm{H}}+\sum_{0<\|h\|\leqslant\mathrm{H}}\frac{1}{\mathrm{M}(h)}|\mathrm{W}(ah;s)|\Big).$$

Étendre la somme sur a à tous les $a\,(\mathrm{mod}\,s)$, et invoquer le lemme 3.7 permet de conclure la démonstration.

4. Preuve du théorème 1.4

Notre but est d'estimer la somme

$$\sum_{q\in\mathcal{Q}(x)}\mathrm{disc}(\Delta_q),$$

en fonction de la quantité

$$\mathrm{P} := \sum_{\substack{p\leqslant x\\ \varrho(p)\geqslant 1}}\Big(1-\frac{\lambda(p)}{\varrho(p)}\Big)\frac{1}{p}.$$

On peut supposer que $\mathrm{P}\geqslant 10$, sinon il n'y a rien à démontrer, et poser $z=x^{1/\mathrm{P}}$. Ci-dessous, on va factoriser tout $q\in\mathcal{Q}(x)$ comme $q=rs$ où tous les facteurs premiers de s sont inférieurs à z, et tous les facteurs premiers de r sont au-dessus de z. Ici les lettres r et s sont utilisées pour suggérer les parties "rugueuse" et "lisse" de q.[1]

Considérons d'abord la contribution des termes avec $s\leqslant x^{1/3}$. En appliquant le lemme 3.8 avec $\mathrm{H}=e^{\mathrm{P}}$, on obtient

$$\sum_{\substack{q=rs\in\mathcal{Q}(x)\\ s\leqslant x^{1/3}}}\mathrm{disc}(\Delta_{rs}) \ll \sum_{\substack{s\leqslant x^{1/3}\\ s\in\mathcal{Q}}}\frac{\mathrm{P}x}{\varphi(s)\log x}\Big(e^{-\mathrm{P}}+\mathrm{P}^n\prod_{p^v\|s}\Big(\frac{\sqrt{\lambda(p^v)}}{\sqrt{\varrho(p^v)}}+\frac{1}{p^v}\Big)\Big).$$

Notons que

$$\sum_{\substack{s\leqslant x^{1/3}\\ s\in\mathcal{Q}}}\frac{1}{\varphi(s)} \leqslant \prod_{p\leqslant z}\Big(1+\sum_{\substack{v\geqslant 1\\ p^v\in\mathcal{Q}}}\frac{1}{p^{v-1}(p-1)}\Big) \ll \prod_{\substack{p\leqslant z\\ p\in\mathcal{Q}}}\Big(1+\frac{1}{p-1}\Big) \ll \prod_{\substack{p\leqslant x\\ p\in\mathcal{Q}}}\Big(1+\frac{1}{p}\Big).$$

[1] Les lecteurs français pourraient utiliser la lettre f à la place de s (pour "friable") et c à la place de r (pour "criblé") dans la suite [2].

De plus, notons que

$$\sum_{\substack{s\leqslant x^{1/3}\\ s\in\mathcal{Q}}}\frac{1}{\varphi(s)}\prod_{p^v\| s}\Big(\frac{\sqrt{\lambda(p^v)}}{\sqrt{\varrho(p^v)}}+\frac{1}{p^v}\Big)\leqslant\prod_{p\leqslant z}\Big(1+\sum_{\substack{v\geqslant 1\\ p^v\in\mathcal{Q}}}\frac{1}{p^{v-1}(p-1)}\Big(\frac{\sqrt{\lambda(p^v)}}{\sqrt{\varrho(p^v)}}+\frac{1}{p^v}\Big)\Big)$$
$$\ll\prod_{\substack{p\leqslant z\\ p\in\mathcal{Q}}}\Big(1+\frac{1}{p-1}\Big(\frac{\sqrt{\lambda(p)}}{\sqrt{\varrho(p)}}+\frac{1}{p}\Big)\Big)\ll\prod_{\substack{p\leqslant x\\ p\in\mathcal{Q}}}\Big(1+\frac{1}{p}\frac{\sqrt{\lambda(p)}}{\sqrt{\varrho(p)}}\Big)$$
$$\ll\prod_{\substack{p\leqslant x\\ p\in\mathcal{Q}}}\Big(1+\frac{1}{p}\Big)\exp\Big(-\sum_{\substack{p\leqslant x\\ p\in\mathcal{Q}}}\Big(1-\frac{\sqrt{\lambda(p)}}{\sqrt{\varrho(p)}}\Big)\frac{1}{p}\Big),$$

et que, puisque $1-\sqrt{t}\geqslant(1-t)/2$ pour $0\leqslant t\leqslant 1$,

$$\sum_{\substack{p\leqslant x\\ p\in\mathcal{Q}}}\Big(1-\frac{\sqrt{\lambda(p)}}{\sqrt{\varrho(p)}}\Big)\frac{1}{p}\geqslant\frac{1}{2}\sum_{\substack{p\leqslant x\\ p\in\mathcal{Q}}}\Big(1-\frac{\lambda(p)}{\varrho(p)}\Big)\frac{1}{p}=\frac{\mathrm{P}}{2}.$$

On conclut que

$$\sum_{\substack{q=rs\in\mathcal{Q}(x)\\ s\leqslant x^{1/3}}}\mathrm{disc}(\Delta_{rs})\ll\frac{x}{\log x}\prod_{\substack{p\leqslant x\\ p\in\mathcal{Q}}}\Big(1+\frac{1}{p}\Big)\Big(\mathrm{P}e^{-\mathrm{P}}+\mathrm{P}^{n+1}e^{-\mathrm{P}/2}\Big)\ll|\mathcal{Q}(x)|\frac{e^{-\mathrm{P}/3}}{\alpha},\tag{10}$$

en utilisant le lemme 3.1 et en se rappelant que les constantes impliquées peuvent dépendre de n.

Maintenant considérons la contribution des termes $q=rs$ où $s>x^{1/3}$, de telle façon que $r\leqslant x^{2/3}$. En utilisant la borne évidente $\mathrm{disc}(\Delta_q)\leqslant 1$, on voit que de tels termes contribuent

$$\sum_{\substack{q=rs\in\mathcal{Q}(x)\\ s>x^{1/3}}}\mathrm{disc}(\Delta_q)\leqslant\sum_{\substack{r\leqslant x^{2/3}\\ r\in\mathcal{Q}}}\sum_{\substack{x^{1/3}<s\leqslant x/r\\ s\in\mathcal{Q}}}1.$$

En appliquant le lemme 3.2, cette quantité est

$$\ll\sum_{\substack{r\leqslant x^{2/3}\\ r\in\mathcal{Q}}}\frac{x/r}{\log x}\exp\Big(-\frac{\log(x/r)}{\log z}\Big)\prod_{\substack{p\leqslant z\\ p\in\mathcal{Q}}}\Big(1+\frac{1}{p}\Big)\ll\frac{x}{\log x}e^{-\mathrm{P}/3}\prod_{\substack{p\leqslant z\\ p\in\mathcal{Q}}}\Big(1+\frac{1}{p}\Big)\sum_{\substack{r\leqslant x^{2/3}\\ r\in\mathcal{Q}}}\frac{1}{r}$$
$$\ll\frac{x}{\log x}e^{-\mathrm{P}/3}\prod_{\substack{p\leqslant x\\ p\in\mathcal{Q}}}\Big(1+\frac{1}{p}\Big)\ll|\mathcal{Q}(x)|\frac{e^{-\mathrm{P}/3}}{\alpha},$$

où on a utilisé le lemme 3.1 dans la dernière étape. En combinant cette borne avec (10), on obtient le théorème 1.4, et donc également le théorème 1.2.

5. Le résultat technique principal

Dans cette section, on établit une estimation technique générale, à partir de laquelle les théorèmes les plus simples (mais les moins précis) 1.6 et 1.8 seront déduits dans la prochaine

section. En plus de $\mathcal{P}(x)$ (défini dans (5)), on utilisera la quantité

$$\widetilde{\mathcal{P}}(x) = \sum_{\substack{p\leqslant x\\ p\in\mathcal{Q}}} \frac{1}{p}\Big(\frac{\lambda(p)}{\varrho(p)}\Big)^{1/2} + 3. \tag{11}$$

Puisque $\lambda(p)\leqslant\varrho(p)$, notons que $\widetilde{\mathcal{P}}(x)\leqslant\mathcal{P}(x)$.

Proposition 5.1. *Supposons que l'assertion 1.1 soit vérifiée, et soit x grand en fonction de α et x_0.*

(1) *Dans le domaine $k\leqslant\mathcal{P}(x)$*

$$\frac{1}{|\mathcal{Q}_k(x)|}\sum_{q\in\mathcal{Q}_k(x)}\operatorname{disc}(\Delta_q) \ll \frac{k^{6+n}}{\alpha}\Big(\Big(\frac{\widetilde{\mathcal{P}}(x)}{\mathcal{P}(x)}\Big)^{\frac{k-1}{3}} + e^{-k/2}\Big(\frac{k}{\mathcal{P}(x)}\Big)^{\frac{k-1}{2}}\Big). \tag{12}$$

(2) *Dans le domaine $\mathcal{P}(x)<k\leqslant\exp(\sqrt{\log\log x})$*

$$\frac{1}{|\mathcal{Q}_k(x)|}\sum_{q\in\mathcal{Q}_k(x)}\operatorname{disc}(\Delta_q) \ll \frac{1}{\alpha}\exp\Big(\frac{(6+n)k\log k}{\mathcal{P}(x)}\Big)\Big(e^{-k/3} + \Big(\frac{\widetilde{\mathcal{P}}(x)}{\mathcal{P}(x)}\Big)^{\frac{k}{3(1+\log(k/\mathcal{P}(x)))}}\Big). \tag{13}$$

Posons $z=x^{1/(4k)}$ et factorisons $q\in\mathcal{Q}_k(x)$ de manière unique sous la forme $q=rs$, où tous les facteurs premiers de s sont $\leqslant z$ et tous les facteurs premiers de r sont $>z$. Ci-dessous, r et s seront toujours supposés avoir cette signification.

On se débarrasse d'abord d'un cas technique, quand $s>x^{\frac13}$. Puisque s a au plus k facteurs premiers qui sont tous inférieurs à $x^{1/(4k)}$, il s'ensuit que si on écrit $s=s_1s_2^2$ avec s_1 sans facteur carré, alors $s_1\leqslant x^{1/4}$ et $s_2>x^{1/12}$. Puisque $\operatorname{disc}(\Delta_q)\leqslant 1$ pour tout q, il s'ensuit que

$$\sum_{\substack{q\in\mathcal{Q}_k(x)\\ s>x^{1/3}}}\operatorname{disc}(\Delta_q) \ll \sum_{s>x^{1/3}}\frac{x}{s} \ll x^{\frac{11}{12}+\varepsilon} \tag{14}$$

pour tout $\varepsilon>0$. Ainsi la contribution de tels termes est négligeable comparée aux bornes qu'on recherche, et peut être oubliée. Par conséquent, on restreint notre attention aux termes avec $s\leqslant x^{1/3}$.

5.1. **Quand k est petit : preuve de la partie (1).** Dans ce cas $k\leqslant\mathcal{P}(x)$, de telle façon que $k\log k/\mathcal{P}(x)\leqslant\log k$, et le lemme 3.3, avec la formule de Stirling amène

$$|\mathcal{Q}_k(x)| \gg k^{-4}\frac{\alpha x}{\log x}\frac{\mathcal{P}(x)^{k-1}}{(k-1)!} \gg k^{-5}\frac{\alpha x}{\log x}\Big(\frac{e\mathcal{P}(x)}{k}\Big)^{k-1}. \tag{15}$$

Rappelons qu'on a la factorisation $q=rs$, que q a exactement k facteurs premiers, et que s est supposé être $\leqslant x^{1/3}$. Si $\omega(s)=k$ alors r doit être égal à 1, et $q=s\leqslant x^{\frac13}$. Puisqu'on a toujours $\operatorname{disc}(\Delta_q)\leqslant 1$, de tels termes contribuent à hauteur au plus de $x^{\frac13}$. Pour les termes restant quand $\omega(s)<k$, on applique pour chaque s les bornes provenant du lemme 3.8. Ainsi, en utilisant également (14), pour tout $\mathrm{H}\geqslant 2$,

$$\sum_{q\in\mathcal{Q}_k(x)}\operatorname{disc}(\Delta_q) \ll x^{\frac{11}{12}+\epsilon} + \frac{kx}{\log x}\sum_{\substack{s\in\mathcal{Q}(x^{1/3})\\ \omega(s)\leqslant k-1}}\frac{1}{\varphi(s)}\Big(\frac{1}{\mathrm{H}} + (\log\mathrm{H})^n\prod_{p^v\| s}\Big(\frac{\sqrt{\lambda(p^v)}}{\sqrt{\varrho(p^v)}}+\frac{1}{p^v}\Big)\Big). \tag{16}$$

Observons que

$$\sum_{\substack{s\in\mathcal{Q}(x^{1/3})\\ \omega(s)\leqslant k-1}}\frac{1}{\varphi(s)}\leqslant\sum_{j=0}^{k-1}\frac{1}{j!}\Big(\sum_{\substack{p\in\mathcal{Q}\\ p\leqslant z}}\frac{1}{p-1}+\sum_{\substack{p\leqslant z\\ v\geqslant 2}}\frac{1}{p^{v-1}(p-1)}\Big)^j\leqslant\sum_{j=0}^{k-1}\frac{1}{j!}\mathcal{P}(x)^j,$$

en sommant selon le nombre j de facteurs premiers de s. De façon similaire

$$\sum_{\substack{s\in\mathcal{Q}(x^{1/3})\\ \omega(s)\leqslant k-1}}\frac{1}{\varphi(s)}\prod_{p^v\| s}\Big(\frac{\sqrt{\lambda(p^v)}}{\sqrt{\varrho(p^v)}}+\frac{1}{p^v}\Big)\leqslant\sum_{j=0}^{k-1}\frac{1}{j!}\Big(\sum_{\substack{p\in\mathcal{Q}\\ p\leqslant z}}\frac{1}{p-1}\Big(\frac{\sqrt{\lambda(p)}}{\sqrt{\varrho(p)}}+\frac{1}{p}\Big)+\sum_{\substack{p\leqslant z\\ v\geqslant 2}}\frac{1}{\varphi(p^v)}\Big(1+\frac{1}{p^v}\Big)\Big)^j$$

$$\leqslant\sum_{j=0}^{k-1}\frac{1}{j!}\widetilde{\mathcal{P}}(x)^j.$$

Par conséquent, à partir de (16), il s'ensuit que

$$\sum_{q\in\mathcal{Q}_k(x)}\operatorname{disc}(\Delta_q)\ll x^{\frac{11}{12}+\varepsilon}+\frac{kx}{\log x}\sum_{j=0}^{k-1}\Big(\frac{1}{\mathrm{H}}\frac{\mathcal{P}(x)^j}{j!}+(\log\mathrm{H})^n\frac{\widetilde{\mathcal{P}}(x)^j}{j!}\Big)$$

pour tout $\varepsilon>0$. On choisit ici $\mathrm{H}=(1+\mathcal{P}(x)/\widetilde{\mathcal{P}}(x))^k$ de telle façon que pour tout $0\leqslant j\leqslant k-1$ on a $\mathcal{P}(x)^j/\mathrm{H}\leqslant\widetilde{\mathcal{P}}(x)^j$. En notant que

$$(\log\mathrm{H})^n=\Big(k\log\Big(1+\frac{\mathcal{P}(x)}{\widetilde{\mathcal{P}}(x)}\Big)\Big)^n\ll k^n\Big(\frac{\mathcal{P}(x)}{\widetilde{\mathcal{P}}(x)}\Big)^{\frac{1}{10}},$$

on conclut que

$$\sum_{q\in\mathcal{Q}_k(x)}\operatorname{disc}(\Delta_q)\ll\frac{k^{1+n}x}{\log x}\Big(\frac{\mathcal{P}(x)}{\widetilde{\mathcal{P}}(x)}\Big)^{\frac{1}{10}}\sum_{j=0}^{k-1}\frac{\widetilde{\mathcal{P}}(x)^j}{j!},\tag{17}$$

où le terme $x^{\frac{11}{12}+\varepsilon}$ a été absorbé dans la quantité plus grande écrite ci-dessus (pour ε suffisamment petit).

Supposons d'abord que $k\leqslant 2\widetilde{\mathcal{P}}(x)-1$. Dans le domaine $0\leqslant j\leqslant k-1$, la quantité $\widetilde{\mathcal{P}}(x)^j/j!$ atteint son maximum en un certain j_0 qui appartient au domaine $k-1\geqslant j_0\geqslant(k-1)/2$. Notons que, puisque $k\leqslant\mathcal{P}(x)$

$$\frac{\widetilde{\mathcal{P}}(x)^{j_0}}{j_0!}\frac{(k-1)!}{\mathcal{P}(x)^{k-1}}\leqslant\frac{\widetilde{\mathcal{P}}(x)^{j_0}}{j_0!}\frac{j_0!}{\mathcal{P}(x)^{j_0}}\leqslant\Big(\frac{\widetilde{\mathcal{P}}(x)}{\mathcal{P}(x)}\Big)^{\frac{k-1}{2}}.$$

En combinant cela avec (15) et (17), on conclut que dans le domaine de k,

$$\sum_{q\in\mathcal{Q}_k(x)}\operatorname{disc}(\Delta_q)\ll|\mathcal{Q}_k(x)|\frac{k^{6+n}}{\alpha}\Big(\frac{\mathcal{P}(x)}{\widetilde{\mathcal{P}}(x)}\Big)^{\frac{1}{10}}\Big(\frac{\widetilde{\mathcal{P}}(x)}{\mathcal{P}(x)}\Big)^{\frac{k-1}{2}}\ll|\mathcal{Q}_k(x)|\frac{k^{6+n}}{\alpha}\Big(\frac{\widetilde{\mathcal{P}}(x)}{\mathcal{P}(x)}\Big)^{\frac{k-1}{3}}.\tag{18}$$

Supposons maintenant que $\mathcal{P}(x)\geqslant k\geqslant 2\widetilde{\mathcal{P}}(x)-1$. Ici, on note que la somme sur j dans (17) est $\leqslant\exp(\widetilde{\mathcal{P}}(x))\ll e^{(k-1)/2}$. De plus, puisque $\widetilde{\mathcal{P}}(x)\geqslant 2$,

$$e^{(k-1)/2}\Big(\frac{\mathcal{P}(x)}{\widetilde{\mathcal{P}}(x)}\Big)^{\frac{1}{10}}\Big(\frac{k}{e\mathcal{P}(x)}\Big)^{k-1}\leqslant k^{\frac{1}{10}}e^{-(k-1)/2}\Big(\frac{k}{\mathcal{P}(x)}\Big)^{k-1-\frac{1}{10}}.$$

En combinant ces observations avec (15) et (17), on trouve que dans le domaine de k,

$$\sum_{q\in\mathcal{Q}_k(x)} \mathrm{disc}(\Delta_q) \ll |\mathcal{Q}_k(x)|\frac{k^{6+n}}{\alpha}e^{-k/2}\Big(\frac{k}{\mathcal{P}(x)}\Big)^{\frac{k-1}{2}}. \tag{19}$$

Les estimations (18) et (19) établissent la partie (1) de la Proposition 5.1.

5.2. **Quand k est grand : preuve de la partie (2).** Supposons que $\mathcal{P}(x) < k \leqslant \exp(\sqrt{\log\log x})$. Soit $\kappa \leqslant k/3$ un paramètre que l'on fixera ultérieurement. Pour les termes $q = rs$ avec $\omega(r) \geqslant \kappa$, notons que $\mathrm{disc}(\Delta_q) \leqslant 1$ trivialement, et que le lemme 3.4 donne une borne sur le nombre de tels termes. Ainsi

$$\begin{aligned}\sum_{\substack{q\in\mathcal{Q}_k(x)\\ \omega(r)\geqslant\kappa}} \mathrm{disc}(\Delta_q) \leqslant \sum_{\substack{q\in\mathcal{Q}_k(x)\\ \omega(r)\geqslant\kappa}} 1 &\ll \frac{kx}{\log x}\frac{\mathcal{P}(x)^{k-1}}{(k-1)!}\exp\Big(\frac{2k\log k}{\mathcal{P}(x)} - \kappa\Big)\\ &\ll |\mathcal{Q}_k(x)|\frac{1}{\alpha}\exp\Big(\frac{7k\log k}{\mathcal{P}(x)} - \kappa\Big),\end{aligned}$$

où on a utilisé la borne inférieure pour $|\mathcal{Q}_k(x)|$ provenant du lemme 3.3, et le fait que $k \geqslant \mathcal{P}(x)$.

D'un autre côté, on estime les contributions de ces q pour lesquels $\omega(r) < \kappa$ en utilisant le lemme 3.8 exactement comme dans l'argument amenant à (17), avec le même choix de H que précédemment. Ainsi

$$\sum_{\substack{q\in\mathcal{Q}_k(x)\\ \omega(r)<\kappa}} \mathrm{disc}(\Delta_q) \ll \frac{k^{1+n}x}{\log x}\Big(\frac{\mathcal{P}(x)}{\widetilde{\mathcal{P}}(x)}\Big)^{\frac{1}{10}}\sum_{j=k-\kappa}^{k-1}\frac{\widetilde{\mathcal{P}}(x)^j}{j!}.$$

Maintenant pour chaque $k-\kappa \leqslant j \leqslant k-1$ notons que, puisque $\kappa \leqslant k/3$,

$$\frac{\widetilde{\mathcal{P}}(x)^j}{j!}\frac{(k-1)!}{\mathcal{P}(x)^{k-1}} \leqslant \Big(\frac{\widetilde{\mathcal{P}}(x)}{\mathcal{P}(x)}\Big)^j\Big(\frac{k}{\mathcal{P}(x)}\Big)^{k-1-j} \leqslant \Big(\frac{\widetilde{\mathcal{P}}(x)}{\mathcal{P}(x)}\Big)^{\frac{2k}{3}}\Big(\frac{k}{\mathcal{P}(x)}\Big)^{\kappa}.$$

Il s'ensuit que

$$\begin{aligned}\sum_{\substack{q\in\mathcal{Q}_k(x)\\ \omega(r)<\kappa}} \mathrm{disc}(\Delta_q) &\ll \frac{k^{2+n}x}{\log x}\frac{\mathcal{P}(x)^{k-1}}{(k-1)!}\Big(\frac{\widetilde{\mathcal{P}}(x)}{\mathcal{P}(x)}\Big)^{\frac{k}{2}}\Big(\frac{k}{\mathcal{P}(x)}\Big)^{\kappa}\\ &\ll |\mathcal{Q}_k(x)|\frac{k^{2+n}}{\alpha}\exp\Big(\frac{4k\log k}{\mathcal{P}(x)}\Big)\Big(\frac{\widetilde{\mathcal{P}}(x)}{\mathcal{P}(x)}\Big)^{\frac{k}{2}}\Big(\frac{k}{\mathcal{P}(x)}\Big)^{\kappa}.\end{aligned}$$

Rassemblant les bornes dans les deux cas $\omega(r) \geqslant \kappa$ et $\omega(r) < \kappa$, on conclut que

$$\sum_{q\in\mathcal{Q}_k(x)} \mathrm{disc}(\Delta_q) \ll \frac{|\mathcal{Q}_k(x)|}{\alpha}\exp\Big(\frac{(6+n)k\log k}{\mathcal{P}(x)}\Big)\Big(\exp(-\kappa) + \Big(\frac{\widetilde{\mathcal{P}}(x)}{\mathcal{P}(x)}\Big)^{\frac{k}{2}}\Big(\frac{k}{\mathcal{P}(x)}\Big)^{\kappa}\Big). \tag{20}$$

Choisissons

$$\kappa = \min\Big(\frac{k}{3}, \frac{k}{3(1+\log(k/\mathcal{P}(x)))}\log\frac{\mathcal{P}(x)}{\widetilde{\mathcal{P}}(x)}\Big).$$

Un petit calcul nous autorise alors à borner le côté droit de (20) par

$$\ll \frac{|\mathcal{Q}_k(x)|}{\alpha} \exp\Big(\frac{(6+n)k\log k}{\mathcal{P}(x)}\Big)\Big(e^{-k/3} + \Big(\frac{\widetilde{\mathcal{P}}(x)}{\mathcal{P}(x)}\Big)^{\frac{k}{3(1+\log(k/\mathcal{P}(x)))}}\Big).$$

Cela complète la preuve de (13), et donc celle de la proposition 5.1.

6. Preuve des théorèmes 1.6 et 1.8

6.1. **Preuve du théorème 1.6.** À partir de la supposition (1) du théorème 1.6, et puisque $1-\sqrt{t} \geqslant (1-t)/2$ pour $0 \leqslant t \leqslant 1$, il découle que

$$\mathcal{P}(x) - \widetilde{\mathcal{P}}(x) = \sum_{\substack{p\leqslant x\\ p\in\mathcal{Q}}} \Big(1 - \frac{\sqrt{\lambda(p)}}{\sqrt{\varrho(p)}}\Big)\frac{1}{p} \geqslant \frac{1}{2}\sum_{\substack{p\leqslant x\\ p\in\mathcal{Q}}} \Big(1-\frac{\lambda(p)}{\varrho(p)}\Big)\frac{1}{p} \geqslant \frac{\delta}{2}\log\log x.$$

Puisque $\mathcal{P}(x) \leqslant \log\log x + \mathrm{O}(1)$, on conclut que

$$\frac{\widetilde{\mathcal{P}}(x)}{\mathcal{P}(x)} \leqslant 1 - \frac{\delta\log\log x}{2\mathcal{P}(x)} \leqslant 1 - \frac{\delta}{3} \leqslant e^{-\delta/3}.$$

Dans le domaine $k \leqslant \mathcal{P}(x)$, la partie (1) de la proposition 5.1 donne maintenant

$$\frac{1}{|\mathcal{Q}_k(x)|}\sum_{q\in\mathcal{Q}_k(x)} \mathrm{disc}(\Delta_q) \ll \frac{k^{6+n}}{\alpha}e^{-k\delta/9} \ll \frac{1}{\alpha}e^{-k\delta/18},$$

où la dernière étape s'ensuit parce que $k \geqslant 20\delta^{-1}(6+n)\log(20\delta^{-1}(6+n))$.

Dans le domaine

$$\mathcal{P}(x) < k \leqslant \exp\Big(\Big(\frac{\alpha\delta\log\log x}{20(6+n)}\Big)^{1/2}\Big),$$

on utilise la partie (2) de la proposition 5.1. Puisque $\mathcal{P}(x) \geqslant \alpha\log\log x + \mathrm{O}(1)$, la borne supérieure sur k amène

$$\exp\Big(\frac{(6+n)k\log k}{\mathcal{P}(x)}\Big) \ll \exp\Big(\frac{\delta}{18}\frac{k}{(1+\log(k/\mathcal{P}(x)))}\Big),$$

et ainsi la partie (2) donne

$$\begin{aligned}\frac{1}{|\mathcal{Q}_k(x)|}\sum_{q\in\mathcal{Q}_k(x)} \mathrm{disc}(\Delta_q) &\ll \frac{1}{\alpha}\exp\Big(\frac{(6+n)k\log k}{\mathcal{P}(x)}\Big)\Big(e^{-k/3} + \big(e^{-\delta/3}\big)^{\frac{k}{3(1+\log(k/\mathcal{P}(x)))}}\Big)\\ &\ll \frac{1}{\alpha}\exp\Big(-\frac{\delta k}{18(1+\log(k/\mathcal{P}(x)))}\Big) \ll \frac{1}{\alpha}(\log x)^{-\alpha\delta/18},\end{aligned}$$

où la dernière étape s'ensuit parce que $k/(1+\log(k/\mathcal{P}(x))) \geqslant \mathcal{P}(x) \geqslant \alpha\log\log x + \mathrm{O}(1)$. Cela complète la preuve du théorème 1.6.

6.2. **Preuve du théorème 1.8.** Par l'inégalité de Cauchy-Schwarz et la supposition (2) dans le théorème 1.8, on voit que

$$\sum_{\substack{p\leqslant x\\ p\in\mathcal{Q}}}\frac{1}{p}\frac{\sqrt{\lambda(p)}}{\sqrt{\varrho(p)}}\leqslant\Big(\sum_{\substack{p\leqslant x\\ p\in\mathcal{Q}}}\frac{1}{p}\Big)^{\frac12}\Big(\sum_{\substack{p\leqslant x\\ p\in\mathcal{Q}}}\frac{1}{p}\frac{\lambda(p)}{\varrho(p)}\Big)^{\frac12}\leqslant\sqrt{\delta}\sum_{\substack{p\leqslant x\\ p\in\mathcal{Q}}}\frac{1}{p}.$$

Par conséquent, avec la notation de la proposition 5.1

$$\frac{\widetilde{\mathcal{P}}(x)}{\mathcal{P}(x)}\leqslant\sqrt{\delta}+\mathrm{O}\Big(\frac{1}{\alpha\log\log x}\Big)\leqslant\delta^{1/3},$$

en utilisant le fait que $\mathcal{P}(x)\geqslant\alpha\log\log x+\mathrm{O}(1)$ et que x est grand par rapport à α, alors que $\delta\geqslant 1/\log\log x$ (par la supposition à nouveau). Maintenant la partie (1) de la proposition 5.1 implique que pour $k\leqslant\alpha\delta\log\log x+\mathrm{O}(1)$ on a

$$\frac{1}{|\mathcal{Q}_k(x)|}\sum_{q\in\mathcal{Q}_k(x)}\mathrm{disc}(\Delta_q)\ll\frac{k^{6+n}}{\alpha}\Big(\delta^{(k-1)/9}+e^{-k/2}\delta^{(k-1)/2}\Big)\ll\frac{1}{\alpha}\delta^{(k-1)/10},$$

ce qui établit le théorème 1.8.

7. Remarques sur les sommes exponentielles

La méthode décrite ci-dessus doit être placée dans un contexte plus général comme suit. Supposons que soit donnée une fonction V qui associe à chaque nombre premier p et à chaque classe de restes $a \pmod p$ un nombre complexe $\mathrm{V}(a;p)$. Étendre cela à une fonction $\mathrm{V}(a;q)$ où q est sans facteur carré et $a \pmod q$ est une classe de restes par "multiplicativité twistée" : c'est-à-dire, si $q=q_1q_2$ avec $(q_1,q_2)=1$ alors

$$\mathrm{V}(a;q_1q_2)=\mathrm{V}(a\bar{q_1};q_2)\mathrm{V}(a\bar{q_2};q_1). \tag{21}$$

Supposons que $\mathrm{V}(a;q)=0$ si q n'est pas sans facteur carré, ou si $(a,q)>1$. Pour tout nombre premier p, soit $\mathrm{G}(p)\geqslant 0$ tel que

$$\max_{(a,p)=1}|\mathrm{V}(a,p)|\leqslant\mathrm{G}(p), \tag{22}$$

Étendons G à tous les entiers sans facteur carré en utilisant la multiplicativité. Le problème est alors d'obtenir une borne pour

$$\sum_{q\leqslant x}|\mathrm{V}(a;q)|$$

(pour un entier fixé $a\geqslant 1$) qui soit meilleure que la borne triviale

$$\sum_{q\leqslant x}|\mathrm{V}(a;q)|\leqslant\sum_{q\leqslant x}\mathrm{G}(q).$$

Remarque 7.1. *Notre travail dans le théorème 1.4 s'adapte à ce cadre en prenant pour* $\mathrm{V}(a,p)$ *les sommes de Weyl normalisées* $\mathrm{W}(ah;p)$ *pour un certain* h *non nul fixé. La multiplicativité twistée* (21) *a été établie dans la partie (1) du lemme 3.5.*

Une autre classe très naturelle d'exemples s'adaptant bien à ce cadre généralisé proviennent des sommes exponentielles. Soient f_1 et f_2 des monômes entiers, avec f_2 non nul. Pour tout nombre sans facteur carré q, on définit $\mathrm{V}(a;q) = 0$ s'il existe $p \mid q$ tel que $f_2 = 0 \pmod p$, et sinon, on pose

$$\mathrm{V}(a;q) = \frac{1}{\sqrt{q}} \sum_{\substack{n \pmod q \\ f_2(n)\neq 0}} e\Big(\frac{a f_1(n)\overline{f_2(n)}}{q}\Big).$$

Ceux-ci satisfont la relation (21). En utilisant les estimations de Weil pour les sommes exponentielles additives modulo des nombres premiers, on peut prendre $\mathrm{G}(p) = c_{f_1,f_2}$ pour une certaine constante entière dépendant seulement du degré et du nombre de zéros de f_1 et f_2 (en particulier indépendante de p).

Le problème de l'obtention d'estimations non triviales pour

$$\sum_{q\leqslant x} |\mathrm{V}(1;q)|$$

dans ce cas a déjà été traité en profondeur par Fouvry et Michel [6], et le cas particulier des sommes de Kloosterman (notamment, $f_1 = \mathrm{X}^2 + 1$ et $f_2 = \mathrm{X}$) est brièvement mentionné par Hooley [10, §3]. On peut étendre certains aspects du travail de Fouvry et Michel, mais comme ceci est d'une nature différente du présent article, on diffère des considérations plus approfondies à ce sujet pour une autre note [13].

Appendix A. Conjectures modulo des modules premiers et un analogue pour les corps de fonctions

Comme cela a été évoqué dans l'introduction, un des problèmes motivant est celui de la distribution des racines des congruences polynomiales selon des modules premiers. Cela peut être interprété de (au moins) deux manières, dépendant du fait que l'on utilise les mêmes mesures que dans le théorème 1.2, ou bien les mesures de Hooley comme dans la section 2.2. Pour des raisons de complétude, on énonce formellement deux conjectures potentielles (qui sont vraisemblablement l'une et l'autre correctes), et on discute d'un analogue pour les corps de fonctions qui semble indiquer que, dans ce cas, les mesures de Hooley sont dans un certain sens plus naturelles.

Soit $f \in \mathbf{Z}[\mathrm{X}]$ un monôme irréductible de degré $\geqslant 2$, et soit $\Pi_f(x)$ l'ensemble des nombres premiers $p \leqslant x$ tels que le nombre $\varrho_f(p)$ des racines de f modulo p est au moins égal à 1. Soit Δ_p la mesure de probabilité habituelle sur l'ensemble des racines de f modulo p.

La première conjecture, analogue à la forme qualitative du théorème 1.2, est :

Conjecture A.1. *Soit $f \in \mathbf{Z}[\mathrm{X}]$ un monôme irréductible de degré $\geqslant 2$. Alors les mesures*

$$\frac{1}{|\Pi_f(x)|} \sum_{\substack{p\leqslant x \\ p\in\mathcal{Q}}} \Delta_p$$

convergent vers la mesure uniforme lorsque $x \to +\infty$.

Notons que $|\Pi_f(x)| \sim c\pi(x)$ pour une certaine constante $c > 0$, notamment la proportion d'éléments du groupe de Galois du corps de décomposition de f qui a un point fixe, quand on le voit comme des permutations des n racines de f.

En utilisant les mesures de Hooley, la conjecture naturelle (énoncée dans [4] par exemple) est :

Conjecture A.2. *Soit $f \in \mathbf{Z}[\mathrm{X}]$ un monôme irréductible de degré $\geqslant 2$. Alors les mesures*

$$\frac{1}{\pi(x)} \sum_{\substack{p \leqslant x \\ p \in \Omega}} \varrho_f(p) \Delta_p$$

convergent vers la mesure uniforme.

Ici la normalisation par $\pi(x)$ est asymptotiquement correcte, et elle correspond au fait que le nombre moyen de points fixes d'un groupe de permutation transitive est 1.

Remarque A.3. *Hrushovski a également demandé* [11, §4.4] *si les parties fractionnaires des racines des congruences polynomiales équidistribuées modulo les nombres premiers p se restreignaient à avoir $\varrho_f(p)$ égal à un entier fixé $r \geqslant 2$, dans le cas où le groupe de Galois du corps de décomposition de f était cyclique. La version modulo tous les q sans facteur carré découle facilement du théorème 1.4, pour tout f et tout $r \geqslant 2$ tels que le groupe de Galois du corps de décomposition contient au moins une permutation qui a r points fixes quand il agit sur les racines complexes de f.*

Pour déterminer laquelle des deux conjectures est la plus naturelle, on regarde l'analogue dans les corps de fonctions.

Soit $f \in \mathbf{Z}[\mathrm{X}, \mathrm{Y}]$ un polynôme qui est irréductible dans $\mathbf{C}[\mathrm{X}, \mathrm{Y}]$, de degré $\geqslant 2$ selon Y et $\geqslant 1$ selon X.

Pour tout nombre p suffisamment grand, la réduction de f modulo p sera absolument irréductible dans $\mathbf{F}_p[\mathrm{X}, \mathrm{Y}]$; ci-dessous on ne considère que de tels nombres premiers.

Un analogue du fait de regarder les nombres premiers $\leqslant x$ consiste à considérer les polynômes irréductibles π dans $\mathbf{F}_p[\mathrm{X}]$ de degré borné. Les racines d'une congruence polynomiale modulo un nombre premier donné correspondent alors aux racines dans $k = \mathbf{F}_p[\mathrm{X}]/\pi\mathbf{F}_p[\mathrm{X}]$ du polynôme $f \pmod{\pi}$, vu comme un élément de $k[\mathrm{Y}]$.

Pour simplifier la discussion, on regardera les polynômes π de degré 1, i.e., $\pi = \mathrm{X} - x$ pour $x \in \mathbf{F}_p$, mais on posera alors $p \to +\infty$ (c'est possible puisqu'on a commencé avec un polynôme $f \in \mathbf{Z}[\mathrm{X}, \mathrm{Y}]$). Alors, pour un $\pi = \mathrm{X} - x$ donné, on regarde les racines y de $f \pmod{\pi}$ qui appartiennent à $\mathbf{F}_p[\mathrm{X}]/(\mathrm{X} - x)\mathbf{F}_p[\mathrm{X}] \simeq \mathbf{F}_p$, i.e., on regarde les $y \in \mathbf{F}_p$ tels que $f(x, y) = 0 \in \mathbf{F}_p$.

Maintenant les sommes de Weyl à considérer pour l'analogue de la conjecture A.1 sont

$$\frac{1}{\mathrm{Z}_p} \sum_{\substack{x \in \mathbf{F}_p \\ \mathrm{C}_x \neq \varnothing}} \frac{1}{|\mathrm{C}_x|} \sum_{\substack{y \in \mathbf{F}_p \\ f(x,y)=0}} e\Big(\frac{hy}{p}\Big), \tag{23}$$

où

$$\mathrm{C}_x = \{y \in \mathbf{F}_p \mid f(x, y) = 0\},$$
$$\mathrm{Z}_p = |\{x \in \mathbf{F}_p \mid \mathrm{C}_x \neq \varnothing\}|,$$

et celles pour l'analogue de la conjecture A.2 sont

$$\frac{1}{p} \sum_{x \in \mathbf{F}_p} \sum_{\substack{y \in \mathbf{F}_p \\ f(x,y)=0}} e\Big(\frac{hy}{p}\Big), \tag{24}$$

toutes pour $h \in \mathbf{Z}$ non nul (c'est une conséquence de l'hypothèse de Riemann pour les courbes sur les corps finis que p est asymptotiquement la normalisation correcte ici ; cela dépend du fait que f est absolument irréductible).

Comme cela s'avère être le cas, les sommes dans (24) convergent vers 0 lorsque $p \to +\infty$ essentiellement sans condition supplémentaire, et celles dans (23) le font aussi au moins de manière générale, mais l'argument est moins évident dans ce cas.

Convergence de (24). C'est un fait standard (voir e.g. [8]) que si f a un degré $\geqslant 2$ par rapport à Y, alors lorsque $p \to +\infty$, les parties fractionnaires $(\{x/p\}, \{y, p\}) \in (\mathbf{R}/\mathbf{Z})^2$ des points $(x, y) \in \mathrm{C}(\mathbf{F}_p)$ de la courbe plane algébrique définie par l'équation $f(x, y) = 0$ deviennent équidistribuées selon la mesure uniforme, et de plus, l'hypothèse de Riemann pour les courbes implique que

$$|\mathrm{C}(\mathbf{F}_p)| = p + \mathrm{O}(p^{1/2})$$

lorsque $p \to +\infty$. Cela implique (plus que) la convergence vers 0 des sommes de Weyl dans (24).

Convergence de (23). On décompose la somme selon la valeur de $|\mathrm{C}_x|$, qui est un entier $\leqslant d = \deg_{\mathrm{Y}}(f)$. On obtient

$$\frac{1}{\mathrm{Z}_p} \sum_{\substack{x \in \mathbf{F}_p \\ \mathrm{C}_x \neq \varnothing}} \frac{1}{|\mathrm{C}_x|} \sum_{\substack{y \in \mathbf{F}_p \\ f(x,y)=0}} e\Big(\frac{hy}{p}\Big) = \frac{1}{\mathrm{Z}_p} \sum_{1 \leqslant k \leqslant d} \frac{1}{k} \sum_{\substack{x \in \mathbf{F}_p \\ |\mathrm{C}_x|=k}} \sum_{\substack{y \in \mathbf{F}_p \\ f(x,y)=0}} e\Big(\frac{hy}{p}\Big).$$

Fixons k. La fonction caractéristique φ_k de l'ensemble des $x \in \mathbf{F}_p$ tels que $|\mathrm{C}_x| = k$ peut être représentée sous la forme

$$\varphi_k(x) = \sum_{j \in \mathrm{J}} \alpha(k, j) t_j(x; p)$$

où J est un ensemble fini et $\alpha(k, j)$ sont des coefficients complexes, tous étant indépendants de p, et où $t_j(x; p)$ est une fonction de trace modulo p du conducteur borné en fonction de f seulement (plus précisément, cette formule est vérifiée pour tout x excepté pour un nombre de valeurs exceptionnelles en nombre potentiellement borné où le recouvrement $\pi \colon \mathrm{C} \to \mathbf{A}^1$ donné par $(x, y) \to x$ est ramifié, et est obtenu à partir de la théorie de Galois, l'ensemble J étant l'ensemble des représentations irréductibles du groupe de Galois $\mathrm{G}_\pi \subset \mathrm{S}_d$ de π, et les $\alpha(k, j)$ les coefficients de Fourier de la fonction caractéristique de ces $\sigma \in \mathrm{G}_\pi$ avec précisément k points fixes ; voir, e.g., [5, §10.2] pour des calculs similaires). Par conséquent

$$\sum_{\substack{x \in \mathbf{F}_p \\ |\mathrm{C}_x|=k}} \sum_{\substack{y \in \mathbf{F}_p \\ f(x,y)=0}} e\Big(\frac{hy}{p}\Big) = \sum_{j \in \mathrm{J}} \alpha(k, j) \sum_{x \in \mathbf{F}_p} t_j(x; p) \sum_{\substack{y \in \mathbf{F}_p \\ f(x,y)=0}} e\Big(\frac{hy}{p}\Big) + \mathrm{O}(1).$$

Mais la fonction

$$g(x) = \sum_{\substack{y \in \mathbf{F}_p \\ f(x,y)=0}} e\Big(\frac{hy}{p}\Big)$$

est elle-même une fonction de trace avec conducteur borné en fonction de f seulement, et de plus elle est lisse et pure de poids 1 sur un sous-ensemble ouvert dense de $\mathbf{A}^1$.

Maintenant, notons que pour p suffisamment grand, toutes les fonctions de trace t_j sont associées aux faisceaux qui sont partout correctement ramifiés (voir à nouveau [5, §10.2]).

D'un autre côté, si on suppose que f est un monôme de X, alors on peut vérifier[3] que pour p suffisamment grand, la représentation de monodromie à l'infini du faisceau sous-tendant g est totalement "sauvagement" ramifié. Par conséquent, aucun composant géométriquement irréductible de g ne peut alors être géométriquement isomorphe aux fonctions de trace t_j. En appliquand alors l'hypothèse de Riemann sur les corps finis (dans une forme comme [12, Prop. 1.8]), on a

$$\sum_{x\in\mathbf{F}_p} t_j(x;p)g(x) \ll p^{1/2},$$

où la constante impliquée dépend seulement de f (parce que les conducteurs de t_j et g sont bornés en fonction de f).

Un argument similaire utilisant l'hypothèse de Riemann montre que $\mathrm{Z}_p \gg p$ lorsque $p \to +\infty$, et par conséquent, on en déduit (génériquement du moins) que les sommes (23) tendent vers 0 lorsque $p \to +\infty$.

Remarque A.4. *La condition que f soit un monôme en* X *est quelque peu restrictive, et la convergence de (23) vers* 0 *peut être généralisée à d'autres classes variées de polynômes. Puisque notre but est d'illustrer la différence entre les deux types de sommes, nous ne tentons pas de discuter de situations plus générales ici.*

Références

[1] V. Crişan, P. Pollack: *The smallest root of a polynomial congruence*, à paraître dans Math. Res. Letters.

[2] C. Dartyge, G. Martin: *Exponential sums with reducible polynomials*, Discrete Analysis 2019:15, doi:10.19086/da.10793

[3] R. de la Bretèche, G. Tenenbaum: *Sur la conjecture de Manin pour certaines surfaces de Châtelet*, Journal Inst. Math. Jussieu 12 (2013), 759–819.

[4] W. Duke, J. Friedlander, H. Iwaniec : *Equidistribution of roots of a quadratic congruence to prime moduli*, Ann. of Math. 141 (1995), 423–441.

[5] É. Fouvry, E. Kowalski, Ph. Michel: *Algebraic twists of modular forms and Hecke orbits*, Geom. Funct. Anal. 25 (2015), 580–657; doi:10.1007/s00039-015-0310-2.

[6] É. Fouvry, Ph. Michel: *Sommes de modules de sommes exponentielles*, Pacific J. of Math. 209 (2003), 261–288.

[7] A. Granville, P. Kurlberg: *Poisson statistics via the Chinese Remainder Theorem*, Adv. Math. 218 (2008), 2013–2042.

[8] A. Granville, I. Shparlinski, A. Zaharescu: *On the distribution of rational functions along a curve over $\mathbf{F}_p$ and residue races*, J. Number Theory 112 (2005), 216–237.

[9] R.R. Hall: *On pseudo-polynomials*, Mathematika 18 (1971), 71–77.

[10] C. Hooley: *On the distribution of the roots of polynomial congruences*, Mathematika 11 (1964), 39–49.

[11] E. Hrushovski: *Ax's theorem with an additive character*, https://arxiv.org/abs/1911.01096.

[12] E. Kowalski, Ph. Michel, W. Sawin: *Stratification and averaging for exponential sums: bilinear forms with generalized Kloosterman sums*, Annali Scuola Normale Sup. Pisa, à paraître.

[13] E. Kowalski, K. Soundararajan: *A note on a result of Fouvry and Michel*, en préparation.

[14] V. Kuperberg: *A note on pseudo-polynomials divisible only by a sparse set of primes*, https://arxiv.org/abs/2006.02527.

[15] G. Martin, S. Sitar: *Erdös–Turán with a moving target, equidistribution of roots of reducible quadratics and diophantine quadruples*, Mathematika, 57 (2011), 1–29.

[16] A. Tóth : *Roots of quadratic congruences*, Internat. Math. Res. Notices 2000, 719–739.

[3] On remercie W. Sawin d'avoir clarifié cet argument.