Equidistribution problems of squarefree numbers

Ramon Moreira Nunes

UNIVERSITÉ PARIS-SUD

École doctorale 142 :
Mathématiques de la région Paris-Sud

Laboratoire de Mathématiques d'Orsay

THESE DE DOCTORAT

MATHÉMATIQUES

par

Ramon MOREIRA NUNES

Problèmes d'équirépartition des entiers sans facteur carré

Soutenue le 29 juin 2015 devant la Commission d'examen:

M.	Régis de la Bretèche	(Rapporteur)
M.	Antoine Chambert-Loir	(Examinateur)
M.	Étienne Fouvry	(Directeur de thèse)
M.	Joël Rivat	(Examinateur)
M.	Emmanuel Royer	(Examinateur)

Rapporteur absent le jour de la soutenance :

M. Timothy Browning

Thèse préparée au
Département de Mathématiques d'Orsay
Laboratoire de Mathématiques (UMR 8628), Bât. 425
Université Paris-Sud 11
91 405 Orsay CEDEX

Résumé

Cette thèse concerne quelques problèmes liés à la répartition des entiers sans facteur carré dans les progressions arithmétiques. Ces problèmes s'expriment en termes de majorations du terme d'erreur associé à cette répartition.

Les premier, deuxième et quatrième chapitres sont concentrés sur l'étude statistique des termes d'erreur quand on fait varier la progression arithmétique modulo q. En particulier on obtient une formule asymptotique pour la variance et des majorations non triviales pour les moments d'ordre supérieur. On fait appel à plusieurs techniques de théorie analytique des nombres comme les méthodes de crible et les sommes d'exponentielles, notamment une majoration récente pour les sommes d'exponentielles courtes due à Bourgain dans le deuxième chapitre.

Dans le troisième chapitre on s'intéresse à estimer le terme d'erreur pour une progression fixée. On améliore un résultat de Hooley de 1975 dans deux directions différentes. On utilise ici des majorations récentes de sommes d'exponentielles courtes de Bourgain-Garaev et de sommes d'exponentielles tordues par la fonction de Möbius dues à Bourgain et Fouvry-Kowalski-Michel.

Mots-clefs : entiers sans facteur carré; équirépartition en progression arithmétique; sommes d'exponentielles courtes; sommes d'exponentielles sur les nombres premiers.

Equidistribution problems of squarefree numbers

Abstract

This thesis concerns a few problems linked with the distribution of squarefree integers in arithmetic progressions. Such problems are usually phrased in terms of upper bounds for the error term related to this distribution.

The first, second and fourth chapter focus on the satistical study of the error terms as the progressions varies modulo q. In particular we obtain an asymptotic formula for the variance and non-trivial upper bounds for the higher moments. We make use of many technics from analytic number theory such as sieve methods and exponential sums. In particular, in the second chapter we make use of a recent upper bound for short exponential sums by Bourgain.

In the third chapter we give estimates for the error term for a fixed arithmetic progression. We improve on a result of Hooley from 1975 in two different directions. Here we use recent upper bounds for short exponential sums by Bourgain-Garaev and exponential sums twisted by the Möbius function by Bourgain et Fouvry-Kowalski-Michel.

Keywords : squarefree integers; arithmetic progressions; short exponential sums; exponential sums over the prime numbers.

Remerciements

Je tiens tout d'abord à remercier mon directeur de thèse Étienne Fouvry pour tout ce qu'il m'a appris au long de ces 3 ans et demi que nous avons partagé, pour ses encouragements face à chaque défi, pour sa passion captivante pour l'arithmétique, pour son suivi attentif et attentionné et pour sa bonne humeur.

Régis de la Breteche et Timothy Browning, mes deux rapporteurs, ont ma reconnaissance pour avoir accepté de rapporter cette these et pour le sérieux avec lequel ils l'ont fait.

À Antoine Chambert-Loir, Joël Rivat et Emmanuel Royer pour avoir accepté de faire partie de mon jury de thèse. En particulier j'apprécie que ces deux derniers aient accepté de se déplacer depuis Marseille et Clermont-Ferrand spécialement pour cela.

Je remercie aussi Gugu qui m'a écrit une lettre de recommandation pour ma venue en France et qui, j'espére, marquera bientôt son cinque-millième but.

Un grand merci pour la comunauté des étudiants-chercheurs en théorie analytique des nombres pour avoir fourni une ambiance à la fois stimulante et agréable particulièrement propice à la recherche. Je voudrais tout particulièrement remercier Zeev Rudnick et Pierre le Boudec qui se sont montrés intêressés par mes résultats et avec qui j'ai pu profiter de discussions très enricchissantes. Je pense aussi À Djordjo, Kévin, Berke, Sary, Armand, Lucile et d'autres pour les parties de BS, les matchs de foot, les bières, les pique-niques, enfin, toute les activitées hors-recherche qui ont rendu ces conféfrences encore plus agréables.

Je me dois de remercier aussi les sécretaires du labo de math et de l'université, specialement Mme. Lavigne qui a toujours su gérer parfaitement tout les problèmes qui se sont presentés. Je remercie aussi l'efficacité et la simpathie de Mme. Thouvenot.

Merci aux collègues doctorants pour la bonne ambience crée au bâtiment 430 que ce soit pendant les pauses thé, des discussions mathématiques ou les parties de ping-pong.

Je suis reconnaisant à mes amis avec qui j'ai partagé les meilleurs et les pires de mes moments au long de ces trois ans et sans qui je n'aurait jamais pu arriver là : Archibald, Caro, Luco, Çağrı, Aladin, Adrian, Seb, Tarik, Toota et tous les habitués de la colloc, Christina, Adenilson, Edson, Fetter, Tonho, Cleiton, Daniel, Rafael (les tous), Diogo et tous les membres fondateurs ou non-fondateurs du CL.

Pour finir, je remercie ma famille pour leur compréhension, patience et surtout pour leur soutien intense et inconditionel pour lesquels il est parfois difficile de rendre la pareille. Merci aussi à mes amis au Brésil qui font de mes vacances au soleil des moments encore plus joyeux et vivifiants.

Table des matières

Table des matières **7**

Introduction **9**

I Répartition de fonctions arithmétiques 9

II Majorations en moyenne sur a modulo q 13

III Une question de dépendance de variables aléatoires 15

IV Moments d'ordre supérieur 17

V Sommes d'exponentielles 19

1 Squarefree numbers in arithmetic progressions [1] **22**

1.1 Introduction 22

1.2 Notation 27

1.3 Proof of Theorem 1.1.3 assuming Theorem 1.1.4 27

1.4 Initial Steps 28

1.5 Preparatory results 31

1.6 Main term 38

1.7 Bounding $S_{>y}[m](X, q)$ 39

1.8 Proof of Theorem 1.1.4 49

1.9 Exponential Sums 50

2 On Bourgain's Bound and applications to squarefree numbers **54**

2.1 Introduction 54

2.2 Notation 56

2.3 Initial Steps 57

2.4 Useful lemmata 58

2.5 Study of $S[\gamma_{r,s}](X,q)$ 71
2.6 Proof of the main Theorem 72

3 On two conjectures concerning squarefree numbers in arithmetic progressions 73

3.1 Introduction 73
3.2 Preliminary results 77
3.3 Proofs of the results 80

4 On a result of R. R. Hall on squarefree numbers in short intervals 92

4.1 Introduction 92
4.2 Notation 100
4.3 Preparatory results 100
4.4 Estimating $E_\ell(Y;\mathbf{r})$ 107
4.5 Proof of Theorem 4.1.6 111
4.6 Counting tuples of squarefree numbers 114
4.7 Proofs of Corollaries 4.1.2 and 4.1.7 117

Bibliographie 121

Introduction

I Répartition de fonctions arithmétiques

En théorie analytique des nombres, la répartition de suites arithmétiques en progressions arithmétiques joue un rôle central .On considère $\mathcal{A}$ un ensemble infini d'entiers strictement positifs. Pour $X \geq 1$, pour a, q des entiers tels que $(a, q) = 1$ et $1 \leq q \leq X$, on définit

$$\begin{aligned} S_{\mathcal{A}}(X, q, a) &:= \#\{n \in \mathcal{A},\, n \leq X,\, n \equiv a \pmod q\}, \\ \text{et} \quad S_{\mathcal{A}}(X, q) &:= \#\{n \in \mathcal{A},\, n \leq X,\, (n, q) = 1\}. \end{aligned}$$

Plus généralement, pour une fonction $f : \mathbb{Z}_{>0} \to \mathbb{R}_{\geq 0}$, on définit les deux fonctions de comptage

$$S_f(X, q, a) := \sum_{\substack{n \leq X \\ n \equiv a \pmod q}} f(n) \quad \text{et} \quad S_f(X, q) := \sum_{\substack{n \leq X \\ (n,q)=1}} f(n). \tag{1}$$

On note que l'on peut récupérer la notion précédente en faisant $f = \mathbf{1}_{\mathcal{A}}$, où $\mathbf{1}_{\mathcal{A}}$ est la fonction caractéristique de l'ensemble $\mathcal{A} \subset \mathbb{Z}_{>0}$.
Une première question qui se pose est celle de trouver un équivalent asymptotique pour $S_f(X, q, a)$. Si la fonction f est suffisamment régulière, on peut s'attendre à ce que pour tout entier $q \geq 1$ et tout a tel que $(a, q) = 1$, on ait

$$S_f(X, q, a) \sim \frac{1}{\varphi(q)} S_f(X, q), \quad (X \to \infty). \tag{2}$$

Dans ce contexte, on appellera $S_f(X, q)$ *le terme principal*. Par exemple, quand

$$f(n) = \begin{cases} \frac{1}{n}, \text{ si } n \text{ est un nombre premier,} \\ 0, \text{ sinon,} \end{cases}$$

cette formule asymptotique est un célèbre théorème de Dirichlet datant de 1837. En particulier, Dirichlet a prouvé que pour tous a, q tels que $q \geq 1$ et $(a, q) = 1$, il existe une infinité de nombres premiers congrus à a modulo q.
Dans la plupart des applications, la seule connaissance de la formule (2) n'est pas suffisante. On y rencontre alors deux autres importantes questions. La première concerne l'uniformité par rapport à q. La deuxième repose sur l'ordre de grandeur du terme d'erreur

$$E_f(X, q, a) := S_f(X, q, a) - \frac{1}{\varphi(q)} S_f(X, q). \tag{3}$$

Donnons quelques exemples pour clarifier les idées. On reviendra plusieurs fois à ces exemples pour parler des différents problèmes liés à la répartition de f dans les progressions arithmétiques.

Exemple 1. La suite des nombres premiers.
Soit $\mathcal{P} = \{2, 3, 5, \ldots\}$ l'ensemble des nombres premiers. D'après le théorème de Siegel-Walfisz sur les régions sans zéro des fonctions L de Dirichlet, on sait que pour tout réel $A \geq 1$, on a

$$\begin{aligned} S_{\mathcal{P}}(X, q, a) &= \frac{S_{\mathcal{P}}(X, q)}{\varphi(q)} + O_A\left(\frac{X}{(\log X)^A}\right) \\ &= \frac{1}{\varphi(q)} \int_2^X \frac{dt}{\log t} + O_A\left(\frac{X}{(\log X)^A}\right), \end{aligned} \tag{4}$$

uniformément pour tout $X \geq 2$, pour tous a, q tels que $(a, q) = 1$ et $1 \leq q \leq X$. De plus les constantes implicites ne dépendent que de A. Cela veut dire que la formule asymptotique (2) reste vraie uniformément pour q aussi grand qu'une puissance de $\log X$ et le terme d'erreur est également plus petit que le terme principal par un facteur d'une puissance de $\log X$.
L'hypothèse de Riemann généralisée pour les fonctions L de Dirichlet (notée HRG dans la suite) entraînerait, pour tout $\epsilon > 0$, la formule asymptotique

$$S_{\mathcal{P}}(X, q, a) = \frac{S_{\mathcal{P}}(X, q)}{\varphi(q)} + O_\epsilon\left(X^{\frac{1}{2}+\epsilon}\right), \tag{5}$$

où la constante implicite ne dépend que de ϵ. On aurait donc que la formule asymptotique (2) serait valable uniformément pour $q \leq X^{\frac{1}{2}-\epsilon}$, ce qui est bien meilleur que ce que l'on peut prouver inconditionnellement (voir (4)). Néanmoins, Montgomery a conjecturé quelque chose de plus fort encore que (5) :

Conjecture A. *Soit $\epsilon > 0$. Pour tout $X \geq 1$ et pour tous a, q entiers tels que $q \leq X$ et $(a, q) = 1$, on a l'inégalité*

$$E_{\mathcal{P}}(X, q, a) \ll_\epsilon X^\epsilon \, (X/q)^{\frac{1}{2}},$$

où la constante implicite ne dépend que de ϵ.

Remarquons que la conjecture originale de Montgomery [31, Formula (15.9)] a été infirmée par Friedlander et Granville [14] quand q est extrêmement proche de X. La version que nous présentons a été proposée par Friedlander et Granville dans [14] et répond à cette critique. Avant de passer à l'exemple suivant, on donne une définition qui nous permettra de mieux décrire le domaine de validité de la formule asymptotique (2).

Définition 1. Soit f une fonction arithmétique telle que, pour tout $n \geq 1$, $f(n) \geq 0$. On définit l'*exposant de répartition* de f, dénoté $\theta(f)$ comme étant la plus grande valeur de θ telle que pour tout $\epsilon > 0$ et pour tout $A \geq 1$ il existe $C(\epsilon, A) > 0$ telle que, pour tout $X \geq 2$, tout a et q tels que $1 \leq q \leq X^{\theta-\epsilon}$, $(a, q) = 1$, on ait l'inégalité

$$|E_f(X, q, a)| \leq C(\epsilon, A) \frac{S_f(X, q)}{\varphi(q)} (\log X)^{-A}.$$

On définit également $\theta(\mathcal{A}) := \theta(\mathbf{1}_{\mathcal{A}})$ pour $\mathcal{A}$ un ensemble d'entiers strictement positifs.

Noter qu'avec cette définition, HRG donne que $\theta(\mathcal{P}) \geq \frac{1}{2}$.

Exemple 2. Les fonctions nombre de diviseurs généralisées.
On considère la fonction nombre de diviseurs classique donnée, pour tout $n \geq 1$, par

$$d(n) := \#\{d \geq 1;\ d \mid n\}.$$

Plus généralement, on considère, pour $k \geq 2$ les fonctions données, pour tout $n \geq 1$, par

$$d_k(n) := \#\{(n_1, \dots, n_k) \in \mathbb{Z}_{\geq 1}^k;\ n_1 \dots n_k = n\}.$$

On remarque que $d = d_2$. Une simple application de la méthode de l'hyperbole de Dirichlet fournit que $\theta(d_k) \geq \frac{1}{k}$. Cependant, on peut faire mieux. En effet, il a été démontré indépendamment par Selberg, Hooley et Linnik que l'on a $\theta(d_2) \geq \frac{2}{3}$. Une preuve simple de ce fait peut être obtenue à partir de la formule de Voronoi combinée avec les majorations de Weil pour les sommes de Kloosterman.

La seule autre valeur de k pour laquelle on sait que l'exposant de répartition de d_k est strictement supérieur à $\frac{1}{2}$ est $k = 3$, grâce au profond résultat de Friedlander et Iwaniec [16] qui garantit que $\theta(d_3) \geq \frac{1}{2} + \frac{1}{230}$. Très récemment, Fouvry-Kowalski-Michel [12] ont amélioré ce résultat en démontrant que l'on peut prendre $\theta(d_3) \geq \frac{1}{2} + \frac{1}{46}$.

Pour $k = 4$, il aurait été connue à Linnik que $\theta(d_4) \geq \frac{1}{2}$, mais une référence précise de ce résultat semble difficile à trouver. Pour finir, lorsque $k \geq 5$, le meilleur résultat est dÃ» à Friedlander et Iwaniec [15]. Ils établissent que $\theta(d_k) \geq \theta_k$, avec

$$\theta_k = \begin{cases} \frac{9}{20}, & \text{pour } k = 5, \\ \frac{5}{12}, & \text{pour } k = 6, \\ \frac{8}{3k}, & \text{pour } k \geq 7. \end{cases}$$

On discutera du terme d'erreur pour d_k en section II.

Enfin, notre dernier exemple porte sur la suite des entiers sans facteur carré.

Exemple 3. La suite des entiers sans facteur carré.
Soit $\mathcal{Q}$ l'ensemble des entiers positifs sans facteur carré. On note que

$$\mathcal{Q} = \{n \in \mathbb{Z}_{>0}; \mu^2(n) = 1\},$$

où μ est la fonction de Möbius définie de la manière suivante :

$$\mu(n) = \begin{cases} 1, & \text{pour } n = 1, \\ (-1)^k, & \text{si } n \text{ est le produit de } k \text{ premiers distincts}, \\ 0, & \text{s'il existe } p \text{ premier tel que } p^2 \text{ divise } n. \end{cases}$$

En ce qui concerne la répartition de μ^2 dans les progressions arithmétiques, un premier résultat de Prachar [34] permet d'établir, pour tout $\epsilon > 0$, l'inégalité

$$E_{\mu^2}(X, q, a) \ll_\epsilon X^{\frac{1}{2}+\epsilon} q^{-\frac{1}{4}} + q^{\frac{1}{2}+\epsilon}, \ \ ((a, q) = 1),$$

où la constante implicite ne dépend que de ϵ. Cela démontre que $\theta(\mu^2) \geq \frac{2}{3}$. Sans améliorer la borne pour l'exposant de répartition, Hooley [23] a pu améliorer la majoration de $E_{\mu^2}(X, q, a)$ lorsque $X^{\frac{1}{2}} \leq q \leq X^{\frac{2}{3}-\epsilon}$. Plus précisément, il a démontré que pour tout $\epsilon > 0$, on a l'inégalité

$$E_{\mu^2}(X, q, a) \ll_\epsilon X^{\frac{1}{2}} q^{-\frac{1}{2}} + q^{\frac{1}{2}+\epsilon}, \tag{6}$$

où la constante implicite ne dépend que de ϵ. À la connaissance de l'auteur il n'existe pas de résultat améliorant les estimations de $E_{\mu^2}(X,q,a)$ sous HRG. On cite néanmoins le résultat de Jia [24] qui fournit actuellement le meilleur terme d'erreur dans la formule asymptotique pour $S_{\mu^2}(X,1)$. Plus précisément, il établit que si l'hypothèse de Riemann est vraie, alors pour tout $\epsilon > 0$, on a l'égalité

$$S_{\mu^2}(X,1) = \frac{6}{\pi^2}X + O_\epsilon\big(X^{\frac{17}{54}+\epsilon}\big), \tag{7}$$

où la constante implicite ne dépend que de ϵ (rappelons que l'on obtient trivialement $O(X^{1/2})$). Réciproquement, la formule asymptotique (7) avec un terme d'erreur $O_\epsilon\big(X^{\frac{1}{4}+\epsilon}\big)$ implique l'hypothèse de Riemann pour la fonction ζ. Comme dans le cas des nombres premiers, la conjecture suivante due à Montgomery [2] laisse penser que HRG associée à nos méthodes actuelles d'analyse complexe ne donnent pas l'ordre de grandeur correct pour $E_{\mu^2}(X,q,a)$:

Conjecture B. *Soit $\epsilon > 0$. Pour tout $X \geq 1$ et pour tous a, q entiers tels que $q \leq X$ et $(a,q) = 1$, on a l'inégalité*

$$E_{\mu^2}(X,q,a) \ll_\epsilon X^\epsilon\,(X/q)^{\frac{1}{4}},$$

où la constante implicite ne dépend que de ϵ.

Comme pour la Conjecture A, la Conjecture B ne semble pas abordable par les méthodes dont on dispose aujourd'hui. Des progrès ont tout de même été effectués dans cette direction (voir Théorème 2 ci-dessus).

Premiers résultats

Dans cette partie, on énonce quelques-uns de nos résultats liés à l'exposant de répartition et au terme d'erreur relatif à la répartition des entiers sans facteur carré dans les progressions arithmétiques.
On a vu que les majorations de Prachar et Hooley (voir l'exemple 3) permettent d'obtenir la formule asymptotique (2) uniformément pour $q \leq X^{\frac{2}{3}-\epsilon}$, où $\epsilon > 0$ est une constante arbitraire. Dans le Chapitre 3 nous démontrons comment dépasser légèrement cette barrière. Plus précisément, on a le résultat suivant, conséquence directe du Corollaire 3.1.6.

Théorème 1. *Pour tout $\epsilon > 0$, on a la formule asymptotique*

$$\sum_{\substack{n\leq X\\ n\equiv a \pmod q}} \mu^2(n) \sim \frac{1}{\varphi(q)} \sum_{\substack{n\leq X\\ (n,q)=1}} \mu^2(n) \quad \left(\sim \frac{6}{\pi^2}\prod_{p\mid q}\left(1-\frac{1}{p^2}\right)^{-1}\frac{X}{q}\right),$$

lorsque $X \to \infty$, pourvu que q soit premier, $(a,q) = 1$ et $q \leq X^{\frac{2}{3}}(\log X)^{\frac{1}{6}-\epsilon}$.

En ce qui concerne le terme d'erreur, on peut voir grâce à la majoration de Hooley (6) que pour tout $\epsilon > 0$, on a l'inégalité

$$E_{\mu^2}(X,q,a) \ll_\epsilon \left(\frac{X}{q}\right)^{\frac{1}{2}}, \tag{8}$$

2. La conjecture apparaît initialement dans [7, page 145]. Nous donnons la version de Le Boudec [28] qui tient compte d'une erreur dans la version originale quand q est extrêmement proche de X. C'est exactement l'analogue de la correction suggérée par Friedlander et Granville [14] dans le cas des nombres premiers.

uniformément pour $q \leq X^{\frac{1}{2}-\epsilon}$. Le théorème suivant dit que l'on peut remplacer $\frac{1}{2}$ par des exposants plus petits dans la majoration (8) (se souvenir que la Conjecture B prévoit que l'on devrait même avoir l'exposant $\frac{1}{4}+\epsilon$).

Théorème 2. *(voir Théorème 3.1.4) Pour tout $\eta > 0$, il existe $\delta = \delta(\eta) > 0$ tel qu'on ait l'inégalité*

$$E_{\mu^2}(X, q, a) \ll_\eta \left(\frac{X}{q}\right)^{\frac{1}{2}-\delta},$$

uniformément pour tout $X \geq 1$, tout q premier tel que $X^\eta \leq q \leq X^{\frac{1}{2}-\eta}$ et tout entier a premier avec q.

Si $X^\alpha \leq q \leq 2X^\alpha$ avec $0 < \alpha < \frac{2}{5}$, on peut même être plus précis. Le Théorème 3.1.2 ainsi que la remarque qui le suit nous permettent d'établir le résultat suivant.

Théorème 3. *Pour tout α et tout ϵ vérifiant $0 < \alpha < \frac{2}{5}$ et $\epsilon > 0$, il existe $C(\alpha, \epsilon) > 0$ telle que pour tout $X \geq 1$, pour tout q premier vérifiant $X^\alpha \leq q \leq 2X^\alpha$ et tout entier a premier avec q, on ait l'inégalité*

$$\left|E_{\mu^2}(X, q, a)\right| \leq C(\alpha, \epsilon)\left(\frac{X}{q}\right)^{\frac{1}{2}-\delta(\alpha)+\epsilon},$$

où on a posé

$$\delta(\alpha) = \min\left(\frac{\alpha}{192(1-\alpha)}, \frac{2-5\alpha}{196(1-\alpha)}\right).$$

II Majorations en moyenne sur a modulo q

L'étude individuelle des termes d'erreur $E_f(X, q, a)$ est souvent ardue. En revanche un effet de moyenne sur a modulo q peut simplifier l'estimation. Considérons par exemple la variance

$$V_f(X, q) := \sideset{}{^*}\sum_{a \pmod q} E_f(X, q, a)^2,$$

où l'ast'erisque indique que l'on ne somme que sur les résidus a tels que $(a, q) = 1$. Il serait peut-être plus naturel de considérer simplement la moyenne

$$M_f(X, q) := \sideset{}{^*}\sum_{a \pmod q} \left|E_f(X, q, a)\right|.$$

Cependant, du point de vue analytique, la variance $V_f(X, q)$ est beaucoup plus agréable à manipuler. En général, on donne des estimations pour $V_f(X, q)$ et on en déduit une éstimation pour $M_f(X, q)$ par une application de Cauchy-Schwarz :

$$M_f(X, q) \leq \varphi(q)^{\frac{1}{2}} V_f(X, q)^{\frac{1}{2}}.$$

Revenons à présent aux trois exemples de la partie précédente.

La suite des nombres premiers

L'étude de cette suite est tellement compliquée que l'on ne peut rien prouver de satisfaisant sans supposer quelque chose de très profond comme HRG. Dans ce cadre, Túran [38] a prouvé que sous HRG, on a l'inégalité

$$V_{\mathcal{P}}(X,q) \ll X(\log X)^4,$$

uniformément pour $q \leq X$. Cela implique que le nombre d'exceptions à la conjecture de Montgomery (A) est négligeable. Plus précisément, pour tout $\epsilon > 0$, on définit

$$\mathcal{E}_{\mathcal{P}}(X,q;\epsilon) := \#\left\{ a \in (\mathbb{Z}/q\mathbb{Z})^* ;\ |E_{\mathcal{P}}(X,q,a)| > X^{\epsilon}\,(X/q)^{\frac{1}{2}} \right\}.$$

On a alors l'estimation $\mathcal{E}_{\mathcal{P}}(X,q) \ll_{\epsilon} q^{1-\epsilon}$ uniformément pour $q \leq X$.

Les fonctions nombre de diviseurs

Pour la fonction d, des moyennes sur a modulo q ont été étudiées par plusieurs auteurs (voir par exemple [1] et [2]). Un résultat de Lau et Zhao [27] donne en particulier une formule asymptotique pour $V_d(X,q)$ lorsque $q \geq X^{\frac{1}{2}+\epsilon}$. En effet, ils établissent qu'il existe un polynôme P_3 de degré trois tel que, pour tout $\epsilon > 0$, on ait l'égalité

$$V_d(X,q) = P_3\left(\log \frac{q^2}{X}\right) X + O\left(d(q)X^{\frac{5}{6}}q^{\frac{1}{6}} + d(q)X^{\frac{5}{4}}q^{-\frac{1}{4}}\right),$$

uniformément pour $X^{\frac{1}{2}} \leq q \leq X$. Autrement dit, l'ordre de grandeur moyen de $E_d(X,q,a)$ est de $(X/\varphi(q))^{\frac{1}{2}}\left(\log \frac{q^2}{X}\right)^{3/2}$. Dans le même article, Lau et Zhao prouvent que pour tout $\epsilon > 0$, il existe $\delta = \delta(\epsilon) > 0$ telle qu'on ait $V_d(X,q) \ll_{\epsilon} X^{1-\delta}$ uniformément pour $q \leq X^{\frac{1}{2}-\epsilon}$. Cela indique un changement de comportement lorsque $q = X^{\frac{1}{2}}$ rendant très difficile de conjecturer l'ordre de grandeur de $E_d(X,q,a)$ lorsque q franchit la borne $X^{\frac{1}{2}}$.

Pour les fonctions d_k, $k \geq 3$, Kowalski et Ricotta [26] ont démontré une formule asymptotique pour $V_{d_k}(X,q)$ pour q premier tel que $X^{\frac{1}{k}+\epsilon} \leq q \leq X^{\frac{2}{2k-1}-\epsilon}$.

La suite des entiers sans facteur carré

Dans l'article [2] cité ci-dessus, Blomer a aussi étudié la variance $V_{\mu^2}(X,q)$, pour laquelle il a démontré la majoration

$$V_{\mu^2}(X,q) \ll_{\epsilon} X^{\epsilon}\left(X + \min\left(X^{\frac{5}{3}}q^{-1}, q^2\right)\right), \tag{9}$$

uniformément pour $q \leq X$. La preuve de (9) se réduit à trouver une formule asymptotique pour la somme

$$\sum_{0<\ell\leq\frac{X}{q}} \sum_{n\leq X-\ell q} \mu^2(n)\mu^2(n+\ell q). \tag{10}$$

Blomer obtient cette formule asymptotique en utilisant des majorations de sommes d'exponentielles, mais sans tirer parti de la somme sur $0 < \ell \leq \frac{X}{q}$.

Remarque. D'après la conjecture de Montgomery, la majoration (9) ne devrait être optimale pour aucune valeur de $q \leq X^{1-\epsilon}$. Remarquons tout de même qu'en modifiant très légèrement la preuve de Blomer, il est possible de remplacer le terme $X^{1+\epsilon}$ par $X^{\frac{1}{2}+\epsilon}q^{\frac{1}{2}}$, obtenant ainsi une estimation en accord avec la conjecture de Montgomery pour $q \geq X^{\frac{7}{9}+\epsilon}$.

Dans le théorème suivant, on a repris la démarche de Blomer, mais en y apportant deux modifications. La première consiste à utiliser le crible à carrés de Heath-Brown [22] pour obtenir des compensations grâce la somme sur ℓ dans (10). Deuxièmement, on s'inspire de la technique de Croft [7] qui avait démontré une formule asymptotique pour

$$\sum_{q \leq Q} V_{\mu^2}(X, q),$$

lorsque $Q \geq X^{\frac{1}{2}+\epsilon}$, pour tout $\epsilon > 0$. Cela nous permet d'obtenir une formule asymptotique pour $V_{\mu^2}(X, q)$ lorsque q est suffisamment grand par rapport à X, sans avoir besoin de la somme sur $q \leq Q$. On a donc le Théorème suivant (voir Théorème 1.1.1).

Théorème 4. *Il existe une constante absolue $C > 0$ telle que, pour tout $\epsilon > 0$, on a, uniformément pour $1 \leq q \leq X$, l'égalité*

$$V_{\mu^2}(X, q) = C \prod_{p|q} \left(1 + 2p^{-1}\right)^{-1} X^{\frac{1}{2}} q^{\frac{1}{2}} + O_\epsilon\left(X^{\frac{1}{3}+\epsilon} q^{\frac{2}{3}} + X^{\frac{23}{15}+\epsilon} q^{-\frac{13}{15}}\right),$$

où la constante implicite ne dépend que de ϵ.

On en déduit alors la formule asymptotique

$$V_{\mu^2}(X, q) \sim C \prod_{p|q} \left(1 + 2p^{-1}\right)^{-1} X^{\frac{1}{2}} q^{\frac{1}{2}},$$

lorsque $X \to \infty$, avec $X^{\frac{31}{41}+\epsilon} \leq q \leq X^{1-\epsilon}$.

Nous signalons que Le Boudec [28] a récemment démontré une majoration du bon ordre de grandeur pour $V_{\mu^2}(X, q)$ lorsque $q \geq X^{\frac{1}{2}+\epsilon}$, pour tout $\epsilon > 0$. Sa preuve s'appuie sur des résultats de géométrie des nombres.

III Une question de dépendance de variables aléatoires

Une question très intéressante qui a été étudiée dans le cadre de la fonction d par Fouvry *et al.* [9] est celle de la corrélation entre les variables aléatoires

$$a \mapsto \frac{E_f(X, q, a)}{\left(V_f(X, q)/\varphi(q)\right)^{1/2}} \quad \text{et} \quad a \mapsto \frac{E_f(X, q, \gamma(a))}{\left(V_f(X, q)/\varphi(q)\right)^{1/2}}, \tag{11}$$

pour une fonction $\gamma : \mathbb{Z}/q\mathbb{Z} \to \mathbb{Z}/q\mathbb{Z}$ de nature algébrique. Plus précisément, ils se sont intéressés au cas où q est premier et γ est une fonction homographique de la droite projective $\mathbb{P}^1(\mathbb{F}_q)$. C'est-à-dire

$$\gamma(a) = \frac{ra + s}{ta + u}, \quad (a \neq \bar{t}u) \tag{12}$$

avec $r, s, t, u \in \mathbb{Z}$, $\Delta_\gamma := ru - st \neq 0$, où l'on note $\bar{x}$ l'inverse multiplicatif d'un résidu primitif x modulo q. On a étudié ce problème dans le cadre de la fonction μ^2 pour γ une fonction affine, *i.e.* $\gamma : \mathbb{Z}/q\mathbb{Z} \to \mathbb{Z}/q\mathbb{Z}$ donnée par

$$\gamma(a) = ra + s \tag{13}$$

Cela correspond à la définition (12) dans le cas particulier où $t = 0$ et $u = 1$. Le Théorème 5 ci-dessous résume nos résultats sur ce sujet. Pour toute fonction γ comme en (12), on définit la somme de covariance

$$C[\gamma](X, q) := \sum_{\substack{a \pmod q \\ a \neq 0, -\bar{r}s, -\bar{t}u}} E_{\mu^2}(X, q, a) E_{\mu^2}(X, q, \gamma(a)). \tag{14}$$

On a le résultat suivant, qui combine les Théorèmes 1.1.3 et 2.1.2.

Théorème 5. *Soit γ une fonction affine comme en* (13) *et soit $C[\gamma](X, q)$ comme en* (14). *Il existe des constantes C_γ et $\delta > 0$ telles que pour tout $\epsilon > 0$, on ait l'égalité*

$$C[\gamma](X, q) = C_\gamma X^{\frac{1}{2}} q^{\frac{1}{2}} + O_{\epsilon, r}\left(X^{\frac{1}{2}} q^{\frac{1}{2}} (\log X)^{-\delta}\right)$$

uniformément pour $X \geq 2$ et pour q premier tel que $q > |r|$, $q \nmid s$, et $X^{\frac{7}{9}+\epsilon} \leq q \leq X^{1-\epsilon}$, où la constante implicite ne dépend que de ϵ et r. De plus, si s est différent de 0, alors $C_\gamma = 0$.

Nous traitons les cas $s = 0$ et $s \neq 0$ séparément. Si $s = 0$, alors la preuve suit les mêmes lignes que celles employées dans le cadre du Théorème 4 et que nous avons décrites dans la partie précédente. Si $s \neq 0$, le fait que $C_\gamma = 0$ est une conséquence d'une majoration de sommes d'exponentielles due à Bourgain (voir Théorème F ci-dessous).

Nous croyons que les méthodes ci-dessus s'étendent à l'étude de $C[\gamma](X, q)$ pour toute fonction γ comme en (12) avec $t = 0$. De plus, le cas où γ est telle que $t \neq 0$, un argument se basant sur la majoration de Weil sur les sommes de Kloosterman classiques devrait donner un résultat analogue au Théorème 5 avec $C_\gamma = 0$ pour tout γ avec $t \neq 0$.

Le Théorème 5 peut être interprété de la manière suivante.
Soit $(X_n)_{n\geq 1}$ une suite croissante de réels et $(q_n)_{n\geq 1}$ une suite croissante de nombres premiers tels que $X_n, q_n \to \infty$ avec la contrainte $X_n^{\frac{7}{9}+\epsilon} \leq q_n \leq X_n^{1-\epsilon}$. Alors le coefficient de corrélation entre les suites de variables aléatoires

$$a \mapsto E_f(X_n, q_n, a) \quad \text{et} \quad a \mapsto E_f(X_n, q_n, \gamma(a))$$

converge, lorsque q tend vers l'infini, vers

- une constante $C'_r \neq 0$ si $s = 0$. Donc ces variables ne sont pas asymptotiquement indépendantes.
- 0 si $s \neq 0$. Cela suggère que ces variables peuvent être asymptotiquement indépendantes. Mais, il nous faudrait plus d'informations sur les moments mixtes d'ordre supérieur comme dans [9] et [26] pour pouvoir établir l'indépendance.

IV Moments d'ordre supérieur

Nous pouvons aussi considérer les moments d'ordre supérieur

$$\mathcal{M}_f(X,q;\ell) = \sideset{}{^*}\sum_{a \pmod q} E_f(X,q,a)^\ell. \tag{15}$$

Dans le cas où $f = d$, Fouvry *et al.* ont démontré, pour tout $\ell \geq 2$ et tout $\epsilon > 0$, une formule asymptotique valable uniformément pour $X^{\frac{1}{2}+\epsilon} \leq q \leq X^{\frac{\ell}{2\ell-1}-\epsilon}$. Comme conséquence ils ont obtenu une loi de répartition gaussienne pour $E_d(X,q,a)$ lorsque q est proche de $X^{\frac{1}{2}}$.

Nous nous sommes inspirés de ce résultat pour étudier les moments $\mathcal{M}_f(X,q;\ell)$ dans le cas où $f = \mu^2$. Hall [19] avait considéré le problème des moments pour la répartition des entiers sans facteur carré dans les petits intervalles. Il existe une analogie entre la répartition de suites arithmétiques dans les progressions arithmétiques et dans les petits intervalles. Nous développons cette analogie dans le cas de la fonction μ^2 dans le Chapitre 4. En particulier les résultats de Hall se traduisent dans le contexte des progressions arithmétiques de la faÃ§on suivante :

Théorème C. *(Hall) Soit $\ell \geq 2$ un entier et soit $\mathcal{M}_{\mu^2}(X,q;\ell)$ comme en (15) avec $f = \mu^2$. Alors il existe $\delta(\ell) > 0$ telle que*

$$\mathcal{M}_{\mu^2}(X,q;\ell) \ll_{\epsilon,\ell} \varphi(q)\left(\frac{X}{q}\right)^{\frac{\ell-1}{2}},$$

uniformément pour $X \geq 1$ et $X^{1-\delta(\ell)} \leq q \leq X^{1-\epsilon}$, où la constante implicite ne dépend que de ϵ et de ℓ.

Si la Conjecture B est vraie, on pourrait remplacer le second membre de l'inégalité du Théorème C par $\varphi(q)\,(X/q)^{\frac{\ell}{4}+\epsilon}$.

La méthode de Hall est assez différente de celle de Fouvry *et al.* La dernière se base sur une application de la formule de Voronoi combinée avec des estimations de sommes de corrélations liées aux sommes de Kloosterman (il s'agit d'un théorème assez profond d'indépendance de groupes de monodromie liés à ces sommes).

Dans le cas de la fonction μ^2, nous n'avons pas d'équivalent de la formule de Voronoi (Les fonctions L associées ont une infinité de pôles dans la bande $0 < \Re(s) < \frac{1}{4}$). Il reste l'alternative naïve : développer le terme $E_{\mu^2}(X,q,a)^\ell$ et changer l'ordre de sommation. Nous devons alors étudier, pour $0 \leq j \leq \ell$, les termes de la forme

$$T_{\ell,j}(X,q) := (-1)^{\ell-j}\binom{\ell}{j}\left(\frac{S_{\mu^2}(X,q)}{\varphi(q)}\right)^{\ell-j} \sideset{}{^*}\sum_{\substack{0<n_1,\dots,n_j\leq X \\ n_1\equiv\dots\equiv n_j \pmod q}} \cdots \sideset{}{^*}\sum \mu^2(n_1)\dots\mu^2(n_j), \tag{16}$$

où $S_{\mu^2}(X,q)$ est comme défini dans (1). Il est facile de donner un équivalent asymptotique de chaque $T_{\ell,j}(X,q)$. On parvient alors à la majoration

$$\mathcal{M}_{\mu^2}(X,q;\ell) \ll_\ell \varphi(q)\left(\frac{X}{q}\right)^{\ell-\frac{3}{2}},$$

ce qui est moins bon que le Théorème C pour tout $\ell \geq 3$. Il est donc impératif d'étudier la contribution simultanée des termes dans (16). Cela se fait grâce à la proposition suivante (voir par exemple l'équation (4.95)).

Proposition 6. *Soit $\psi : \mathbb{R} \to \left[-\frac{1}{2}, \frac{1}{2}\right]$ la fonction définie par*

$$\lfloor x \rfloor = x - \frac{1}{2} + \psi(x).$$

Soit $\ell \geq 3$ un entier et soit $\mathcal{M}_{\mu^2}(X, q; \ell)$ comme en (15) avec $f = \mu^2$. Soit $\mathcal{C}_\ell : \mathbb{R}_{>0} \times \mathbb{Z}_{>0} \to \mathbb{R}$ donnée par

$$\mathcal{C}_\ell\,(Y, q) = \sum_{\substack{r_1=1 \\ (r_1,q)=1}}^{\infty} \cdots \sum_{\substack{r_\ell=1 \\ (r_\ell,q)=1}}^{\infty} \frac{\mu(r_1)\dots\mu(r_\ell)}{\hat{r}^2} E_\ell(Y; r_1, \dots, r_\ell), \tag{17}$$

où $\hat{r} = \mathrm{ppcm}[r_1, \dots, r_\ell]$ et

$$E_\ell(Y; r_1, \dots, r_\ell) := \int_0^{\hat{r}^2} \prod_{j=1}^{\ell} \left(\psi\left(\frac{Y-u}{r_j^2}\right) - \psi\left(\frac{-u}{r_j^2}\right)\right) du.$$

Alors, il existe $\delta(\ell) > 0$ telle que pour tout $\epsilon > 0$ et tout q entier vérifiant $X^{1-\delta(\ell)} \leq q \leq X^{1-\epsilon}$, on ait l'égalité

$$\frac{1}{\varphi(q)} \mathcal{M}_{\mu^2}(X, q; \ell) = \mathcal{C}_\ell\left(\frac{X}{q}, q\right) + O_\epsilon(X^{-\frac{1}{100}}).$$

La Proposition 6 réduit le problème des moments $\mathcal{M}_{\mu^2}(X, q; \ell)$ à une étude du comportement asymptotique de la fonction $\mathcal{C}_\ell$, du moins pour q assez grand par rapport à X. En particulier, les méthodes de Hall fournissent l'inégalité

$$\mathcal{C}_\ell\left(\frac{X}{q}, q\right) \ll_\ell \left(\frac{X}{q}\right)^{\frac{\ell-1}{2}}.$$

Pour ce faire, Hall fait appel au lemme fondamental de Montgomery et Vaughan (voir [32, Lemma 1]). Nous remarquons que la fonction $C_\ell(k)$ définie par Hall dans [19] semble être assez différente de celle définie dans (17), mais nous verrons dans le Chapitre 4 que ces deux fonctions peuvent être traitées de la même faÃ§on. Quand $\ell = 2$, on démontre que

$$\left|E_\ell(Y; r_1, r_2)\right| = \left|2d^2 \int_0^{\frac{Y}{d^2}} \psi(v) dv\right| \leq \min\left(d^2, Y\right), \tag{18}$$

où $d = \mathrm{pgcd}(r_1, r_2)$ et cela suffit pour obtenir une majoration du bon ordre de grandeur pour $V_{\mu^2}(X, q) = M_{\mu^2}(X, q; 2)$. Pour $\ell \geq 3$ nous n'avons pas trouvé d'analogue à (18). Nous avons tout de même une majoration de $E_\ell(Y; r_1, \dots, r_\ell)$, qui s'écrit essentiellement comme

$$E_\ell(Y; r_1, \dots, r_\ell) \ll_{\epsilon,\ell} \min\left(\hat{r}_2^2, Y^\ell \hat{r}_2^{-1-\frac{2}{\ell}} + Y^{\ell-2}\right),$$

où $\hat{r}_2$ designe le produit de tous les premiers divisant au moins deux des $r_1, \dots, r_\ell$. Cela fournit une majoration pour $\mathcal{M}_{\mu^2}(X, q; \ell)$. On parvient alors au théorème suivant (voir Corollaire 4.1.7).

Théorème 7. *Soit $\ell \geq 3$ un entier et soit $\mathcal{M}_{\mu^2}(X, q; \ell)$ comme en (15) avec $f = \mu^2$. Soit θ_ℓ donnée par*

$$\theta_\ell := \begin{cases} \dfrac{\ell^2}{3\ell+2}, \text{ for } \ell = 3, 4, \\ \dfrac{\ell-2}{2}, \text{ for } \ell \geq 5. \end{cases}$$

Soit δ_ℓ donnée par

$$\delta_\ell := \frac{1}{(\ell+1)(\ell-\theta_\ell)}.$$

Alors pour tout $\epsilon > 0$ et tout $\ell \geq 3$ il existe $C_{\epsilon,\ell} > 0$ tel que pour tout $X \geq 1$ et tout entier positif $q \leq X$, on ait l'inégalité

$$\left|\mathcal{M}_{\mu^2}(X, q; \ell)\right| \leq C_{\epsilon,\ell} \left(\varphi(q) \left(\frac{X}{q}\right)^{\theta_\ell+\epsilon} + X^{\frac{\ell}{\ell+1}} \left(\frac{X}{q}\right)^{\ell-1} \right).$$

En particulier, pour tout $\epsilon > 0$, pour tout $\ell \geq 3$, pour tout $X \geq 1$ et tout entier positif q tel que $X^{1-\delta_\ell+\epsilon} \leq q \leq X$, on a l'inégalité

$$\left|\mathcal{M}_{\mu^2}(X, q; \ell)\right| \leq 2C_{\epsilon,\ell}\, \varphi(q) \left(\frac{X}{q}\right)^{\theta_\ell+\epsilon}.$$

En particulier, pour tout $\ell \geq 3$, on a $\theta_\ell < \frac{\ell-1}{2}$ (comparer avec le Théorème C). Selon la Conjecture B, les valeurs de θ_ℓ dans le Théorème 7 ne devraient pas être optimales. En fait, la Conjecture B et les résultats de [9] pour la fonction d nous permettent d'espérer que la conjecture suivante soit vraie :

Conjecture 8. *Pour tout entier $\ell \geq 1$ et tout $\epsilon > 0$, il existe $\delta_\ell > 0$, $\eta_\ell > 0$, $X_0(\ell, \epsilon) > 0$ et une fonction positive et multiplicative c_ℓ tels qu'on ait l'inégalité*

$$\left| \mathcal{M}_{\mu^2}(X, q; \ell) - c_\ell(q)\varphi(q) \left(\frac{X}{q}\right)^{\frac{\ell}{4}} \right| \leq \varphi(q) \left(\frac{X}{q}\right)^{\frac{\ell}{4}-\eta_\ell}, \tag{19}$$

pour tous q et X tels que

$$X^{1-\delta_\ell} \leq q \leq X^{1-\epsilon},\ X \geq X_0(\ell, \epsilon).$$

De plus

- *si ℓ est pair, la fonction $q \mapsto c_\ell(q)$ est bornée,*
- *si ℓ est impair, $c_\ell(q) = 0$ pour tout q.*

Remarquons que pour $\ell = 1$ cette conjecture est triviale, vu que le membre de gauche vaut 0, et pour $\ell = 2$, la conjecture est vraie avec $\eta_2 < \frac{1}{6}$ et $\delta_2 > \frac{18}{23}$ grâce au Théorème 4.

V Sommes d'exponentielles

Une partie cruciale des résultats des Chapitres 2 et 3 vient de majorations de sommes d'exponentielles. Nous voulons donc dans cette partie faire un panorama des résultats utilisés.

Majorations classiques

La majoration suivante est une conséquence des travaux de Weil sur l'hypothèse de Riemann pour les courbes sur les corps finis. Rappelons que $e(x) := \exp(2\pi i x)$.

Théorème D. *On a l'inégalité*

$$\left| \sum_{n=1}^{q}{}^{*} e\left(\frac{an + b\bar{n}^2}{q}\right) \right| \leq 3q^{\frac{1}{2}}(q, a, b)^{\frac{1}{2}}$$

pour tous a et b entiers et q premier suffisamment grand.

Sommes d'exponentielles (très) courtes

Le Théorème D donne une excellente majoration pour la somme complète (sur tous les résidus primitifs modulo q). Par la méthode de complétion, on accède à une majoration non-triviale pour toutes les sommes de la forme

$$\sum_{n=M+N}^{N}{}^{*} e\left(\frac{an + b\bar{n}^2}{q}\right) \tag{20}$$

dès que $N \geq q^{\frac{1}{2}} \log q$. Cependant, pour quelques applications, nous avons besoin d'estimations non-triviales pour des sommes avec N plus petit. Karatsuba [25] a étudié des sommes de ce type avec $M = 0$ et N très petit ($N \geq q^{\epsilon}$, pour ϵ fixé). La version que nous donnons ici est due à Bourgain et Garaev [5].

Théorème E. *On a l'inégalité*

$$\sum_{n \leq N}^{*} e\left(\frac{a\bar{n}}{q}\right) \ll N \frac{\log N (\log\log N)^3}{(\log q)^{\frac{3}{2}}}$$

uniformément sur $N \geq 3$, q premier et a entier avec $(a, q) = 1$.

Remarque. La condition $M = 0$ (voir (20)) est essentielle ici, vu que la technique utilisée dépend fortement de la factorisation des entiers sommés.

Plus récemment, Bourgain a développé [4] une version quadratique de ce résultat pour étudier l'équation de Pell à l'instar de Fouvry [8]. Le Théorème F est essentiel dans la preuve du Théorème 5 dans le cas où $s \neq 0$.

Théorème F. *Il existe une constante δ absolue telle que pour tout $\epsilon > 0$, on ait l'inégalité*

$$\sum_{n \leq N}^{*} e\left(\frac{a\bar{n}^2}{q}\right) \ll_{\epsilon} N(\log N)^{-\delta}$$

uniformément pour tout q premier, $N \geq q^{\epsilon}$ et a entier avec $(a, q) = 1$.

Sommes d'exponentielles tordues par la fonction μ

Dans le Chapitre 3 on considère des sommes d'exponentielles tordues par la fonction μ pour lesquelles nous avons besoin d'estimations non-triviales. On présente ici les deux résultats principaux dont nous nous servons. Ici, comme dans plusieurs théorèmes en théorie analytique de nombres, les techniques permettant d'étudier ces sommes permettent aussi de traiter les sommes sur les nombres premiers.
Pour tout $N \geq 1$, tout q entier et pour tout a premier avec q, on considère les sommes d'exponentielles suivantes :

$$\Sigma_\mu(N;q,a) := \sum_{n\leq N} \mu(n) e\left(\frac{a\bar{n}^2}{q}\right) \text{ et } \Sigma_{\mathcal{P}}(N;q,a) := \sum_{p\leq N} e\left(\frac{a\bar{p}^2}{q}\right), \tag{21}$$

où dans $\Sigma_{\mathcal{P}}(N;q,a)$ on somme sur les nombres premiers $p \leq N$.
La première estimation que nous utilisons est un cas très particulier de [11, Theorem 1.7].

Théorème G. *Soit $\Sigma_\mu(N;q,a)$ comme dans (21). Alors pour tout $\epsilon > 0$ on a l'inégalité*

$$\Sigma_\mu(N;q,a) \ll_\epsilon N\left(1+\frac{q}{N}\right)^{\frac{1}{12}} q^{-\frac{1}{48}+\epsilon}$$

uniformément pour $N \geq 1$, q premier et a premier avec q. La constante implicite ne dépend que de ϵ.

Le Théorème G donne une majoration non-triviale pour tout $N \geq q^{\frac{3}{4}+\epsilon}$ et nous pouvons quantifier le gain par rapport à la borne triviale. Dans [3], Bourgain présente une méthode permettant d'avoir des majorations non triviales pour $N \geq q^{\frac{1}{2}+\epsilon}$ mais où le gain n'est pas explicite. Le théorème suivant est une conséquence de [3, Theorem A.9].

Théorème H. *Soit $\Sigma_\mu(N;q,a)$ comme dans (21). Alors pour tout $\epsilon > 0$, il existe $\delta = \delta(\epsilon) > 0$ telle qu'on ait, uniformément pour q entier, $q^{\frac{1}{2}+\epsilon} \leq N \leq q$ et a premier avec q, l'inégalité*

$$\Sigma_\mu(N;q,a) \ll_\epsilon N^{1-\delta},$$

où la constante implicite ne dépend que de ϵ.

Remarque. Comme dans la sous-section précédente, les Théorèmes G et H utilisent fortement la factorisation des n sur lesquels on somme et donc la méthode n'est valable essentiellement que pour des sommes commenÃ§ant en 0.

Remarque. Les Théorèmes G et H restent vrais avec $\Sigma_{\mathcal{P}}(N;q,a)$ à la place de $\Sigma_\mu(N;q,a)$.

Chapitre 1

Squarefree numbers in arithmetic progressions [1]

1.1 Introduction

For a positive real number X and positive integers a, q with $(a, q) = 1$, let $E(X, q, a)$ be defined by the formula

$$\sum_{\substack{n \leq X \\ n \equiv a \pmod q}} \mu^2(n) = \frac{6}{\pi^2} \prod_{p|q} \left(1 - \frac{1}{p^2}\right)^{-1} \frac{X}{q} + E(X, q, a), \tag{1.1}$$

where, as usual, μ is the Möbius function. In (1.1) the first term heuristically appears to be a good approximation to the number of squarefree integers $\leq X$ congruent to $a \pmod q$. In this paper, we are concerned with the so called error term $E(X, q, a)$. Trivially, one has

$$|E(X, q, a)| \leq \frac{X}{q} + 1, \tag{1.2}$$

while in [23], Hooley proved

$$E(X, q, a) = O_\epsilon \left(\left(\frac{X}{q} \right)^{\frac{1}{2}} + q^{\frac{1}{2}+\epsilon} \right), \tag{1.3}$$

where the O_ϵ-constant depends only on $\epsilon > 0$ arbitrary. This is the best result available for fixed a. Furthermore, (1.3) gives an asymptotic formula for the left-hand side of (1.1) for $q \leq X^{\frac{2}{3}-\epsilon}$. The same range of validity for this asymptotic formula had already been established by Prachar [34], with a weaker error term than (1.3). We believe that such an asymptotic formula should hold for $q \leq X^{1-\epsilon}$ and it is a challenging problem to go beyond $X^{\frac{2}{3}-\epsilon}$ for a general q, in particular when q is prime. The situation is quite similar to that of the analogous problem for

1. Appeared in Journal of Number Theory (see [33])

the divisor function. By this we mean that an asymptotic formula is known for

$$\sum_{\substack{n\leq X\\ n\equiv a \pmod q}} d(n)$$

in the range $q \leq X^{\frac{2}{3}-\epsilon}$, $(a,q)=1$ and we do not know how to overcome this threshold for general q (in particular when q is prime). And in this case it is also strongly expected that such an asymptotic formula should hold for $q \leq X^{1-\epsilon}$.

It is in general easier to study the error terms on average. Blomer [2] considered the second moment of the $E(X,q,a)$

$$V_{\mu^2}(X,q) := \sideset{}{^*}\sum_{a \pmod q} |E(X,q,a)|^2, \tag{1.4}$$

where the $*$ symbol means that we only sum over the classes that are relatively prime to q. In [2, Theorem 1.3], he showed that

$$V_{\mu^2}(X,q) \ll X^{\epsilon}\left(X + \min\left(\frac{X^{\frac{5}{3}}}{q}, q^2\right)\right) \tag{1.5}$$

holds for every $\epsilon > 0$, uniformly for $1 \leq q \leq X$. Several years before, Croft [7] considered a variation of $V_{\mu^2}(X,q)$ by summing not only over the classes relatively prime to q but over all classes (mod q). Let

$$V_{\mu^2}^{'}(X,q) := \sum_{a \pmod q}\left\{\sum_{\substack{n\leq X\\ n\equiv a \pmod q}} \mu^2(n) - \frac{\mu^2(d)q_0}{\varphi(q_0)}\frac{6}{\pi^2}\prod_{p\mid q}\left(1+p^{-1}\right)^{-1}\frac{X}{q}\right\}^2,$$

where $d=(a,q)$ and $q_0 = q/d$. The last term between the curly brackets on the expression above can be seen as the expected value of the sum

$$\sum_{\substack{n\leq X\\ n\equiv a \pmod q}} \mu^2(n)$$

when a is not necessarily relatively prime to q. Observe that it reduces to the first term on the right-hand side of (1.1) whenever $(a,q)=1$. By taking an extra average over q, Croft [7, Theorem 2] proved the following formula

$$\sum_{q\leq Q} V_{\mu^2}^{'}(X,q) = BX^{\frac{1}{2}}Q^{\frac{3}{2}} + O\left(X^{\frac{2}{5}}Q^{\frac{8}{5}}\log^{\frac{13}{5}} X + X^{\frac{3}{2}}\log^{\frac{7}{2}} X\right), \tag{1.6}$$

uniformly for $Q \leq X$, where B is an explicit constant. For $Q \geq X^{\frac{2}{3}+\epsilon}$, (1.6) gives an asymptotic formula for

$$\sum_{q\leq Q} V_{\mu^2}^{'}(X,q)$$

which is an analogue of the classical Barban-Davenport-Halberstam Theorem with a main term (see Montgomery [30]). This result was further improved by several authors. We mention the

works of Warlimont [40], Brüdern *et al.* [6] and Vaughan [39]. It is worth mentioning that the later two results deal with the more general case of k-free numbers.

Ignoring for the moment the difference between $V'_{\mu^2}(X,q)$ and $V_{\mu^2}(X,q)$, formula (1.6) above can be interpreted as saying that, at least on average over $q \leq Q$, (1.5) is far from the truth. In this paper we investigate if such a phenomenon can be observed without the need of the extra average over q. This is indeed possible for q large enough relative to X. Our main theorem goes in this direction

Theorem 1.1.1. *Let $V_{\mu^2}(X,q)$ be defined as in* (1.4) *and $\epsilon > 0$ arbitrary. Then, uniformly for $q \leq X$, we have*

$$V_{\mu^2}(X,q) = C \prod_{p|q} \left(1 + 2p^{-1}\right)^{-1} X^{\frac{1}{2}} q^{\frac{1}{2}} + O_\epsilon\left(X^{\frac{1}{3}+\epsilon} q^{\frac{2}{3}} + X^{\frac{23}{15}+\epsilon} q^{-\frac{13}{15}}\right),$$

where

$$C = \frac{\zeta\left(\frac{3}{2}\right)}{\pi} \prod_{p} \left(\frac{p^3 - 3p + 2}{p^3}\right) = 0.167\ldots \tag{1.7}$$

and the O_ϵ-constant depends at most on ϵ.

As pointed out to the author by Zeev Rudnick, the same constant was found by Hall [18] on the main term of the second moment for the problem of squarefree numbers in short intervals. Notice that for $X^{\frac{8}{13}+\epsilon} < q < X^{1-\epsilon}$, Theorem 1.1.1 improves upon the upper bound (1.5). We have further the following direct consequence of Theorem 1.1.1

Corollary 1.1.2. *Let $V_{\mu^2}(X,q)$ be defined as in* (1.4) *and $\epsilon > 0$ arbitrary. Then we have*

$$V_{\mu^2}(X,q) \sim C \prod_{p|q} \left(1 + 2p^{-1}\right)^{-1} X^{\frac{1}{2}} q^{\frac{1}{2}} \tag{1.8}$$

as $X, q \to \infty$, with q satisfying $X^{\frac{31}{41}+\epsilon} \leq q \leq X^{1-\epsilon}$, where C is as in (1.7).

Remark 1.1.1. Asymptotic formula (1.8) gives an average order of magnitude of $O\left((X/q)^{\frac{1}{4}+\epsilon}\right)$ for the terms $E(X,q,a)$. This remark goes in the direction of a conjecture due to Montgomery (see [7, top of the page 145]), which we write under the form

$$E(X,q,a) = O_\epsilon\left((X/q)^{\frac{1}{4}+\epsilon}\right),\ \epsilon > 0 \text{ arbitrary}$$

uniformly for $(a,q) = 1$, $X^{\theta_1} < q < X^{\theta_2}$ where the values of the constants θ_1 and θ_2 satisfying $0 < \theta_1 < \theta_2 < 1$ have to be made precise.

Note that the same phenomena can be observed in the work of Croft, with an extra average over q. Such a conjecture may, of course, be interpreted in terms of the poles of the functions $\frac{L(\chi,s)}{L(\chi^2,2s)}$, where χ is a Dirichlet character modulo q.

Our technique is more general since we can also shed a light on the correlation between $E(X,q,a)$ and $E(X,q,ma)$ for fixed m with $(m,q)=1$. For $X>0$ and integers m and q such that $m\neq 0$, $(m,q)=1$, $q\geq 1$ we define

$$C[m](X,q)=\sideset{}{^*}\sum_{a \pmod q} E(X,q,a)E(X,q,ma). \tag{1.9}$$

Theorem 1.1.1 above can be deduced as a consequence of the following

Theorem 1.1.3. *Let m be a squarefree integer of arbitrary sign and $\epsilon>0$ be arbitrary. Also let $C[m](X,q)$ be defined as in* (1.9)*. Then, uniformly for $q\leq X$, $(m,q)=1$ we have*

$$C[m](X,q)=\frac{C}{2}\Gamma_{\mathrm{an}}(m)\Gamma_{\mathrm{ar}}(m)\prod_{p\mid q}\left(1+2p^{-1}\right)^{-1}X^{\frac{1}{2}}q^{\frac{1}{2}}+O_{\epsilon,m}\left(X^{\frac{1}{3}+\epsilon}q^{\frac{2}{3}}+X^{\frac{23}{15}+\epsilon}q^{-\frac{13}{15}}\right),$$

where C is as in (1.7)*, the analytic factor $\Gamma_{\mathrm{an}}(m)$ is defined by*

$$\Gamma_{\mathrm{an}}(m):=\begin{cases}\dfrac{\sqrt{m}+1-\sqrt{m-1}}{m}, \text{ if } m>0,\\[2ex] \dfrac{\sqrt{1-m}-\sqrt{-m}-1}{-m}, \text{ if } m<0,\end{cases} \tag{1.10}$$

and the arithmetic factor $\Gamma_{\mathrm{ar}}(m)$ is

$$\Gamma_{\mathrm{ar}}(m):=\prod_{p\mid m}\left(1+\frac{p+p^{\frac{1}{2}}+1}{p^{\frac{3}{2}}+p^{\frac{1}{2}}+1}\right)^{-1}; \tag{1.11}$$

and the $O_{\epsilon,m}$-constant depends at most on ϵ and m.

We restrict to the case where m is squarefree to avoid further complications, but we expect the proof to work for general m. It also follows from the proof that the dependency of the error term on m is polynomial.

The error term $O(X^{23/15+\epsilon}q^{-13/15})$ comes from the use of the square sieve (see [22]). The proof could be simplified by avoiding the use of this sieve, obtaining a worse error term. One can obtain $O(X^{5/3+\epsilon}q^{-1})$ in a rather elementary way. That would imply that the asymptotic formula (1.8) would only hold for $X^{7/9+\epsilon}\leq q\leq X^{1-\epsilon}$. Finally, notice that making the choice $m=1$, one has $\Gamma_{\mathrm{an}}(1)=2,\Gamma_{\mathrm{ar}}(1)=1$ and we retrieve Theorem 1.1.1.

1.1.1 Discussion about $\Gamma_{\mathrm{an}}(m)$ and $\Gamma_{\mathrm{ar}}(m)$

Let m be a squarefree integer. Formula (1.1.3) shows that the random variables

$$\mathbf{X}: a \pmod q \mapsto \frac{E(X,q,a)}{(X/q)^{\frac{1}{4}}} \text{ and } \mathbf{X}_m: a \pmod q \mapsto \frac{E(X,q,ma)}{(X/q)^{\frac{1}{4}}}$$

are not asymptotically independent as $X, q \to \infty$, with q satisfying $X^{\frac{31}{41}+\epsilon} \leq q \leq X^{1-\epsilon}$. This is a consequence of the fact that these random variables have asymptotic mean equal to zero (see lemma 1.3.1 below). The fact that $\mathbf{X}$ and $\mathbf{X}_m$ are dependent (when $m > 0$) can be guessed similarly as in [9, Remark 1.8], by the trivial fact that if a squarefree n satisfies

$$n \equiv a \,(\mathrm{mod}\ q), 1 \leq n \leq X/m, (n, m) = 1,$$

then $n' = mn$ satisfies

$$n' \text{ squarefree}, n' \equiv ma \,(\mathrm{mod}\ q), 1 \leq n' \leq X.$$

Such an interpretation obviously fails when $m < 0$ or m is not squarefree, which may explain the signs of $\Gamma_{\mathrm{an}}(m)$. We also remark that the random variable

$$\frac{1}{\varphi(q)} \sideset{}{^*}\sum_{m \ (\mathrm{mod}\ q)} \mathbf{X}\mathbf{X}_m$$

has asymptotic mean zero, again by lemma 1.3.1.

Finally we would like to point out some differences between Theorem 1.1.3 and [9, Theorem 1.5] from which this study was inspired. In [9, Corollary 1.7], the correlation for the divisor function exists if and only if $m > 0$, with a correlation coefficient that is always positive, while in our setting, the correlation always exists and the sign might depend on m.

1.1.2 A double sum over squarefree integers

Developing the squares in $C[m](X, q)$, we obtain the equality

$$C[m](X, q) = S[m](X, q) - 2C(q)\frac{X}{q} \sum_{\substack{n \leq X \\ (n,q)=1}} \mu^2(n) + \varphi(q)\left(C(q)\frac{X}{q}\right)^2, \tag{1.12}$$

where

$$C(q) = \frac{6}{\pi^2} \prod_{p|q} \left(1 - \frac{1}{p^2}\right)^{-1}, \tag{1.13}$$

and $S[m](X, q)$ is the double sum

$$S[m](X, q) = \sum_{\substack{n_1, n_2 \leq X \\ (n_1 n_2, q)=1 \\ mn_1 = n_2 \ (\mathrm{mod}\ q)}} \sum \mu^2(n_1)\mu^2(n_2). \tag{1.14}$$

Thus an important step in proving Theorem 1.1.1 is providing an asymptotic formula for $S[m](X, q)$, which is the subject of our next Theorem.

Theorem 1.1.4. *Let $X > 2$ be a real number and $\epsilon > 0$ be arbitrary. Let m be a squarefree integer of arbitrary sign. Then, uniformly for $q \leq X$, $(m, q) = 1$, we have*

$$S[m](X,q)=\varphi(q)\left(\frac{C(q)X}{q}\right)^2+\frac{C}{2}\Gamma_{\mathrm{an}}(m)\Gamma_{\mathrm{ar}}(m)\prod_{p\mid q}\left(1+2p^{-1}\right)^{-1}X^{\frac{1}{2}}q^{\frac{1}{2}}$$
$$+O_{\epsilon,m}\left(X^{\frac{1}{3}+\epsilon}q^{\frac{2}{3}}+X^{\frac{23}{15}+\epsilon}q^{-\frac{13}{15}}\right),$$

where C, $C(q)$ are as in (1.7) *and* (1.13) *respectively, $\Gamma_{\mathrm{an}}(m)$ and $\Gamma_{\mathrm{ar}}(m)$ are as in* (1.10) *and* (1.11) *respectively; and the implied $O_{\epsilon,m}$-constant depends at most on ϵ and m.*

The notation used throughout the paper is given in section 1.2. In section 1.3 we prove that Theorem 1.1.4 implies Theorem 1.1.3. In section 1.4 we break up $S[m](X,q)$ (see (1.14) above) into two sums $S_{\leq y}[m](X,q)$ and $S_{>y}[m](X,q)$, and begin the study of the first of these sums. In section 1.5 we prove some lemmas that prove to be useful in the following section, where we evaluate the main term. Section 1.7 is dedicated to the estimation of $S_{>y}[m](X,q)$ by means of the square sieve. In this section, we use some upper bounds for exponential sums that are proven in section 1.9. Finally, the proof of Theorem 1.1.4 is given in section 1.8.

1.2 Notation

For a finite set S, $\#S$ denotes its cardinality. Let ω be the well-known function defined by

$$\omega(n)=\#\{p \text{ prime }; p\mid n\},$$

for every integer $n\geq 1$. For $N>0$, we use the notation $n\sim N$ to mean $N<n\leq 2N$. Let $\psi(v)$ denote the sawtooth function defined by

$$\lfloor v\rfloor = v-\frac{1}{2}+\psi(v). \tag{1.15}$$

For $n\in\mathbb{Z}, n\neq 0$ we define

$$\sigma(n)=\prod_{p^2\mid n}p. \tag{1.16}$$

If $A\subset\mathbb{R}$ and $\alpha\in\mathbb{R}$, then

$$\alpha A:=\{\alpha x;\ x\in A\}.$$

For a measurable set $A\subset\mathbb{R}$, $|A|$ denotes its Lebesgue measure.

1.3 Proof of Theorem 1.1.3 assuming Theorem 1.1.4

We start with the following lemma, whose proof follows closely that of [20, Theorem 333]

Lemma 1.3.1. *Let $\epsilon>0$ be given. We then have the equality*

$$\sum_{\substack{n\leq X\\(n,q)=1}}\mu^2(n)=\frac{\varphi(q)}{q}\frac{6}{\pi^2}\prod_{p\mid q}\left(1-\frac{1}{p^2}\right)^{-1}X+O_\epsilon\left(X^{\frac{1}{2}+\epsilon}\right),$$

uniformly for $1\leq q\leq X$, where the O_ϵ-constant depends on ϵ alone.

By Lemma 1.3.1 and (1.12), we have the equality

$$C[m](X,q) = S[m](X,q) - \varphi(q)\left(C(q)\frac{X}{q}\right)^2 + O(X^{\frac{3}{2}+\epsilon}q^{-1}).$$

Now, we use Theorem 1.1.4 for the term $S[m](X,q)$ and the main terms disappear. We deduce

$$C[m](X,q) = \frac{C}{2}\Gamma_{\mathrm{an}}(m)\Gamma_{\mathrm{ar}}(m)\prod_{p|q}\left(1+2p^{-1}\right)^{-1}X^{\frac{1}{2}}q^{\frac{1}{2}} + O_{\epsilon,m}(X^{\frac{1}{3}+\epsilon}q^{\frac{2}{3}} + X^{\frac{23}{15}+\epsilon}q^{-\frac{13}{15}} + X^{\frac{3}{2}+\epsilon}q^{-1}),$$

and the second error term dominates the last one. This concludes the proof of Theorem 1.1.3.

1.4 Initial Steps

We are considering the sum

$$S[m](X,q) = \sum_{\substack{n_1,n_2\leq X\\(n_1n_2,q)=1\\ mn_1=n_2 \pmod q}}\sum \mu^2(n_1)\mu^2(n_2).$$

We put $\ell q = n_2 - mn_1$ and write $S[m](X,q)$ as

$$S[m](X,q) = \sum_{\ell\in\mathbb{Z}}\sum_{\substack{n\in I(\ell)\\(n,q)=1}}\mu^2(n)\mu^2(mn+\ell q), \tag{1.17}$$

where $I(\ell)$ is the interval defined by

$$I(\ell) = \begin{cases}(0,X)\cap\left(\frac{-\ell q}{m},\frac{X-\ell q}{m}\right) & \text{if } m>0\\ (0,X)\cap\left(\frac{X-\ell q}{m},\frac{-\ell q}{m}\right) & \text{if } m<0.\end{cases} \tag{1.18}$$

Note that since $\mu^2(n)\mu^2(mn+h)=1$ if and only if $\sigma(n)\sigma(mn+h)=1$ (recall definition (1.16)), we have

$$\mu^2(n)\mu^2(mn+h) = \sum_{d|\sigma(n)\sigma(mn+h)}\mu(d). \tag{1.19}$$

We now use formula (1.19) with $h=\ell q$ in equation (1.17) and change the order of summation. We thus obtain

$$S[m](X,q) = \sum_{\ell\in\mathbb{Z}}\sum_{\substack{1\leq d\leq X\\(d,q)=1}}\mu(d)N_d(\ell), \tag{1.20}$$

where

$$N_d(\ell) := \#\{n\in I(\ell); (n,q)=1 \text{ and } \sigma(n)\sigma(mn+\ell q)\equiv 0 \pmod d\}. \tag{1.21}$$

Let $0 < y < X$ be a parameter to be chosen later depending on X and q. We break up the sum in (1.20) as follows

$$S[m](X,q) = S_{\leq y}[m](X,q) + S_{>y}[m](X,q), \tag{1.22}$$

where

$$\begin{cases} S_{\leq y}[m](X,q) = \sum_{\ell\in\mathbb{Z}} \sum_{\substack{d\leq y \\ (d,q)=1}} \mu(d) N_d(\ell), \\ S_{>y}[m](X,q) = \sum_{\ell\in\mathbb{Z}} \sum_{\substack{y<d\leq X \\ (d,q)=1}} \mu(d) N_d(\ell). \end{cases} \tag{1.23}$$

Lemma 1.4.1. *Let $m \neq 0$ be a squarefree number and $y > 1$. Let $S_{\leq y}[m](X,q)$ be defined by (1.23). Then we have*

$$S_{\leq y}[m](X,q) = \sum_{\ell\in\mathbb{Z}} f_q(\ell,m)\, |I(\ell)| + O_m\left(\frac{X}{q}\left(d(q)y + Xy^{-1}\right)\log y\right),$$

uniformly for $X, y > 1$ and $q \geq 1$ satisfying $(m,q) = 1$, where

$$f_q(\ell,m) = C_2 \prod_{p\mid m}\left(\frac{p^2-1}{p^2-2}\right)\prod_{p\mid q}\left(\frac{p^2-p}{p^2-2}\right)\kappa((\ell,m^2))\prod_{\substack{p^2\mid\ell \\ p\nmid mq}}\left(\frac{p^2-1}{p^2-2}\right), \tag{1.24}$$

$$C_2 = \prod_p\left(1-\frac{2}{p^2}\right), \tag{1.25}$$

κ is the multiplicative function defined by

$$\kappa(p^\alpha) = \begin{cases} \dfrac{p^2-p-1}{p^2-1}, & \text{if } \alpha = 1, \\ \dfrac{p^2-p}{p^2-1}, & \text{if } \alpha = 2, \\ 0, & \text{if } \alpha \geq 3, \end{cases} \tag{1.26}$$

and the implied constant depends at most on m.

Démonstration. Let

$$u_p(\ell) := \#\{v \pmod{p^2}; v \equiv 0 \pmod{p^2} \text{ or } mv + \ell \equiv 0 \pmod{p^2}\}. \tag{1.27}$$

Notice that if $(p,r) = 1$, then $u_p(\ell r) = u_p(\ell)$.

Using Möbius inversion, we have that for every squarefree d coprime to q,

$$N_d(\ell) = \sum_{d'\mid q}\mu(d')\widetilde{N}_{d,d'}(\ell), \tag{1.28}$$

where

$$\widetilde{N}_{d,d'}(\ell) = \#\left\{n' \in \frac{1}{d'}I(\ell); \sigma(d'n')\sigma(d'(mn'+\ell q')) \equiv 0 \pmod{d}\right\}$$

and $q' = q/d'$. Since we have $(d, d') = 1$, then

$$\widetilde{N}_{d,d'}(\ell) = \# \left\{ n' \in \frac{1}{d'} I(\ell); \sigma(n')\sigma(mn' + \ell q') \equiv 0 \pmod{d} \right\}.$$

By the Chinese remainder theorem and (1.27) (notice that $(p, q') = 1$, whenever $p \mid d$), we have

$$\widetilde{N}_{d,d'}(\ell) = \frac{U_d(\ell)}{d^2} \frac{|I(\ell)|}{d'} + O(U_d(\ell)), \tag{1.29}$$

where

$$U_d(\ell) := \prod_{p|d} u_p(\ell).$$

Injecting (1.29) in (1.28), we deduce

$$N_d(\ell) = \frac{\varphi(q)}{q} |I(\ell)| \frac{U_d(\ell)}{d^2} + O\left(d(q) U_d(\ell)\right). \tag{1.30}$$

Notice further that if $(p, m) = 1$, then $u_p(\ell) \leq 2$. Hence we have the upper bound

$$U_d(\ell) \ll_m 2^{\omega(d)}. \tag{1.31}$$

From (1.30) and the upper bound (1.31), we deduce

$$\begin{aligned} \sum_{\substack{d \leq y \\ (d,q)=1}} \mu(d) N_d(\ell) &= \frac{\varphi(q)}{q} |I(\ell)| \sum_{\substack{d \leq y \\ (d,q)=1}} \frac{\mu(d) U_d(\ell)}{d^2} + O_m\left(d(q) y \log y\right) \\ &= \frac{\varphi(q)}{q} \prod_{p \nmid q} \left(1 - \frac{u_p(\ell)}{p^2}\right) |I(\ell)| + O_m\left(d(q) y \log y + X y^{-1} \log y\right), \end{aligned} \tag{1.32}$$

where in the second line we used the trivial bound $|I(\ell)| \leq X$ as well as the convergence of the infinite product appearing. Observe that if $|\ell| > \dfrac{(|m|+1)X}{q}$, the set $I(\ell)$ is empty and hence $N_d(\ell) = 0$ for every d. Combining this observation and equation (1.32), we deduce

$$\begin{aligned} S_{\leq y}[m](X, q) &= \sum_{|\ell| \leq \frac{(|m|+1)X}{q}} \sum_{\substack{d \leq y \\ (d,q)=1}} \mu(d) N_d(\ell) \\ &= \frac{\varphi(q)}{q} \sum_{|\ell| \leq \frac{(|m|+1)X}{q}} \prod_{p \nmid q} \left(1 - \frac{u_p(\ell)}{p^2}\right) |I(\ell)| + O_m\left(\frac{X}{q} \left(d(q) y + X y^{-1}\right) \log y\right) \\ &= \frac{\varphi(q)}{q} \sum_{\ell \in \mathbb{Z}} \prod_{p \nmid q} \left(1 - \frac{u_p(\ell)}{p^2}\right) |I(\ell)| + O_m\left(\frac{X}{q} \left(d(q) y + X y^{-1}\right) \log y\right). \end{aligned} \tag{1.33}$$

We finish by computing of $u_p(\ell)$ for every $p \nmid q$. We distinguish five different cases.

— If $p \mid m$, $p^2 \mid \ell$, then

$$u_p(\ell) = p;$$

— If $p \mid m$, $p \mid \ell$ but $p^2 \nmid \ell$, then
$$u_p(\ell) = p + 1;$$
— If $p \mid m$, $p \nmid \ell$, then
$$u_p(\ell) = 1;$$
— If $p \nmid m$, $p^2 \mid \ell$, then
$$u_p(\ell) = 1;$$
— If $p \nmid m$, $p^2 \nmid \ell$, then
$$u_p(\ell) = 2.$$

The proof now follows from (1.33) and the different values of $u_p(\ell)$. □

Using Lemma 1.4.1 for $S_{\leq y}[m](X, q)$ in (1.22), we obtain

$$S[m](X, q) = \mathcal{A}[m](X, q) + S_{>y}[m](X, q) + O_m\left(\frac{X}{q}\left(d(q)y + Xy^{-1}\right)\log y\right), \tag{1.34}$$

where

$$\mathcal{A}[m](X, q) = \sum_{\ell\in\mathbb{Z}} f_q(\ell, m)|I(\ell)|. \tag{1.35}$$

1.5 Preparatory results

In the next section we evaluate the sum $\mathcal{A}[m](X, q)$. But first we prove some preliminary results that shall be useful. We start with a lemma that is a simplified version of [7, Lemma 1].

Lemma 1.5.1. *For $X > 1$, $0 < s < 2$, and $\psi(v)$ defined by (1.15),*

$$\int_0^X \psi(v)v^{-\frac{s}{2}}dv = \frac{\zeta(\frac{s}{2} - 1)}{(\frac{s}{2} - 1)} + O\left(X^{-\frac{s}{2}}\right),$$

where the O-constant is absolute.

Démonstration. We have the formula (see [36, equation (2.1.6)])

$$\zeta\left(\frac{s}{2} - 1\right) = \left(\frac{s}{2} - 1\right)\int_0^\infty \psi(v)v^{-\frac{s}{2}}dv,\ (0 < \sigma < 2),$$

where σ denotes the real part of s. We estimate the tail of the integral

$$I = \int_X^\infty \psi(v)v^{-\frac{s}{2}}dv. \tag{1.36}$$

Let $\Psi(v)$ be given by

$$\Psi(v) := \int_0^v \psi(u)du. \tag{1.37}$$

Integration by parts gives

$$I = \Psi(X)X^{-\frac{s}{2}} + \frac{s}{2}\int_X^\infty \Psi(v)v^{-\frac{s}{2}-1}dv.$$

Notice that since $\int_0^1 \psi(v)dv = 0$, Ψ is periodic and thus bounded. Hence, we have

$$I \ll X^{-\frac{s}{2}},$$

which concludes the proof. □

Let $h(d)$ be the multiplicative function defined by

$$h(d) := \mu^2(d)\prod_{p|d}\left(1-2p^{-2}\right)^{-1}. \tag{1.38}$$

This function appears naturally when we study $\mathcal{A}[m](X,q)$ (see (1.35)). The next lemma expresses the function $h(d)$ as a convolution between the identity and a function of rapid decay.

Lemma 1.5.2. *Let $h(d)$ be as in* (1.38)*. Then we have*

$$h(d) = \sum_{d_1d_2=d}\beta(d_1),$$

where $\beta(t)$ is supported on cubefree numbers. Furthermore, for every cubefree integer t, if we write $t = ab^2$ with a, b squarefree, $(a,b) = 1$, we have

$$\beta(t) \ll \frac{d(a)}{a^2}.$$

Démonstration. It is easy to calculate the values of β on prime powers

$$\beta(p^k) = \begin{cases} 1, \text{ if } k = 0, \\ \frac{2}{p^2-2}, \text{ if } k = 1, \\ \frac{-p^2}{p^2-2}, \text{ if } k = 2, \\ 0, \text{ otherwise.} \end{cases}$$

The lemma now follows because the product

$$\prod_p\left(\frac{p^2}{p^2-2}\right)$$

is convergent.

□

The next lemma is based on [7, Lemma 3]. However, there are some confusing steps in the corresponding proof as it was also pointed out by Vaughan (see [39, page 574]). In particular, the value for the constant B (see [7, equation 6.3]) is wrong.

Lemma 1.5.3. *For $Y > 0$ and r an integer ≥ 1, let*

$$G(Y,r) := \sum_{(d,r)=1} h(d)\Psi\left(\frac{Y}{d^2}\right), \tag{1.39}$$

where $\Psi(v)$ is as in (1.37) and $h(d)$ by (1.38). We have, uniformly for $Y \geq 1$ and $r \neq 0$,

$$G(Y,r) = C' \prod_{p|r} \left(1 + p(p^2-2)^{-1}\right)^{-1} Y^{\frac{1}{2}} + O\left(d(r)Y^{\frac{1}{3}}\right), \tag{1.40}$$

where C' is given by

$$C' = \frac{\zeta\left(\frac{3}{2}\right)}{2\pi} \prod_{p} \left(\frac{p^3 - 3p + 2}{p(p^2-2)}\right), \tag{1.41}$$

and the O-constant is absolute.

Démonstration. We first prove the related formula

$$\sum_{(d,r)=1} \Psi\left(\frac{Y}{d^2}\right) = \frac{\varphi(|r|)}{|r|} \frac{\zeta(\frac{3}{2})}{2\pi} Y^{\frac{1}{2}} + O\left(d(r)Y^{\frac{1}{3}}\right). \tag{1.42}$$

Let $D = D(Y) > 0$ to be chosen later. We have, since Ψ is bounded,

$$\sum_{(d,r)=1} \Psi\left(\frac{Y}{d^2}\right) = \sum_{\substack{d>D \\ (d,r)=1}} \Psi\left(\frac{Y}{d^2}\right) + O(D). \tag{1.43}$$

Changing the order of summation and integration, we have

$$\begin{aligned}
\sum_{\substack{d>D \\ (d,r)=1}} \Psi\left(\frac{Y}{d^2}\right) &= \int_0^{\frac{Y}{D^2}} \psi(v) \sum_{\substack{D<d\leq\sqrt{\frac{Y}{v}} \\ (d,r)=1}} 1 dv \\
&= \int_0^{\frac{Y}{D^2}} \psi(v) \left(\frac{\varphi(|r|)}{|r|}\left((Y/v)^{\frac{1}{2}} - D\right) + O(d(r))\right) dv \\
&= \frac{\varphi(|r|)}{|r|} Y^{\frac{1}{2}} \int_0^{\frac{Y}{D^2}} \psi(v) v^{-\frac{1}{2}} dv + O\left(D + d(r)\frac{Y}{D^2}\right).
\end{aligned}$$

By lemma 1.5.1, the above equation implies

$$\sum_{\substack{d>D\\(d,r)=1}} \Psi\left(\frac{Y}{d^2}\right) = \frac{-2\varphi(|r|)}{|r|}\zeta\left(-\frac{1}{2}\right)Y^{\frac{1}{2}} + O\left(D + d(r)\frac{Y}{D^2}\right). \tag{1.44}$$

We make the choice $D = Y^{\frac{1}{3}}$. Formula (1.42) is now just a consequence of (1.43), (1.44) and the functional equation for the Riemann zeta function, which for $s = -1/2$ gives

$$\zeta\left(-\frac{1}{2}\right) = -\frac{\zeta\left(\frac{3}{2}\right)}{4\pi}.$$

We now deduce (1.40) from (1.42). We can write

$$G(Y,r) = \sum_{(d_1,r)=1} \beta(d_1) \sum_{(d_2,r)=1} \Psi\left(\frac{Y}{d_1^2 d_2^2}\right). \tag{1.45}$$

We have two possibilities. If $d_1^2 \leq Y$, we shall use formula (1.42) for the inner sum on the right-hand side of (1.45). If, otherwise, $d_1^2 > Y$, we shall use the trivial bound

$$\sum_{(d_2,r)=1} \Psi\left(\frac{Y}{d_1^2 d_2^2}\right) \leq \sum_{d_2} \frac{Y}{d_1^2 d_2^2} \ll \frac{Y}{d_1^2}.$$

Thus, we deduce from (1.45) that

$$G(Y,r) = \frac{\varphi(|r|)}{|r|}\frac{\zeta(\frac{3}{2})}{2\pi}Y^{\frac{1}{2}} \sum_{\substack{d_1\leq\sqrt{Y}\\(d_1,r)=1}} \frac{\beta(d_1)}{d_1} + O\left(d(r)Y^{\frac{1}{3}} \sum_{\substack{d_1\leq\sqrt{Y}\\(d_1,r)=1}} \frac{\beta(d_1)}{d_1^{\frac{2}{3}}} + Y \sum_{\substack{d_1>\sqrt{Y}\\(d_1,r)=1}} \frac{\beta(d_1)}{d_1^2}\right).$$

By completing the first term and using lemma 1.5.2, we have

$$G(Y,r) = C_\beta(r)\frac{\varphi(|r|)}{|r|}\frac{\zeta(\frac{3}{2})}{2\pi}Y^{\frac{1}{2}} + O\left(d(r)Y^{\frac{1}{3}}\sum_{ab^2\leq\sqrt{Y}}\sum\frac{d(a)}{a^{\frac{8}{3}}b^{\frac{4}{3}}}\right) + O\left(Y^{\frac{1}{2}}\sum_{ab^2>\sqrt{Y}}\sum\frac{d(a)}{a^3b^2} + Y\sum_{ab^2>\sqrt{Y}}\sum\frac{d(a)}{a^4b^4}\right), \tag{1.46}$$

where

$$C_\beta(r) = \sum_{(d_1,r)=1}\frac{\beta(d_1)}{d_1} = \prod_p\left(1-\frac{p-2}{p(p^2-2)}\right)\prod_{p|r}\left(1-\frac{p-2}{p(p^2-2)}\right)^{-1}.$$

The first error term on the right-hand side of (1.46) is clearly $\ll d(r)Y^{\frac{1}{3}}$. For the second one, we have

$$\sum_{ab^2>\sqrt{Y}}\frac{d(a)}{a^3b^2} \leq \sum_{ab>Y^{\frac{1}{4}}}\frac{d(a)}{a^2b^2} \ll Y^{-\frac{1}{4}}(\log Y)^2,$$

and analogously, the last one satisfies

$$\sum_{ab^2>\sqrt{Y}} \frac{d(a)}{a^4b^4} \ll Y^{-\frac{3}{4}}(\log Y)^2.$$

Once we inject these upper bounds in equation (1.46), we obtain

$$G(Y,r) = C' \prod_{p|r} \left(1 + p(p^2-2)^{-1}\right)^{-1} Y^{\frac{1}{2}} + O\left(d(r)Y^{\frac{1}{3}} + Y^{\frac{1}{4}}(\log Y)^2\right),$$

which concludes the proof of formula (1.40). □

In the following lemma we gather a series of identities that shall be useful later on, and whose proofs are routine and hence omitted.

Lemma 1.5.4. *Let m be a squarefree integer and let $\kappa(\rho)$ be as in* (1.26)*, then we have the equalities*

$$\begin{cases} \displaystyle\sum_{\rho\sigma|m^2} \frac{\kappa(\rho)\mu(\sigma)}{\rho\sigma} = \prod_{p|m} \left(\frac{p^2-1}{p^2}\right), \\ \displaystyle\sum_{\rho\sigma|m^2} \kappa(\rho)\mu(\sigma) = \prod_{p|m} \left(\frac{p^2-p}{p^2-1}\right), \\ \displaystyle\sum_{\rho\sigma|m^2} \kappa(\rho)\mu(\sigma)\rho^{\frac{1}{2}}\sigma^{\frac{1}{2}} = \prod_{p|m} \left(\frac{p^2-p^{\frac{3}{2}}+p-1}{p^2-1}\right). \end{cases}$$

Also, let $r \neq 0$ be an integer, and let $h(d)$ be as in (1.38)*. Then we have further the equalities*

$$\begin{cases} \displaystyle\sum_{(d,r)=1} \frac{h(d)}{d^4} = \prod_{p} \left(\frac{(p^2-1)^2}{p^2(p^2-2)}\right) \prod_{p|r} \left(\frac{(p^2-1)^2}{p^2(p^2-2)}\right)^{-1}, \\ \displaystyle\sum_{(d,r)=1} \frac{h(d)}{d^2} = \prod_{p} \left(\frac{p^2-1}{p^2-2}\right) \prod_{p|r} \left(\frac{p^2-1}{p^2-2}\right)^{-1}. \end{cases}$$

Finally, let $m \neq 0$ be squarefree and q be a positive integer. Also let $f_q(\ell, m)$ be as in (1.24) *and $C(q)$ be as in definition* (1.13)*. Then, we have the following equality*

$$f_q(0,m) = \frac{\varphi(|mq|)}{|mq|} C(mq).$$

Let

$$\mathfrak{S}[m](Y,q) := \sum_{0<\ell\leq Y} f_q(\ell,m)(Y-\ell). \tag{1.47}$$

The following Proposition gives a formula for $\mathfrak{S}[m](Y,q)$ by means of the previous lemmas.

Proposition 1.5.5. *Let $m \neq 0$ be an integer and let $f_q(\ell,m)$ be defined by* (1.24)*. Then, uniformly for $Y, q \geq 1$, we have*

$$\mathfrak{S}[m](Y,q) = \frac{\varphi(q)}{2q} C(q)^2 Y^2 - \frac{\varphi(|mq|)}{2|mq|} C(mq) Y + \frac{C}{2} \Gamma_{\mathrm{ar}}(m) \prod_{p|q} (1+2p^{-1})^{-1} Y^{\frac{1}{2}} + O_m(d(q)Y^{\frac{1}{3}}),$$

where C and $\Gamma_{\mathrm{ar}}(m)$ are as in (1.7) *and* (1.11) *respectively, $C(r)$ is as in* (1.13) *for $r = q, mq$, and the implied O_m-constant depends at most on m.*

Démonstration. We recall (1.24) and use Lemma 1.5.4 for the innermost product. We have

$$f_q(\ell, m) = C_2 \prod_{p|m} \left(\frac{p^2-1}{p^2-2}\right) \prod_{p|q} \left(\frac{p^2-p}{p^2-2}\right) \kappa((\ell, m^2)) \sum_{\substack{d^2|\ell \\ (d,mq)}} \frac{h(d)}{d^2},$$

where C_2 is as in (1.25). We notice that the first three factors on the right-hand side of the above equation are independent of ℓ. Therefore, in order to evaluate $\mathfrak{S}[m](Y,q)$, we need to study

$$\begin{aligned}
\mathfrak{S}'[m](Y,q) &:= \sum_{0<\ell\leq Y} \kappa((\ell, m^2)) \sum_{\substack{d^2|\ell \\ (d,mq)=1}} \frac{h(d)}{d^2} (Y-\ell) \\
&= \sum_{\rho|m^2} \kappa(\rho) \sum_{\substack{0<\ell\leq Y \\ (\ell,m^2)=\rho}} (Y-\ell) \sum_{\substack{d^2|\ell \\ (d,mq)=1}} \frac{h(d)}{d^2} \\
&= \sum_{\rho\sigma|m^2} \kappa(\rho)\mu(\sigma)\rho\sigma \sum_{(d,mq)=1} \frac{h(d)}{d^2} \sum_{\substack{0<\ell_0\leq \frac{Y}{\rho\sigma} \\ d^2|\ell_0}} \left(\frac{Y}{\rho\sigma} - \ell_0\right)
\end{aligned} \tag{1.48}$$

where in the third line we used Möbius inversion to detect the coprimality condition. We proceed by writing the inner sum as an integral. We have

$$\begin{aligned}
\sum_{\substack{0<\ell_0<\frac{Y}{\rho\sigma} \\ d^2|\ell_0}} \left(\frac{Y}{\rho\sigma} - \ell_0\right) &= \sum_{\substack{0<\ell_0\leq\frac{Y}{\rho\sigma} \\ d^2|\ell_0}} \int_{\ell_0}^{\frac{Y}{\rho\sigma}} 1du \\
&= \int_0^{\frac{Y}{\rho\sigma}} \sum_{\substack{0<\ell_0\leq u \\ d^2|\ell_0}} 1du = \int_0^{\frac{Y}{\rho\sigma}} \left\lfloor \frac{u}{d^2} \right\rfloor du.
\end{aligned} \tag{1.49}$$

Recall formula (1.15) defining the sawtooth function ψ

$$\lfloor x \rfloor = x - \frac{1}{2} + \psi(x).$$

This formula when used in equation (1.49) gives

$$\sum_{\substack{0<\ell_0\leq\frac{Y}{\rho\sigma} \\ d^2|\ell_0}} \left(\frac{Y}{\rho\sigma} - \ell_0\right) = \frac{Y^2}{2\rho^2\sigma^2 d^2} - \frac{Y}{2\rho\sigma} + d^2\Psi\left(\frac{Y}{\rho\sigma d^2}\right).$$

Injecting this formula in (1.48), we deduce the equality

$$\mathfrak{S}'[m](Y,q) = \lambda_2(m,q)Y^2 - \lambda_1(m,q)Y + \sum_{\rho\sigma|m^2} \kappa(\rho)\mu(\sigma)\rho\sigma G\left(\frac{Y}{\rho\sigma}, mq\right), \tag{1.50}$$

where

$$\lambda_2(m,q)=\frac{1}{2}\sum_{\rho\sigma|m^2}\frac{\kappa(\rho)\mu(\sigma)}{\rho\sigma}\times\sum_{(d,mq)=1}\frac{h(d)}{d^4},$$
$$\lambda_1(m,q)=\frac{1}{2}\sum_{\rho\sigma|m^2}\kappa(\rho)\mu(\sigma)\times\sum_{(d,mq)=1}\frac{h(d)}{d^2},$$

and $G(Y,q)$ is as defined in (1.39). The study of the last sum in the right-hand side of (1.50) is divided in two cases. If $\frac{Y}{\rho\sigma}\geq 1$, we use formula (1.40) to obtain

$$G\left(\frac{Y}{\rho\sigma},mq\right)=C'\prod_{p|mq}\left(1+p(p^2-2)^{-1}\right)^{-1}\left(\frac{Y}{\rho\sigma}\right)^{\frac{1}{2}}+O\left(d(mq)\left(\frac{Y}{\rho\sigma}\right)^{\frac{1}{3}}\right).$$

On the other hand, if $\frac{Y}{\rho\sigma}<1$, we have both $\left(\frac{Y}{\rho\sigma}\right)^{\frac{1}{2}}\ll 1$ and

$$G\left(\frac{Y}{\rho\sigma},mq\right)\ll\sum_{d\geq 1}\frac{Y}{\rho\sigma d^2}\ll 1.$$

Hence in this case we can write

$$G\left(\frac{Y}{\rho\sigma},mq\right)=C'\prod_{p|mq}\left(1+p(p^2-2)^{-1}\right)^{-1}\left(\frac{Y}{\rho\sigma}\right)^{\frac{1}{2}}+O\left(1\right).$$

Combining the estimates above we get

$$\sum_{\rho\sigma|m^2}\kappa(\rho)\mu(\sigma)\rho\sigma G\left(\frac{Y}{\rho\sigma},mq\right)=\lambda(m,q)Y^{\frac{1}{2}}+O_m(d(q)Y^{\frac{1}{3}}),\tag{1.51}$$

where

$$\lambda(m,q)=C'\prod_{p|mq}\left(1+\frac{p}{p^2-2}\right)^{-1}\sum_{\rho\sigma|m^2}\kappa(\rho)\mu(\sigma)\rho^{\frac{1}{2}}\sigma^{\frac{1}{2}}.$$

Now, putting together (1.50) and (1.51), we obtain

$$\mathfrak{S}'[m](Y,q)=\lambda_2(m,q)Y^2-\lambda_1(m,q)Y+\lambda(m,q)Y^{\frac{1}{2}}+O_m(d(q)Y^{\frac{1}{3}}).$$

Hence

$$\mathfrak{S}[m](Y,q)=\Lambda_2(m,q)Y^2-\Lambda_1(m,q)Y+\Lambda(m,q)Y^{\frac{1}{2}}+O_m(d(q)Y^{\frac{1}{3}}),\tag{1.52}$$

where

$$\begin{cases}\Lambda(m,q)=C_2\prod_{p|m}\left(\frac{p^2-1}{p^2-2}\right)\prod_{p|q}\left(\frac{p^2-p}{p^2-2}\right)\lambda(m,q),\\ \Lambda_i(m,q)=C_2\prod_{p|m}\left(\frac{p^2-1}{p^2-2}\right)\prod_{p|q}\left(\frac{p^2-p}{p^2-2}\right)\lambda_i(m,q),\ i=1,2.\end{cases}$$

Lemma 1.5.4 ensures that the constants $\Lambda_2(m,q),\Lambda_1(m,q)$ and $\Lambda(m,q)$ correspond to the constants in Proposition (1.5.5). Hence the result follows from (1.52). □

1.6 Main term

In this section we show how to use the results from the previous section to exhibit an asymptotic formula for $\mathcal{A}[m](X,q)$ (see (1.35)). We prove the following

Proposition 1.6.1. *For $X>1$, and integers m,q such that m is squarefree and $q\geq 1$, let $\mathcal{A}[m](X,q)$ be defined by formula (1.35). Then we have, uniformly for $X,q>1$,*

$$\mathcal{A}[m](X,q)=\varphi(q)\left(C(q)\frac{X}{q}\right)^2+\frac{C}{2}\Gamma_{\mathrm{an}}(m)\Gamma_{\mathrm{ar}}(m)\prod_{p\mid q}(1+2p^{-1})^{-1}X^{\frac{1}{2}}q^{\frac{1}{2}}+O_m\left(d(q)X^{\frac{1}{3}}q^{\frac{2}{3}}\right),$$

where C, $C(q)$, $\Gamma_{\mathrm{an}}(m)$ and $\Gamma_{\mathrm{ar}}(m)$ are as in (1.7), (1.13), (1.10) and (1.11), respectively, and the implied O_m-constant depends at most on m.

Démonstration. There is a slight difference depending on whether $m>0$ or $m<0$. So we study the two cases separately.

The case $m>0$

By analyzing the possible values of $|I(\ell)|$, we have

$$\mathcal{A}[m](X,q)=f_q(0,m)\frac{X}{m}+\sum_{0<\ell\leq\frac{X}{q}}f_q(\ell,m)\left(\frac{X-\ell q}{m}\right)+\sum_{-\frac{(m-1)X}{q}\leq\ell<0}f_q(\ell,m)\frac{X}{m}+\sum_{-\frac{mX}{q}\leq\ell<-\frac{(m-1)X}{q}}f_q(\ell,m)\left(X+\frac{\ell q}{m}\right).\quad(1.53)$$

We remark that for m,q fixed, $f_q(\ell,m)$ only depends on the positive divisors of ℓ (see formula (1.24)). Hence $f_q(\ell,m)=f_q(-\ell,m)$. As a consequence, formula (1.53) implies that

$$\mathcal{A}[m](X,q)=f_q(0,m)\frac{X}{m}+\frac{1}{m}\sum_{0<\ell\leq\frac{X}{q}}f_q(\ell,m)\left(X-\ell q\right)-\frac{1}{m}\sum_{0<\ell\leq\frac{(m-1)X}{q}}f_q(\ell,m)\left((m-1)X-\ell q\right)+\frac{1}{m}\sum_{0<\ell\leq\frac{mX}{q}}f_q(\ell,m)\left(mX-\ell q\right).$$

That is

$$\mathcal{A}[m](X,q)=f_q(0,m)\frac{X}{m}+\frac{q}{m}\Big\{\mathfrak{S}[m](X/q,q)-\mathfrak{S}[m]((m-1)X/q,q)+\mathfrak{S}[m](mX/q,q)\Big\},\quad(1.54)$$

where $\mathfrak{S}[m](Y,q)$ is as in (1.47). By Proposition 1.5.5, we have

$$\mathfrak{S}[m](Y,q)=\frac{\varphi(q)}{2q}C(q)^2Y^2+\frac{\varphi(|mq|)}{2|mq|}C(mq)Y+\frac{C}{2}\Gamma_{\mathrm{ar}}(m)\prod_{p|q}(1+2p^{-1})^{-1}Y^{\frac{1}{2}}+O_m\left(d(q)Y^{\frac{1}{3}}\right).$$

Hence, (1.54) implies that

$$\mathcal{A}[m](X,q)=f_q(0,m)\frac{X}{m}+\varphi(q)C(q)^2\left(\frac{X}{q}\right)^2-\frac{\varphi(|mq|)}{|mq|}C(mq)\frac{X}{m}$$
$$+\frac{C}{2}\Gamma_{\mathrm{an}}(m)\Gamma_{\mathrm{ar}}(m)\prod_{p|q}(1+2p^{-1})^{-1}X^{\frac{1}{2}}q^{\frac{1}{2}}+O_m\left(d(q)X^{\frac{1}{3}}q^{\frac{2}{3}}\right),$$

where $\Gamma_{\mathrm{an}}(m)$ is as in (1.10). Now, by lemma 1.5.4, the first and third terms cancel each other out. This concludes the proof of the Proposition when $m>0$.

The case $m<0$

Analogously to the previous case, we have

$$\mathcal{A}[m](X,q)=\frac{q}{m}\left\{\mathfrak{S}[m](X/q,q)+\mathfrak{S}[m](-mX/q,q)-\mathfrak{S}[m]((1-m)X/q,q)\right\}$$

and, again by Proposition 1.5.5, the result holds in this case as well.

□

1.7 Bounding $S_{>y}[m](X,q)$

In the present section we give a bound for $S_{>y}[m](X,q)$ (recall (1.23)). We start by noticing that $d^2\mid\sigma(n)\sigma(mn+\ell q)$ if and only if there exist j,k such that $d=jk$ and both $j^2\mid n$ and $k^2\mid mn+\ell q$. Moreover since we are supposing $n,mn+\ell q<X$, we have $j,k<X^{\frac{1}{2}}$. From this observation we deduce

$$\begin{aligned}S_{>y}[m](X,q)&\leq\sum_{\substack{j,k\leq X^{\frac{1}{2}}\\ jk>y\\ (jk,q)=1}}\#\{(n,\ell)\in\mathbb{Z}^2;0<n,mn+\ell q<X\text{ and }j^2\mid n,k^2\mid mn+\ell q\}\\&=:\sum_{\substack{j,k\leq X^{\frac{1}{2}}\\ jk>y\\ (jk,q)=1}}N[m](X,q;j,k),\end{aligned}\tag{1.55}$$

say. We shall divide the possible values of j and k into sets of the form

$$\mathcal{B}(J,K):=\{(j,k);(jk,q)=1,j\sim J,k\sim K\}.$$

We can do the division using at most $O((\log X)^2)$ such sets since we are summing over $j,k \leq X^{\frac{1}{2}}$. Let

$$\begin{aligned}\mathcal{N}[m](J,K) &= \sum_{\substack{(jk,q)=1\\ j\sim J, k\sim K}} N[m](X,q;j,k)\\ &= \#\left\{(j,k,u,v); j\sim J, k\sim K, 0<j^2u,k^2v<X, \text{ and } mj^2u\equiv k^2v \pmod q\right\}\end{aligned} \tag{1.56}$$

By taking the maximum over all J,K, we obtain a pair (J,K) with $J,K\leq X^{\frac{1}{2}}$ such that

$$S_{>y}[m](X,q) \ll_\epsilon X^\epsilon \mathcal{N}[m](J,K). \tag{1.57}$$

By the condition

$$jk > y$$

in (1.55), we can also impose

$$JK \geq \frac{y}{4}.$$

Our problem now is to bound $\mathcal{N}[m](J,K)$. Notice that, since we bound $S_{>y}[m](X,q)$ as in (1.57), we will not be able to benefit from oscillations of the coefficients $\mu(d)$ in (1.23). Although formula (1.56) is not symmetrical with respect to J and K, we would like to benefit from some symmetry. With that in mind, let $m_1,m_2\in\mathbb{Z}$ we define

$$\begin{aligned}\mathcal{N}[m_1,m_2](J,K) := \#\big\{(j,k,u,v); j,k\in\mathcal{B}(J,K), 0<j^2u,k^2v<X,\\ \text{and } m_1j^2u\equiv m_2k^2v \pmod q\big\}.\end{aligned} \tag{1.58}$$

We also suppose

$$\max(|m_1|,|m_2|)\leq |m|. \tag{1.59}$$

In the following we estimate the general $\mathcal{N}[m_1,m_2](J,K)$ from which we can directly deduce an estimate for $\mathcal{N}[m](J,K)$ itself. The first bound we give is an auxiliary one and will be useful later on.

1.7.1 Auxiliary bound

Lemma 1.7.1. *Let $X\geq 1$ and let $q\geq 1$ be an integer. Also let m,m_1,m_2 such that $0<|m_1|,|m_2|\leq|m|$. Let $\mathcal{N}[m_1,m_2](J,K)$ be as in (1.58), then for every $J,K\leq X$ and every $\epsilon>0$, we have*

$$\mathcal{N}[m_1,m_2](J,K) \ll_{\epsilon,m} \frac{X^{2+\epsilon}}{q}\left((JK)^{-1}+J^{-2}K\right),$$

where the implied constant depends at most on ϵ and m.

Démonstration. Putting $\ell q = m_1 j^2 u - m_2 k^2 v$, we have that $|\ell| \leq \frac{2|m|X}{q}$. Hence we have the inequality

$$\mathcal{N}[m_1, m_2](J, K) \leq \sum_{|\ell| \leq \frac{2|m|X}{q}} \sum_{\substack{k \sim K \\ (k,q)=1}} \sum_{u \leq XJ^{-2}} \sum_{\substack{j \sim J \\ m_1 j^2 u \equiv -\ell q \pmod{k^2}}} 1.$$

To estimate the above quadruple sum, we make a change of variables. First we write $f = (j, k)$. Since $(k, q) = 1$, we must have $f^2 \mid \ell$. We make a change of variables

$$j_0 = \frac{j}{f}, k_0 = \frac{k}{f} \text{ and } \ell_0 = \frac{\ell}{f^2}.$$

The congruence in the innermost sum then becomes

$$m_1 j_0^2 u \equiv -\ell_0 q \pmod{k_0^2}. \tag{1.60}$$

Now, let $g = (k_0^2, m_1)$. We have $g \mid \ell_0$. We write

$$r = \frac{k_0^2}{g}, s = \frac{m_1}{g} \text{ and } t = \frac{\ell_0}{g}.$$

Finally, let $h = (r, t)$. This implies that $h \mid u$. We write

$$r' = \frac{r}{h}, t' = \frac{t}{h} \text{ and } u' = \frac{u}{h}.$$

So (1.60) becomes

$$su' j_0^2 \equiv -t' q \pmod{r'}$$

and since $(t'q, r') = 1$, it has at most $2^{\omega(r')+1} \leq 2d(k)$ solutions in $j_0 \pmod{t'}$. Therefore we have

$$\begin{aligned}
\mathcal{N}[m_1, m_2](J, K) &\leq \sum_{f \geq 1} \sum_{\ell_0 \leq \frac{X}{f^2 q}} \sum_{\substack{k_0 \sim K/f \\ (k_0, q)=1}} \sum_{u' \leq XJ^{-2}h^{-1}} \sum_{\substack{j_0 \sim J/f \\ su' j_0^2 \equiv -t' q \pmod{r'}}} 1 \\
&\leq 2 \sum_{f \geq 1} \sum_{\ell \leq \frac{X}{f^2 q}} \sum_{k_0 \sim K/f} XJ^{-2}h^{-1} \left\{ \frac{Jgh}{fk_0^2} + 1 \right\} d(k) \\
&\ll_m \sum_{f \geq 1} \sum_{\ell \leq \frac{X}{f^2 q}} \sum_{k_0 \sim K/f} XJ^{-2} \left\{ \frac{J}{fk_0^2} + 1 \right\} d(k) \\
&\ll_\epsilon \sum_{f \geq 1} \frac{X^{2+\epsilon}}{J^2 f^2 q} \left\{ \frac{J}{K^2} + 1 \right\} K \\
&\ll \frac{X^{2+\epsilon}}{q} \left\{ \frac{1}{JK} + \frac{K}{J^2} \right\}.
\end{aligned}$$

□

Remark 1.7.1. We certainly have a result similar to Lemma 1.7.1 with the roles of J and and K interchanged.

1.7.2 Square Sieve

We must now proceed to obtain a more precise bound. We start from the equality

$$\mathcal{N}[m_1,m_2](J,K)=\sum_{u\leq XJ^{-2}}\mathcal{N}_u[m_1,m_2](J,K),$$

where

$$\mathcal{N}_u[m_1,m_2](J,K)=\#\left\{(j,k,v);j,k\in\mathcal{B}(J,K),0<k^2v<X \text{ and } m_1j^2u\equiv m_2k^2v \pmod q\right\}.$$

In other words, $\mathcal{N}_u[m_1,m_2](J,K)$ counts the contribution to $\mathcal{N}[m_1,m_2](J,K)$ for a fixed $u\leq XJ^{-2}$. Again by dyadic decomposition, we see that there is a certain U satisfying

$$U\leq XJ^{-2}, \tag{1.61}$$

such that

$$\mathcal{N}[m_1,m_2](J,K)\ll_\epsilon X^\epsilon\mathcal{N}[m_1,m_2](J,K,U), \tag{1.62}$$

where

$$\mathcal{N}[m_1,m_2](J,K,U)=\sum_{u\sim U}\mathcal{N}_u[m_1,m_2](J,K).$$

If we analyze the possible values for v and $\ell:=\frac{m_2k^2v-m_1j^2u}{q}$ contributing to $\mathcal{N}_u[m_1,m_2](J,K)$, we obtain

$$\mathcal{N}_u[m_1,m_2](J,K)\leq\#\Bigg\{(j,k,\ell,v);j\sim J,k\sim K,m_1j^2u=m_2k^2v-\ell q,|\ell|\leq\frac{|m|X}{q},\\ v\leq XK^{-2},(j,k)=1\Big\},$$

for every $u\sim U$.

We now appeal to the square sieve as in [22]. We state the main result here for easier reference.

Theorem 1.7.2. *([22, Theorem 1]) Let $\mathcal{P}$ be a set of P odd primes and $(w(n))_{n\geq1}$ a sequence of real numbers. Suppose that $w(n)=0$ for $n=0$ or $n\geq e^P$. Then*

$$\sum_{n\geq1}w(n^2)\ll P^{-1}\sum_{n\geq1}w(n)+P^{-2}\sum_{\substack{p_1\neq p_2\\p_1,p_2\in\mathcal{P}}}\left|\sum_n w(n)\left(\frac{n}{p_1p_2}\right)\right|,$$

where $\left(\frac{n}{p_1p_2}\right)$ is the Jacobi symbol and the implied constant is absolute.

Fix $K \leq X^{\frac{1}{2}}$, and integers m, m_1, m_2 such that $0 < |m_1|, |m_2| \leq |m|$. For each $u \sim U$, we apply the square-sieve to the multi-set of integers $\mathcal{A}_u = \mathcal{A}_u[m, m_1, m_2](K)$ given by

$$\mathcal{A}_u = \left\{ \frac{m_1(m_2k^2v - \ell q)}{u}; u \mid m_2k^2v - \ell q, k \sim K, \ell \leq \frac{2|m|X}{q}, v \leq XK^{-2} \right\},$$

For an integer n, let $w_u(n)$ denote the multiplicity of n in $\mathcal{A}$. We have

$$\mathcal{N}_u[m_1, m_2](J, K) \leq \sum_{j \geq 1} w_u((m_1 j)^2) \leq \sum_{n \geq 1} w_u(n^2).$$

For the set of primes, we take

$$\mathcal{P} = \left\{ p \text{ prime }; p \nmid 2m_1m_2u,\ \widehat{P} < p \leq 2\widehat{P} \right\},$$

where $\widehat{P}$ will be chosen later depending on J, K, X, q, and subject to the condition

$$(\log |m|^2X)^2 \leq \widehat{P} \leq |m|^2X. \tag{1.63}$$

We have $P = \#\mathcal{P} \sim \widehat{P}(\log \widehat{P})^{-1}$ as $\widehat{P} \to \infty$ and thus

$$w_u(n) = 0 \text{ for } n \geq e^P,$$

because, for X sufficiently large,

$$e^P \geq e^{\widehat{P}^{\frac{1}{2}}} \geq |m|^2X,$$

and $w_u(n) = 0$ for $n > |m|^2X$. Theorem 1.7.2 and the definition of $\mathcal{P}$ then give the inequality

$$\mathcal{N}_u[m_1, m_2](J, K) \ll \widehat{P}^{-1}(\log X) \sum_{n \geq 1} w_u(n) + P^{-2} \sum_{\substack{p_1, p_2 \\ p_1, p_2 \in \mathcal{P} \\ p_1 \neq p_2}} \left| \sum_{k, \ell, v} \left(\frac{m_2k^2v - \ell q}{p_1p_2} \right) \right|, \tag{1.64}$$

where the conditions in the last sum are

$$k \sim K,\ \ell \leq Xq^{-1},\ v \leq XK^{-2},\ u \mid m_2k^2v - \ell q,\ m_2k^2v - \ell q \neq 0. \tag{1.65}$$

To simplify, we write

$$T_1(u) = \widehat{P}^{-1}(\log X) \sum_{n \geq 1} w_u(n)$$

$$T_2(u) = P^{-2} \sum_{\substack{p_1, p_2 \\ p_1, p_2 \in \mathcal{P}}} \left| \sum_{k, \ell, v} \left(\frac{m_2k^2v - \ell q}{p_1p_2} \right) \right|.$$

So that (1.64) implies the inequality

$$\mathcal{N}[m_1,m_2](J,K,U) \ll \sum_{u\sim U} T_1(u) + \sum_{u\sim U} T_2(u). \tag{1.66}$$

Study of $T_1(u)$

By the definition of $w_u(n)$, we have

$$\begin{aligned}\sum_{u\sim U} T_1(u) &\ll \widehat{P}^{-1}(\log X)\sum_{k,\ell,v}\sum_{u\mid m_2k^2v-\ell q} 1\\ &\ll \widehat{P}^{-1}(\log X)\sum_{k,\ell,v} d(m_2k^2v-\ell q),\end{aligned}$$

where the conditions on the sum are

$$k\sim K,\ \ell\le \frac{X}{q},\ v\le XK^{-2},\ m_2k^2v-\ell q\ge 1.$$

Using the classical bound for the divisor function, we have

$$\sum_{u\sim U} T_1(u) \ll_\epsilon K^{-1}\widehat{P}^{-1}X^{2+\epsilon}q, \tag{1.67}$$

for every $\epsilon>0$, where the implied constant depends at most on ϵ and m.

Study of $T_2(u)$

We have

$$\begin{aligned}\sum_{u\sim U} T_2(u) &= P^{-2}\sum_{p_1\neq p_2}\sum_{u\sim U}\left|\sum_{k,\ell,v}\left(\frac{m_2k^2v-\ell q}{p_1p_2}\right)\right|\\ &\le \sum_{u\sim U}\max_{\substack{p_i\nmid 2m_1m_2u\\ \widehat{P}<p_1<p_2\le 2\widehat{P}}}\left|\sum_{k,\ell,v}\left(\frac{m_2k^2v-\ell q}{p_1p_2}\right)\right|.\end{aligned} \tag{1.68}$$

For each $u\sim U$, we pick $(p_1,p_2)=(p_1(u),p_2(u))$ for which the maximum is attained, and we proceed to estimate the sum

$$S_u := \sum_{k,\ell,v}\left(\frac{m_2k^2v-\ell q}{p_1p_2}\right), \tag{1.69}$$

where the conditions on k, ℓ, v are as in (1.65), and we recall $p_1\neq p_2$. Thus, (1.68) implies that

$$\sum_{u\sim U} T_2(u) \ll \sum_{u\sim U}|S_u|. \tag{1.70}$$

We write

$$\begin{aligned}
S_u &= \sum_{\substack{\alpha,\beta,\gamma=0\\ u\mid m_2\alpha^2\beta-q\gamma}}^{up_1p_2-1}\left(\frac{m_2\alpha^2\beta-q\gamma}{p_1p_2}\right)\sum_{\substack{k\sim K\\ k\equiv\alpha \pmod{up_1p_2}}}\sum_{\substack{v\leq XK^{-2}\\ v\equiv\beta \pmod{up_1p_2}}}\sum_{\substack{\ell\leq Xq^{-1}\\ \ell\equiv\gamma \pmod{up_1p_2}}}1\\
&= \sum_{\substack{\alpha,\beta,\gamma\\ u\mid m_2\alpha^2\beta-q\gamma}}\left(\frac{m_2\alpha^2\beta-q\gamma}{p_1p_2}\right)\left\{\frac{1}{up_1p_2}\sum_{\lambda=1}^{up_1p_2}\sum_{k\sim K}e\left(\frac{\lambda(\alpha-k)}{up_1p_2}\right)\right\}\\
&\quad\times\left\{\frac{1}{up_1p_2}\sum_{\mu=1}^{up_1p_2}\sum_{v\leq XK^{-2}}e\left(\frac{\mu(\beta-v)}{up_1p_2}\right)\right\}\left\{\frac{1}{up_1p_2}\sum_{\nu=0}^{up_1p_2-1}\sum_{\ell\leq Xq^{-1}}e\left(\frac{\nu(\gamma-\ell)}{up_1p_2}\right)\right\}\\
&=(up_1p_2)^{-3}\sum_{\lambda,\mu,\nu=0}^{up_1p_2-1}S(u,p_1p_2;m_2,q;\lambda,\mu,\nu)\Theta_\lambda\Phi_\mu\Psi_\nu,
\end{aligned}\tag{1.71}$$

where

$$\begin{cases}
S(u,p_1p_2;m_2,q;\lambda,\mu,\nu)=\displaystyle\sum_{\substack{\alpha,\beta,\gamma=0\\ u\mid m_2\alpha^2\beta-q\gamma}}^{up_1p_2-1}\left(\frac{m_2\alpha^2\beta-q\gamma}{p_1p_2}\right)e\left(\frac{\lambda\alpha+\mu\beta+\nu\gamma}{up_1p_2}\right),\\
\Theta_\lambda=\displaystyle\sum_{K<k\leq 2K}e\left(\frac{-\lambda k}{up_1p_2}\right)\ll\min\left(K,\left\|\frac{\lambda}{up_1p_2}\right\|^{-1}\right),\\
\Phi_\mu=\displaystyle\sum_{v\leq XK^{-2}}e\left(\frac{-\mu v}{up_1p_2}\right)\ll\min\left(XK^{-2},\left\|\frac{\mu}{up_1p_2}\right\|^{-1}\right),\\
\Psi_\nu=\displaystyle\sum_{\ell\leq Xq^{-1}}e\left(\frac{-\nu\ell}{up_1p_2}\right)\ll\min\left(Xq^{-1},\left\|\frac{\nu}{up_1p_2}\right\|^{-1}\right);
\end{cases}\tag{1.72}$$

here $\|x\|$ denotes the distance from x to the nearest integer. The Chinese remainder theorem allows us to write

$$S(u,p_1p_2;m_2,q;\lambda,\mu,\nu)=S_1(p_1;m_2,q;b,c,d)S_1(p_2;m_2,q;b,c,d)\prod_{r^f\|u}S_2(r^f;m_2,q;b,c,d),\tag{1.73}$$

where $u=\prod r^f$ is the prime factorization of u, b, c and d are some integers such that

$$\begin{cases}
(b,up_1p_2)=(\lambda,up_1p_2),\\
(c,up_1p_2)=(\mu,up_1p_2),\\
(d,up_1p_2)=(\nu,up_1p_2),
\end{cases}$$

and

$$\begin{cases} S_1(p;m_2,q;b,c,d) = \displaystyle\sum_{\alpha,\beta,\gamma=0}^{p-1} \left(\frac{m_2\alpha^2\beta - q\gamma}{p}\right) e\left(\frac{b\alpha+c\beta+d\gamma}{p}\right) \\ S_2(r^f;m_2,q;b,c,d) = \displaystyle\sum_{\substack{\alpha,\beta,\gamma=0 \\ r^f \mid m_2\alpha^2\beta - q\gamma}}^{r^f-1} e\left(\frac{b\alpha+c\beta+d\gamma}{r^f}\right). \end{cases}$$

For these sums we have the following upper bounds whose proofs are elementary and are given in section 1.9 (see Lemma 1.9.1).

$$\begin{cases} S_1(p;m_2,q;b,c,0) = 0, \\ S_1(p;m_2,q;b,c,d) \ll p^{\frac{3}{2}}, \\ |S_2(r;m_2,q;b,c,d)| \le 2r(r,b,c,dm_2) \\ |S_2(r^f;m_2,q;b,c,d)| \le 2r^{\frac{3f}{2}}(r^f,b,c,dm_2)^{\frac{1}{2}}, \text{ if } r \text{ is odd, } f \ge 2, \\ |S_2(2^f;m_2,q;b,c,d)| \le 4.2^{\frac{3f}{2}}(2^f,b,c,dm_2)^{\frac{1}{2}}, \ f \ge 2. \end{cases}$$

If we multiply these upper bounds in (1.73), we have, whenever $d \not\equiv 0 (\text{mod } up_1p_2)$,

$$\begin{aligned} S(u,p_1p_2;m_2,q;b,c,d) &\ll d(u)\widehat{P}^3U^{\frac{3}{2}}(u^\dagger)^{-\frac{1}{2}}(u,b,c,dm_2) \\ &\ll_m d(u)\widehat{P}^3U^{\frac{3}{2}}(u^\dagger)^{-\frac{1}{2}}(u,b,c,d), \end{aligned} \tag{1.74}$$

where

$$u^\dagger = \prod_{\substack{p\mid u \\ p^2\nmid u}} p. \tag{1.75}$$

We also have

$$S(u,p_1p_2;m_2,q;b,c,0) = 0.$$

Hence, by (1.71), we deduce the inequality

$$S_u \ll_m d(u)\widehat{P}^{-3}U^{-\frac{3}{2}}(u^\dagger)^{-\frac{1}{2}} \sum_{\nu=1}^{up_1p_2-1} \sum_{\lambda,\mu=0}^{up_1p_2-1} |\Theta_\lambda\Phi_\mu\Psi_\nu|(u,\lambda,\mu,\nu). \tag{1.76}$$

Now, we separate the inner sum in four parts accordingly to whether λ and μ are zero or not. We also use the bounds coming from (1.72). We use the first term inside the min-symbol in the zero case and the second term otherwise. We then have

$$\begin{aligned} \sum_{\lambda,\mu=0}^{up_1p_2-1} \sum_{\nu=1}^{up_1p_2-1} |\Theta_\lambda\Phi_\mu\Psi_\nu|(u,\lambda,\mu,\nu) &\ll K^{-1}\widehat{P}^2UX \sum_{1\le\nu\le\frac{up_1p_2}{2}} \nu^{-1}(u,\nu) \\ + K\widehat{P}^4U^2 \sum_{1\le\mu,\nu\le\frac{up_1p_2}{2}} \mu^{-1}\nu^{-1}(u,\mu,\nu) &+ K^{-2}\widehat{P}^4U^2X \sum_{1\le\lambda,\nu\le\frac{up_1p_2}{2}} \lambda^{-1}\nu^{-1}(u,\lambda,\nu) \\ &+ \widehat{P}^6U^3 \sum_{1\le\lambda,\mu,\nu\le\frac{up_1p_2}{2}} \lambda^{-1}\mu^{-1}\nu^{-1}(u,\lambda,\mu,\nu). \end{aligned} \tag{1.77}$$

For the sums involving greatest common divisors, we have the following elementary Lemma

Lemma 1.7.3. *For every $\epsilon > 0$, we have the following inequalities*

$$\sum_{1\leq\lambda\leq Z} \lambda^{-1}(u,\lambda) \ll_\epsilon (Zu)^\epsilon, \tag{1.78}$$

$$\sum_{1\leq\lambda,\mu\leq Z} \lambda^{-1}\mu^{-1}(u,\lambda,\mu) \ll_\epsilon (Zu)^\epsilon, \tag{1.79}$$

$$\sum_{1\leq\lambda,\mu,\nu\leq Z} \lambda^{-1}\mu^{-1}\nu^{-1}(u,\lambda,\mu,\nu) \ll_\epsilon Z^\epsilon, \tag{1.80}$$

uniformly for $Z \geq 1$ and every positive integer u, where the implied constants depend on ϵ alone.

If we insert the inequalities (1.78), (1.79) and (1.80) (with $Z = \frac{up_1p_2}{2}$) in (1.77), we deduce

$$S_u \ll_{\epsilon,m} (u^\dagger)^{-\frac{1}{2}} X^\epsilon \left\{ K^{-1}\widehat{P}^{-1}U^{-\frac{1}{2}}X + K\widehat{P}U^{\frac{1}{2}} + K^{-2}\widehat{P}U^{\frac{1}{2}}X + \widehat{P}^3U^{\frac{3}{2}} \right\}. \tag{1.81}$$

In order to compute the contribution of S to $\mathcal{N}[m_1,m_2](J,K,U)$ we must sum over u. We notice that

$$\sum_{u\sim U} (u^\dagger)^{-\frac{1}{2}} \leq \sum_{v\leq U} v^{-\frac{1}{2}} \sum_{\substack{w\sim U/v \\ w \text{ squarefull}}} 1 \ll_\epsilon U^{\frac{1}{2}+\epsilon}, \tag{1.82}$$

by the well-known bound

$$\sum_{\substack{w\leq W \\ w \text{ squarefull}}} 1 \ll W^{\frac{1}{2}}.$$

Gathering (1.70), (1.81), and (1.82), we obtain

$$\sum_{u\sim U} T_2(u) \ll_{\epsilon,m} X^\epsilon \left\{ K^{-1}\widehat{P}^{-1}X + K\widehat{P}U + K^{-2}\widehat{P}UX + \widehat{P}^3U^2 \right\}.$$

Appealing to (1.61), we deduce the inequality

$$\sum_{u\sim U} T_2(u) \ll_{\epsilon,m} X^\epsilon \left\{ K^{-1}\widehat{P}^{-1}X + J^{-2}K\widehat{P}X + J^{-2}K^{-2}\widehat{P}X^2 + J^{-4}\widehat{P}^3X^2 \right\}. \tag{1.83}$$

From (1.66), (1.67) and (1.83), we deduce an inequality for $\mathcal{N}[m_1,m_2](J,K,U)$

$$\begin{aligned}\mathcal{N}[m_1,m_2](J,K,U) \ll_{\epsilon,m} X^\epsilon \Big\{ & K^{-1}\widehat{P}^{-1}X^2q^{-1} + K^{-1}\widehat{P}^{-1}X \\ & + J^{-2}K\widehat{P}X + J^{-2}K^{-2}\widehat{P}X^2 + J^{-4}\widehat{P}^3X^2 \Big\}.\end{aligned}$$

Since $q \leq X$, the second term is dominated by the first one. Therefore,

$$\mathcal{N}[m_1,m_2](J,K,U) \ll_{\epsilon,m} X^{\epsilon}\Big\{K^{-1}\widehat{P}^{-1}X^2q^{-1} + J^{-2}K\widehat{P}X + J^{-2}K^{-2}\widehat{P}X^2 + J^{-4}\widehat{P}^3X^2\Big\}.$$

By taking $(m_1,m_2)=(m,1)$, we deduce

$$\mathcal{N}[m](J,K,U) \ll_{\epsilon,m} X^{\epsilon}\Big\{K^{-1}\widehat{P}^{-1}X^2q^{-1} + J^{-2}K\widehat{P}X + J^{-2}K^{-2}\widehat{P}X^2 + J^{-4}\widehat{P}^3X^2\Big\}. \tag{1.84}$$

Remark 1.7.2. Notice that since we also have the identity

$$\mathcal{N}[m](J,K) = \mathcal{N}[1,m](K,J),$$

the upper bound (1.84) still holds if we replace the roles of J and K. In other words, there is no loss of generality in supposing $J \geq K$.

Now, the upper bound (1.84), together with (1.57) and (1.62) gives us

$$S_{>y}[m](X,q) \ll_{\epsilon,m} X^{\epsilon}\Big\{K^{-1}\widehat{P}^{-1}X^2q^{-1} + J^{-2}K\widehat{P}X + J^{-2}K^{-2}\widehat{P}X^2 + J^{-4}\widehat{P}^3X^2\Big\}. \tag{1.85}$$

At this point we make the choice

$$\widehat{P} = JK^{-\frac{1}{4}}q^{-\frac{1}{4}} + (\log|m|^2X)^2, \tag{1.86}$$

which makes the second and the last terms of (1.85) similar. Hence we have

$$S_{>y}[m](X,q) \ll_{\epsilon,m} X^{\epsilon}\Big\{J^{-1}K^{-\frac{3}{4}}X^2q^{-\frac{3}{4}} + J^{-1}K^{\frac{3}{4}}Xq^{-\frac{1}{4}} + J^{-1}K^{-\frac{9}{4}}X^2q^{-\frac{1}{4}} + J^{-2}KX + J^{-2}K^{-2}X^2 + J^{-4}X^2\Big\}.$$

Since $J \geq K$, $JK \gg y$, we see that

$$S_{>y}[m](X,q) \ll_{\epsilon,m} X^{\epsilon}\Big\{X^2q^{-\frac{3}{4}}y^{-\frac{7}{8}} + Xq^{-\frac{1}{4}}y^{-\frac{1}{8}} + J^{-1}K^{-\frac{9}{4}}X^2q^{-\frac{1}{4}} + Xy^{-\frac{1}{2}} + X^2y^{-2}\Big\}. \tag{1.87}$$

1.8 Proof of Theorem 1.1.4

Assume

$$y \geq X^{\frac{1}{2}}. \tag{1.88}$$

Putting together (1.34) and (1.87), we deduce

$$S[m](X,q) = \mathcal{A}[m](X,q) + R[m](X,q), \tag{1.89}$$

where $R[m](x,q)$ satisfies

$$\begin{aligned} R[m](X,q) \ll_{\epsilon,m} X^{\epsilon} \Big\{ & Xq^{-1}y + X^2 q^{-\frac{3}{4}} y^{-\frac{7}{8}} + Xq^{-\frac{1}{4}} y^{-\frac{1}{8}} \\ & + J^{-1}K^{-\frac{9}{4}} X^2 q^{-\frac{1}{4}} + Xy^{-\frac{1}{2}} + X^2 y^{-2} \Big\}, \end{aligned}$$

thanks to (1.88). We now make the choice

$$y = X^{\frac{8}{15}} q^{\frac{2}{15}} \tag{1.90}$$

to make the first two terms similar. Notice that this choice of y satisfies (1.88). Hence we have

$$\begin{aligned} R[m](X,q) &\ll_{\epsilon,m} X^{\epsilon} \Big\{ X^{\frac{23}{15}} q^{-\frac{13}{15}} + X^{\frac{14}{15}} q^{-\frac{4}{15}} \\ &\qquad + J^{-1}K^{-\frac{9}{4}} X^2 q^{-\frac{1}{4}} + X^{\frac{11}{15}} q^{-\frac{1}{15}} \Big\} \\ &\ll X^{\epsilon} \Big\{ X^{\frac{23}{15}} q^{-\frac{13}{15}} + \mathcal{E}_1 \Big\}, \end{aligned} \tag{1.91}$$

where

$$\mathcal{E}_1 = X^2 J^{-1} K^{-\frac{9}{4}} q^{-\frac{1}{4}}$$

since $q \leq X$. Now Lemma 1.7.1 together with (1.22), (1.34), (1.57) and the choice for y give us

$$\begin{aligned} R[m](X,q) &\ll_{\epsilon,m} X^{\epsilon} \left\{ Xq^{-1}y + X^2 J^{-1} K^{-1} q^{-1} + X^2 J^{-2} K q^{-1} \right\} \\ &\ll X^{\epsilon} \left\{ Xq^{-1}y + X^2 q^{-1} y^{-1} + \mathcal{E}_2 \right\} \\ &\ll X^{\epsilon} \Big\{ X^{\frac{23}{15}} q^{-\frac{13}{15}} + \mathcal{E}_2 \Big\}, \end{aligned} \tag{1.92}$$

thanks to (1.88), and

$$\mathcal{E}_2 = X^2 J^{-2} K q^{-1}.$$

The importance of Lemma 1.7.1 is that since $J \geq K$, we cannot give a good estimate for the term $\mathcal{E}_1$ using that $JK \gg y$. So we look for a mixed term that lies between $\mathcal{E}_1$ and $\mathcal{E}_2$ for which we have a good bound (much better than the one for $\mathcal{E}_2$, for example). Notice that

$$\begin{aligned}\min(\mathcal{E}_1, \mathcal{E}_2) \leq & \mathcal{E}_1^{\frac{12}{17}} \mathcal{E}_2^{\frac{5}{17}} \\ = & X^2 (JK)^{-\frac{22}{17}} q^{-\frac{8}{17}} \\ \ll & X^2 q^{-\frac{8}{17}} y^{-\frac{22}{17}} \\ \ll & X^{\frac{334}{255}} q^{-\frac{164}{255}}. \end{aligned} \tag{1.93}$$

Now, (1.91), (1.92) and (1.93) imply

$$\begin{aligned} R[m](X,q) \ll_{\epsilon,m} & X^{\epsilon} \left\{ X^{\frac{23}{15}} q^{-\frac{13}{15}} + X^{\frac{334}{255}} q^{-\frac{164}{255}} \right\} \\ \ll & X^{\frac{23}{15+\epsilon}} q^{-\frac{13}{15}}, \end{aligned} \tag{1.94}$$

since $q \leq X$. Theorem 1.1.4 now follows from Proposition 1.6.1, (1.89) and (1.94).

1.9 Exponential Sums

Here we give the proofs for the bounds on exponential sums used in section 1.7. We have the following

Lemma 1.9.1. *Let b, c, d, m_2, p and q be integers, $m_2 \neq 0$, p a prime number and $p \nmid m_2 q$. We define*

$$S_1(p; m_2, q; b, c, d) = \sum_{\alpha,\beta,\gamma=0}^{p-1} \left(\frac{m_2 \alpha^2 \beta - q\gamma}{p} \right) e\left(\frac{b\alpha + c\beta + d\gamma}{p} \right).$$

Let r be a prime number such that $r \nmid q$ and $f > 0$ an integer,

$$S_2(r^f; m_2, q; b, c, d) = \sum_{\substack{\alpha,\beta,\gamma=0 \\ r^f \mid m_2\alpha^2\beta - q\gamma}}^{r^f-1} e\left(\frac{b\alpha + c\beta + d\gamma}{r^f} \right).$$

Then, we have

$$\begin{cases} S_1(p; m_2, q; b, c, 0) = 0, & (1.95) \\ S_1(p; m_2, q; b, c, d) \ll p^{\frac{3}{2}}, & (1.96) \\ |S_2(r; m_2, q; b, c, d)| \leq 2r(r, b, c, dm_2), & (1.97) \\ |S_2(r^f; m_2, q; b, c, d)| \leq 2r^{\frac{3f}{2}} (r^f, b, c, dm_2)^{\frac{1}{2}} \text{ if } r \text{ is odd, } f \geq 2, & (1.98) \\ |S_2(2^f; m_2, q; b, c, d)| \leq 4.2^{\frac{3f}{2}} (2^f, b, c, dm_2)^{\frac{1}{2}}, \ f \geq 2. & (1.99) \end{cases}$$

Démonstration. We start by studying S_2. We have

$$\begin{aligned} S_2(r; m_2, q; b, c, d) &= \sum_{\alpha,\beta=0}^{r-1} e\left(\frac{b\alpha + c\beta + dm_2\overline{q}\alpha^2\beta}{r}\right) \\ &= \sum_{\alpha=0}^{r-1} e\left(\frac{b\alpha}{r}\right) \sum_{\beta=0}^{r-1} e\left(\frac{(c + dm_2\overline{q}\alpha^2)\beta}{r}\right) \\ &= \sum_{\alpha=0}^{r-1} e\left(\frac{b\alpha}{r}\right) \delta(c + dm_2\overline{q}\alpha^2, r), \end{aligned} \tag{1.100}$$

where

$$\delta(x, n) = \begin{cases} n \text{ if } n \mid x, \\ 0 \text{ otherwise.} \end{cases}$$

If $r \mid dm_2$, equation (1.100) becomes

$$S_2(r; m_2, q; b, c, d) = \sum_{\alpha=0}^{r-1} e\left(\frac{b\alpha}{r}\right) \delta(c, r) = \delta(b, r)\delta(c, r).$$

So, $S_2(r, q; b, c, d) = 0$ unless r divides both b and c, in which case,

$$S_2(r; m_2, q; b, c, d) = r^2 = r(r, b, c, dm_2).$$

That proves (1.97) when $r \mid dm_2$.

We now assume $r \nmid dm_2$. We analyze when the symbol $\delta(c + dm_2\overline{q}\alpha^2)$ is non-zero. That means we consider the equation

$$dm_2\alpha^2 \equiv -cq \pmod{r}.$$

This equation has at most two solutions for $1 \leq \alpha \leq r$. Thus, again by equation (1.100),

$$|S_2(r; m_2, q; b, c, d)| = \left|\sum_{\alpha=0}^{r-1} e\left(\frac{b\alpha}{r}\right) \delta(c + dm_2\overline{q}\alpha^2, r)\right| \leq 2r,$$

which completes the proof of (1.97).

We proceed to prove the inequalities (1.98) and (1.99). Analogously to the previous case, we have

$$S_2(r^f; m_2, q; b, c, d) = \sum_{\alpha=0}^{r^f-1} e\left(\frac{b\alpha}{r^f}\right) \delta(c + dm_2\overline{q}\alpha^2, r^f).$$

We write $(c, r^f) = r^s$, $(dm_2, r^f) = r^t$, So we have $0 \leq s, t \leq f$.
If $s < t$, for any α, the largest power of r that divides $c + dm_2\overline{q}\alpha^2$ is always r^s. So the δ symbol is always zero. Hence the sum is itself always zero.

Hence we may suppose $s \geq t$. In this case, we write $c = r^s\tilde{c}, dm_2 = r^t\tilde{d}$. Then, the condition $r^f \mid c + dm_2\overline{q}\alpha^2$ is equivalent to

$$r^{f-t} \mid r^{s-t}\tilde{c} + \tilde{d}\overline{q}\alpha^2. \tag{1.101}$$

Notice that for any α for which (1.101) is true, we must have

$$r^u \mid \alpha,$$

where $u = \lceil \frac{s-t}{2} \rceil$. We write $\alpha = r^u\tilde{\alpha}$, with $1 \leq \tilde{\alpha} \leq r^{f-u}$. Condition (1.101) now translates to

$$r^{f-s} \mid \tilde{c} + r^{2u-s+t}\tilde{d}\overline{q}\tilde{\alpha}^2, \tag{1.102}$$

which has at most 2 solutions for $\tilde{\alpha} \pmod{r^{f-s}}$, if r is odd.

Remark 1.9.1. If $r = 2$ the quadratic equation above can have up to 4 solutions $\pmod{r^{f-s}}$, which is in fact the only difference between the cases r odd and $r = 2$.

In the following, we only prove (1.98). The proof of (1.99) is exactly the same, except that one must take into account Remark 1.9.1. We now have

$$\begin{aligned} S_2(r^f; m_2, q; b, c, d) &= r^f {\sum_{\tilde{\alpha}=0}^{r^{f-u}-1}}' e\left(\frac{b\tilde{\alpha}}{r^{f-u}}\right) \\ &= r^f {\sum_{\tilde{\alpha}=0}^{r^{f-s}-1}}' e\left(\frac{b\tilde{\alpha}}{r^{f-u}}\right) \sum_{h=0}^{r^{s-u}} e\left(\frac{br^{f-s}h}{r^{f-u}}\right) \\ &= r^f\delta(b, r^{s-u}) {\sum_{\tilde{\alpha}=0}^{r^{f-s}-1}}' e\left(\frac{b\tilde{\alpha}}{r^{f-u}}\right), \end{aligned} \tag{1.103}$$

where the $'$ in the sum means that we only sum over the $\tilde{\alpha}$ satisfying (1.102). From (1.103), we see that $S_2(r^f; m_2, q; b, c, d)$ is zero unless

$$r^{s-u} \mid b. \tag{1.104}$$

Hence we may assume (1.104). Then, (1.103) gives the inequality

$$|S_2(r^f; m_2, q; b, c, d)| \leq 2r^{f+s-u}. \tag{1.105}$$

And since $u \geq \frac{s-t}{2}$, we have

$$f + s - u \leq f + \frac{s+t}{2} \leq \frac{3f}{2} + \frac{t}{2}.$$

As a consequence, (1.105) becomes

$$|S_2(r^f; m_2, q; b, c, d)| \leq 2r^{\frac{3f}{2}}(r^t)^{\frac{1}{2}}. \tag{1.106}$$

We want to prove that

$$(r^f, b, c, dm_2) = r^t. \tag{1.107}$$

Since $t \leq s$ holds, equation (1.104) tells us that we only need to prove that $t \leq s - u$. That is

$$\left\lceil \frac{s-t}{2} \right\rceil \leq s - t,$$

which holds since $s - t \geq 0$. Thus, (1.107) is true. This completes the proof of (1.98) and (1.99)

At last, for (1.95), (1.96), we write

$$\begin{aligned} S_1(p; m_2, q; b, c, d) &= \sum_{\alpha,\beta=0}^{p-1} \sum_{h=1}^{p-1} \left(\frac{h}{p}\right) e\left(\frac{b\alpha + c\beta + d\overline{q}(m_2\alpha^2\beta - h)}{p}\right) \\ &= \left(\sum_{h=1}^{p-1} \left(\frac{h}{p}\right) e\left(\frac{-d\overline{q}h}{p}\right)\right) S_2(p; m_2, q; b, c, d). \end{aligned}$$

Hence, we see that (1.96) follows from (1.97) and the well-known estimates for Gauss sums. Finally, we see that (1.95) follows from the equation above and the identity

$$\sum_{h=1}^{p-1} \left(\frac{h}{p}\right) = 0.$$

This concludes the proof of the lemma. □

Chapitre 2

On Bourgain's Bound and applications to squarefree numbers

2.1 Introduction

As usual, let

$$e(x) := e^{2i\pi x}, \text{ for } x \in \mathbb{R}.$$

In a recent paper, Bourgain [4] proved a non trivial bound for exponential sums such as

$$\sum_{\substack{n\leq N\\(n,q)=1}} e\left(\frac{a\overline{n}^2}{q}\right),$$

where $q > 1$ is an integer and $\bar{n}$ denotes the multiplicative inverse of $n \pmod q$. His result holds in the range $N \geq q^{\epsilon}$, for an arbitrarily small, but fixed, $\epsilon > 0$. In his paper, Bourgain was interested in an application related to the size of fundamental solutions $\epsilon_D > 1$ to the Pell equation

$$t^2 - Du^2 = 1.$$

He followed the lead of Fouvry [8], who suggested that such an upper bound could help to improve the lower bounds for the counting function

$$S^f(x,\alpha) := \#\Big\{(\epsilon_D, D); 2 \leq D \leq x, D \text{ is not a square, and } \epsilon_D \leq D^{\frac{1}{2}+\alpha}\Big\},$$

for small values of α. We are interested in a different application of Bourgain's result (see Proposition 2.4.2 below) related to squarefree numbers in arithmetic progressions.

Let $X \geq 1$. Let a and q be coprime integers such that $q \geq 2$. We let

$$E(X,q,a) := \sum_{\substack{n\leq X\\ n\equiv a \pmod q}} \mu^2(n) - \frac{6}{\pi^2}\prod_{p|q}\left(1-\frac{1}{q^2}\right)^{-1}\frac{X}{q}. \tag{2.1}$$

For fixed q, the last term is known to be asymptotically equivalent to

$$\frac{1}{\varphi(q)} \sum_{\substack{n \leq X \\ (n,q)=1}} \mu^2(n)$$

as $X \to \infty$. So that $E(X;q,a)$ can be seen as an error term of the distribution of squarefree numbers in arithmetic progressions. One naturally has the trivial bound

$$\Big|E(X,q,a)\Big| \leq \frac{X}{q} + 1. \tag{2.2}$$

In Chapter 1, we proved

Theorem 2.1.1. *There exists an absolute constant $C > 0$, such that, for every $\epsilon > 0$, we have*

$$\sum_{\substack{a \pmod q \\ (a,q)=1}} E(X,q,a)^2 \sim C \prod_{p|q} \left(1 + 2p^{-1}\right)^{-1} X^{1/2} q^{1/2}, \tag{2.3}$$

for $X \to \infty$, uniformly for integers q satisfying $X^{31/41+\epsilon} \leq q \leq X^{1-\epsilon}$.

This theorem gives the asymptotic variance of the above mentioned distribution.
Inspired by an equivalent problem considered by Fouvry *et al* [9, Theorem 1.5.], we studied how $E(X,q,a)$ correlates with $E(X,q,\gamma(a))$ for suitable choices of $\gamma : \mathbb{Z}/q\mathbb{Z} \to \mathbb{Z}/q\mathbb{Z}$. It is natural to choose γ to be an affine linear map, *i.e.*

$$\gamma_{r,s}(a) = ra + s, \tag{2.4}$$

where $r, s \in \mathbb{Z}$, $r \neq 0$ are fixed. Thus our object of study is the following correlation sum

$$C[\gamma_{r,s}](X,q) := \sum_{\substack{a \pmod q \\ a \neq 0, \gamma_{r,s}^{-1}(0)}} E(X,q,a)E(X,q,\gamma_{r,s}(a)), \tag{2.5}$$

for q prime. In Chapter 1, we already considered the case $s = 0$ and we found that correlation always existed for any non zero value of r. In particular, there exists $C_r \neq 0$ such that for $X \to \infty$, $X^{31/41+\epsilon} \leq q \leq X^{1-\epsilon}$, one has

$$C[\gamma_{r,0}](X,q) \sim C_r \left(\sum_{\substack{a \pmod q \\ (a,q)=1}} E(X,q,a)^2 \right). \tag{2.6}$$

Our main result is the following theorem which exhibits a certain independence between the functions $a \mapsto E(X,q,a)$ and $a \mapsto E(X,q,\gamma_{r,s}(a))$ considered as random variables on $\mathbb{Z}/q\mathbb{Z}$, which confirms our intuition on this question when $\gamma_{r,s}$ is not a homothety.

Theorem 2.1.2. *There exists an absolute $\delta > 0$ such that for every $\epsilon > 0$ and for every integer $r \neq 0$, there exists $C_{\epsilon,r}$ such that one has the inequality*

$$\left|C[\gamma_{r,s}](X,q)\right| \leq C_{\epsilon,r}\left(q^{1+\epsilon} + X^{1/2}q^{1/2}(\log q)^{-\delta} + \frac{X^{5/3+\epsilon}}{q} + \left(\frac{X}{q}\right)^2\right) \tag{2.7}$$

uniformly for $X \geq 2$, integers s and prime numbers $q \leq X$ such that $q \nmid rs$.

A consequence of Theorems 2.1.1 and 2.1.2 (not necessarily with the same ϵ) is the following

Corollary 2.1.3. *For every $\epsilon > 0$ and $r \neq 0$, there exists a function $\Phi_{\epsilon,r} : \mathbb{R}^+ \to \mathbb{R}^+$, tending to zero at infinity, such that for every $X \geq 2$, for every integer s and for every prime q such that $q \nmid rs$ and $X^{7/9+\epsilon} \leq q \leq X^{1-\epsilon}$, one has the inequality*

$$\left|C[\gamma_{r,s}](X,q)\right| \leq \Phi_{\epsilon,r}(X)\left(\sum_{\substack{a \pmod q \\ (a,q)=1}} E(X,q,a)^2\right). \tag{2.8}$$

Inequality (2.8) shows a behavior different from (2.6) corresponding to the case where $q \mid s$. In other words, it suggests a certain independence of the random variables

$$a \mapsto E(X,q,a) \quad \text{and} \quad a \mapsto E(X,q,\gamma_{r,s}(a))$$

Here, as in Chapter 1, we give results that are true for a general $r \neq 0$, but in order to simplify the presentation, we give proofs that are only complete when r is squarefree (the case where $\mu^2(r) = 0$ implies a more difficult definition of the κ function in (2.27)).

2.2 Notation

We define the Bernoulli polynomials $B_k(x)$ for $k \geq 1$, on $[0,1)$, in the following recursive way

$$B_1(x) := x - 1/2$$
$$\frac{d}{dx}B_{k+1}(x) = B_k(x),$$
$$\int_0^1 B_k(x)dx = 0.$$

We can extend these functions to periodic functions defined in the whole real line by posing

$$B_k(x) := B_k(\{x\}).$$

We further notice that $B_1(x)$ satisfies the following relation

$$\lfloor x \rfloor = x - \frac{1}{2} - B_1(x) \tag{2.9}$$

and $B_2(x)$ satisfies

$$B_2(x) = \frac{x^2}{2} - \frac{x}{2} + \frac{1}{12} \text{ for } 0 \leq x \leq 1. \tag{2.10}$$

In the course of the proof oh Theorem 2.1.2 we will make repetitive use of the following multiplicative function

$$h(d) = \mu^2(d) \prod_{p|d} \left(1 - 2p^{-2}\right)^{-1}. \tag{2.11}$$

We also define here the closely related product

$$C_2 = \prod_p \left(1 - \frac{2}{p^2}\right). \tag{2.12}$$

We denote, as usual, by $d(n)$ and $d_3(n)$ the classical binary and ternary divisor functions, respectively. We write $\omega(n)$ for the number of primes dividing n. We write $n \sim N$ as an alternative to $N < n \leq 2N$. If S is a finite set, $\#S$ denotes its cardinality. If $I \subset R$ is an interval, $|I|$ denotes its length. We use indistinguishably the notations $f = O(g)$ and $f \ll g$ when there is an absolute constant C such that

$$|f| \leq Cg,$$

on a certain domain of the variables which will be clear by the context, and the the same for the symbols O_ϵ, O_r, $O_{\epsilon,r}$ and $\ll_\epsilon$, $\ll_r$, $\ll_{\epsilon,r}$, but with constants that may depend on the subindexed variables.

2.3 Initial Steps

Let $X \geq 2$. Let $\gamma = \gamma_{r,s}$ be given by (2.4) and let q be a prime number $\leq X$ such that $q \nmid rs$.
We start by completing the sum defining $C[\gamma](X, q)$ (see (2.5)) and we bound trivially the additional terms. By (2.2), we see that

$$C[\gamma](X, q) = \sum_{a=0}^{q-1} E(X, q, a)E(X, q, \gamma(a)) + O\left(\left(\frac{X}{q}\right)^2\right), \tag{2.13}$$

In what follows, for simplification, we shall write

$$C(q) = \frac{6}{\pi^2}\left(1 - \frac{1}{q^2}\right)^{-1}. \tag{2.14}$$

As we develop the sum on the right-hand side of (2.13), we obtain

$$C[\gamma](X, q) = S[\gamma](X, q) - 2C(q)\frac{X}{q}\sum_{n\leq X} \mu^2(n) + C(q)^2\frac{X^2}{q} + O\left(\frac{X^2}{q^2}\right), \tag{2.15}$$

where $S[\gamma](X, q)$ is defined by the double sum

$$S[\gamma](X, q) = \sum_{\substack{n_1,n_2\leq X \\ n_2\equiv\gamma(n_1) \pmod q}}\sum \mu^2(n_1)\mu^2(n_2). \tag{2.16}$$

We point out that $S[\gamma](X,q)$ is the only difficult term appearing in equation (2.15), since we have the well-known formula

$$\begin{aligned}\sum_{n\leq X}\mu^2(n) &= \frac{6}{\pi^2}X + O(\sqrt{X})\\ &= C(q)X + O\left(\frac{X}{q^2}+\sqrt{X}\right),\end{aligned} \tag{2.17}$$

uniformly for $1 \leq q \leq X$. An asymptotic expansion of $S[\gamma](X,q)$ will be given in Proposition 2.5.1.

2.4 Useful lemmata

We start with a lemma concerning the multiplicative function $h(d)$ which will follow easily from Lemma 1.5.2.

Lemma 2.4.1. *Let $h(d)$ be as in* (2.11) *and let β be the multiplicative function defined by the formula*

$$h(d) = \sum_{mn=d}\beta(m),\ d \geq 1.$$

Then $\beta(m)$ satisfies

$$\sum_{m\geq M}\frac{\beta(m)}{m} \ll M^{-\frac{1}{2}}, \tag{2.18}$$

$$\sum_{m\leq M}\beta(m) \ll M, \tag{2.19}$$

uniformly for every $M \geq 1$.

Démonstration. By Lemma 1.5.2, we know that $\beta(m)$ is supported on cubefree numbers and, if we write $m = ab^2$ with a, b squarefree and relatively prime, then

$$\beta(m) \ll \frac{d(a)}{a^2}.$$

In particular, $\beta(m) \ll 1$, which is sufficient to prove (2.19). In order to prove (2.18), we notice that

$$\begin{aligned}\sum_{m\geq M}\frac{\beta(m)}{m} &\ll \sum\sum_{ab^2\geq M}\frac{d(a)}{a^3b^2}\\ &\ll M^{-\frac{1}{2}}\sum_{a=1}^{\infty}\frac{d(a)}{a^2} \ll M^{-\frac{1}{2}}.\end{aligned}$$

□

The next proposition is the main result from [4], which is crucial to our proof.

Proposition 2.4.2. *(see [4, Proposition 4]) There exist constants c, C, C' such that for every $N, q \geq 2$ and $\frac{1}{\log 2N} < \beta < \frac{1}{10}$, there exist a subset $E_N \subset \{1, 2, \ldots, N\}$ (independent of q) satisfying*

$$|E_N| \leq C'\beta \left(\log \frac{1}{\beta}\right)^C N \tag{2.20}$$

and such that, uniformly for $(a, q) = 1$, one has

$$\left| \sum_{\substack{n \leq N \\ n \notin E_N, (n,q)=1}} e\left(\frac{a\bar{n}^2}{q}\right) \right| \leq C'(\log 2N)^C N^{1-c\left(\beta \frac{\log N}{\log q}\right)^C}. \tag{2.21}$$

In fact we need the following corollary.

Corollary 2.4.3. *There exists an absolute $\delta > 0$ such that for every $\epsilon > 0$, we have*

$$\sum_{\substack{n \leq N \\ (n,q)=1}} e\left(\frac{a\bar{n}^2}{q}\right) \ll_\epsilon N(\log q)^{-\delta},$$

uniformly for $N, q \geq 2$ and $N \geq q^\epsilon$.

Remark 2.4.1. More generally, we may consider the sum

$$\Sigma(I, q) = \sum_{\substack{n \in I \\ (n,q)=1}} e\left(\frac{a\bar{n}^2}{q}\right)$$

where I is a general interval of length $N \pmod q$. By the completion of exponential sums and Weil's bound for complete sums, we know that

$$\Sigma(I, q) \ll q^{1/2} \log q, \tag{2.22}$$

for prime numbers q. Hence, (2.22) is non trivial as soon as $N \geq q^{\frac{1}{2}+\epsilon}$ (for any $\epsilon > 0$). Obvioulsy, Bourgain's result is much stronger than (2.22), but it only applies to intervals starting at 1.

Démonstration. (of Corollary 2.4.3) We use Proposition 2.4.2 and make the choice $\beta = (\log N)^{-\delta_1}$, where $\delta_1 = \min\left(\frac{1}{2}, \frac{1}{2C}\right)$. We add together inequalities (2.20) and (2.21) to obtain

$$\sum_{n \leq N, (n,q)=1} e\left(\frac{a\bar{n}^2}{q}\right) \ll N \frac{(\log\log N)^C}{(\log N)^{-\delta_1}} + N \frac{(\log N)^C}{\exp(c\epsilon^C (\log N)^{1/2})}.$$

The corollary now follows by taking, for example, $\delta = \delta_1/2$. □

Remark 2.4.2. Corollary 2.4.3 will be essential to the proof of Proposition 2.5.1, in which we use it for values of N which are roughly of size $\sqrt{\frac{X}{q}}$. Since we want to take q as large as $X^{1-\epsilon}$, it is very important that Bourgain's result holds for N as small as q^ϵ.

The next lemma is very similar in essence to many others to be found in literature, for example [37, Theorem 1], [2, Proposition 1.4] or [35, Theorem 3]. The proof, for instance, follows the lines of [2, Proposition 1.4].

Lemma 2.4.4. *Let $X \geq 1$ and let ℓ, r be integers such that r is squarefree. Let*

$$I(X,\ell,r) := \Big\{ u \in \mathbb{R}; u \text{ and } ru+\ell \in (0,X) \Big\} \tag{2.23}$$

and

$$S(\ell,r) := \sum_{n \in I(X,\ell,r)} \mu^2(n)\mu^2(rn+\ell). \tag{2.24}$$

Then, for every $r>0$, we have the equality

$$S(\ell,r) = f(\ell,r)|I(X,\ell,r)| + O_r\left(d_3(\ell)X^{2/3}(\log 2X)^{7/3}\right), \tag{2.25}$$

uniformly for $X \geq 2$ and integers ℓ, where

$$f(\ell,r) = C_2 \prod_{p|r}\left(\frac{p^2-1}{p^2-2}\right) \prod_{\substack{p^2|\ell \\ p\nmid r}} \left(\frac{p^2-1}{p^2-2}\right) \kappa((\ell,r^2)), \tag{2.26}$$

where κ is the multiplicative function defined by

$$\kappa(p^\alpha) = \begin{cases} \dfrac{p^2-p-1}{p^2-1}, & \text{if } \alpha = 1, \\ \dfrac{p^2-p}{p^2-1}, & \text{if } \alpha = 2, \\ 0, & \text{if } \alpha \geq 3. \end{cases} \tag{2.27}$$

We recall that C_2 is defined in (2.12).

Démonstration. We start by defining

$$\sigma(n) = \prod_{p^2|n} p, \ \ n \neq 0,$$

and

$$\xi(n) = \sigma(n)\sigma(rn+\ell). \tag{2.28}$$

Notice that the right-hand side of equation (2.28) above actually depends on ℓ and r, but since these numbers will be held fixed in the following calculations, we omit this dependency.
Since $\xi(n)$ is an integer ≥ 1 and since

$$\mu^2(n)\mu^2(rn+\ell) = 1 \iff \xi(n) = 1,$$

we deduce the equality

$$S(\ell,r) = \sum_{n \in I(X,\ell,r)} \sum_{d|\xi(n)} \mu(d) = \sum_{d \geq 1} \mu(d) N_d(\ell,r),$$

where

$$N_d(\ell, r) = \#\Big\{n \in I(X, \ell, r);\ \xi(n) \equiv 0 \pmod d\Big\}.$$

Notice that the condition

$$p \mid \xi(n)$$

only depends on the congruence class of $n \pmod{p^2}$, for fixed values of ℓ and r. We let

$$u_p(\ell, r) := \#\Big\{0 \le v \le p^2 - 1; \xi(v) \equiv 0 \pmod p\Big\}, \tag{2.29}$$

and

$$U_d(\ell, r) := \prod_{p \mid d} u_p(\ell, r).$$

Then, by the Chinese remainder theorem, we have the equality

$$N_d(\ell, r) = U_d(\ell, r)\frac{|I(X, \ell, r)|}{d^2} + O\left(U_d(\ell, r)\right), \tag{2.30}$$

for every positive squarefree integer d. We also notice that if $(p, r) = 1$, then $|u_p(\ell, r)| \le 2$ and that $|u_p(\ell, r)| \le p^2$ in general. Therefore we have the upper bound

$$U_d(\ell, r) \ll_r 2^{\omega(d)}.$$

Let $2 \le y \le X$ be a parameter, which will be chosen later to be a power of X. We multiply formula (2.30) by $\mu(d)$ and sum for $d \le y$, thus obtaining the equality

$$\sum_{d \le y} \mu(d) N_d(\ell, r) = \sum_{d \le y} \mu(d) U_d(\ell, r)\frac{|I(X, \ell, r)|}{d^2} + O_r\left(\sum_{d \le y} 2^{\omega(d)}\right). \tag{2.31}$$

By completing the first sum on the right-hand side of (2.31), we have

$$\sum_{d \le y} \mu(d) N_d(\ell, r) = \prod_p \left(1 - \frac{u_p(\ell, r)}{p^2}\right) |I(X, \ell, r)| + O_r\left(\frac{X \log y}{y} + y \log y\right). \tag{2.32}$$

For large values of d, formula (2.30) is useless. Instead of it we will deduce by different means an estimation for

$$N_{>y}(\ell, r) := \sum_{d > y} \mu(d) N_d(\ell, r)$$

from which we will deduce the result.

We notice that $d \mid \xi(n)$ if and only if there exist $j, k \ge 1$ such that $d = jk$, $j^2 \mid n$ and $k^2 \mid rn + \ell$. Moreover since $n, rn + \ell < X$, we have $j, k < \sqrt{X}$. From this observation we deduce

$$\begin{aligned}
|N_{>y}(\ell, r)| &= \left| \sum_{y < d \le X} \mu(d) \left| \Big\{n \in I(X, \ell, r);\ \xi(n) \equiv 0 \pmod d\Big\} \right| \right| \\
&\le \sum_{\substack{j,k \le \sqrt{X} \\ jk > y}} \left| \Big\{n \in \mathbb{Z}; 0 < n, rn + \ell < X \text{ and } j^2 \mid n, k^2 \mid rn + \ell\Big\} \right| \\
&= \sum_{\substack{j,k \le \sqrt{X} \\ jk > y}} N(j, k),
\end{aligned}$$

say.
We shall divide the possible values of j and k into sets of the form

$$\mathcal{B}(J,K) := \Big\{(j,k) \in \mathbb{Z}^2; j \sim J, k \sim K\Big\}.$$

We can do the division using at most $O((\log X)^2)$ of these sets since we are summing over $j, k \leq X^{1/2}$.
Let

$$\begin{aligned}\mathcal{N}(J,K) &:= \sum_{j\sim J, k\sim K} N(j,k) \\ &= \#\Big\{(j,k,u,v); j \sim J, k \sim K, 0 < j^2u, k^2v < X, \text{ and } k^2v = rj^2u + \ell\Big\}\end{aligned}$$

By taking the maximum over all J, K, we obtain a pair (J,K) with $J, K \leq X^{1/2}$ such that $JK \geq y/4$ and we have the upper bound

$$N_{>y}(\ell, r) \ll \mathcal{N}(J,K)(\log X)^2. \tag{2.33}$$

At last, we estimate $\mathcal{N}(J,K)$ in the following way :

$$\mathcal{N}(J,K) \leq \sum_{k\sim K} \sum_{u \leq XJ^{-2}} \sum_{\substack{j\sim J \\ j^2ru \equiv -\ell \pmod{k^2}}} 1.$$

For j, k relevant to the sum above, we write $f = (j,k)$. From the congruence condition in the inner sum, we have that $f^2 \mid \ell$. So we write

$$j_0 = \frac{j}{f},\ k_0 = \frac{k}{f} \text{ and } \ell_0 = \frac{\ell}{f^2}.$$

The congruence then becomes

$$j_0^2 ru \equiv -\ell_0 \pmod{k_0^2}.$$

Now, let $g = (k_0^2, r)$ as above we have $g \mid \ell_0$. We write

$$k_1 = \frac{k_0^2}{g}, s = \frac{r}{g} \text{ and } t = \frac{\ell_0}{g}.$$

That transforms the congruence into

$$j_0^2 su \equiv -t \pmod{k_1}.$$

Finally, let $h = (k_1, t)$. From the considerations above, we must have $h \mid u$. We write

$$k' = \frac{k_1}{h}, t' = \frac{t}{h} \text{ and } u' = \frac{u}{h}.$$

So the congruence becomes

$$j_0^2 su' \equiv -t' \pmod{k'}$$

and since $(t', k') = 1$, it has at most $2.2^{\omega(k')} \leq 2d(k_0)$ solutions in $j_0 \pmod{k'}$. Therefore we have

$$\begin{aligned}
\mathcal{N}(J,K) &\leq \sum_{g|r} \sum_{f^2h|\ell} \sum_{\substack{k_0 \sim K/f \\ gh|k_0^2}} \sum_{u' \leq XJ^{-2}h^{-1}} \sum_{\substack{j_0 \sim J/f \\ j_0^2 su' \equiv -t' \pmod{k_0^2/gh}}} 1 \\
&\leq 2 \sum_{g|r} \sum_{f^2h|\ell} \sum_{k_0 \sim K/f} XJ^{-2}h^{-1} \left\{ \frac{Jgh}{fk_0^2} + 1 \right\} d(k_0) \\
&\ll_r \sum_{f^2h|\ell} \sum_{k_0 \sim K/f} XJ^{-2} \left\{ \frac{J}{fk_0^2} + 1 \right\} d(k_0) \\
&\ll \sum_{f^2h|\ell} XJ^{-2} \left\{ \frac{J}{K^2} + \frac{1}{f} \right\} K \log K \\
&\ll d_3(\ell) XJ^{-2} \left\{ \frac{J}{K^2} + 1 \right\} K \log X.
\end{aligned}$$

Hence

$$\mathcal{N}(J,K) \ll_r d_3(\ell) \left\{ Xy^{-1} + XJ^{-2}K \right\} \log X.$$

A similar inequality with the roles of J and K interchanged on the right hand side can be obtained in an analogous way. Combining the two formulas, we deduce

$$\begin{aligned}
\mathcal{N}(J,K) &\ll_r d_3(\ell) \left\{ Xy^{-1} + X(JK)^{-1/2} \right\} \log X \\
&\ll d_3(\ell) Xy^{-1/2} \log X. \qquad (2.34)
\end{aligned}$$

Replacing (2.34) in (2.33) and adding the latter to (2.32), it gives

$$S(\ell, r) = \prod_p \left(1 - \frac{u_p(\ell, r)}{p^2} \right) |I(X, \ell, r)| + O_r \left(y \log y + d_3(\ell) Xy^{-1/2} (\log X)^3 \right).$$

We make the choice $y = X^{2/3} (\log X)^{4/3}$ obtaining

$$S(\ell, r) = \prod_p \left(1 - \frac{u_p(\ell, r)}{p^2} \right) |I(X, \ell, r)| + O_r \left(d_3(\ell) X^{2/3} (\log X)^{7/3} \right). \qquad (2.35)$$

We finish by a study of $u_p(\ell, r)$. We distinguish five different cases (we recall that r is squarefree)

— If $p \mid r$, $p^2 \mid \ell$ then

$$u_p(\ell, r) = p,$$

— If $p \mid r$, $p \mid \ell$ but $p^2 \nmid \ell$ then

$$u_p(\ell, r) = p + 1,$$

— If $p \mid r$, $p \nmid \ell$ then

$$u_p(\ell, r) = 1,$$

— If $p \nmid r$, $p^2 \mid \ell$ then
$$u_p(\ell, r) = 1,$$
— If $p \nmid r$, $p^2 \nmid \ell$ then
$$u_p(\ell, r) = 2.$$
The lemma is now a consequence of formula (2.35) and the different values of $u_p(\ell, r)$. □

2.4.1 Sums involving the B_2 function

In the following we study certain sums involving the Bernoulli polynomials $B_2(x)$. In the next lemma, we deal with the simplest case
$$A(Y; q, a) = \sum_{\substack{n \geq 1 \\ (n,q)=1}} \left\{ B_2\left(\frac{Y^2}{n^2} + \frac{a\bar{n}^2}{q}\right) - B_2\left(\frac{a\bar{n}^2}{q}\right) \right\}, \tag{2.36}$$
where Y is a positive real number, a, q are coprime integers. The sum above will serve as an archetype for more complicated sums appearing in the proof of Proposition 2.4.6, which in turn will be central for estimating $C[\gamma](X, q)$. One elementary bound for $A(Y; q, a)$ can be given by noticing that we have both
$$B_2\left(\frac{Y^2}{n^2} + \frac{a\bar{n}^2}{q}\right) - B_2\left(\frac{a\bar{n}^2}{q}\right) \ll 1, \tag{2.37}$$
since B_2 is bounded, and
$$\begin{aligned} B_2\left(\frac{Y^2}{n^2} + \frac{a\bar{n}^2}{q}\right) - B_2\left(\frac{a\bar{n}^2}{q}\right) &= \int_{\frac{a\bar{n}^2}{q}}^{\frac{Y^2}{n^2} + \frac{a\bar{n}^2}{q}} B_1(v)dv \\ &\ll \frac{Y^2}{n^2}, \end{aligned} \tag{2.38}$$
since B_1 is also a bounded function. Gathering (2.37) and (2.38), we obtain
$$\begin{aligned} A(Y; q, a) &\ll \sum_{n \leq Y} 1 + \sum_{n > Y} \frac{Y^2}{n^2} \\ &\ll Y. \end{aligned} \tag{2.39}$$
In the following lemma we give a non-trivial bound for the sum above by means of Bourgain's bound, via Corollary 2.4.3. What we obtain is better than trivial by just a small power of $\log q$, but it is sufficient to obtain Theorem 2.1.2.

Lemma 2.4.5. *There exists $\delta > 0$ such that for every $\epsilon > 0$, we have the inequality*
$$A(Y; q, a) \ll_\epsilon Y(\log q)^{-\delta}, \tag{2.40}$$
uniformly for integers a and q such that $q \geq 2$, $(a, q) = 1$ and real numbers $Y > q^\epsilon$.

Démonstration. By Corollary 2.4.3, we know that there exists $\delta_1 > 0$ such that

$$\sum_{\substack{n\leq Y\\(n,q)=1}} e\left(\frac{a\bar{n}^2}{q}\right) \ll_\epsilon Y(\log q)^{-\delta_1}, \tag{2.41}$$

uniformly for $(a,q)=1$ and $Y > q^{\epsilon/10}$. For simplificity, we write

$$\Delta_Y(n;q,a) = B_2\left(\frac{Y^2}{n^2} + \frac{a\bar{n}^2}{q}\right) - B_2\left(\frac{a\bar{n}^2}{q}\right). \tag{2.42}$$

The sum on the left-hand side of (2.41) appears naturally once we use the Fourier series development for $B_2(x)$

$$B_2(x) = \sum_{h\neq 0} \frac{1}{4\pi^2 h^2} e(hx) \tag{2.43}$$

in formula (2.36). Let

$$\theta(q) = (\log q)^{\delta_1/2}. \tag{2.44}$$

By (2.37) and the Fourier decomposition of $B_2(x)$ (2.43), we have

$$\begin{aligned}
\sum_{\substack{n\leq Y\theta(q)\\(n,q)=1}} \Delta_Y(n;q,a) &= \sum_{\substack{Y\theta(q)^{-1}\leq n\leq Y\theta(q)\\(n,q)=1}} \Delta_Y(n;q,a) + O(Y\theta(q)^{-1}) \\
&= \sum_{h\neq 0} \frac{1}{4\pi^2 h^2} \sum_{\substack{Y\theta(q)^{-1}\leq n\leq Y\theta(q)\\(n,q)=1}} \left(e\left(\frac{hY^2}{n^2}\right) - 1\right) e\left(\frac{ah\bar{n}^2}{q}\right) + O(Y\theta(q)^{-1}) \\
&= \sum_{1\leq |h|\leq \theta(q)^3} \frac{1}{4\pi^2 h^2} \sum_{\substack{Y\theta(q)^{-1}\leq n\leq Y\theta(q)\\(n,q)=1}} \left(e\left(\frac{hY^2}{n^2}\right) - 1\right) e\left(\frac{ah\bar{n}^2}{q}\right) + O(Y\theta(q)^{-1}).
\end{aligned} \tag{2.45}$$

Summing by parts, we see that the inner sum of the right-hand side of inequality (2.45) is

$$\ll \sum_{Y\theta(q)^{-1}\leq m\leq Y\theta(q)} \frac{|h|Y^2}{m^3} \left| \sum_{\substack{Y\theta(q)^{-1}\leq n\leq m\\(n,q)=1}} e\left(\frac{ah\bar{n}^2}{q}\right)\right| + \left| \sum_{\substack{Y\theta(q)^{-1}\leq n\leq Y\theta(q)\\(n,q)=1}} e\left(\frac{ah\bar{n}^2}{q}\right)\right|.$$

Now, if q is prime and sufficiently large, then any integer h satisfying $1 \leq |h| \leq \theta(q)^3$ is coprime with q. Then, by (2.41), the above expression is

$$\begin{aligned}
&\ll \sum_{Y\theta(q)^{-1}\leq m\leq Y\theta(q)} \frac{|h|Y^2}{m^2}(\log q)^{-\delta_1} + Y\theta(q)^{-1} \\
&\ll |h|Y\theta(q)^{-1}.
\end{aligned} \tag{2.46}$$

As we insert the upper-bound (2.46) in formula (2.45), we obtain

$$\sum_{\substack{n\leq Y\theta(q)\\(n,q)=1}} \Delta_Y(n;q,a) \ll Y\theta(q)^{-1}\log\log q \ll Y(\log q)^{-\delta_1/4}. \tag{2.47}$$

For the remainder terms we use the trivial upper bound (2.38) to deduce the inequality

$$\begin{aligned}\sum_{\substack{n>Y\theta(q)\\(n,q)=1}} \Delta_Y(n;q,a) &\ll \sum_{n>Y\theta(q)} \frac{Y^2}{n^2}\\ &\ll Y\theta(q)^{-1}.\end{aligned} \tag{2.48}$$

Combining (2.47) and (2.48), we obtain that

$$\sum_{\substack{n\geq 1\\(n,q)=1}} \Delta_Y(n;q,a) \ll Y(\log q)^{-\delta_1/4},$$

uniformly for $(a,q)=1$ and $Y>q^{\epsilon}$. The proof of lemma 2.4.5 is now complete. □

Remark 2.4.3. Among the hypotheses of lemma (2.4.5), it is essential that we have $(a,q)=1$. In the case where $q \mid a$, one cannot improve on (2.39). Indeed, it is possible to show that (see formula (1.42))

$$A(Y;q,0) = -\frac{\varphi(q)}{q}\frac{\zeta(3/2)}{2\pi}Y + O(d(q)Y^{2/3}) \quad (Y\geq 1).$$

2.4.2 A consequence of Lemma 2.4.5

In order to evaluate $S[\gamma](X,q)$ (see (2.16)), it is important to consider the following sum which appears in equation (2.25).

Definition 2.4.1. For integers q,r,s such that $q\geq 1$ and $q\nmid rs$, let

$$\mathfrak{S}[\gamma_{r,s}](X,q) := \sum_{\ell\equiv s \pmod q} f(\ell,r)|I(X,\ell,r)|.$$

Remark that the sum defined above is actually a finite sum since whenever $|\ell|>2|r|X$, we have $I(X,\ell,r)=\emptyset$.
The purpose of this subsection is to prove the following.

Proposition 2.4.6. *Let $C(q)$ be as in (2.14). There exists $\delta>0$ and every $\epsilon>0$, for every $r\neq 0$ such that r is squarefree, one has*

$$\mathfrak{S}[\gamma_{r,s}](X,q) = \left(\frac{6}{\pi^2}\right)^2\left(1+\frac{1}{q^2(q^2-2)}\right)^{-1}X^2/q + O_{\epsilon,r}(q^{1+\epsilon}+X^{1/2}q^{1/2}(\log q)^{-\delta}), \tag{2.49}$$

uniformly for $X\geq 2$, for integers s and prime numbers q psuch that $q\nmid rs$.

The special case $r = 1$ simplifies many of the calculations in the proof below. For instance, the sums over ρ, σ and τ disappear. Although, this simpler result is, in fact, equally deep and it shows more clearly the connection between the upper bound (2.40) and the error term in (2.49).

Démonstration. We start by recalling (2.26)

$$f(\ell, r) = C_2 \prod_{p|r} \left(\frac{p^2-1}{p^2-2}\right) \prod_{\substack{p^2|\ell \\ p\nmid r}} \left(\frac{p^2-1}{p^2-2}\right) \kappa((\ell, r^2)),$$

where C_2 is as in (2.12). We notice that the term

$$C_2 \prod_{p|r} \left(\frac{p^2-1}{p^2-2}\right)$$

is independent of ℓ. We consider the sum

$$\begin{aligned} \mathfrak{S}'[\gamma_{r,s}](X, q) &= C_2^{-1} \prod_{p|r} \left(\frac{p^2-1}{p^2-2}\right)^{-1} \mathfrak{S}[\gamma_{r,s}](X, q) \\ &= \sum_{\ell \equiv s \pmod q} |I(X, \ell, r)| \prod_{\substack{p^2|\ell \\ p\nmid r}} \left(\frac{p^2-1}{p^2-2}\right) \kappa((\ell, r^2)). \end{aligned} \tag{2.50}$$

We expand the product $\displaystyle\prod_{\substack{p^2|\ell \\ p\nmid r}} \left(\frac{p^2-1}{p^2-2}\right)$ as follows.

$$\prod_{\substack{p^2|\ell \\ p\nmid r}} \left(\frac{p^2-1}{p^2-2}\right) = \sum_{\substack{d^2|\ell \\ (d,r)=1}} \frac{h(d)}{d^2},$$

from which we deduce

$$\begin{aligned} \mathfrak{S}'[\gamma_{r,s}](X, q) &:= \sum_{\rho|r^2} \kappa(\rho) \sum_{\substack{\ell \equiv s \,(\mathrm{mod}\, q) \\ (\ell, r^2)=\rho}} |I(X, \ell, r)| \sum_{\substack{d^2|\ell \\ (d,r)=1}} \frac{h(d)}{d^2} \\ &= \sum_{\rho\sigma|r^2} \kappa(\rho)\mu(\sigma) \sum_{\ell_0 \equiv \overline{\rho\sigma} s \,(\mathrm{mod}\, q)} |I\left(X, \rho\sigma\ell_0, r\right)| \sum_{\substack{d^2|\ell_0 \\ (d,r)=1}} \frac{h(d)}{d^2} \\ &= \sum_{\rho\sigma|r^2} \kappa(\rho)\mu(\sigma) \sum_{(d,qr)=1} \frac{h(d)}{d^2} \sum_{\ell_1 \equiv \overline{(\rho\sigma d^2)} s \,(\mathrm{mod}\, q)} \left|I(X, \rho\sigma d^2\ell_1, r)\right| \end{aligned} \tag{2.51}$$

where in the second line we used Möbius inversion formula for detecting the gcd condition and we noticed that the congruence satisfied by ℓ_0 implies $(d, q) = 1$.

We write the inner sum as an integral :

$$\sum_{\ell_1 \equiv \overline{(\rho\sigma d^2)}s \,(\mathrm{mod}\ q)} \left|I(X, \rho\sigma d^2\ell_1, r)\right| = \int_0^X \sum_{\ell_1 \equiv \overline{(\rho\sigma d^2)}s \,(\mathrm{mod}\ q)} \mathbf{1}_{(0,X)}(ru + \rho\sigma d^2\ell_1)du, \tag{2.52}$$

where $\mathbf{1}_{(0,X)}$ is the characteristic function of the interval $(0, X)$. Hence the inner sum above equals

$$\left\lfloor \frac{X - ru}{\rho\sigma d^2 q} - \frac{\overline{(\rho\sigma d^2)}s}{q} \right\rfloor - \left\lfloor \frac{-ru}{\rho\sigma d^2 q} - \frac{\overline{(\rho\sigma d^2)}s}{q} \right\rfloor$$
$$= \frac{X}{\rho\sigma d^2 q} - B_1\left(\frac{X - ru}{\rho\sigma d^2 q} - \frac{\overline{(\rho\sigma d^2)}s}{q}\right) + B_1\left(\frac{-ru}{\rho\sigma d^2 q} - \frac{\overline{(\rho\sigma d^2)}s}{q}\right),$$

for almost all $u \in (0, X)$ in the sense of Lebesgue measure.
If we use this formula in equation (2.52), we deduce the equality

$$\sum_{\ell_1 \equiv \overline{(\rho\sigma d^2)}s \,(\mathrm{mod}\ q)} \left|I(X, \rho\sigma d^2\ell_1, r)\right| =$$
$$\frac{X^2}{\rho\sigma d^2 q} - \frac{\rho\sigma d^2 q}{r}\left\{B_2\left(\frac{X^2}{\rho\sigma d^2 q} - \frac{\overline{(\rho\sigma d^2)}s}{q}\right) - B_2\left(-\frac{\overline{(\rho\sigma d^2)}s}{q}\right)\right.$$
$$\left. - B_2\left(\frac{(1-r)X}{\rho\sigma d^2 q} - \frac{\overline{(\rho\sigma d^2)}s}{q}\right) + B_2\left(\frac{-rX}{\rho\sigma d^2 q} - \frac{\overline{(\rho\sigma d^2)}s}{q}\right)\right\}. \tag{2.53}$$

From this point on, we suppose $r < 0$. The case $r > 0$ requires only minor modifications. With this hypothesis, we have that both

$$\frac{(1-r)X}{\rho\sigma d^2 q} \text{ and } \frac{-rX}{\rho\sigma d^2 q}$$

are positive for every $\rho, \sigma \geq 1$.

We inject (2.53) above in equation (2.51) and we define

$$B(D; q, a; r) := \sum_{(d,qr)=1} h(d)\Delta_D(d, q; a),$$

where $\Delta_D(d, q; a)$ is as in (2.42). From (2.51) and (2.53) we deduce the equality

$$\mathfrak{S}'[\gamma_{r,s}](X, q) = \lambda(q, r)\frac{X^2}{q} - \frac{q}{r}\left\{G\left(\frac{X}{q}; q, -s; r\right)\right.$$
$$\left. - G\left(\frac{(1-r)X}{q}; q, -s; r\right) + G\left(\frac{-rX}{q}; q, -s; r\right)\right\}, \tag{2.54}$$

where

$$G(Y;q,s;r)=\sum_{\rho\sigma|r^2}\sum\kappa(\rho)\mu(\sigma)\rho\sigma B\left(\sqrt{\frac{Y}{\rho\sigma}},q,\overline{\rho\sigma}s;r\right),$$

and

$$\lambda(q,r)=\sum_{\rho\sigma|r^2}\frac{\kappa(\rho)\mu(\sigma)}{\rho\sigma}\times\sum_{(d,qr)=1}\frac{h(d)}{d^4}.$$

Returning to the function $\beta(m)$ defined in Lemma 2.4.1, we observe that for a general $D>0$, one has

$$\begin{aligned}B\left(D;q,a;r\right)&=\sum_{(m,qr)=1}\beta(m)\sum_{(n,qr)=1}\Delta_D(mn;q,a)\\&=\sum_{(m,qr)=1}\beta(m)\sum_{(n,qr)=1}\Delta_{D/m}(n;q,\overline{m}^2a)\\&=\sum_{(m,qr)=1}\beta(m)\sum_{\tau|r}\mu(\tau)\sum_{(n,q)=1}\Delta_{D/\tau m}(n;q,\overline{\tau}^2\overline{m}^2a)\\&=\sum_{(m,qr)=1}\beta(m)\sum_{\tau|r}\mu(\tau)A(D/\tau m,q;\overline{\tau}^2\overline{m}^2a).\end{aligned}$$

We apply the equality above with $D=\sqrt{\frac{Y}{\rho\sigma}}$ and $a=\overline{\rho\sigma}s$, multiply by $\kappa(\rho)\mu(\sigma)\rho\sigma$ and sum over ρ,σ such that $\rho\sigma\mid r^2$, we have

$$G(Y;q,s;r)=\sum_{\rho\sigma|r^2}\sum\sum_{\tau|r}\sum_{(m,qr)=1}\kappa(\rho)\mu(\sigma)\mu(\tau)\rho\sigma\beta(m)A\left(\sqrt{\frac{Y}{\rho\sigma\tau^2m^2}};q,\overline{\rho\sigma\tau^2m^2}s\right).\quad(2.55)$$

Our discussion depends on the size of Y.

— If $Y\leq q^\epsilon$, we have the trivial bound (see (2.39))

$$A\left(\sqrt{\frac{Y}{\rho\sigma\tau^2m^2}};q,\overline{\rho\sigma\tau^2m^2}s\right)\ll\sqrt{\frac{Y}{\rho\sigma\tau^2m^2}}\leq\frac{Y^{1/2}}{m},$$

for every $\rho,\sigma,\tau\geq1$. Summing over ρ,σ,τ and m, it gives

$$\begin{aligned}G(Y;q,s;r)&\ll_r Y^{1/2}\sum_{m\geq1}\frac{\beta(m)}{m}\\&\ll q^{\epsilon/2},\end{aligned}\quad(2.56)$$

as a consequence of upper bound (2.18).

— If $Y>q^\epsilon$, we separate the quadruple sum on the right-hand side of (2.55) as

$$\sum\sum\sum\sum_{\substack{m\leq q^{\epsilon/2}\\ \rho\sigma\tau^2m^2>Y/q^{\epsilon}}}+\sum\sum\sum\sum_{\substack{m\leq q^{\epsilon/2}\\ \rho\sigma\tau^2m^2\leq Y/q^{\epsilon}}}+\sum\sum\sum\sum_{m>q^{\epsilon/2}}.$$

For the first sum we have, again, the trivial bound

$$A\left(\sqrt{\frac{Y}{\rho\sigma\tau^2m^2}};q,\overline{\rho\sigma\tau^2m^2}s\right)\ll\sqrt{\frac{Y}{\rho\sigma\tau^2m^2}}\leq q^{\epsilon/2}, \tag{2.57}$$

The most delicate sum is the second one, since we appeal to (2.40). This gives

$$A\left(\sqrt{\frac{Y}{\rho\sigma\tau^2m^2}};q,\overline{\rho\sigma\tau^2m^2}s\right)\ll_{\epsilon}\sqrt{\frac{Y}{\rho\sigma\tau^2m^2}}(\log q)^{-\delta}. \tag{2.58}$$

For the third one, we use the trivial bound,

$$A\left(\sqrt{\frac{Y}{\rho\sigma\tau^2m^2}};q,\overline{\rho\sigma\tau^2m^2}s\right)\ll\sqrt{\frac{Y}{\rho\sigma\tau^2m^2}}, \tag{2.59}$$

Gathering the inequalities (2.57), (2.58) and (2.59) in (2.55), we obtain

$$G(Y;q,s;r)\ll_{\epsilon,r}q^{\epsilon/2}\sum_{m\leq q^{\epsilon/2}}|\beta(m)|+\sqrt{Y}(\log q)^{-\delta}\sum_{m\leq q^{\epsilon/2}}\frac{|\beta(m)|}{m}+\sqrt{Y}\sum_{m>q^{\epsilon/2}}\frac{|\beta(m)|}{m},$$

and finally, by Lemma 2.4.1

$$G(Y;q,s;r)\ll_{\epsilon,r}q^{\epsilon}+\sqrt{Y}(\log q)^{-\delta}\qquad(Y>q^{\epsilon}). \tag{2.60}$$

Comparing with (2.56), we have that (2.60) is true for any $Y\geq 1$.

Combining (2.60) and (2.54), one has

$$\mathfrak{S}'[\gamma_{r,s}](X,q)=\lambda(q,r)\frac{X^2}{q}+O_{\epsilon,r}(q^{1+\epsilon}+X^{1/2}q^{1/2}(\log q)^{-\delta}). \tag{2.61}$$

If we multiply the formula above by $C_2\prod_{p|r}\left(\frac{p^2-1}{p^2-2}\right)$ (recall formula (2.50)), we deduce

$$\mathfrak{S}[\gamma_{r,s}](X,q)=\Lambda(q,r)\frac{X^2}{q}+O_{\epsilon,r}(q^{1+\epsilon}+X^{1/2}q^{1/2}(\log q)^{-\delta}), \tag{2.62}$$

where

$$\Lambda(q,r)=C_2\prod_{p|r}\left(\frac{p^2-1}{p^2-2}\right)\sum_{\rho\sigma|r^2}\frac{\kappa(\rho)\mu(\sigma)}{\rho\sigma}\times\sum_{(d,qr)=1}\frac{h(d)}{d^4}$$

Since for r squarefree, we have the equality

$$\sum_{\rho\sigma|r^2}\frac{\kappa(\rho)\mu(\sigma)}{\rho\sigma}=\prod_{p|r}\left(\frac{p^2-1}{p^2}\right),$$

then, by some standard calculations, we notice that $\Lambda(q,r)$ does not depend on r. More precisely, since, q is prime and $(q,r)=1$, we have

$$\Lambda(q,r)=\left(\frac{6}{\pi^2}\right)^2\left(1+\frac{1}{q^2(q^2-2)}\right)^{-1}.$$

As a consequence, formula (2.62) completes the proof of Proposition 2.4.6. □

2.5 Study of $S[\gamma_{r,s}](X,q)$

We rewrite $S[\gamma_{r,s}](X,q)$ (see (2.16)) as

$$S[\gamma_{r,s}](X,q)=\sum_{\ell\equiv s(\mathrm{mod}\ q)}\sum_{n\in I(X,\ell,r)}\mu^2(n)\mu^2(rn+\ell). \tag{2.63}$$

Recall that for $|\ell|>2|r|X$ we have $I(X,\ell,r)$. Hence, by (2.25), we have that (recall Definition 2.4.1)

$$\begin{aligned}S[\gamma_{r,s}](X,q)&=\sum_{\substack{\ell\equiv s\ (\mathrm{mod}\ q)\\ |\ell|\leq 2|r|X}}f(\ell,r)|I(X,\ell,r)|+O_r\left(\frac{X}{q}X^{2/3+\epsilon}\right)\\&=\mathfrak{S}[\gamma_{r,s}](X,q)+O_r\left(\frac{X^{5/3+\epsilon}}{q}\right).\end{aligned}$$

From Proposition 2.4.6, we deduce the equality

$$\begin{aligned}S[\gamma_{r,s}](X,q)=\left(\frac{6}{\pi^2}\right)^2\left(1+\frac{1}{q^2(q^2-2)}\right)^{-1}\frac{X^2}{q}\\+O_{\epsilon,r}\left(q^{1+\epsilon}+X^{1/2}q^{1/2}(\log q)^{-\delta}+\frac{X^{5/3+\epsilon}}{q}\right).\end{aligned} \tag{2.64}$$

By the definition (2.14) for $C(q)$, one can easily see that

$$\left(\frac{6}{\pi^2}\right)^2\left(1+\frac{1}{q^2(q^2-2)}\right)^{-1}=C(q)^2+O\left(\frac{1}{q^2}\right).$$

In conclusion, we proved

Proposition 2.5.1. *Let $C(q)$ be as in (2.14). There exists $\delta>0$ such that for every $\epsilon>0$ and every $r\neq 0$, one has the asymptotic formula*

$$S[\gamma_{r,s}](X,q)=C(q)^2\frac{X^2}{q}+O_{\epsilon,r}\left(q^{1+\epsilon}+X^{1/2}q^{1/2}(\log q)^{-\delta}+\frac{X^{5/3+\epsilon}}{q}+\frac{X^2}{q^3}\right), \tag{2.65}$$

uniformly for $X\geq 2$, for integers s and prime numbers q such that $q\nmid rs$ and $q\leq X$.

2.6 Proof of the main Theorem

We start by recalling (2.15)

$$C[\gamma_{r,s}](X,q) = S[\gamma_{r,s}](X,q) - 2C(q)\frac{X}{q}\sum_{n\leq X}\mu^2(n) + C(q)^2\frac{X^2}{q} + O\left(\frac{X^2}{q^2}\right).$$

By Proposition 2.5.1 and formula (2.17), we deduce the inequality

$$C[\gamma](X,q) \ll_{\epsilon,r} q^{1+\epsilon} + X^{1/2}q^{1/2}(\log q)^{-\delta} + \frac{X^{5/3+\epsilon}}{q} + \frac{X^2}{q^2}.$$

The proof of Theorem 2.1.2 is now complete.

Chapitre 3

On two conjectures concerning squarefree numbers in arithmetic progressions

3.1 Introduction

The distribution of arithmetic sequences in arithmetic progressions is a central subject in analytic number theory. Let $f : \mathbb{Z}_{>0} \to \mathbb{R}_{>0}$ be a positive arithmetic sequence. If f is sufficiently reasonable, one expects that, for all $(a, q) = 1$, we have

$$\sum_{\substack{n \leq X \\ n \equiv a \,(\mathrm{mod}\ q)}} f(n) \sim \frac{1}{\varphi(q)} \sum_{\substack{n \leq X \\ (n,q)=1}} f(n) \qquad (X \to \infty). \tag{3.1}$$

Two important questions that arise naturally concern the uniformity of such a formula (see section 3.1.1 below) and the size of the error term

$$E_f(X, q, a) := \sum_{\substack{n \leq X \\ n \equiv a \,(\mathrm{mod}\ q)}} f(n) - \frac{1}{\varphi(q)} \sum_{\substack{n \leq X \\ (n,q)=1}} f(n). \tag{3.2}$$

These questions are intimately related to the analytic properties of the associated L-functions

$$L_f(s, \chi) := \sum_{n=1}^{\infty} f(n)\chi(n)n^{-s},$$

where χ is a Dirichlet character. Two particularly interesting cases occur when $f = \Lambda$ is the van Mangoldt function or $f = \mu^2$, where μ is the Möbius function. The first one is closely related to the distribution of prime numbers while the latter corresponds to squarefree numbers. For such choices the associated L-functions are, respectively,

$$L_\Lambda(s,\chi) = \frac{L'(s,\chi)}{L(s,\chi)} \quad \text{and} \quad L_{\mu^2}(s,\chi) = \frac{L(s,\chi)}{L(s,\chi^2)},$$

where $L(s,\chi)$ is the classical Dirichlet L-function. In that context, H. L. Montgomery stated two conjectures whose implications are much deeper than the generalized Riemann Hypothesis for Dirichlet L-functions (GRH). The original conjectures can be found, respectively in [31, Formula (15.9), page 136] and [7, top of page 145]. We state them in slightly improved forms, which, in the case of the van Mangoldt function, is due to Friedlander and Granville [14] and in the case of squarefree numbers can be found in a recent preprint by Le Boudec [28].

Conjecture 3.1.1. *Let $\epsilon, X > 0$. Let a and q be integers such that $(a,q) = 1$ and $1 \leq q \leq X$, then we have*

— *for primes,*

$$E_\Lambda(X,q,a) = O\left(X^\epsilon \left(\frac{X}{q}\right)^{\frac{1}{2}}\right), \tag{3.3}$$

— *for squarefree numbers,*

$$E_{\mu^2}(X,q,a) = O\left(X^\epsilon \left(\frac{X}{q}\right)^{\frac{1}{4}}\right), \tag{3.4}$$

where the implied constants depend at most on ϵ.

Concerning (3.3), it is not known, for the moment, if there exists $\delta > 0$ such that

$$E_\Lambda(X,q,a) = O\left(\left(\frac{X}{q}\right)^{1-\delta}\right)$$

holds in any range whatsoever. For instance, GRH would imply that for every $\alpha < \frac{1}{2}$, there exists $\delta = \delta(\alpha) > 0$, such that

$$E_\Lambda(X,q,a) = O\left(\left(\frac{X}{q}\right)^{1-\delta}\right),$$

uniformly for $1 \leq q \leq X^\alpha$ and $(a,q) = 1$. Still under GRH, Turán [38] proved that (3.3) holds on average : Uniformly for $1 \leq q \leq X$, we have

$$\sum_{\substack{a=0 \\ (a,q)=1}}^{q-1} E_\Lambda(X,q,a)^2 \ll X(\log X)^4.$$

If one seeks for unconditional results, one needs an extra sum over $q \leq Q$, for a certain $Q \leq X$. In this direction, Montgomery proved that for every $A > 0$, one has

$$\sum_{q \leq Q} \sum_{\substack{a=0 \\ (a,q)=1}}^{q-1} E_\Lambda(X,q,a)^2 = QX\log X + O_A\left(QX\log\frac{2X}{Q} + QX(\log X)^{-A}\right), \tag{3.5}$$

uniformly for $Q \leq X$, where the implied constant depends at most on A. Therefore, for every $A > 0$, (3.5) implies that (3.3) holds true on average over $q \leq X(\log X)^{-A}$ and a modulo q, with $(a, q) = 1$.

In the case of squarefree numbers, Prachar [34] proved that for every $\epsilon > 0$, uniformly for $(a, q) = 1$, $X \geq 2$,

$$E_{\mu^2}(X, q, a) \ll_\epsilon X^{\frac{1}{2}+\epsilon} q^{-\frac{1}{4}} + q^{\frac{1}{2}+\epsilon},$$

where the implied constant depends at most on ϵ. This result was later improved by Hooley [23] who showed that the above error term can be replaced by

$$O_\epsilon \left(X^{\frac{1}{2}} q^{-\frac{1}{2}} + q^{\frac{1}{2}+\epsilon} \right). \tag{3.6}$$

Both this results show that for every $\epsilon > 0$, there exists $\delta = \delta(\epsilon) > 0$

$$E_{\mu^2}(X, q, a) \ll_\epsilon \left(\frac{X}{q} \right)^{1-\delta},$$

uniformly for $q \leq X^{\frac{2}{3}-\epsilon}$. In a parallel to Túran's result, Corollary 1.1.2 gives the asymptotic formula

$$\sum_{\substack{a=0 \\ (a,q)=1}}^{q-1} E_{\mu^2}(X, q, a)^2 \sim C \prod_{p|q} \left(1 + \frac{2}{p^2} \right)^{-1} X^{\frac{1}{2}} q^{\frac{1}{2}},$$

as $X, q \to \infty$ and q satisfying $X^{\frac{31}{41}+\epsilon} \leq q \leq X^{1-\epsilon}$, where C is an absolute positive constant. This implies (3.4) on average on the above mentioned range. In a subsequent work, le Boudec [28] proves that if one seeks for an upper bound rather than an asymptotic formula, one gets a larger range. He proved that

$$\sum_{\substack{a=0 \\ (a,q)=1}}^{q-1} E_{\mu^2}(X, q, a)^2 \ll_\epsilon X^{\frac{1}{2}+\epsilon} q^{\frac{1}{2}},$$

uniformly for $X^{\frac{1}{2}} \leq q \leq X$.

Suppose $q \leq X^{\frac{1}{2}}$. In this case Hooley's result shows an approximation of (3.4), with $1/2$ instead of $1/4$. In this paper, we improve the exponent $1/2$ for $X^\epsilon \leq q \leq X^{\frac{1}{2}-\epsilon}$, therefore making a further step towards (3.4). For simplicity, we shall henceforth write $E(X, q, a)$ instead of $E_{\mu^2}(X, q, a)$.

Theorem 3.1.2. *For every $\epsilon > 0$, we have*

$$E(X, q, a) \ll_\epsilon \left(\frac{X}{q} \right)^{\frac{1}{2}+\epsilon} q^{-\frac{1}{192}} + \left(\frac{X}{q} \right)^{\frac{24}{49}+\epsilon} q^{\frac{3}{196}},$$

uniformly for every $X > 1$, every prime number q such that $q \leq X$, and every integer a such that $(a, q) = 1$.

Note that for $X^\alpha < q < 2X^\alpha$, $\alpha \leq \frac{2}{5}$, Theorem 3.1.2 shows that

$$E(X,q,a) \ll_\epsilon \left(\frac{X}{q}\right)^{\frac{1}{2}-\frac{\alpha}{192(1-\alpha)}+\epsilon} + \left(\frac{X}{q}\right)^{\frac{1}{2}-\frac{2-5\alpha}{196(1-\alpha)}+\epsilon}.$$

For example, when $\alpha = \frac{96}{283} < \frac{2}{5}$, the exponent is $\frac{93}{187} < \frac{1}{2}$, which is the best exponent given by Theorem 3.1.2. Therefore, we have the following corollary

Corollary 3.1.3. *For every $0 < \epsilon < \frac{1}{5}$, let $\delta(\epsilon) = \min\left(\frac{\epsilon}{192(1-\epsilon)}, \frac{25\epsilon}{196(3+5\epsilon)}\right)$. Then we have*

$$E(X,q,a) \ll_\epsilon \left(\frac{X}{q}\right)^{\frac{1}{2}-\delta(\epsilon)},$$

uniformly for every $X > 1$ and every prime number q such that $X^\epsilon \leq q \leq X^{\frac{2}{5}-\epsilon}$, and every integer a such that $(a,q) = 1$.

Our next result states that we can still obtain an exponent below $\frac{1}{2}$ for q as large as $X^{\frac{1}{2}-\epsilon}$, but one cannot quantify the exponent in this case

Theorem 3.1.4. *For every $0 < \eta < \frac{1}{4}$, there exists $\delta = \delta(\eta) > 0$ such that we have*

$$E(X,q,a) \ll_\eta \left(\frac{X}{q}\right)^{\frac{1}{2}-\delta},$$

uniformly for every $X > 1$ and every prime number q such that $X^\eta \leq q \leq X^{\frac{1}{2}-\eta}$, and integer a such that $(a,q) = 1$.

The main new input in the proofs of Theorems 3.1.2 and 3.1.4 are bounds for exponentials sums twisted by the Möbius function given by Fouvry *et al.* [11] and Bourgain [3]. The same exponential sums were estimated trivially in [23].

3.1.1 Range of uniformity

Concerning the range of uniformity, it is largely believed that if f is sufficiently reasonable, then (3.1) should hold uniformly for $q \leq X^{1-\epsilon}$. In the case where $f = \mu^2$, we know, thanks to Prachar [34] that this is true in the range $q \leq X^{\frac{2}{3}-\epsilon}$. Our next result proves that we can overcome the threshold $X^{\frac{2}{3}}$ by a small power of $\log X$. More precisely, we prove

Theorem 3.1.5. *For every $0 < \gamma < \frac{1}{2}$, there exists $C(\gamma)$ such that for every $X > 3$, for every prime q, for every a coprime with q, one has the inequality*

$$|E(X,q,a)| \leq C(\gamma)\left(\frac{X^{\frac{1}{3}}(\log\log X)^{\frac{11}{6}}}{(\log X)^{\frac{1}{6}-\frac{\gamma}{3}}} + \frac{X\log\log X}{q(\log X)^{\frac{\gamma}{2}}}\right).$$

Perhaps more interesting is the following corollary (obtained by choosing $\gamma = \frac{1-6\alpha}{5}$ in Theorem 3.1.5 above) :

Corollary 3.1.6. *For every $0 < \alpha < \frac{1}{6}$, there exists $C(\alpha)$ such that for every $X > 3$, for every prime q such that $q \leq X^{\frac{2}{3}}(\log X)^{\alpha}$, for every a coprime with q, one has the inequality*

$$|E(X,q,a)| \leq C(\alpha)\frac{X(\log\log X)^{\frac{11}{6}}}{q(\log X)^{\frac{1-6\alpha}{10}}}.$$

In particular, for every constant $\epsilon > 0$, the asymptotic formula

$$\sum_{\substack{n\leq X\\ n\equiv a \pmod q}} \mu^2(n) \sim \frac{1}{\varphi(q)} \sum_{\substack{n\leq X\\ (n,q)=1}} \mu^2(n) \left(\sim \frac{6}{\pi^2}\left(1-\frac{1}{p^2}\right)^{-1}\frac{X}{q}\right)$$

holds as $X \to \infty$, uniformly for $q \leq X^{\frac{2}{3}}(\log X)^{\frac{1}{6}-\epsilon}$ and integers $(a,q) = 1$. This is the first time ocurrence of such an asymptotic formule for *prime* values of q tending to infinity faster than $X^{\frac{2}{3}}$.

Finally, We remark that Corollary 3.1.6 implies that if $n(a,q)$ denotes the least positive squarefree number that is congruent to a modulo q, then for every $\epsilon > 0$, we have the inequality

$$n(a,q) \ll_{\epsilon} q^{\frac{3}{2}}(\log q)^{-\frac{1}{6}+\epsilon},$$

where the implied constant depends only on ϵ. The best result in this direction is due to Heath-Brown [21], who proved that

$$n(a,q) \ll (d(q)\log q)^6 q^{\frac{13}{9}}.$$

3.2 Preliminary results

The next lemma is a simple consequence of Weil's bound for exponential sums that come from algebraic curves over finite fields and classical estimates for Gauss sums.

Lemma 3.2.1. *Let $A < B$ be real number, let a and q be integers satisfying $(a,q) = 1$, $q \geq 1$. Then for every $\epsilon > 0$, we have*

$$\sum_{A<r\leq B} e\left(\frac{a\bar{r}^2}{q}\right) \ll_{\epsilon} q^{\epsilon}\left(\frac{B-A}{q^{\frac{1}{2}}} + q^{\frac{1}{2}}\right)$$

where $\bar{r}$ denotes the multiplicative inverse of $r \pmod q$, $e(z) = e^{2\pi i z}$ and the implicit constant depends at most on ϵ.

3.2.1 Approximation to the ψ function

The next lemma is an useful analytic tool to avoid the problems arising from the lack of continuity of the sawtooth function. The version we use here can be found in [10], and is inspired by an idea of Vinogradov.

Lemma 3.2.2. *(see [10, Lemma 4]) Let $\psi(x) = x - \lfloor x \rfloor - \frac{1}{2}$ and $Y > 1$. There are two functions A and B with period 1 such that, for every real x, one has*

$$|\psi(x) - A(x)| \leq B(x),$$

where

$$A(x) = \sum_{h \neq 0} A_h e(hx),$$

$$B(x) = Y^{-1} + \sum_{h \neq 0} B_h e(hx),$$

with

$$A_h, B_h \ll C_h := \min\left(\frac{1}{|h|}, \frac{Y^3}{|h|^4}\right), \ (h \neq 0). \tag{3.7}$$

3.2.2 Exponential sums twisted by the Möbius function

We now state the estimates for exponential sums twisted by the Möbius functions that were mentioned in the introduction. The first one is a very particular case of [11, Theorem 1.7] by Fouvry, Kowalski and Michel, which was based on a previous work by Fouvry and Michel [13]. It gives non-trivial bounds for $R \geq q^{\frac{3}{4}+\epsilon}$ and will be used in several places of the proof of Theorem 3.1.2.

Theorem 3.A. *For every $\epsilon > 0$, there exists $C(\epsilon)$ such that, for every $R \geq 1$, for every prime q, and every a coprime with q, one has the inequality*

$$\left|\sum_{n \leq R} \mu(n) e\left(\frac{a\overline{n}^2}{q}\right)\right| \leq C(\epsilon) R \left(1 + \frac{q}{R}\right)^{\frac{1}{12}} q^{-\frac{1}{48}+\epsilon}. \tag{3.8}$$

To prove Theorem 3.1.4, we need to replace Theorem 3.A by an estimate that gives something non-trivial in the larger range $R \geq q^{\frac{1}{2}+\epsilon}$. For this we have the next result which is a combination of a remarkable result by Bourgain [3], which is non-trivial in the range $q^{\frac{1}{2}+\epsilon} \leq R \leq q$, and Theorem 3.A itself.

Theorem 3.B. *For every $\eta > 0$, there exists $\delta(\eta) > 0$ and $C(\eta)$ such that, for every $R \geq 1$, for every prime q satisfying $q^{\frac{1}{2}+\eta} \leq R \leq q^{\frac{1}{\eta}}$, and every a coprime with q, one has*

$$\left|\sum_{n \leq R} \mu(n) e\left(\frac{a\overline{n}^2}{q}\right)\right| \leq C(\eta) R^{1-\delta(\eta)}. \tag{3.9}$$

Démonstration. For $q^{\frac{1}{2}+\eta} \leq R \leq q$, this is exactly [3, Theorem A.9]. For $q < R \leq q^{\frac{1}{2\eta}}$, it follows from Theorem 3.A. □

3.2.3 Short exponential sums

In the course of the proof of Theorem 3.1.5, we are led to deal with very short exponential sums, for which we use the following result by Bourgain-Garaev. It gives non-trivial results for short Kloosterman sums $\pmod q$ where the length is as small as q^ϵ for any $\epsilon > 0$.

Theorem 3.C. *(see [5, Theorem 16]) There exists an absolute constant C such that for every $M \geq 2$, every prime q, and every a coprime with q, one has the inequality*

$$\left|\sum_{m\leq M} e\left(\frac{a\overline{m}}{q}\right)\right| \leq C\frac{M\log q(\log\log q)^3}{(\log M)^{\frac{3}{2}}},$$

The following lemma is obtained by combining Lemma 3.2.2 and Theorem 3.C above.

Lemma 3.2.3. *Let $\psi(x)$ be as in Lemma 3.2.2. Then we have the inequality*

$$\sum_{m\leq M}\psi\left(N+\frac{a\overline{m}}{q}\right) \ll \frac{M}{\log q} + \frac{M\log q(\log\log q)^4}{(\log M)^{\frac{3}{2}}}.$$

uniformly for every pair of real numbers M, N such that $M > 1$ and prime $q > 2$, where the implied constant is absolute.

Démonstration. Let $1 \leq Y \leq q$ to be chosen later. By Lemma 3.2.2, we deduce that

$$\sum_{m\leq M}\psi\left(N+\frac{a\bar{m}}{q}\right) \ll \frac{M}{Y} + M\sum_{\substack{h=-\infty\\ h\neq 0}}^{\infty} C_{hq} + \sum_{q\nmid h} C_h\left|\sum_{m\leq M} e\left(\frac{ah\bar{m}}{q}\right)\right|,$$

where C_h is as in (3.7). By Theorem 3.C and the bounds (3.7), we have that

$$\sum_{m\leq M}\psi\left(N+\frac{a\bar{m}}{q}\right) \ll \frac{M}{Y} + \frac{M\log q(\log\log q)^3}{(\log M)^{\frac{3}{2}}}\log Y,$$

since $Y \leq q$. We conclude by choosing $Y = \log q$. □

3.2.4 Selberg's Sieve

Another important input to the proof of Theorem 3.1.5 is the Selberg sieve for detecting squares (cf. [17, Chapter 8]). We shall need the following result.

Theorem 3.D. *Let $\mathcal{A} = (a_n)$ be a finite sequence of non-negative numbers. Let P be a squarefree number. For each $p \mid P$, let Ω_p be a set of congruence classes $\pmod p$. For every $d \mid P$ we write*

$$|\mathcal{A}_d| = \sum_{\substack{n \pmod d \in \Omega_p\\ \text{for every } p\mid d}} a_n = g(d)Y + r_d(\mathcal{A}), \tag{3.10}$$

where $Y > 0$ and $g(d)$ is a multiplicative function with $0 < g(p) < 1$ for $p \mid P$. Let $h(d)$ be the multiplicative function given by $h(p) = g(p)(1 - g(p))^{-1}$ and for any $D > 1$ define

$$J = J(D) := \sum_{\substack{d|P \\ d<\sqrt{D}}} h(d).$$

Then, for any $D > 1$ we have the inequality

$$\sum_{\substack{n \pmod d \notin \Omega_p \\ \text{for every } p|P}} a_n \leq YJ^{-1} + \sum_{\substack{d|P \\ d\leq\sqrt{D}}} \tau_3(d) \left|r_d(\mathcal{A})\right|,$$

where τ_3 is the generalized divisor function.

Démonstration. The proof follows exactly as that of [17, Theorem 7.1], taking into account the simple inequality

$$\sum_{\substack{n \pmod p \notin \Omega_p \\ \text{for every } p|P}} a_n \ \leq \ \sum_n a_n \Bigg(\sum_{\substack{d \\ n \,(\mathrm{mod}\ p) \in \Omega_p \\ \text{for every } p|d}} \rho_d \Bigg)^2,$$

for any real numbers ρ_d supported on $d \mid P$ with $\rho_1 = 1$. □

The optimal choice of these ρ_d is the heart of the Selberg's sieve.

3.3 Proofs of the results

3.3.1 Proof of Theorem 3.1.2

Let $X > 1$ and $\epsilon > 0$ be real numbers and let q be a prime number. Since the upper bound given by Theorem 3.1.2 is worse than (3.6) for $q \leq X^{2/5}$, we may suppose $q \leq X^{2/5}$. Let

$$S := \sum_{(r,q)=1} \mu(r) \sum_{\substack{m\leq X/r^2 \\ m\equiv a\bar{r}^2 \pmod q}} 1, \tag{3.11}$$

and

$$S_0 := \frac{1}{\varphi(q)} \sum_{\substack{n\leq X \\ (n,q)=1}} \mu^2(n), \tag{3.12}$$

We have

$$E(X, q, a) = S - S_0. \tag{3.13}$$

It is rather elementary to see that S_0 satisfies (recall that q is prime)

$$S_0 = \frac{6}{\pi^2}\left(1-\frac{1}{q^2}\right)^{-1}\frac{X}{q} + O_\epsilon(X^{\frac{1}{2}}q^{-1+\epsilon}). \tag{3.14}$$

Let $1 < R \leq X^{\frac{1}{2}}$ be a parameter to be chosen later depending on X and q. We split S as

$$S = S_I + S_{II}, \tag{3.15}$$

where

$$\begin{cases} S_I = \displaystyle\sum_{\substack{r\leq R\\(r,q)=1}} \mu(r) \sum_{\substack{m\leq X/r^2\\ m\equiv a\bar{r}^2 \pmod q}} 1, \\ S_{II} = \displaystyle\sum_{\substack{R<r\leq X^{\frac{1}{2}}\\(r,q)=1}} \mu(r) \sum_{\substack{m\leq X/r^2\\ m\equiv a\bar{r}^2 \pmod q}} 1. \end{cases} \tag{3.16}$$

For the first sum in (3.16), we have that

$$\begin{aligned} S_I &= \sum_{\substack{r\leq R\\(r,q)=1}} \mu(r)\left\{\frac{X}{qr^2} - \psi\left(\frac{X}{qr^2} - \frac{a\bar{r}^2}{q}\right) + \psi\left(-\frac{a\bar{r}^2}{q}\right)\right\} \\ &=: \mathcal{T} - \mathcal{U} + \mathcal{V}, \end{aligned} \tag{3.17}$$

say. The first term satisfies

$$\mathcal{T} = \frac{6}{\pi^2}\left(1-\frac{1}{q^2}\right)^{-1}\frac{X}{q} + O\left(R^{-1}Xq^{-1}\right). \tag{3.18}$$

Study of $\mathcal{V}$

Let $1 < Y \leq X$ be a parameter to be chosen optimally later depending on X and q, then Lemma 3.2.2 gives us two functions A and B whose Fourier coefficients satisfy (3.7), and such that

$$|\mathcal{V}| \leq \mathcal{V}_1 + \mathcal{V}_2, \tag{3.19}$$

where

$$\mathcal{V}_1 = \left|\sum_{\substack{r\leq R\\(r,q)=1}} \mu(r) A\left(-\frac{a\bar{r}^2}{q}\right)\right|, \ \mathcal{V}_2 = \sum_{\substack{r\leq R\\(r,q)=1}} B\left(-\frac{a\bar{r}^2}{q}\right).$$

Writing down the Fourier development for $A(x)$, and using (3.7), we see that

$$\mathcal{V}_1 \leq \sum_{h\neq 0} C_h \left| \sum_{\substack{r\leq R\\(r,q)=1}} \mu(r) e\left(-\frac{ah\bar{r}^2}{q}\right)\right|. \tag{3.20}$$

The contribution of the terms where $q \mid h$ is trivially seen to be

$$\ll R\sum_{h\neq 0} C_{hq} \ll_\epsilon X^\epsilon R q^{-1}, \tag{3.21}$$

by (3.7). For the remaining terms, we use Theorem 3.A and see that their contribution is

$$\ll_\epsilon X^\epsilon \left(Rq^{-\frac{1}{48}} + R^{\frac{11}{12}} q^{\frac{1}{16}}\right), \tag{3.22}$$

again by (3.7). Hence, by (3.20), (3.21) and (3.22), we have

$$\mathcal{V}_1 \ll_\epsilon X^\epsilon \left(Rq^{-\frac{1}{48}} + R^{\frac{11}{12}} q^{\frac{1}{16}}\right). \tag{3.23}$$

The analysis of $\mathcal{V}_2$ is completely analogous. The only difference is that we shall need Lemma 3.2.1 instead of Theorem 3.A. We obtain

$$\mathcal{V}_2 \ll_\epsilon X^\epsilon \left(Rq^{-\frac{1}{2}} + q^{\frac{1}{2}} + RY^{-1}\right). \tag{3.24}$$

Gathering (3.23) and (3.24) in (3.19), we have that

$$\mathcal{V} \ll_\epsilon X^\epsilon \left(Rq^{-\frac{1}{48}} + R^{\frac{11}{12}} q^{\frac{1}{16}} + q^{\frac{1}{2}} + RY^{-1}\right). \tag{3.25}$$

Study of $\mathcal{U}$

This part is very similar to the study of $\mathcal{V}$ but with the difference that we need an Abel summation to take care of the oscillation of the term X/qr^2. Let $1 < R_0 \leq (X/q)^{\frac{1}{2}}$ to be chosen optimally later. We write

$$\mathcal{U} = \mathcal{W} + O(R_0), \tag{3.26}$$

where

$$\mathcal{W} := \sum_{\substack{R_0<r\leq R\\(r,q)=1}} \mu(r)\psi\left(\frac{X}{qr^2} - \frac{a\bar{r}^2}{q}\right).$$

Again by Lemma 3.2.2, we obtain two functions A and B satisfying (3.7) and such that

$$|\mathcal{W}| \leq \mathcal{W}_1 + \mathcal{W}_2, \tag{3.27}$$

where

$$\mathcal{W}_1 = \left| \sum_{\substack{R_0<r\leq R\\(r,q)=1}} \mu(r) A\left(\frac{X}{qr^2} - \frac{a\bar{r}^2}{q}\right)\right|,\ \mathcal{W}_2 = \sum_{\substack{R_0<r\leq R\\(r,q)=1}} B\left(\frac{X}{qr^2} - \frac{a\bar{r}^2}{q}\right).$$

We write down the Fourier development of $A(x)$ and again, we separate the contribution from the terms where $q \mid h$ as we did for $\mathcal{V}_1$. We deduce

$$\mathcal{W}_1 \leq \sum_{(h,q)=1} C_h \left| \sum_{\substack{R_0<r\leq R\\(r,q)=1}} \mu(r) e\left(\frac{hX}{qr^2} - \frac{ah\bar{r}^2}{q}\right)\right| + O_\epsilon\left(X^\epsilon R q^{-1}\right). \tag{3.28}$$

Summing by parts, we see that

$$\sum_{\substack{R_0<r\leq R\\(r,q)=1}} \mu(r) e\left(\frac{hX}{qr^2} - \frac{ah\bar{r}^2}{q}\right) \ll \frac{|h|X}{q} \sum_{\substack{R_0<t\leq R\\(t,q)=1}} \frac{1}{t^3} S(t,q) + S(R,q) + S(R_0,q),$$

where

$$S(t,q) := \max_{(a,q)=1} \left| \sum_{\substack{r\leq t\\(r,q)=1}} \mu(r) e\left(\frac{a\bar{r}^2}{q}\right)\right| \tag{3.29}$$

The terms on the right-hand side of the above inequality can be estimated by means of Theorem 3.A giving

$$\sum_{\substack{R_0<r\leq R\\(r,q)=1}} \mu(r) e\left(\frac{hX}{qr^2} - \frac{ah\bar{r}^2}{q}\right) \ll_\epsilon X^\epsilon \Big(|h| R_0^{-1} X q^{-\frac{49}{48}} + |h| R_0^{-\frac{13}{12}} X q^{-\frac{15}{16}} + R q^{-\frac{1}{48}} + R^{\frac{11}{12}} q^{\frac{1}{16}} + R_0 \Big).$$

Injecting it in (3.28) and using (3.7), we deduce

$$\mathcal{W}_1 \ll_\epsilon X^\epsilon \left(R_0^{-1} XY q^{-\frac{49}{48}} + R_0^{-\frac{13}{12}} XY q^{-\frac{15}{16}} + R q^{-\frac{1}{48}} + R^{\frac{11}{12}} q^{\frac{1}{16}} + R_0 \right). \tag{3.30}$$

The treatment of $\mathcal{W}_2$ goes in a similar fashion, replacing Theorem 3.A by Lemma 3.2.1 in the appropriate places. We end up with

$$\mathcal{W}_2 \ll_\epsilon X^\epsilon \left(R_0^{-1} XY q^{-\frac{3}{2}} + R_0^{-2} XY q^{-\frac{1}{2}} + R q^{-\frac{1}{2}} + q^{\frac{1}{2}} + RY^{-1} + R_0 \right). \tag{3.31}$$

Gathering (3.30) and (3.31) in (3.27), we have that

$$\mathcal{W} \ll_\epsilon X^\epsilon \Big(R_0^{-1} XY q^{-\frac{49}{48}} + R_0^{-\frac{13}{12}} XY q^{-\frac{15}{16}} + Rq^{-\frac{1}{48}} + R^{\frac{11}{12}} q^{\frac{1}{16}} + R_0^{-2} XY q^{-\frac{1}{2}} + q^{\frac{1}{2}} + RY^{-1} + R_0 \Big). \quad (3.32)$$

Putting together (3.17), (3.18), (3.25), (3.26) and (3.32), we see that

$$S_I = \frac{6}{\pi^2} \left(1 - \frac{1}{q^2}\right) \frac{X}{q} + O_\epsilon \Big(X^\epsilon \Big(R^{-1} X q^{-1} + Rq^{-\frac{1}{48}} + R^{\frac{11}{12}} q^{\frac{1}{16}} + q^{\frac{1}{2}} + RY^{-1} + R_0^{-1} XY q^{-\frac{49}{48}} + R_0^{-\frac{13}{12}} XY q^{-\frac{15}{16}} + R_0^{-2} XY q^{-\frac{1}{2}} + R_0 \Big) \Big). \quad (3.33)$$

Study of S_{II}

We procceed now to estimate S_{II}. We follow the lines of [23, Lemma 2]. Ignoring the oscillation of μ, we see that

$$\begin{aligned} S_{II} &\ll \sum_{R < r \leq \sqrt{X}} \sum_{\substack{m \leq \frac{X}{r^2} \\ r^2 m \equiv a \pmod q}} \log \left(3\sqrt{\frac{X}{r^2 m}} \right) \\ &= \sum_{R < r \leq \sqrt{X}} \sum_{\substack{m \leq \frac{X}{r^2} \\ r^2 m \equiv a \pmod q}} \int_r^{3\sqrt{\frac{X}{m}}} \frac{dt}{t} \\ &\ll \int_R^{3\sqrt{X}} \sum_{m \leq \frac{9X}{t^2}} \sum_{\substack{r \leq t \\ r^2 m \equiv a \pmod q}} 1 \frac{dt}{t}. \end{aligned} \quad (3.34)$$

We put

$$Z = \max(R, q) \quad (3.35)$$

and break up the integral on the right-hand-side from (3.34) as

$$\int_R^Z \sum_{m \leq \frac{9X}{t^2}} \sum_{\substack{r \leq t \\ r^2 m \equiv a \pmod q}} 1 \frac{dt}{t} + \int_Z^{3\sqrt{X}} \sum_{m \leq \frac{9X}{t^2}} \sum_{\substack{r \leq t \\ r^2 m \equiv a \pmod q}} 1 \frac{dt}{t}$$

For the first integral, we use additive characters to detect the congruence condition. We have

$$\sum_{m \leq \frac{9X}{t^2}} \sum_{\substack{r \leq t \\ r^2 m \equiv a \pmod q}} 1 = \frac{1}{q^2} \sum_{\alpha=0}^{q-1} \sum_{\beta=0}^{q-1} \mathcal{S}(q; \alpha, a\beta) \Theta(t, \alpha) \Theta\left(\frac{9X}{t^2}, \beta \right), \quad (3.36)$$

where

$$\mathcal{S}(q;\alpha,\beta) := \sum_{h=1}^{q-1} e\left(\frac{\alpha h + \beta \bar{h}^2}{q}\right),$$

and

$$\Theta(t,\alpha) := \sum_{n\leq t} e\left(-\frac{\alpha n}{q}\right) \ll \min\left(t, \left\|\frac{\alpha}{q}\right\|^{-1}\right). \tag{3.37}$$

In order to estimate the sum on the right-hand side of (3.36), we need bounds for $S(q;\alpha,\beta)$. In the cases where $\alpha\beta \equiv 0 \pmod q$, the sum is either trivial, a Ramanujan sum or a Gauss sum. And the classical upper-bound for these sums are used. If both α and β are $\not\equiv 0 \pmod q$, then we shall use the following upper-bound that follows from the work of Weil

$$S(q;\alpha,\beta) \ll q^{\frac{1}{2}},\ (\alpha,\beta \not\equiv 0 \,(\mathrm{mod}\ q)).$$

Combining these bounds with (3.37), we see that

$$\begin{aligned}\sum_{m\leq \frac{9X}{t^2}} \sum_{\substack{r\leq t\\ r^2m\equiv a \pmod q}} 1 &\ll \left(\frac{X}{qt} + \frac{t}{q^{\frac{3}{2}}}\sum_{\beta=1}^{q-1}\left\|\frac{\beta}{q}\right\|^{-1} + \frac{X}{q^3t}\sum_{\alpha=1}^{q-1}\left\|\frac{\alpha}{q}\right\|^{-1} + \frac{1}{q^{\frac{3}{2}}}\sum_{\alpha=1}^{q-1}\sum_{\beta=1}^{q-1}\left\|\frac{\alpha}{q}\right\|^{-1}\left\|\frac{\beta}{q}\right\|^{-1}\right)\\ &\ll_\epsilon X^\epsilon\left(\frac{X}{qt} + \frac{t}{q^{1/2}} + q^{1/2}\right)\end{aligned} \tag{3.38}$$

Notice that if $Z = R$, this first integral vanishes. So we can suppose $Z = q$. With that in mind, if we integrate both sides of inequality (3.38) against $\dfrac{dt}{t}$, we obtain

$$\int_R^Z \sum_{m\leq \frac{9X}{t^2}} \sum_{\substack{r\leq t\\ r^2m\equiv a \pmod q}} 1\frac{dt}{t} \ll_\epsilon X^\epsilon\left(\frac{X}{Rq} + q^{1/2}\right). \tag{3.39}$$

For the remaining integral, we notice that for fixed m, the equation $r^2m \equiv a \,(\mathrm{mod}\ q)$ has at most two solutions for $r \pmod q$ (recall that q is prime). Thus, we have (since $Z \geq q$)

$$\int_Z^{3\sqrt{X}} \sum_{m\leq \frac{9X}{t^2}} \sum_{\substack{r\leq t\\ r^2m\equiv a \pmod q}} 1\frac{dt}{t} \ll \frac{X}{Zq} \leq \frac{X}{Rq}. \tag{3.40}$$

Adding up (3.39) and (3.40), we have, in view of (3.34), that

$$S_{II} \ll_\epsilon X^\epsilon\left(R^{-1}Xq^{-1} + q^{1/2}\right). \tag{3.41}$$

Adding together (3.15), (3.33) and (3.41), we have

$$S - \frac{6}{\pi^2}\left(1-\frac{1}{q^2}\right)^{-1}\frac{X}{q} \ll_\epsilon X^\epsilon \Big(R^{-1}Xq^{-1} + Rq^{-\frac{1}{48}} + R^{\frac{11}{12}}q^{\frac{1}{16}} + q^{\frac{1}{2}} + RY^{-1} + R_0^{-1}XYq^{-\frac{49}{48}} + R_0^{-\frac{13}{12}}XYq^{-\frac{15}{16}} + R_0^{-2}XYq^{-\frac{1}{2}} + R_0\Big). \quad (3.42)$$

Forcing the first, the fifth and the last terms to be equal, we are faced with the choices

$$R = \left(\frac{X}{q}\right)^{\frac{1}{2}} Y^{\frac{1}{2}},\ R_0 = \left(\frac{X}{q}\right)^{\frac{1}{2}} Y^{-\frac{1}{2}}.$$

Injecting these values in (3.42), we see that

$$S - \frac{6}{\pi^2}\left(1-\frac{1}{q^2}\right)^{-1}\frac{X}{q} \ll_\epsilon X^\epsilon \left(\left(\frac{X}{q}\right)^{\frac{1}{2}} Y^{-\frac{1}{2}} + \left(\frac{X}{q}\right)^{\frac{1}{2}} Y^{\frac{3}{2}}q^{-\frac{1}{48}} + \left(\frac{X}{q}\right)^{\frac{11}{24}} Y^{\frac{37}{24}}q^{\frac{1}{16}} + Y^2 q^{\frac{1}{2}}\right). \quad (3.43)$$

Take $Y = \min\left(q^{\frac{1}{96}}, X^{\frac{1}{49}}q^{-\frac{5}{98}}, X^{\frac{1}{5}}q^{-\frac{2}{5}}\right)$ to optimize the right-hand side of (3.43). Then (3.13), (3.14) and (3.43) imply that we have

$$E(X,q,a) \ll_\epsilon X^\epsilon \left(\left(\frac{X}{q}\right)^{\frac{1}{2}} q^{-\frac{1}{192}} + \left(\frac{X}{q}\right)^{\frac{24}{49}} q^{\frac{3}{196}} + \left(\frac{X}{q}\right)^{\frac{2}{5}} q^{\frac{1}{10}}\right),$$

and the last term is dominated by the first in the range $q \leq X^{\frac{2}{5}}$. Hence we conclude the proof of Theorem 3.1.2.

3.3.2 Proof of Theorem 3.1.4

Let $X > 1$ and $\eta > 0$ be real numbers and let q be a prime number such that $X^\eta \leq q \leq X^{\frac{1}{2}-\eta}$. We let again S and S_0 be as in the previous section (see (3.11) and (3.12)). Notice that we have

$$\left(\frac{X}{q}\right)^{\frac{1}{2}} \geq q^{\frac{1}{2}+\eta}.$$

Let $\delta_1 > 0$ to be chosen later depending on η. Also let

$$R = \left(\frac{X}{q}\right)^{\frac{1}{2}+\delta_1},\ R_0 = \left(\frac{X}{q}\right)^{\frac{1}{2}-\delta_1},\ Y = \left(\frac{X}{q}\right)^{2\delta_1}. \quad (3.44)$$

Notice that we can choose δ_1 sufficiently small so that

$$R_0 \geq q^{\frac{1}{2}+\frac{\eta}{2}}.$$

Theorem 3.B now gives us a certain $\delta_2 > 0$ depending on η such that

$$S(t,q) \leq t^{1-\delta_2},\ (t \geq R_0), \tag{3.45}$$

where $S(t,q)$ is as in (3.29). We start as in the last section, writing

$$S = S_I + S_{II}, \tag{3.46}$$

where S_I and S_{II} are as in (3.16). We deal S_I in the exact same way as before, only replacing each use of Theorem 3.A by the upper bound (3.45). Thus we obtain

$$S_I = \frac{6}{\pi^2}\left(1-\frac{1}{q^2}\right)\frac{X}{q} + O_{\epsilon,\eta}\left(X^{\epsilon}\left(R^{-1}Xq^{-1} + R^{1-\delta_2} + RY^{-1} + R_0^{-1-\delta_2}XYq^{-1} \right.\right. \\ \left.\left. + R_0^{-1}XYq^{-\frac{3}{2}} + R_0^{-2}XYq^{-\frac{1}{2}} + R_0\right)\right), \tag{3.47}$$

for any $\epsilon > 0$ (compare with (3.33)).

As for S_{II}, we have the exactly same bound as in the previous case (see (3.41)). Gathering (3.41), (3.47) and (3.46), we see that

$$S - \frac{6}{\pi^2}\left(1-\frac{1}{q^2}\right)\frac{X}{q} \ll_{\epsilon,\eta} X^{\epsilon}\left(R^{-1}Xq^{-1} + R^{1-\delta_2} + RY^{-1} + R_0^{-1-\delta_2}XYq^{-1} \right. \\ \left. + R_0^{-1}XYq^{-\frac{3}{2}} + R_0^{-2}XYq^{-\frac{1}{2}} + R_0\right).$$

Now, we deduce from (3.13), (3.14) and (3.44) the inequality (recall that $X^{\eta} \leq q \leq X^{\frac{1}{2}-\eta}$)

$$E(X,q,a) \ll_{\epsilon,\eta} X^{\epsilon}\left(\left(\frac{X}{q}\right)^{\frac{1}{2}-\delta_1} + \left(\frac{X}{q}\right)^{\frac{1}{2}+3\delta_1-\frac{\delta_2}{2}+\delta_1\delta_2} + \left(\frac{X}{q}\right)^{\frac{1}{2}+3\delta_1-\frac{\eta}{2}} + \left(\frac{X}{q}\right)^{\frac{1}{2}+4\delta_1-2\eta}\right).$$

Notice that since $q \leq X^{1/2}$, one has $X^{\epsilon} \leq (X/q)^{2\epsilon}$. Now, taking $\epsilon < \delta_1/4$ and δ sufficiently small, we deduce

$$E(X,q,a) \ll_{\eta} \left(\frac{X}{q}\right)^{\frac{1}{2}-\frac{\delta_1}{2}}.$$

Taking $\delta := \delta_1/2$ concludes the proof of Theorem 3.1.4.

3.3.3 Proof of Theorem 3.1.5

Let $X > 1$ and let q be a prime number such that $q \leq X$. Since the upper bound from Theorem 3.1.5 is worse than (3.6) for $q \leq X^{\frac{1}{2}}$, we can suppose that $q \geq X^{\frac{1}{2}}$. Let S and S_0 be as in (3.11) and (3.12), respectively, and $1 < R \leq X^{\frac{1}{3}}$ be a parameter to be chosen optimally later. We split S as before, writing

$$S = S_I + S_{II}, \tag{3.48}$$

where S_I and S_{II} are as in (3.16). For S_I, it suffices to detect the congruence trivially. We have

$$S_I = \sum_{\substack{r \leq R \\ (r,q)=1}} \mu(r) \left(\frac{X}{qr^2} + O(1) \right) = \frac{6}{\pi^2} \prod_{p \mid q} \left(1 - \frac{1}{p^2} \right)^{-1} \frac{X}{q} + O(R + R^{-1} X q^{-1}). \tag{3.49}$$

For S_{II}, by estimating the μ function trivially and changing the order of summation, we have that

$$\begin{aligned} |S_{II}| &\leq \sum_{m \leq X/R^2} \sum_{\substack{r \leq (X/m)^{1/2} \\ r^2 m \equiv a \pmod q}} 1 \\ &= S_{III} + S_{IV}, \end{aligned} \tag{3.50}$$

where

$$\begin{cases} S_{III} = \displaystyle\sum_{m \leq \frac{X}{R^2 (\log X)}} \sum_{\substack{r \leq (X/m)^{1/2} \\ r^2 m \equiv a \pmod q}} 1, \\ S_{IV} = \displaystyle\sum_{\frac{X}{R^2 (\log X)} < m \leq \frac{X}{R^2}} \sum_{\substack{r \leq (X/m)^{1/2} \\ r^2 m \equiv a \pmod q}} 1. \end{cases} \tag{3.51}$$

For S_{III}, we detect the congruence trivially, obtaining

$$\begin{aligned} S_{III} &= \sum_{m \leq \frac{X}{R^2 (\log X)}} \left(\frac{X^{\frac{1}{2}}}{m^{\frac{1}{2}} q} + O(1) \right) \\ &\ll \frac{X}{Rq (\log X)^{\frac{1}{2}}} + \frac{X}{R^2 (\log X)}. \end{aligned} \tag{3.52}$$

As for S_{IV}, we proceed by dyadic decomposition of the values of m. Doing so, we find that there exists $M \geq 1$, a power of two, such that

$$\frac{X}{2R^2(\log X)} < M \leq \frac{2X}{R^2}, \tag{3.53}$$

and

$$S_{IV} \ll \mathfrak{S} \log\log X, \tag{3.54}$$

where $\mathfrak{S} = \mathfrak{S}(X, M; q, a)$ is given by

$$\mathfrak{S} := \sum_{M<m\leq 2M} \sum_{\substack{r\leq (X/M)^{1/2} \\ r^2 m \equiv a \pmod q}} 1. \tag{3.55}$$

In what follows, we show how to use the Selberg's sieve (see Theorem 3.D) to estimate $\mathfrak{S}$.

Implementing the Selberg's sieve

Let

$$a_n = \sum_{\substack{M<m\leq 2M \\ mn \equiv a \pmod q}} 1, \text{ if } n \leq \frac{X}{M}, \tag{3.56}$$

and $a_n = 0$, otherwise. Then

$$\mathfrak{S} = \sum_{n=\square} a_n,$$

where the condition $n = \square$ means that we only sum over the n that are perfect squares.

Let P be a product of distinct odd primes such that $p \nmid q$. For each $p \mid P$, let Ω_p denote the set of non-square residue classes (mod p). Note that we can soften the condition $n = \square$ to $n \notin \Omega_p$ for every $p \mid P$. In other words, the following inequality holds :

$$\mathfrak{S} \leq \sum_{\substack{n\notin\Omega_p \\ \text{for every } p|P}} a_n.$$

We want to use Theorem 3.D. Thus, we need to give asymptotic formulas for $|\mathcal{A}_d|$ (see (3.10)). We notice that with a_n as in (3.56), we have

$$|\mathcal{A}_d| = \sum_{\substack{\alpha \pmod d \\ \alpha \pmod p \in \Omega_p \\ \text{for every } p|d}} \mathcal{G}(d, \alpha), \tag{3.57}$$

where

$$\mathcal{G}(d,\alpha) := \sum_{n\equiv\alpha \pmod d} a_n. \tag{3.58}$$

We use the ψ function to evaluate $\mathcal{G}(d,\alpha)$. Injecting (3.56) in (3.58) and interchanging the order of summation, gives

$$\mathcal{G}(d,\alpha) = \sum_{M<m\leq 2M}\left(\frac{X}{Mdq} - \psi\left(\frac{X}{Mdq} - \frac{a\overline{dm}}{q} - \frac{\alpha\overline{q}}{d}\right) + \psi\left(-\frac{a\overline{dm}}{q} - \frac{\alpha\overline{q}}{d}\right)\right),$$

for every d coprime with q and $\alpha \pmod d$. By Lemma 3.2.3, we obtain that

$$\mathcal{G}(d,\alpha) = \frac{X}{dq} + O\left(\frac{M\log q(\log\log q)^4}{(\log M)^{\frac{1}{2}}}\right). \tag{3.59}$$

Note that the inequality (3.53) implies

$$M \geq X^{\frac{1}{3}}(\log X)^{-1}.$$

Hence, (3.57) and (3.59) imply

$$|\mathcal{A}_d| = g(d)\frac{X}{q} + O\left(g(d)d\frac{M(\log\log X)^4}{(\log X)^{\frac{1}{2}}}\right), \tag{3.60}$$

where $g(d)$ is the multiplicative function supported on squarefree numbers and such that

$$g(p) = \frac{p-1}{2p}.$$

Let $D > 1$ and

$$P := \prod_{\substack{2<p\leq\sqrt{D}\\ p\nmid q}} p.$$

We use Theorem 3.D for $Y = \frac{X}{q}$ and D and P as above. We obtain, in view of (3.60), the inequality

$$\mathfrak{S} \leq \sum_{\substack{n\notin\Omega_p\\ \text{for every } p|P}} a_n \ll \frac{X}{q}J^{-1} + \frac{M(\log\log X)^4}{(\log X)^{\frac{1}{2}}}\sum_{d\leq\sqrt{D}}\tau_3(d)g(d)d,$$

where (recall that q is prime)

$$J = \sum_{\substack{d<\sqrt{D}\\ d|P}} h(d) \gg \sqrt{D}.$$

Thus

$$\mathfrak{S} \ll \frac{X}{q\sqrt{D}} + \frac{DM(\log D)^{\frac{1}{2}}(\log\log X)^4}{(\log X)^{\frac{1}{2}}}. \tag{3.61}$$

Gathering (3.53), (3.54) and (3.61), we see that

$$S_{IV} \ll \frac{X\log\log X}{D^{\frac{1}{2}}q} + \frac{DX(\log D)^{\frac{1}{2}}(\log\log X)^5}{R^2(\log X)^{\frac{1}{2}}}.$$

For each $0 < \gamma < \frac{1}{2}$, the choice $D = (\log X)^\gamma$ gives the inequality

$$S_{IV} \ll \frac{X\log\log X}{q(\log X)^{\frac{\gamma}{2}}} + \frac{X(\log\log X)^{\frac{11}{2}}}{R^2(\log X)^{\frac{1}{2}-\gamma}}. \tag{3.62}$$

Putting together (3.48), (3.49), (3.50), (3.52) and (3.62), we obtain

$$S - \frac{6}{\pi^2}\left(1-\frac{1}{q^2}\right)^{-1}\frac{X}{q} \ll R + R^{-1}Xq^{-1} + \frac{X\log\log X}{q(\log X)^{\frac{\gamma}{2}}} + \frac{X(\log\log X)^{\frac{11}{2}}}{R^2(\log X)^{\frac{1}{2}-\gamma}}. \tag{3.63}$$

Forcing the first and last terms to be equal, we are faced with the choice

$$R = X^{\frac{1}{3}}(\log X)^{-\frac{1}{6}+\frac{\gamma}{3}}(\log\log X)^{\frac{11}{6}}.$$

Replacing it in (3.63) gives the inequality

$$S - \frac{6}{\pi^2}\left(1-\frac{1}{q^2}\right)^{-1}\frac{X}{q} \ll \frac{X^{\frac{1}{3}}(\log\log X)^{\frac{11}{6}}}{(\log X)^{\frac{1}{6}-\frac{\gamma}{3}}} + \frac{X\log\log X}{q(\log X)^{\frac{\gamma}{2}}}. \tag{3.64}$$

Theorem 3.1.5 now follows by combining (3.13), (3.14) and (3.64).

Chapitre 4

On a result of R. R. Hall on squarefree numbers in short intervals

4.1 Introduction

Let μ denote, as usual, the Möbius function, so that μ^2 is the arithmetic function which detects the squarefree numbers. The sequence of squarefree numbers has a natural density of $\frac{6}{\pi^2}$. Indeed, one has the classical asymptotic formula with a power saving error term

$$\sum_{n\leq X}\mu^2(n) = \frac{6}{\pi^2}X + O(\sqrt{X}), \text{ uniformly for } X > 1.$$

Under the Riemann hypothesis, the formula would hold with an even smaller error term. The best conditional estimate for the error term was obtained by Jia [24], who proves that we can replace $O(\sqrt{X})$ by $O_\epsilon(X^{17/54+\epsilon})$, for every $\epsilon > 0$.

4.1.1 Short intervals

If we switch to the question of squarefree numbers lying in short intervals, much less is known. The question was addressed by Hall in [19], where he studied the following counting function

$$N(n,k) := \sum_{0\leq h<k}\mu^2(n+h),$$

for n and k positive integers. In view of the density of squarefree numbers, we may hope that we have

$$N(n,k) \sim \frac{6}{\pi^2}k$$

as n and k tend to infinity, with a large uniformity on k and n. Thus it is natural to define the discrepancy

$$D(n,k) := N(n,k) - \frac{6}{\pi^2}k.$$

Hall's main goal was to give an estimate, for $X > 0$, of the following (upper) density

$$d_k(X) = \limsup_{x\to\infty} \frac{1}{x}\#\big\{n \le x; |D(n,k)| > X\big\} \ \ (\ell \ge 1).$$

In order to establish his result, he considered the moments

$$\mathfrak{M}(x,k;\ell) := \sum_{0<n\le x} D(n,k)^\ell. \tag{4.1}$$

Expanding $D(n,k)^\ell$, he was immediately led to consider the sum

$$S(x;\mathbf{h}) := \sum_{n\le x} \mu^2(n+h_1)\dots\mu^2(n+h_\ell), \tag{4.2}$$

where $\mathbf{h} = (h_1,\dots,h_\ell)$ is a fixed $\ell-$tuple of nonnegative integers. He recovers the asymptotics (see also [29])

$$S(x;\mathbf{h}) \sim A(\mathbf{h})\, x, \qquad \text{as } x\to\infty, \tag{4.3}$$

where

$$A(\mathbf{h}) = \prod_p \left(1 - \frac{u_p(\mathbf{h})}{p^2}\right), \tag{4.4}$$

and

$$u_p(\mathbf{h}) = \#\big\{h_1,\dots,h_\ell \pmod{p^2}\big\}, \tag{4.5}$$

i.e. $u_p(\mathbf{h})$ counts the number of distinct residue classes $\pmod q$ covered by $h_1,\dots,h_\ell$. Each factor on the right side of (4.4) is the probability of the event

$$p^2 \nmid n+h_1,\dots,p^2 \nmid n+h_\ell,$$

and (4.3) states that these events are (asymptotically) independent. From the definition (4.1) and the asymptotic formula (4.3), Hall deduces the asymptotic formula (for fixed integers k and $\ell \ge 1$) :

$$\mathfrak{M}(x,k;\ell) \sim \mathfrak{C}_\ell(k)x, \qquad \text{as } x\to\infty, \tag{4.6}$$

where

$$\mathfrak{C}_\ell(k) := \sum_{j=0}^{\ell} \binom{\ell}{j} \left(-\frac{6}{\pi^2}k\right)^{\ell-j} \mathfrak{B}_j(k), \tag{4.7}$$

with

$$\mathfrak{B}_0(k) := 1,$$

and, for $j \ge 1$,

$$\mathfrak{B}_j(k) := \sum_{h_1=0}^{k-1} \dots \sum_{h_j=0}^{k-1} A(\mathbf{h}). \tag{4.8}$$

Since $|A(\mathbf{h})| \leq 1$, the trivial bound is

$$\mathfrak{C}_\ell(k) \ll_\ell k^\ell, \text{ uniformly for } k \geq 1, \tag{4.9}$$

which is certainly far from the true order of magnitude since one expects cancellations due to the sign changes in formula (4.7). Among other results, Hall proved (see [18] and [19]) the following improvements on the trivial bound (4.9)

$$\mathfrak{C}_2(k) = Ck^{1/2} + O_\epsilon(k^{1/3+\epsilon}), \tag{4.10}$$

for every $\epsilon > 0$, as $k \to \infty$, where

$$C = \frac{\zeta\left(\frac{3}{2}\right)}{\pi\zeta(2)} \prod_p \left(\frac{p^3 - 3p + 2}{p^3}\right) = 0,167\ldots; \tag{4.11}$$

and, for each $\ell \geq 3$,

$$\mathfrak{C}_\ell(k) \ll_\ell k^{(\ell-1)/2}, \tag{4.12}$$

uniformly for $k \geq 1$. This has obvious consequences to the moments $\mathfrak{M}_\ell(x,k)$, or even to the general absolute moments

$$\mathfrak{M}^+(x,k;\lambda) := \sum_{0<n\leq x} |D(n,k)|^\lambda, \tag{4.13}$$

where λ is a positive real number. Indeed, the upper bound (4.12), the asymptotic formula (4.6) and Hölder's inequality imply

$$\liminf_{x\to\infty} \frac{1}{x}\mathfrak{M}^+(x,k;\lambda) \gg_\lambda \begin{cases} k^{\lambda/4}, & \lambda \geq 2, \\ k^{(\lambda-1)/2}, & 1 \leq \lambda < 2. \end{cases}$$

and

$$\limsup_{x\to\infty} \frac{1}{x}\mathfrak{M}^+(x,k;\lambda) \ll_\lambda \begin{cases} k^{(\lambda-1)/2}, & \lambda \geq 2, \\ k^{\lambda/4}, & 1 \leq \lambda < 2. \end{cases}$$

Inspired by the results from Chapter 1, we are able to improve (4.12) following a somewhat involved but rather elementary method. We now state our results

Theorem 4.1.1. *For each integer $\ell \geq 3$, we let*

$$\theta_\ell := \begin{cases} \dfrac{\ell^2}{3\ell+2}, \text{ for } \ell = 3,4 \\ \\ \dfrac{\ell-2}{2}, \text{ for } \ell \geq 5, \end{cases} \tag{4.14}$$

and let $\mathfrak{C}_\ell(k)$ be defined by (4.7). Then for every $\epsilon > 0$ and every $\ell \geq 3$ there exists $C_{\epsilon,\ell} > 0$ such that for every $k \geq 1$, we have

$$|\mathfrak{C}_\ell(k)| \leq C_{\epsilon,\ell} k^{\theta_\ell+\epsilon}. \tag{4.15}$$

As a direct consequence of Theorem 4.1.1 and Theorem 4.6.1 (cf. Section 4.6 below), which is an effective version of (4.3), we have the following.

Corollary 4.1.2. *Let $\mathfrak{M}(x,k;\ell)$ be defined as in (4.1). Let θ_ℓ be as in (4.14). For every $\epsilon>0$ and every $\ell\geq 3$ there exists $D_{\epsilon,\ell}>0$ such that for every $1\leq k\leq x$, we have*

$$|\mathfrak{M}(x,k;\ell)|\leq D_{\epsilon,\ell}\left(k^{\theta_\ell+\epsilon}x+k^\ell x^{\frac{\ell}{\ell+1}+\epsilon}\right), \tag{4.16}$$

In particular, for every $\epsilon>0$, for every $\ell\geq 3$, for every $1\leq k\leq x^{\delta_\ell-\epsilon}$, we have the inequality

$$|\mathfrak{M}(x,k;\ell)|\leq 2D_{\epsilon,\ell}k^{\theta_\ell+\epsilon}x,$$

where

$$\delta_\ell:=\frac{1}{(\ell+1)(\ell-\theta_\ell)}. \tag{4.17}$$

As in [19], we can also give estimates for the absolute moments $\mathfrak{M}^+$ (see (4.13)). Indeed we have

Corollary 4.1.3. *For every $\epsilon,\lambda>0$, there exists $c^+_{\epsilon,\lambda}>0$ such that for every positive integer k, we have the inequality*

$$\liminf_{x\to\infty}\frac{1}{x}\mathfrak{M}^+(x,k;\lambda)\geq c^+_{\epsilon,\lambda}k^{\alpha_\lambda-\epsilon},$$

where

$$\alpha_\lambda=\begin{cases}\frac{\lambda}{4}, & \lambda\geq 2,\\ \frac{9\lambda-4}{28}, & 0<\lambda<2.\end{cases}$$

Similarly, for every $\epsilon,\lambda>0$, there exists $C^+_{\epsilon,\lambda}>0$ such that for every positive integer k, we have the upper bounds

$$\limsup_{x\to\infty}\frac{1}{x}\mathfrak{M}^+(x,k;\lambda)\leq C^+_{\epsilon,\lambda}k^{\beta_\lambda+\epsilon},$$

where

$$\beta_\lambda=\begin{cases}\frac{\lambda-2}{2}, & \lambda\geq 6,\\ \frac{3\lambda-4}{7}, & 4\leq\lambda<6.\\ \frac{9\lambda-4}{28}, & 2\leq\lambda<4.\\ \frac{\lambda}{4}, & 0<\lambda<2.\end{cases}$$

Démonstration. Suppose $0<\lambda\leq 2$. By Hölder's inequality, we have both

$$\mathfrak{M}(x,k;2)\leq\mathfrak{M}^+(x,k;\lambda)^{\frac{2}{4-\lambda}}\mathfrak{M}(x,k;4)^{\frac{2-\lambda}{4-\lambda}},$$

and

$$\mathfrak{M}^+(x,k;\lambda)\leq x^{\frac{2-\lambda}{2}}\mathfrak{M}(x,k;2)^{\frac{\lambda}{2}}$$

The bounds from Corollary 4.1.3 are now a consequence of the asymptotic formula for $\mathfrak{M}(x,k;2)$ (see (4.6), (4.10)) and the upper bound for $\mathfrak{M}_4(x,k)$ (see Corollary 4.1.2). The other cases follow similarly. □

We could give more precise, but at the same time, more cumbersome statements by avoiding taking limits. In the next corollary we do it for the special case $\lambda=1$.

Corollary 4.1.4. *For every $\epsilon > 0$, the inequalities*

$$k^{\frac{5}{28}-\epsilon}x \ll_\epsilon \mathfrak{M}^+(x,k;1) \ll k^{\frac{1}{4}}x,$$

hold uniformly for $1 \leq k \leq x^{\frac{1}{20}+\epsilon}$

This improves on the similar bound from [19], where $\frac{5}{28} - \epsilon$ is replaced by 0.

4.1.2 Arithmetic progressions

The distribution of arithmetic sequences in short intervals shares many similarities with the distribution of these sequences in arithmetic progressions. The deepest example concerns the sequence of primes. In the following we introduce the basic elements to the study of squarefree numbers in arithmetic progressions, trying to emphasize as much as possible the origin of this duality, at least in the current case.

Let $X > 1$ and let q be a positive integer. It is easy to prove that the number of squarefree numbers $\leq X$ which are coprime with q is asymptotically equivalent to

$$\frac{6}{\pi^2}\prod_{p|q}\left(1-\frac{1}{p^2}\right)^{-1}\frac{\varphi(q)}{q}X.$$

The question of whether these numbers are well distributed among the arithmetic progressions (mod q) amounts to study the following error terms. Let a be an integer such that $(a,q)=1$. Then we define the error term $E(X,q,a)$ by the following equation

$$\sum_{\substack{n\leq X\\ n\equiv a \,(\mathrm{mod}\ q)}}\mu^2(n) = \frac{6}{\pi^2}\prod_{p|q}\left(1-\frac{1}{p^2}\right)^{-1}\frac{X}{q} + E(X,q,a).$$

It is clear that $E(X,q,a)$ satisfies

$$\left|E(X,q,a)\right| \leq \frac{X}{q}+1. \tag{4.18}$$

We are interested in finding regions for X and q in which

$$E(X,q,a) = o\left(X/q\right). \tag{4.19}$$

In Chapter 4, we proved that for every $\epsilon > 0$, (4.19) holds true as $X \to \infty$, for arbitrary $q \leq X^{\frac{2}{3}}(\log X)^{\frac{1}{6}-\epsilon}$ and $(a,q)=1$, thus breaking the barrier of $X^{\frac{2}{3}}$ from the results of Prachar [34] and Hooley [23]. We only recall the result of Hooley [23], who showed

$$E(X,q,a) = O_\epsilon\left(\left(\frac{X}{q}\right)^{1/2} + q^{1/2+\epsilon}\right), \tag{4.20}$$

for $\epsilon > 0$ arbitrary, where the O_ϵ-constant depends on ϵ alone. We believe that (4.19) should hold as $X \to \infty$ for arbitrary $q \leq X^{1-\epsilon}$ and $(a,q)=1$. In the region $q \leq X^{1/2-\epsilon}$, formula

(4.20) gives square root cancellation relative to the main term. Montgomery conjectured (see [7, top of the page 145]) that something even stronger should hold :

$$E(X,q,a) = O_\epsilon\left((X/q)^{\frac{1}{4}+\epsilon}\right),\ \epsilon > 0 \text{ arbitrary} \tag{4.21}$$

uniformly for $(a,q)=1$, $X^{\theta_1} < q < X^{\theta_2}$ where the values of the constants θ_1 and θ_2 were not made precise. In Chapter 4, we make progress towards (4.21) by proving that for every $\epsilon > 0$ there exists $\delta = \delta(\epsilon) > 0$ such that for every $X^\epsilon \leq q \leq X^{\frac{1}{2}-\epsilon}$, we have

$$E(X,q,a) = O_\epsilon\left(\left(\frac{X}{q}\right)^{\frac{1}{2}-\delta}\right).$$

We define the ℓ-th moment for this distribution as

$$\mathcal{M}(X,q;\ell) = \sideset{}{^*}\sum_{a \pmod q} E(X,q,a)^\ell, \tag{4.22}$$

where the $*$ symbol means that we only sum over the classes that are relatively prime to q. Inspired by Montgomery's conjecture (cf. (4.21)), we make the following related conjecture for the moments :

Conjecture 4.1.5. *For every integer $\ell \geq 1$ and every $\epsilon > 0$, there exists $\delta_\ell > 0$, $\eta_\ell > 0$ and a positive multiplicative function c_ℓ such that*

$$\left|\mathcal{M}(X,q;\ell) - c_\ell(q)\varphi(q)\left(\frac{X}{q}\right)^{\frac{\ell}{4}}\right| \leq \varphi(q)\left(\frac{X}{q}\right)^{\frac{\ell}{4}-\eta_\ell}, \tag{4.23}$$

for every q and X satisfying

$$X^{1-\delta_\ell} \leq q \leq X^{1-\epsilon},\ X \geq 2.$$

Furthermore

— *if ℓ is even, c_ℓ is a bounded function,*

— *if ℓ is odd, $c_\ell(q) = 0$ for every integer q.*

For simplicity of notation in subsequent formulas, we define

$$A_q = \frac{6}{\pi^2}\prod_{p\mid q}\left(1-\frac{1}{p^2}\right)^{-1}. \tag{4.24}$$

In an analogous way to the case of short intervals, the study of $\mathcal{M}(X,q;\ell)$ depends highly on the behavior of $\mathfrak{C}_\ell\left(\frac{X}{q};q\right)$, where $\mathfrak{C}_\ell(.,.)$ is the following analogue of $\mathfrak{C}_\ell(k)$. For positive integers ℓ and q, and $Y \geq 1$, we write

$$\mathfrak{C}_\ell(Y;q) := \sum_{j=0}^{\ell}\binom{\ell}{j}(-A_qY)^{\ell-j}\,\mathfrak{B}_j(Y;q), \tag{4.25}$$

with

$$\mathfrak{B}_0(Y;q) := 1,$$

and

$$\mathfrak{B}_j(Y;q) := \int_0^1 \sum_{-u<h_1\le Y-u} \dots \sum_{-u<h_j\le Y-u} A_q(\mathbf{h})du, \text{ for } j \ge 1, \tag{4.26}$$

where

$$A_q(\mathbf{h}) := \prod_p \left(1-\frac{u_p(\mathbf{h})}{p^2}\right)\prod_{p|q}\left(1-\frac{u_p(\mathbf{h})}{p^2}\right)^{-1}, \tag{4.27}$$

and the $u_p(\mathbf{h})$ are as in (4.5). To illustrate how definition (4.26) generalizes (4.8), we note that if $Y=k$ is an integer and $q=1$, then for every $u\in(0,1)$, the condition

$$-u < h_i \le k-u$$

is equivalent to $0\le h_i\le k-1$. Thus we see that

$$\begin{aligned}\mathfrak{B}_j(k;1) &= \int_0^1 \sum_{0\le h_1\le k-1} \dots \sum_{0\le h_j\le k-1} A(\mathbf{h})du\\ &= \mathfrak{B}_j(k).\end{aligned}$$

Thus we have (note that $A_1=\frac{6}{\pi^2}$),

$$\mathfrak{C}_\ell(k;1) = \mathfrak{C}_\ell(k), \text{ for every positive integer } k. \tag{4.28}$$

The precise relationship between $\mathcal{M}(X,q;\ell)$ and $\mathfrak{C}_\ell\left(\frac{X}{q};q\right)$ is given by formula (4.95). This formula is an effective analogue of (4.6) in the case of arithmetic progressions.
Identity (4.28) and the similarity between (4.6) and (4.95) are the cornerstone of the analogy between the distributions of squarefree integers in short intervals and in arithmetic progressions. This resemblance had already appeared in [19, Theorem 1.1], where we proved the formula

$$\mathcal{M}(X,q;2) = C\prod_{p|q}\left(\frac{p^2+p-2}{p^2}\right)^{-1} X^{\frac12}q^{\frac12} + O_\epsilon\big(d(q)X^{\frac13}q^{\frac23} + X^{\frac{23}{15}+\epsilon}q^{-\frac{13}{15}}\big), \tag{4.29}$$

where C is as in (4.11).
In view of identity (4.28), Theorem 4.1.1 is a particular case of

Theorem 4.1.6. *For every $\epsilon>0$ and for every $\ell\ge 3$ there exists $C_{\epsilon,\ell}>0$ such that for every $Y\ge 1$ and every $q\ge 1$, one has the inequality*

$$|\mathfrak{C}_\ell(Y;q)| \le C'_{\epsilon,\ell}Y^{\theta_\ell+\epsilon}, \tag{4.30}$$

where θ_ℓ is as in (4.14).

Theorem 4.1.6 is our main result and we dedicate a large part of the paper to its proof.
In the same spirit of Corollary 4.1.2 (i.e. as a consequence of Theorem 4.6.1), we have the following corollary.

Corollary 4.1.7. *Let $\mathcal{M}(X,q;\ell)$ be defined by* (4.22). *Let θ_ℓ be as defined in* (4.14) *and let δ_ℓ be as in* (4.17). *Then for every $\epsilon>0$ and every $\ell\ge 3$ there exists $D'_{\epsilon,\ell}>0$ such that for every $X\ge 1$ and every positive integer $q\le X$, we have*

$$|\mathcal{M}(X,q;\ell)| \le D_{\epsilon,\ell}\left(\varphi(q)\left(\frac{X}{q}\right)^{\theta_\ell+\epsilon} + X^{\frac{\ell}{\ell+1}}\left(\frac{X}{q}\right)^{\ell-1}\right), \tag{4.31}$$

In particular, for every $\epsilon > 0$, for every $\ell \geq 3$, for every $X \geq 1$ and every positive integer q such that $X^{1-\delta_\ell+\epsilon} \leq q \leq X$, we have

$$|\mathcal{M}(X, q; \ell)| \leq 2D_{\epsilon,\ell}\, \varphi(q) \left(\frac{X}{q}\right)^{\theta_\ell+\epsilon}.$$

Notice that this result makes a step towards Conjecture 4.1.5 for $\ell \geq 3$. For example, in the particular case where $\ell = 3$, we notice that Corollary 4.1.7 gives that for every $\epsilon > 0$, we have

$$|\mathcal{M}(X, q; 3)| \ll_\epsilon \varphi(q) \left(\frac{X}{q}\right)^{\frac{9}{11}+\epsilon},$$

uniformly for $X \geq 1$ and integers q such that $X^{\frac{85}{96}+\epsilon} \leq q \leq X$. This upper bound is quite close to what is predicted by Conjecture 4.1.5, where $\frac{9}{11} + \epsilon$ is replaced by $\frac{3}{4} - \eta$ for some $\eta > 0$. We also remark that Hölder's inequality can give similar results to Corollaries 4.1.3 and 4.1.4 in the context of arithmetic progressions. That means that we can get lower and upper bound for the absolute moments defined by

$$\mathcal{M}^+(X, q; \lambda) := \sideset{}{^*}\sum_{a \pmod q} |E(X, q, a)|^\lambda.$$

In the particular case where $\lambda = 3$, we have that for every $\epsilon > 0$, the inequalities

$$\varphi(q) \left(\frac{X}{q}\right)^{\frac{3}{4}} \ll \mathcal{M}^+(X, q; 3) \ll_\epsilon \varphi(q) \left(\frac{X}{q}\right)^{\frac{23}{28}+\epsilon},$$

hold uniformly for $X \geq 1$ and integers q such that $X^{\frac{19}{20}+\epsilon} \leq q \leq X$.

4.1.3 Overview of the methods

As remarked by Hall (see the remark at the bottom of [18, p. 12]), for $\ell \geq 3$, obtaining asymptotic formulas for $\mathfrak{B}_j(Y; q)$ (resp. $\mathfrak{B}_j(k)$), $j = 1, \dots, \ell$ is not enough to obtain good results for $\mathfrak{C}_\ell(Y; q)$ (resp. $\mathfrak{C}_j(k)$). The reason is that many secondary main terms are hidden in $\mathfrak{B}_j(Y; q)$. Lemma 4.3.5 plays a major role in getting rid of these secondary terms. At this point, we need good estimates for $E_\ell(Y; \mathbf{r})$ (see (4.40)). This comes in the form of Proposition 4.3.8, Lemma 4.4.1 and Lemma 4.4.2.

These results are linked to counting points in boxes of $\mathbb{Z}^\ell$ with congruence conditions. For example, let $\mathbf{r} = (r_1, \dots, r_\ell)$ be an ℓ-tuple of positive integers. We consider

$$\mathcal{N}(Y; \mathbf{r}) := \#\left\{\mathbf{h} \in \mathbb{Z}^\ell; 0 < h_1, \dots, h_\ell \leq Y \text{ and } (r_i, r_j)^2 \mid h_i - h_j \text{ for all } 1 \leq i, j \leq \ell\right\}.$$

An asymptotic formula for $\mathcal{N}(Y; \mathbf{r})$ is available for small values of the r_j. This is, in some sense, captured by Lemma 4.4.1. As for large values of the r_j, we do not obtain such an asymptotic formula. We are content with upper bounds. In this context, Proposition 4.3.8 deals with the diagonal terms (when some of the h_j are equal) and Lemma 4.4.2 concerns the non-diagonal terms. Proposition 4.3.8 and Lemma 4.4.2 can be replaced by a very slight modification of Lemma 4.3.6 giving

$$E_\ell(Y; \mathbf{r}) \ll_\ell Y^{\ell-1},$$

which would suffice to retrieve Hall's upper bound for $\mathfrak{C}_\ell(k)$ (see (4.12) above).
The upper bound in Lemma 4.4.2 seems far from optimal, but improving it would only have an effect on Theorem 4.1.6 for $\ell = 3$ or 4, since for larger values the other error term dominates, and we are not certain that one coumd get a much better error term in Proposition 4.3.8.
In a different direction, when $\ell = 2$, one can deduce from (4.40) and Lemma 4.3.1 that

$$E_2(Y; r_1, r_2) = 2d^2 \int_0^{\frac{Y}{d^2}} \psi(u)du,$$

where $d = (r_1, r_2)$. This identity is essential in obtaining the asymptotic formula (4.29). It would be very interesting to obtain a generalization of such an identity for $\ell \geq 3$.

4.2 Notation

We use the classical notations
— $a \sim A$ for $A/2 < a \leq A$;

— $\tau_k(n)$ are the generalized divisor functions and count the number of $k-$tuples of positive integers $(d_1, \dots, d_k)$ such that $n = d_1 \dots d_k$, $\tau(n) := \tau_2(n)$ is the classical divisor function;

— We write $\omega(n)$ to denote the number of its prime divisors;

— $\mathbb{Z}_{>0}$ denotes the set of positive integers, and $[\ell] := \{1, \dots, \ell\}$;

— If $\mathbf{r} = (r_1, \dots, r_\ell)$ is a $\ell-$tuple of positive integers, we denote

$$\mathrm{lcm}[\mathbf{r}] := \mathrm{lcm}[r_1, \dots, r_\ell]; \text{ and } \gcd[\mathbf{r}] := \gcd[r_1, \dots, r_\ell];$$

— If A and B are two sets, we write

$$B^A = \{\mathbf{x} = (x_\alpha)_{\alpha \in A}; x_\alpha \in B \ \forall \alpha \in A\};$$

— For a finite set S, $\#S$ denotes its cardinality and for an interval $I \subset \mathbb{R}$, $|I|$ denotes its length.

— For a finite set T and i a positive integer, we use the abbreviations $\mathcal{P}_{\geq i}(T) = \{S \subset T; \#S \geq i\}$. Furthermore we write $\mathcal{P}_{\geq i}(\ell) = \mathcal{P}_{\geq i}([\ell])$;

— Unless otherwise stated, the implied constant by the symbols O and $\ll$ depend at most on the subscribed variables (e.g. the implied constant by the symbol $\ll_{\epsilon,\ell}$ depends at most on ϵ and ℓ);

— The ψ function is the classical sawtooth function defined by

$$\psi(x) = \lfloor x \rfloor - x + \frac{1}{2}. \tag{4.32}$$

4.3 Preparatory results

We start with the following simple lemma

Lemma 4.3.1. *Let n be a positive integer and x a real number. Let ψ be as defined in* (4.32)*. Then we have the equality*

$$\sum_{k=0}^{n-1} \psi\left(x + \frac{k}{n}\right) = \psi(nx). \tag{4.33}$$

Démonstration. Since both sides of (4.33) are invariant by $x \mapsto x + \frac{1}{n}$, we can restrict ourselves to the case where $0 \leq x < \frac{1}{n}$. In which case, the left-hand side of (4.33) equals

$$\begin{aligned}\sum_{k=0}^{n-1} \left(\frac{1}{2} - x - \frac{k}{n}\right) &= \frac{1}{2} - nx, \\ &= \psi(nx).\end{aligned}$$

This concludes the proof of the lemma.

□

4.3.1 Total decomposition sets

One of the main technical difficulties in this paper is to work out computations involving the greatest common divisors and the least common multiples of subsets of $\{r_1, \ldots, r_\ell\}$ for $\mathbf{r} = (r_1, \ldots, r_\ell)$ an ℓ-tuple of positive integers. The following lemma is particularly convenient to do so. A proof of it can be found in [19, page 112].

Lemma 4.3.2. *For each $\mathbf{r} \in \mathbb{Z}_{>0}^{\ell}$, there exists a unique $(2^\ell - 1)-$tuple of integers $(d(\mathbf{r}, S))_{S \in \mathcal{P}_{\geq 1}(\ell)}$, called the total decomposition set of $\mathbf{r}$, such that for every $T \in \mathcal{P}_{\geq 1}(\ell)$, we have*

$$\gcd(r_j;\ j \in T) = \prod_{S \supset T} d(\mathbf{r}; S), \tag{4.34}$$

and

$$\operatorname{lcm}[r_j;\ j \in T] = \prod_{S \cap T \neq \emptyset} d(\mathbf{r}; S). \tag{4.35}$$

In particular, we have

$$r_j = \prod_{S \ni j} d(\mathbf{r}; S).$$

Remark 4.3.1. In these notes we only use Lemma 4.3.2 in the case where all the r_j are squarefree. Following Hall's proof, we see that in this case the $d(\mathbf{r}, S)$ take the form

$$d(\mathbf{r}, S) := \prod_{\substack{p \mid \gcd(r_j; j \in S) \\ p \mid \operatorname{lcm}[r_j; j \notin S]}} p.$$

We also remark that (4.35) implies that the r_i are squarefree if and only if the $d(\mathbf{r}, S)$ are squarefree and pairwise coprime.

4.3.2 Unfolding $A_q(\mathbf{h})$

We point out that it is not very practical to work with $A_q(\mathbf{h})$ under the form of an infinite product. Thus we unfold this infinite product in order to obtain a simpler expression. More precisely, we have the following

Lemma 4.3.3. *Let $\mathbf{h} = (h_1, \dots, h_\ell) \in \mathbb{Z}^\ell$, and let $A_q(\mathbf{h})$ be as in (4.27). Then we have the equality*

$$A_q(\mathbf{h}) = \sum_{\substack{r_1=1 \\ (r_1,q)=1}}^{\infty} \dots \sum_{\substack{r_\ell=1 \\ (r_\ell,q)=1}}^{\infty} \frac{\mu(r_1)\dots\mu(r_\ell)}{\operatorname{lcm}[\mathbf{r}]^2} \kappa(\mathbf{r};\mathbf{h}),$$

where $\mathbf{r} = (r_1, \dots, r_\ell)$, and

$$\kappa(\mathbf{r};\mathbf{h}) = \begin{cases} 1 \text{ if } \gcd(r_i, r_j)^2 \mid h_i - h_j, \text{ for all } i, j \in [\ell] \\ 0 \text{ otherwise.} \end{cases} \tag{4.36}$$

Démonstration. A proof in the case $q = 1$ can be found in [18, page 16], and the general case follows in a completely analogous way. □

Using Lemma 4.3.3in the defnition 4.26, we deduce that

$$\mathfrak{B}_\ell(Y; q) = \sum_{\substack{r_1=1 \\ (r_1,q)=1}}^{\infty} \dots \sum_{\substack{r_\ell=1 \\ (r_\ell,q)=1}}^{\infty} \frac{\mu(r_1)\dots\mu(r_\ell)}{\operatorname{lcm}[\mathbf{r}]^2} H_\ell(Y;\mathbf{r}), \tag{4.37}$$

where $\mathbf{r} = (r_1, \dots, r_\ell)$ and

$$H_\ell(Y;\mathbf{r}) := \int_0^1 \sum_{\substack{-u < h_j \le Y-u, \\ \forall j \in [\ell]}} \dots \sum \kappa(\mathbf{r};\mathbf{h})\, du, \tag{4.38}$$

with $\kappa(\mathbf{r};\mathbf{h})$ as in (4.36).

4.3.3 Analysis of $H_\ell(Y;\mathbf{r})$

Lemma 4.3.4. *Let $\ell \ge 1$ and $\mathbf{r} = (r_1, \dots, r_\ell) \in \mathbb{Z}_{>0}^\ell$, where all the r_j are squarefree. Let $H_\ell(Y;\mathbf{r})$ be as in (4.38) with $Y \ge 1$. Then we have the equality*

$$H_\ell(Y;\mathbf{r}) = \int_0^1 \sum_{\beta \,(\mathrm{mod}\ \operatorname{lcm}[\mathbf{r}]^2)} \prod_{j=1}^{\ell} \left(\frac{Y}{r_j^2} + \psi\left(\frac{Y-u-\beta}{r_j^2}\right) - \psi\left(\frac{-u-\beta}{r_j^2}\right)\right) du.$$

Démonstration. Notice that the innermost product on the right-hand side above equals

$$\#\left\{(h_1,\dots,h_\ell)\in\mathbb{Z}^\ell;\ -u<h_1,\dots,h_\ell\le Y-u \text{ and } h_j\equiv\beta \pmod{r_j^2} \text{ for all } j\in[\ell]\right\}$$

Hence, it suffices to prove that $\kappa(\mathbf{r};\mathbf{h})=1$ if and only if there exists (a unique) β modulo $\mathrm{lcm}[\mathbf{r}]^2$ such that $h_j\equiv\beta \pmod{r_j^2}$ for every $j\in[\ell]$. One direction is easy. Indeed, if we suppose that such β exists, then for every $i,j\in[\ell]$, we have that $h_i\equiv h_j\equiv\beta \pmod{\gcd(r_i,r_j)^2}$. Thus for every $i,j\in[\ell]$, $\gcd(r_i,r_j)^2\mid h_i-h_j$. This proves that $\kappa(\mathbf{r},\mathbf{h})=1$.

The opposite implication is more involved and uses the total decomposition set of $\mathbf{r}$. Let $\{d(\mathbf{r};S)\}$ be the total decomposition set of $\mathbf{r}$. Since all the r_j are squarefree, then the $d(\mathbf{r},S)$ are pairwise coprime. Thus the conditions

$$\gcd(r_i,r_j)^2\mid h_i-h_j, \text{ for all } i,j\in[\ell]$$

are equivalent to

$$h_i\equiv h_j \pmod{d(\mathbf{r},S)^2}, \text{ for every } S\in\mathcal{P}_{\ge1}(\ell) \text{ and } i,j\in S.$$

This is equivalent to the existence, for every $S\in\mathcal{P}_{\ge1}(\ell)$, of certain $\beta_S \pmod{d(\mathbf{r},S)^2}$ such that

$$h_j\equiv\beta_S \pmod{d(\mathbf{r},S)^2}, \text{ for every } S\in\mathcal{P}_{\ge1}(\ell) \text{ and } j\in S.$$

The Chinese remainder theorem now gives the result (recall that the $d(\mathbf{r},S)$ are pairwise coprime). □

The following Lemma should be compared to (4.38) and Lemma 4.3.4. This is the point of the proof where the cancellation of the secondary terms mentioned in section 4.1.3 take place.

Lemma 4.3.5. *Let $\mathfrak{C}_\ell(Y;q)$ be as in* (4.25)*. Then for every $Y\ge1$, and positive integers ℓ and q, the following holds :*

$$\mathfrak{C}_\ell(Y;q)=\sum_{\substack{r_1=1\\(r_1,q)=1}}^{\infty}\ \dots\ \sum_{\substack{r_\ell=1\\(r_\ell,q)=1}}^{\infty}\frac{\mu(r_1)\dots\mu(r_\ell)}{\mathrm{lcm}[\mathbf{r}]^2}E_\ell(Y;\mathbf{r}),\tag{4.39}$$

where

$$E_\ell(Y;\mathbf{r})=\int_0^1\sum_{\beta \pmod{\mathrm{lcm}[\mathbf{r}]^2}}\prod_{j=1}^{\ell}\left(\psi\left(\frac{Y-u-\beta}{r_j^2}\right)-\psi\left(\frac{-u-\beta}{r_j^2}\right)\right)du.\tag{4.40}$$

Démonstration. Let $\mathfrak{C}'_\ell(Y;q)$ be the right-hand side of (4.39). By inclusion-exclusion, the inner product on the right-hand side of (4.40) equals

$$\sum_{T\subset[\ell]}\left\{\prod_{j\notin T}\left(\frac{-Y}{r_j^2}\right)\prod_{j\in T}\left(\frac{Y}{r_j^2}+\psi\left(\frac{Y-u-\beta}{r_j^2}\right)-\psi\left(\frac{-u-\beta}{r_j^2}\right)\right)\right\}.$$

By replacing it in (4.40) and interchanging the order of summation and integration, we see that

$$E_\ell(Y;\mathbf{r}) = \sum_{T\subset[\ell]} \prod_{j\notin T} \frac{-Y}{r_j^2}\, \omega_T(\mathbf{r}), \tag{4.41}$$

where

$$\omega_T(\mathbf{r}) := \int_0^1 \sum_{\beta \,(\mathrm{mod}\ \mathrm{lcm}[\mathbf{r}]^2)} \prod_{j\in T} \left(\frac{Y}{r_j^2} + \psi\left(\frac{Y-u-\beta}{r_j^2}\right) - \psi\left(\frac{-u-\beta}{r_j^2}\right)\right) du. \tag{4.42}$$

Notice that the inner product on the right-hand side of the above equation only depends on the class of $\beta \pmod{\mathrm{lcm}[\mathbf{r}|_T]^2}$, where for each $T=\{i_1,\dots,i_{\#T}\}$, with $1\le i_1<\ldots<i_{\#T}\le\ell$, we define

$$\mathbf{r}|_T := (r_{i_1},\dots,r_{i_{\#T}}). \tag{4.43}$$

Hence

$$\begin{aligned}\omega_T(\mathbf{r}) :&= \frac{\mathrm{lcm}[\mathbf{r}]^2}{\mathrm{lcm}[\mathbf{r}|_T]^2}\int_0^1 \sum_{\beta \,(\mathrm{mod}\ \mathrm{lcm}[\mathbf{r}|_T]^2)} \prod_{j\in T} \left(\frac{Y}{r_j^2} + \psi\left(\frac{Y-u-\beta}{r_j^2}\right) - \psi\left(\frac{-u-\beta}{r_j^2}\right)\right) du \\ &= \frac{\mathrm{lcm}[\mathbf{r}]^2}{\mathrm{lcm}[\mathbf{r}|_T]^2} H_{\#T}\left(Y;\mathbf{r}|_T\right), \end{aligned} \tag{4.44}$$

from Lemma 4.3.4. Gathering (4.41) and (4.44), we obtain

$$E_\ell(Y;\mathbf{r}) = \mathrm{lcm}[\mathbf{r}]^2 \sum_{T\subset[\ell]} \left(\prod_{j\notin T}\left(\frac{-Y}{r_j^2}\right)\right) \frac{H_{\#T}\left(Y;\mathbf{r}|_T\right)}{\mathrm{lcm}[\mathbf{r}|_T]^2}. \tag{4.45}$$

Changing the order of summation, we deduce the inequality

$$\mathfrak{C}'_\ell(Y;q) = \sum_{T\subset[\ell]} \Theta(T)\Theta'([\ell]\backslash T), \tag{4.46}$$

where

$$\begin{aligned}\Theta(T) &= \sum_{\substack{r_{i_1}=1\\(r_{i_1},q)=1}}^{\infty} \ \dots \sum_{\substack{r_{i_{\#T}}=1\\(r_{i_{\#T}},q)=1}}^{\infty} \frac{\mu(r_{i_1})\dots\mu(r_{i_{\#T}})}{\mathrm{lcm}[\mathbf{r}|_T]^2} H_{\#T}\left(Y;\mathbf{r}|_T\right) \\ &= \mathfrak{B}_{\#T}(Y;q), \end{aligned} \tag{4.47}$$

and

$$\begin{aligned}\Theta'([\ell]\backslash T) &= (-Y)^{\ell-\#T} \prod_{j\notin T}\left(\sum_{\substack{r_j=1\\(r_j,q)=1}}^{\infty} \frac{\mu(r_j)}{r_j^2}\right) \\ &= (-A_qY)^{\ell-\#T}. \end{aligned} \tag{4.48}$$

Finally, putting together (4.46), (4.47) and (4.48) gives

$$\begin{aligned}\mathfrak{C}'_\ell(Y;q) &= \sum_{j=0}^{\ell}\binom{\ell}{j}(-A_qY)^{\ell-j}\mathfrak{B}_j(Y;q),\\ &= \mathfrak{C}_\ell(Y;q).\end{aligned}$$

□

4.3.4 A modification of $H_\ell(Y;\mathbf{r})$

In the following we introduce a slight modification of $H_\ell(Y;\mathbf{r})$ (defined in (4.38)) which will be very important when estimating $E_\ell(Y;\mathbf{r})$ for large values of the r_j (see Lemma 4.4.2 below). For positive integers ℓ and q, and for $Y \geq 1$, we let

$$H^*_\ell(Y;\mathbf{r}) = \int_0^1 \sum_{\substack{-u<h_j\leq Y-u,\ \forall j\in[\ell]\\ h_j \text{ distinct}}}\cdots\sum \kappa(\mathbf{r};\mathbf{h})du. \tag{4.49}$$

The rest of this section is dedicated to the study of the interplay between $H_\ell(Y;\mathbf{r})$ and $H^*_\ell(Y;\mathbf{r})$, specially when it comes to their contribution to $\mathfrak{C}_\ell(Y;q)$.

Lemma 4.3.6. *Let $H^*_\ell(Y;\mathbf{r})$ be as in* (4.49)*. Then we have the equality*

$$H^*_\ell(Y;\mathbf{r}) = \frac{\mathrm{lcm}[\mathbf{r}]^2}{r_1^2\dots r_\ell^2}Y^\ell + O(\ell^2(Y+1)^{\ell-1}),$$

uniformly for every $Y \geq 1$, every $\ell \geq 1$ and every $\mathbf{r} \in \mathbb{Z}^\ell_{>0}$.

Démonstration. We prove it by induction. For $\ell = 1$, $\kappa(r,h) = 1$ for every integer h and every $r \in \mathbb{Z}_{>0}$. Hence

$$H^*_1(Y;r) = Y + O(1).$$

Suppose now that Lemma 4.3.6 is true for a certain $\ell \geq 1$. Let $\mathbf{r} = (r_1,\dots,r_{\ell+1}) \in \mathbb{Z}^{\ell+1}_{>0}$. Then, with the notation from the previous lemma, we have

$$H^*_{\ell+1}(Y;\mathbf{r}) = \int_0^1 \left(\sum_{\substack{-u<h_j\leq Y-u,\ \forall j\in[\ell]\\ h_j \text{ distinct}}}\cdots\sum \kappa(\mathbf{r}|_{[\ell]};h_1,\dots,h_\ell)\sum_{\substack{-u<h_{\ell+1}\leq Y-u\\ h_{\ell+1}\notin\{h_1,\dots,h_\ell\}}}\nu(\mathbf{r},\mathbf{h})\right)du. \tag{4.50}$$

where

$$\nu(\mathbf{r},\mathbf{h}) := \begin{cases}1, \text{ if } (r_j,r_{\ell+1})^2 \mid h_j - h_{\ell+1} \text{ for all } j = 1,2,\dots,\ell,\\ 0, \text{ otherwise.}\end{cases}$$

By the Chinese remainder theorem, whenever $\kappa(\mathbf{r}|_{[\ell]},h_1,\dots,h_\ell) = 1$, the inner sum equals (in this case, the congruences are always compatible)

$$\frac{Y}{\gcd(r_{\ell+1}, \operatorname{lcm}[\mathbf{r}|_{[\ell]}])^2} + O(\ell).$$

Replacing it in (4.50), we have the equality

$$H^*_{\ell+1}(Y;\mathbf{r}) = \frac{Y}{\gcd(r_{\ell+1}, \operatorname{lcm}[\mathbf{r}|_{[\ell]}])^2} H^*_\ell\left(Y;\mathbf{r}|_{[\ell]}\right) + O(\ell(Y+1)^\ell).$$

since $H^*_\ell\left(Y;\mathbf{r}|_{[\ell]}\right) \leq (Y+1)^\ell$. The result for $\ell+1$ is now a consequence of the induction hypothesis. This concludes the proof of the Lemma.

□

Lemma 4.3.7. *Let $H_\ell(Y;\mathbf{r})$ be as in (4.38) and $H^*_\ell(Y;\mathbf{r})$ as in (4.49). Then we have the equality*

$$H_\ell(Y;\mathbf{r}) = H^*_\ell(Y;\mathbf{r}) + \frac{\operatorname{lcm}[\mathbf{r}]^2}{r_1^2 \dots r_\ell^2} Y^{\ell-1} \sum_{1 \leq j_1 < j_2 \leq \ell} \gcd(r_{j_1}, r_{j_2})^2 + O(\ell^4 (Y+1)^{\ell-2}),$$

uniformly for every $Y \geq 1$, every $\ell \geq 2$ and every $\mathbf{r} \in \mathbb{Z}^\ell_{>0}$.

Démonstration. The inner sum in (4.38) counts $\ell-$tuples satisfying a certain congruence condition. We break up this counting in three terms. The first consisting of the $\ell-$tuples containing exactly ℓ distinct elements, the second of those containing exactly $\ell-1$ distinct elements, and the last one of those containing at most $\ell-2$ distinct elements. The third one can be bounded by $\ell^4(Y+1)^{\ell-2}$. After integrating with respect to u, we obtain the equality

$$H_\ell(Y;\mathbf{r}) = H^*_\ell(Y;\mathbf{r}) + \int_0^1 \sum_{\substack{-u < h_j \leq Y-u,\ \forall j \in [\ell] \\ \#\{h_1,\dots,h_\ell\} = \ell-1}} \dots \sum \kappa(\mathbf{r};\mathbf{h}) du + O\left(\ell^4 (Y+1)^{\ell-2}\right). \tag{4.51}$$

Notice that the condition $\#\{h_1,\dots,h_\ell\} = \ell-1$ means that exactly two of the h_j that are equal and all the other are distinct and different from this common value.

For each j_1, j_2 such that $1 \leq j_1 < j_2 \leq \ell$, let $\mathbf{s}_{j_1,j_2}$ be the $(\ell-1)-$tuple given by

$$\mathbf{s}_{j_1,j_2} = (r_1, \dots, \widehat{r_{j_1}}, \dots, \widehat{r_{j_2}}, \dots, r_\ell, \operatorname{lcm}[r_{j_1}, r_{j_2}]),$$

where the $\widehat{\ }$ means that these entries must be suppressed. Then the middle term on the right-hand side in (4.51) equals

$$\sum_{1 \leq j_1 < j_2 \leq \ell} H^*_{\ell-1}(Y;\mathbf{s}_{j_1,j_2}) = \frac{\operatorname{lcm}[\mathbf{r}]^2}{r_1^2 \dots r_\ell^2} Y^{\ell-1} \sum_{1 \leq j_1 < j_2 \leq \ell} \frac{r_{j_1}^2 r_{j_2}^2}{\operatorname{lcm}[r_{j_1}, r_{j_2}]^2} + O(\ell^4 (Y+1)^{\ell-2}), \tag{4.52}$$

by Lemma 4.3.6. Finally, Lemma 4.3.7 now follows from (4.51) and (4.52). □

Inspired by (4.45), we define

$$E^*_\ell(Y;\mathbf{r}) := \mathrm{lcm}[\mathbf{r}]^2 \sum_{T\subset[\ell]} \prod_{j\notin T} \left(\frac{-Y}{r_j^2}\right) \frac{H^*_{\#T}(Y;\mathbf{r}|_T)}{\mathrm{lcm}[\mathbf{r}|_T]^2}. \tag{4.53}$$

By Lemma 4.3.7 we have the equality

$$E_\ell(Y;\mathbf{r}) = E^*_\ell(Y;\mathbf{r}) + \frac{\mathrm{lcm}[\mathbf{r}^2]}{r_1^2\dots r_\ell^2} Y^{\ell-1} \sum_{T\subset[\ell]} (-1)^{\ell-\#T} \sum_{\substack{1\le j_1<j_2\le \ell\\ j_1,j_2\in T}} \gcd(r_{j_1},r_{j_2})^2 + O\left(2^\ell \ell^4 (Y+1)^{\ell-2}\right).$$

Actually, for $\ell \ge 3$, the sum over $T\subset[\ell]$ in the above equation vanishes. Indeed, by changing the order of summation, this sum equals

$$\sum_{1\le j_1<j_2\le \ell} \gcd(r_{j_1},r_{j_2})^2 \sum_{\substack{T\subset[\ell]\\ T\ni j_1,j_2}} (-1)^{\ell-\#T} = 0,$$

as a consequence of the binomial formula for the inner sum on the right-hand side above. We have just proved

Proposition 4.3.8. *Let $\ell \ge 3$ be an integer. Let $Y \ge 1$. Let $\mathbf{r} \in \mathbb{Z}^\ell_{>0}$, where all the r_j are squarefree. Let $E_\ell(Y;\mathbf{r})$ be as in* (4.40) *and $E^*_\ell(Y;\mathbf{r})$ as in* (4.53)*. Then we have the equality*

$$E_\ell(Y;\mathbf{r}) = E^*_\ell(Y;\mathbf{r}) + O\left(2^\ell \ell^4 (Y+1)^{\ell-2}\right),$$

where the implied constant is absolute.

4.4 Estimating $E_\ell(Y;\mathbf{r})$

In this section we give the two major lemmas that we use to estimate $E_\ell(Y;\mathbf{r})$. They will be applied, roughly speaking, to small and large values of the r_j, respectively.

Lemma 4.4.1. *Let $\ell \ge 1$. Let $\mathbf{r} \in \mathbb{Z}^\ell_{>0}$, where all the r_j are squarefree. Let $\{d(\mathbf{r},S)\}$ be the total decomposition set of $\mathbf{r}$ as in Lemma 4.3.2. Then we have the equality*

$$|E_\ell(Y;\mathbf{r})| \le \prod_{S\in\mathcal{P}_{\ge 2}(\ell)} d(\mathbf{r},S)^2,$$

where $E_\ell(Y;\mathbf{r})$ is as in (4.40)*.*

Démonstration. From (4.40) we deduce the inequality

$$|E_\ell(Y;\mathbf{r})| \le \mathrm{lcm}[\mathbf{r}]^2, \tag{4.54}$$

which is larger than the bound claimed in Lemma 4.4.1 by a factor of $\prod_{j\in[\ell]} d(\mathbf{r},\{j\})^2$ (see (4.35)). We show how to recover the factor $d(\mathbf{r},\{1\})^2$ and the same process can be applied for $d(\mathbf{r},\{j\})$, $j \ge 2$.

Let $e_1 := d(\mathbf{r},\{1\})$ and $\widetilde{r}_1$ be such that $r_1 = e_1\widetilde{r}_1$. Then, by the Chinese remainder theorem, (4.40) can be written as

$$E_\ell(Y;\mathbf{r}) = \int_0^1 \sum_{\beta \,(\mathrm{mod}\ \mathrm{lcm}[\widetilde{r}_1,r_2,\ldots,r_\ell]^2)} \mathfrak{S}_1(\beta) \times \prod_{j=2}^{\ell} \left(\psi\left(\frac{Y-u-\beta}{r_j^2}\right) - \psi\left(\frac{-u-\beta}{r_j^2}\right)\right) du,$$

where

$$\mathfrak{S}_1(\beta) = \sum_{\beta_1 \,(\mathrm{mod}\ e_1^2)} \left(\psi\left(\frac{Y-u}{r_1^2} - \frac{\overline{e_1^2}\beta}{\widetilde{r}_1^2} - \frac{\overline{\widetilde{r}_1^2}\beta_1}{e_1^2}\right) - \psi\left(-\frac{u}{r_1^2} - \frac{\overline{e_1^2}\beta}{\widetilde{r}_1^2} - \frac{\overline{\widetilde{r}_1^2}\beta_1}{e_1^2}\right)\right),$$

where $\overline{e_1}$ denotes the multiplicative inverse of $e_1 \pmod{\widetilde{r}_1^2}$ and $\overline{\widetilde{r}_1}$ the multiplicative inverse of $\widetilde{r}_1 \pmod{e_1^2}$. An application of Lemma 4.3.1 now gives

$$\mathfrak{S}_1(\beta) = \psi\left(\frac{Y-u-\beta}{\widetilde{r}_1^2}\right) - \psi\left(\frac{-u-\beta}{\widetilde{r}_1^2}\right).$$

Summarizing, we have

$$E_\ell(Y;\mathbf{r}) = E_\ell(Y;\widetilde{r}_1,r_2,\ldots,r_\ell).$$

Repeating the process for $j = 2,\ldots,\ell$ and defining $\widetilde{r}_2,\ldots,\widetilde{r}_\ell$ similarly, we obtain that

$$E_\ell(Y;\mathbf{r}) = E_\ell(Y;\widetilde{\mathbf{r}}),$$

where $\widetilde{\mathbf{r}} = (\widetilde{r}_1,\ldots,\widetilde{r}_\ell)$. The lemma now follows from applying (4.54) to the term on the right in the above equation. □

Before stating our next lemma, we shall need some extra notation. These are given in the following definition.

Definition 4.4.1. Let $\ell \geq 1$. Let $\mathbf{D} = (D_S)_{S\in\mathcal{P}_{\geq 2}(\ell)}$ be a $(2^\ell - \ell - 1)-$tuple of positive real numbers. Let $\mathbf{e}$ be an $\ell-$tuple of pairwise coprime squarefree integers.

Let $\mathfrak{X}_\ell(\mathbf{D},\mathbf{e})$ denote the set of $(2^\ell-1)$-tuples of positive integers $\mathbf{d} = (d_S)_{S\in\mathcal{P}_{\geq 1}(\ell)}$ such that the d_S are pairwise pairwise coprime, $d_S \sim D_S$ for all $S \in \mathcal{P}_{\geq 2}(\ell)$, and $d_{\{j\}} = e_j$ for all $j \in [\ell]$.

For every $(2^\ell-1)-$tuple of pairwise coprime squarefree integers $\mathbf{d} = (d_S)_{S\in\mathcal{P}_{\geq 1}(\ell)}$, for every $j \in [\ell]$, we associate the integers

$$r_j(\mathbf{d}) := \prod_{S\ni j} d_S \tag{4.55}$$

and the $\ell-$tuple $\mathbf{r}(\mathbf{d}) := (r_1(\mathbf{d}),\ldots,r_\ell(\mathbf{d}))$.

Finally, for every $Y \geq 1$, define the sum of error terms

$$S(Y;\mathbf{D},\mathbf{e}) := \sum_{\mathbf{d}\in\mathfrak{X}_\ell(\mathbf{D},\mathbf{e})} \ldots \sum |E_\ell^*(Y;\mathbf{r}(\mathbf{d}))|, \tag{4.56}$$

where $E_\ell^*(Y;\mathbf{D},\mathbf{e})$ is as defined in (4.53).

Remark that the $\ell-$tuple $\mathbf{r}(\mathbf{d})$ given by definition (4.55) is the unique ℓ-tuple whose total decomposition set (see Lemma 4.3.2) satisfies $d(\mathbf{r}(\mathbf{d}), S) = d_S$ for every $S \in \mathcal{P}_{\geq 1}(\ell)$.

Lemma 4.4.2. *Let $\epsilon > 0$ and $\ell \geq 2$ be an integer. Then, we have the inequality*

$$S\left(Y;\mathbf{D},\mathbf{e}\right) \ll_{\epsilon,\ell} \frac{Y^{\ell+\epsilon}}{\prod\limits_{S\in\mathcal{P}_{\geq 2}(\ell)} D_S^{2/\ell}}, \tag{4.57}$$

uniformly for $Y \geq 1$, every $(2^\ell - \ell - 1)-$tuple of positive real numbers $\mathbf{D} = (D_S)_{S\in\mathcal{P}_{\geq 2}(\ell)}$ and every $\ell-$tuple of positive integers $\mathbf{e} = (e_1, \ldots, e_\ell)$, where $S(Y;\mathbf{D},\mathbf{e})$ is as in Definition 4.4.1 above.

Démonstration. We first prove the closely related inequality

$$\sum_{\mathbf{d}\in\mathfrak{X}_\ell(\mathbf{D},\mathbf{e})} \ldots \sum H_\ell^*\left(Y;\mathbf{r}(\mathbf{d})\right) \ll_{\ell,\epsilon} \frac{Y^{\ell+\epsilon}}{\prod\limits_{S\in\mathcal{P}_{\geq 2}(\ell)} D_S^{2/\ell}}. \tag{4.58}$$

where, we recall (see (4.49))

$$H_\ell^*\left(Y;\mathbf{r}(\mathbf{d})\right) = \int_0^1 \sum_{-u<h_j\leq Y-u\,\forall j\in[\ell]}{}' \ldots \sum{}' \kappa(\mathbf{r}(\mathbf{d}),\mathbf{h})du,$$

where the $'$ symbol means that the sum is restricted to the $\ell-$tuples $\mathbf{h}$ such that

$$h_i \neq h_j \text{ for all } 1 \leq i < j \leq \ell.$$

Note that $\kappa(\mathbf{r}(\mathbf{d}),\mathbf{h}) = 1$ if and only if for every $S \in \mathcal{P}_{\geq 2}(\ell)$ and for every $i, j \in S$ we have

$$d_S^2 \mid h_i - h_j.$$

Fix $j_0 \in [\ell]$. At the cost of introducing some divisor functions, we can drop from the sum in the left-hand side of (4.58) the sum over the d_S for which $j_0 \notin S$, loosing at most a factor Y^ϵ. Thus we have

$$\sum_{\mathbf{d}\in\mathfrak{X}_\ell(\mathbf{D},\mathbf{e})} \ldots \sum H_\ell^*\left(Y;\mathbf{r}(\mathbf{d})\right) \ll_{\epsilon,\ell} Y^\epsilon \sum_{(d_S)\in\mathfrak{X}_{\ell,j_0}(\mathbf{D})} \ldots \sum \int_0^1 \sum_{-u<h_{j_0}\leq Y-u} \prod_{j\neq j_0} \left(\sum_{\substack{-u<h_j\leq Y-u \\ t_{j,j_0}^2 \mid h_j - h_{j_0}}} 1 \right) du, \tag{4.59}$$

where $\mathfrak{X}_{\ell,j_0}\left(\mathbf{D}\right)$ is a slight modification of $\mathfrak{X}_\ell\left(\mathbf{D},\mathbf{e}\right)$ given by

$$\mathfrak{X}_{\ell,j_0}\left(\mathbf{D}\right) = \big\{(d_S)_{S\in\mathcal{P}_{\geq 2}(\ell),\, j_0\in S};\ d_S \text{ pairwise coprime},\ d_S \sim D_S \text{ for every } S \text{ such that } j_0 \in S \in \mathcal{P}_{\geq 2}(\ell)\big\}, \tag{4.60}$$

and

$$t_{j,j_0} = \prod_{j,j_0 \in S} d_S.$$

Thus the integrand is

$$\ll_\ell \frac{Y^\ell}{\prod_{j \neq j_0} t_{j,j_0}^2} = \frac{Y^\ell}{\prod_{\substack{S \in \mathcal{P}_{\geq 2}(\ell) \\ j_0 \in S}} d_S^{2(\#S-1)}}.$$

Injecting it in (4.59), we obtain that

$$\sum_{\mathbf{d} \in \mathfrak{X}_\ell(\mathbf{D},\mathbf{e})} \dots \sum H_\ell^* \left(Y; \mathbf{r}(\mathbf{d})\right) \ll_{\ell,\epsilon} \frac{Y^{\ell+\epsilon}}{\prod_{\substack{S \in \mathcal{P}_{\geq 2}(\ell) \\ j_0 \in S}} D_S^{2(\#S-1)-1}} \tag{4.61}$$

Note that (4.61) holds for arbitrary $j_0 \in [\ell]$. Thus by taking the minimum over $j_0 \in [\ell]$, we see that the left hand side of (4.61) is

$$\begin{aligned} \ll_{\ell,\epsilon} \min_{j_0 \in [\ell]} \frac{Y^{\ell+\epsilon}}{\prod_{\substack{S \in \mathcal{P}_{\geq 2}(\ell) \\ j_0 \in S}} D_S^{2(\#S-1)-1}} &\leq \left(\prod_{j_0 \in [\ell]} \frac{Y^{\ell+\epsilon}}{\prod_{\substack{S \in \mathcal{P}_{\geq 2}(\ell) \\ j_0 \in S}} D_S^{2(\#S-1)-1}} \right)^{1/\ell} \\ &\leq \frac{Y^{\ell+\epsilon}}{\prod_{S \in \mathcal{P}_{\geq 2}(\ell)} D_S^{\frac{\#S(2\#S-3)}{\ell}}} \leq \frac{Y^{\ell+\epsilon}}{\prod_{S \in \mathcal{P}_{\geq 2}(\ell)} D_S^{2/\ell}}, \end{aligned} \tag{4.62}$$

since the least exponent for the D_S occurs when $\#S = 2$. This concludes the proof of (4.58).

With a very similar argument, we can prove that for every $T \subset [\ell]$, we have the inequality

$$\sum_{\mathbf{d} \in \mathfrak{X}_\ell(\mathbf{D},\mathbf{e})} \dots \sum H_{\#T}^* \left(Y; \mathbf{r}(\mathbf{d})|_T\right) \ll_{\ell,\epsilon} \prod_{\substack{S \in \mathcal{P}_{\geq 2}(\ell) \\ \#S \cap T \leq 1}} D_S \frac{Y^{\#T+\epsilon}}{\prod_{\substack{S \in \mathcal{P}_{\geq 2}(\ell) \\ \#S \cap T \geq 2}} D_S^{2/\ell}}, \tag{4.63}$$

where for every $T = \{i_1, \dots, i_{\#T}\}$ with $1 \leq i_1 < \dots < i_{\#T} \leq \ell$, $\mathbf{r}(d)|_T$ is given by (compare with (4.43))

$$\mathbf{r}(d)|_T = \left(r_{i_1}(\mathbf{d}), \dots, r_{i_{\#T}}(\mathbf{d})\right).$$

If we replace $E^*(Y;\mathbf{r})$ by its definition (4.53) in (4.56), we obtain the inequality

$$\begin{aligned} S(Y;\mathbf{D},\mathbf{e}) &\leq \sum_{\mathbf{d}\in\mathfrak{X}_\ell(\mathbf{D},\mathbf{e})}\dots\sum_{T\subset[\ell]}\sum \frac{\mathrm{lcm}[\mathbf{r}(\mathbf{d})]^2}{\mathrm{lcm}[\mathbf{r}(\mathbf{d})|_T]^2}\prod_{j\notin T}\left(\frac{Y}{r_j(\mathbf{d})^2}\right)H^*_{\#T}(Y;\mathbf{r}(\mathbf{d})|_T) \\ &\ll_\ell \sum_{\mathbf{d}\in\mathfrak{X}_\ell(\mathbf{D},\mathbf{e})}\dots\sum_{T\subset[\ell]}\sum Y^{\ell-\#T}\prod_{\substack{S\in\mathcal{P}_{\geq 1}(\ell)\\ S\cap T=\emptyset}} D_S^2\prod_{S\in\mathcal{P}_{\geq 1}(\ell)} D_S^{-2\#(S\setminus T)}H^*_{\#T}(Y;\mathbf{r}(\mathbf{d})|_T)\,, \quad (4.64)\end{aligned}$$

where in the second line we used (4.55) and the fact that for every $\mathbf{d}\in\mathfrak{X}_\ell(\mathbf{D},\mathbf{e})$, the d_S are pairwise coprime and that for every $S\in\mathcal{P}_{\geq 2}(\ell)$, we have $d_S\sim D_S$.

By changing the order of summation in (4.64) and using (4.63), we obtain the bound

$$S(Y;\mathbf{D},\mathbf{e}) \ll_{\ell,\epsilon} Y^{\ell+\epsilon}\sum_{T\subset[\ell]}\Phi_T(\mathbf{D}), \quad (4.65)$$

where

$$\begin{aligned}\Phi_T(\mathbf{D}) &= \prod_{\substack{S\in\mathcal{P}_{\geq 1}(\ell)\\ S\cap T=\emptyset}} D_S^2\prod_{S\in\mathcal{P}_{\geq 1}(\ell)} D_S^{-2\#(S\setminus T)}\prod_{\substack{S\in\mathcal{P}_{\geq 2}(\ell)\\ \#S\cap T\leq 1}} D_S\prod_{\substack{S\in\mathcal{P}_{\geq 2}(\ell)\\ \#S\cap T\geq 2}} D_S^{-2/\ell} \\ &= \prod_{S\in\mathcal{P}_{\geq 1}(\ell)} D_S^{-\alpha_T(S)}, \quad (4.66)\end{aligned}$$

where

$$\alpha_T(S) = \begin{cases} 0 & \text{if } \#S=1,\\ 2\#S-3 & \text{if } \#S\geq 2,\ \#S\cap T\leq 1,\\ 2\#(S\setminus T)+2/\ell & \text{if } \#S\geq 2,\ \#S\cap T\geq 2.\end{cases}$$

By (4.66) and $\ell\geq 2$, we obtain

$$\Phi_T(\mathbf{D}) \ll_\ell \prod_{S\in\mathcal{P}_{\geq 2}(\ell)} D_S^{-2/\ell}.$$

By injecting it in (4.65), we complete the proof of Lemma 4.4.2. □

4.5 Proof of Theorem 4.1.6

We have (see (4.39))

$$\mathfrak{C}_\ell(Y;q) := \sum_{\substack{r_1=1\\(r_1,q)=1}}^{\infty}\dots\sum_{\substack{r_\ell=1\\(r_\ell,q)=1}}^{\infty}\frac{\mu(r_1)\dots\mu(r_\ell)}{\mathrm{lcm}[\mathbf{r}]^2}E_\ell(Y;\mathbf{r}).$$

Using total decomposition sets (see Lemma 4.3.2 and Remark 4.3.1 following it), we can write it as

$$\mathfrak{C}_\ell(Y;q)=\sum_{\mathbf{d}\in\mathfrak{X}_\ell\langle q\rangle}\frac{\prod_{S\in\mathcal{P}_{\geq 1}(\ell)}\mu(d_S)^{\#S}}{\prod_{S\in\mathcal{P}_{\geq 1}(\ell)}d_S^2}E_\ell(Y;\mathbf{r}(\mathbf{d})), \tag{4.67}$$

where

$$\mathfrak{X}_\ell\langle q\rangle:=\left\{\mathbf{d}\in\mathbb{Z}_{>0}^{\mathcal{P}_{\geq 1}(\ell)};d_S \text{ pairwise coprime}, (d_S,q)=1 \text{ for all } S\in\mathcal{P}_{\geq 1}(\ell)\right\}.$$

and $\mathbf{r}(\mathbf{d})$ is as in (4.55).

For every $\mathbf{d}\in\mathbb{Z}_{>0}^{\mathcal{P}_{\geq 1}(\ell)}$, we define $N_2(\mathbf{d}):=\prod_{S\in\mathcal{P}_{\geq 2}(\ell)}d_S$. We break up the sum in the right-hand side of (4.67) according to the size of $N_2(\mathbf{d})$. Let $\Delta\leq Y^{2^\ell}$ to be chosen optimally later. Then we have

$$\begin{aligned}\mathfrak{C}_\ell(Y;q)&\leq\left(\sum_{\substack{\mathbf{d}\in\mathfrak{X}_\ell\langle q\rangle\\ N_2(\mathbf{d})\leq\Delta}}+\sum_{\substack{\mathbf{d}\in\mathfrak{X}_\ell\langle q\rangle\\ N_2(\mathbf{d})>\Delta}}\right)\frac{|E_\ell(Y;\mathbf{r}(\mathbf{d}))|}{\prod_{S\in\mathcal{P}_{\geq 1}(\ell)}d_S^2}\\&=:S_{\leq\Delta}+S_{>\Delta},\end{aligned} \tag{4.68}$$

say.

4.5.1 Study of $S_{\leq\Delta}$

We use Lemma 4.4.1, giving

$$\begin{aligned}S_{\leq\Delta}&\leq\sum_{\substack{\mathbf{d}\in\mathfrak{X}_\ell\langle q\rangle\\ N_2(\mathbf{d})\leq\Delta}}\frac{1}{\prod_{j\in[\ell]}d_{\{j\}}^2}\\&\leq\sum_{e_1=1}^{\infty}\cdots\sum_{e_\ell=1}^{\infty}\frac{1}{e_1^2\dots e_\ell^2}\sum_{n\leq\Delta}\tau_{2^\ell-\ell-1}(n)\\&\ll_{\ell,\epsilon}\Delta^{1+\epsilon},\end{aligned} \tag{4.69}$$

where, in the second line, we made the change of variables $n=N_2(\mathbf{d})$, and $e_j=d_{\{j\}}$.

4.5.2 Study of $S_{>\Delta}$

By Proposition 4.3.8, we have

$$\begin{aligned} S_{>\Delta} &= \sum_{\substack{\mathbf{d}\in\mathfrak{X}_\ell\langle q\rangle \\ N_2(\mathbf{d})>\Delta}} \frac{|E_\ell^*(Y;\mathbf{r}(\mathbf{d}))|}{\prod_{S\in\mathcal{P}_{\geq 1}(\ell)} d_S^2} + O_\ell\left(Y^{\ell-2}\sum_{\substack{\mathbf{d}\in\mathfrak{X}_\ell\langle q\rangle \\ N_2(\mathbf{d})>\Delta}} 1\right) \\ &\leq \Delta^{-2}\sum_{\substack{\mathbf{d}\in\mathfrak{X}_\ell\langle q\rangle \\ N_2(\mathbf{d})>\Delta}} |E_\ell^*(Y;\mathbf{r}(\mathbf{d}))| + O_\ell\left(Y^{\ell-2}\sum_{e_1=1}^{\infty}\cdots\sum_{e_\ell=1}^{\infty}\frac{1}{e_1^2\dots e_\ell^2}\sum_{n>\Delta}\frac{\tau_{2^\ell-\ell-1}(n)}{n^2}\right) \\ &= T_\Delta + O_{\epsilon,\ell}\left(Y^{\ell-2}\Delta^{-1+\epsilon}\right), \end{aligned} \tag{4.70}$$

say.

Note that whenever $E_\ell^*(Y;\mathbf{r}(\mathbf{d}))\neq 0$, then for every $S\in\mathcal{P}_{\geq 2}(\ell)$, there are distinct h, h' such that

$$h,h'\in(-u,Y-u] \text{ and } d_S^2 \mid h-h'.$$

Hence $d_S<\sqrt{Y}$, for every $S\in\mathcal{P}_{\geq 2}(\ell)$. By dyadic decomposition, there exists $\mathbf{D}=(D_S)_{S\in\mathcal{P}_{\geq 2}(\ell)}$, such that $1\leq D_S\leq\sqrt{Y}$ for every $S\in\mathcal{P}_{\geq 2}(\ell)$, satisfying

$$\prod_{S\in\mathcal{P}_{\geq 2}(\ell)} D_S \gg_\ell \Delta,$$

and

$$T_\Delta \ll_{\epsilon,\ell} Y^\epsilon\Delta^{-2}\sum_{e_1=1}^{\infty}\cdots\sum_{e_\ell=1}^{\infty}\frac{1}{e_1^2\dots e_\ell^2}S(Y;\mathbf{D},\mathbf{e}), \tag{4.71}$$

where $S(Y;\mathbf{D},\mathbf{e})$ is as in (4.56), where $\epsilon>0$ is arbitrary.

By Lemma 4.4.2, we deduce from (4.71)

$$T_\Delta \ll_{\epsilon,\ell} Y^{\ell+\epsilon}\Delta^{-2-\frac{2}{\ell}}.$$

Replacing it in (4.70), we obtain an upper bound for $S_{>\Delta}$:

$$S_{>\Delta} \ll_{\epsilon,\ell} Y^{\ell+\epsilon}\Delta^{-2-\frac{2}{\ell}} + Y^{\ell-2}\Delta^{-1+\epsilon}. \tag{4.72}$$

Gathering (4.68), (4.69) and (4.72), we deduce the inequality

$$\mathfrak{C}_\ell(Y;q) \ll_{\epsilon,\ell} \Delta^{1+\epsilon} + Y^{\ell+\epsilon}\Delta^{-2-\frac{2}{\ell}} + Y^{\ell-2}\Delta^{-1+\epsilon}. \tag{4.73}$$

Theorem 4.1.6 now follows from (4.73) and the optimal choice $\Delta = Y^{\max\left(\frac{\ell^2}{3\ell+2},\frac{\ell-2}{2}\right)}$.

4.6 Counting tuples of squarefree numbers

In this section we study the following generalization of $S(x;\mathbf{h})$ (see (4.2))

$$S(X_1,X_2,q;\mathbf{h})=\sum_{\substack{X_1<n\leq X_2\\(n,q)=1}}\mu^2(n+h_1q)\mu^2(n+h_1q)\dots\mu^2(n+h_jq), \tag{4.74}$$

for an $j-$tuple of integers $\mathbf{h}=(h_1,\dots,h_j)$ and a positive integer q such that $X_1+h_iq\geq 0,\ i=1,\dots,j$. Sums of this type were vastly studied in the past, although, in general, the condition $(n,q)=1$ was not taken into account. For example, we mention the articles by Mirsky [29], Tsang [37] and, more recently, Reuss [35]. The result from [35] allows to obtain quite small error terms but not assuring uniformity relatively to $\max(h_1q,\dots,h_jq)$, which is essential here. We will content ourselves with a more modest result (with a larger error term), but that will be enough for our purposes. The main theorem of this section is the following

Theorem 4.6.1. *For every $\epsilon>0$, for every $j\geq 1$, we have the equality*

$$S(X_1,X_2,q;\mathbf{h})=\frac{\varphi(q)}{q}A_q(\mathbf{h})(X_2-X_1)+O_{\epsilon,j}\left(\max_{1\leq i\leq j}(X_2+h_iq)^{\frac{j}{j+1}+\epsilon}\right), \tag{4.75}$$

for every X_1,X_2 such that $0\leq X_1<X_2$, every $j-$tuple of integers $\mathbf{h}=(h_1,\dots,h_j)$, and every positive integer q such that $q\geq 1$ such that $X_1+h_iq\geq 0,\ i=1,\dots,j$, where $S(X_1,X_2,q;\mathbf{h})$ is as in (4.74) and $A_q(\mathbf{h})$ is as in (4.27).

Remark 4.6.1. A better error term at this point would reflect in a larger value for δ_ℓ (see (4.17)), but would not help to improve the exponent on Theorem 4.1.1.

Démonstration. We start by defining, as in [35] and [37], some functions related to squarefree numbers and the sum we are interested in.
Let

$$\sigma(n):=\prod_{p^2|n}p,\ \ n\neq 0,$$

and

$$\xi(n)=\prod_{1\leq i\leq j}\sigma(n+h_iq). \tag{4.76}$$

Notice that the right-hand side of equation (4.76) above actually depends on $\mathbf{h}$ and q. But since these numbers will be held fixed in the following calculation, we omit this dependency.
Since

$$\prod_{1\leq i\leq j}\mu^2(n+h_iq)=1\iff\xi(n)=1,$$

we have

$$S(X_1,X_2,q;\mathbf{h})=\sum_{\substack{X_1<n\leq X_2\\(n,q)=1}}\sum_{d|\xi(n)}\mu(d)=\sum_{\substack{d\geq 1\\(d,q)=1}}\mu(d)N_d(X_1,X_2,q;\mathbf{h}), \tag{4.77}$$

where

$$N_d(X_1,X_2,q;\mathbf{h})=\{X_1<n\leq X_2;(n,q)=1\text{ and }\xi(n)\equiv 0\pmod d\}.$$

This is the point when the quantity $u_p(\mathbf{h})$ (defined in (4.5)) makes its first appearance. Once again for simplificity, we write u_p instead of $u_p(\mathbf{h})$. Notice that, for p coprime with q, the congruence

$$\xi(n) \equiv 0 \pmod{p}$$

has exactly u_p solutions modulo p^2. Therefore, by the Chinese remainder theorem, the congruence

$$\xi(n) \equiv 0 \pmod{d}$$

has

$$U_d := \prod_{p|d} u_p$$

solutions (mod d^2), for d squarefree, $(d,q)=1$. A simple consequence of this remark is that

$$N_d(X_1, X_2, q; \mathbf{h}) := \frac{\varphi(q)}{q}\frac{U_d}{d^2}(X_2 - X_1) + O(\tau(q)U_d) \tag{4.78}$$

uniformly for $0 \le X_1 < X_2$ and d squarefree, $(d,q)=1$.

Now we break up (4.77) relatively to the possible values of d

$$S(X_1, X_2, q; \mathbf{h}) = S_1 + S_2, \tag{4.79}$$

where

$$\begin{cases} S_1 = \displaystyle\sum_{\substack{1\le d\le y\\(d,q)=1}} \mu(d) N_d(X_1, X_2, q; \mathbf{h}), \\ \\ S_2 = \displaystyle\sum_{\substack{y< d\le X\\(d,q)=1}} \mu(d) N_d(X_1, X_2, q; \mathbf{h}), \end{cases} \tag{4.80}$$

where $X := \max_{1\le i\le j}(X_2 + h_i q)$ and y is a parameter to be chosen later depending on X.
For S_1, a direct application of (4.78) gives

$$\begin{aligned} S_1 &= \sum_{1\le d\le y} \mu(d)\left(\frac{\varphi(q)}{q}\frac{U_d}{d^2}(X_2 - X_1) + O(\tau(q)U_d)\right) \\ &= \frac{\varphi(q)}{q}(X_2 - X_1)\sum_{\substack{d\ge 1\\(d,q)=1}} \frac{\mu(d)U_d}{d^2} + O\left(X\sum_{d>y}\frac{U_d}{d^2} + \sum_{d\le y}\tau(q)U_d\right) \\ &= \frac{\varphi(q)}{q}A_q(\mathbf{h})(X_2 - X_1) + O_{\epsilon,j}(Xy^{-1+\epsilon} + \tau(q)y^{1+\epsilon}), \end{aligned} \tag{4.81}$$

where in the last line we use that $U_d = \prod_{p|d} u_p \le j^{\omega(d)}$.
For large values of d, formula (4.78) is not as meaningful. We look rather for an upper bound

of the term S_2 that will permit us to obtain (4.75). For each d squarefree such that $d \mid \xi(n)$, we decompose d as

$$d = \prod_{1 \leq i \leq j} d_i,$$

where $d_1, \dots, d_j$ are such that

$$d_i^2 \mid n + h_i q,\ 1 \leq i \leq j.$$

Remark that the decomposition above is not in general unique. Furthermore since d is squarefree, the d_i are pairwise coprime. By dyadic decomposition, one can find $1 \leq D_1, \dots, D_j \leq \sqrt{X}$ such that $D_1 \cdots D_j \geq y$ and

$$|S_2| \leq \sum_{y < d \leq X} \left| N_d(X_1, X_2, q; \mathbf{h}) \mu^2(d) \right| \leq \mathcal{N}(D_1, \dots, D_j) \log(2X)^j, \tag{4.82}$$

where

$$\mathcal{N}(D_1, \dots, D_j) = \#\{(d_i, u_i)_{1 \leq i \leq j}; d_i \sim D_i,\ d_i \text{ pairwise coprime}, \\ X_1 < d_1^2 u_1 - h_1 q = \cdots = d_j^2 u_j - h_j q \leq X_2\}.$$

We need to give an upper bound for $\mathcal{N}(D_1, \dots, D_j)$. We start by noticing that we can forget about the variables (d_i, u_i), for $i \geq 3$ at the cost of introducing some divisor function. That is

$$\mathcal{N}(D_1, \dots, D_j) \ll_{\epsilon, j} X^{\epsilon} \mathcal{N}(D_1, D_2), \tag{4.83}$$

where $\mathcal{N}(D_1, D_2)$ is defined similarly to $\mathcal{N}(D_1, \dots, D_j)$. It is clear from the formula above that any u_1 counted above must satisfy

$$1 \leq u_1 \leq \frac{X}{D_1^2}.$$

Thus we have the inequality

$$\mathcal{N}(D_1, D_2) \leq \sum_{d_2 \sim D_2} \sum_{u_1 \leq \frac{X}{D_1^2}} \sum_{\substack{d_1 \sim D_1 \\ d_1^2 u_1 \equiv (h_1 - h_2) q \pmod{d_2^2} \\ (d_1, d_2) = 1}} 1. \tag{4.84}$$

For each $d_2 \sim D_2$, let $g = (d_2^2, (h_1 - h_2)q)$. We write

$$d_2^2 = gz,\ (h_1 - h_2)q = gw.$$

Since $(d_1, d_2) = 1$, the congruence $d_1^2 u_1 \equiv (h_1 - h_2)q \pmod{d_2^2}$ implies $g \mid u_1$. So we write

$$u_1 = gv,$$

and the congruence $d_1^2 u_1 \equiv (h_1 - h_2)q \pmod{d_2^2}$ becomes

$$d_1^2 v \equiv w \pmod{z}.$$

Since $(z, w) = 1$, this congruence has at most $2.2^{\omega(z)} \leq 2\tau(d_2)$ solutions in $d_1 \pmod{z}$. Therefore we have

$$\begin{aligned}\mathcal{N}(D_1,D_2) &\leq \sum_{d_2\sim D_2}\sum_{g|d_2^2}\sum_{v\leq \frac{X}{D_1^2 g}}\sum_{\substack{d_1\sim D_1\\ d_1^2 v\equiv w \pmod z}} 1\\ &\leq 2\sum_{d_2\sim D_2}\sum_{g|d_2^2}\frac{X}{D_1^2 g}\left(\frac{D_1}{z}+1\right)\tau(d_2)\\ &\ll_\epsilon X^\epsilon \sum_{d_2\sim D_2}\frac{X}{D_1^2}\left(\frac{D_1}{d_2^2}+1\right)\\ &\ll X^\epsilon\left(\frac{X}{D_1D_2}+\frac{XD_2}{D_1^2}\right).\end{aligned}$$

As a consequence of (4.83), we deduce

$$\mathcal{N}(D_1,\dots,D_j)\ll_{\epsilon,j} X^\epsilon\left(\frac{X}{D_1D_2}+\frac{XD_2}{D_1^2}\right). \tag{4.85}$$

By a completely similar argument, we have the same result for any pair (D_i,D_j) instead of (D_1,D_2). Thus we can suppose

$$D_1\geq D_2\geq D_i,\ \text{for all } i\geq 3. \tag{4.86}$$

The inequality $D_1\cdots D_j>y$ and (4.86) imply

$$D_1^2D_2^{-1}>y^{\frac{1}{j}}\ \text{and}\ D_1D_2>y^{\frac{2}{j}}.$$

Therefore (4.85) implies

$$\mathcal{N}(D_1,\dots,D_j)\ll_{\epsilon,j} X^{1+\epsilon}y^{-\frac{1}{j}}.$$

Finally, from (4.82), we have

$$S_2\ll_{\epsilon,j} X^{1+\epsilon}y^{-\frac{1}{j}}. \tag{4.87}$$

By (4.81), (4.87) and (4.79) we obtain the equality

$$S(X_1,X_2,q;\mathbf{h})=\frac{\varphi(q)}{q}A_q(\mathbf{h})(X_2-X_1)+O_\epsilon\left(Xy^{-1+\epsilon}+\tau(q)y^{1+\epsilon}+X^{1+\epsilon}y^{-\frac{1}{j}}\right).$$

We make the choice $y=X^{\frac{j}{j+1}}$ in the equation above and establish the equality (4.75). This concludes the proof of Theorem 4.6.1. □

4.7 Proofs of Corollaries 4.1.2 and 4.1.7

Let $0<k\leq x$, k integer. We develop $\mathfrak{M}_\ell(x,k)$ (see (4.1)) as follows

$$\begin{aligned}\mathfrak{M}_\ell(x;k)&=\sum_{n\leq x}\left(\sum_{0\leq h\leq k}\mu^2(n+h)-\frac{6}{\pi^2}k\right)^\ell\\ &=\sum_{j=0}^{\ell}\binom{\ell}{j}\left(-\frac{6}{\pi^2}k\right)^{\ell-j}\sum_{0\leq h_1,\dots,h_j<k}\dots\sum S(0,x,1;\mathbf{h}).\end{aligned} \tag{4.88}$$

where $\mathbf{h} = (h_1, \dots, h_j)$ and $S(0, x, 1; \mathbf{h})$ is as in (4.74). It follows from Theorem 4.6.1 that the sum over the $h_1, \dots, h_j$ equals (cf. definition (4.8))

$$\mathfrak{B}_j(k)x + O_{\epsilon,\ell}\left(k^j x^{\frac{j}{j+1}+\epsilon}\right).$$

By formula (4.88), we obtain the equality

$$\mathfrak{M}_\ell(x;k) = \mathfrak{C}_\ell(k)x + O_{\epsilon,\ell}\left(k^\ell x^{\frac{\ell}{\ell+1}+\epsilon}\right), \tag{4.89}$$

where $\mathfrak{C}_\ell(k)$ is defined in (4.7). Corollary 4.1.2 is now a simple consequence of Theorem 4.1.1 and equation (4.89) above.

Corollary 4.1.7 follows in a much similar fashion. We start, as before, by expanding $\mathcal{M}(X, q; \ell)$ (see (4.22)). We obtain the formula

$$\begin{aligned}\mathcal{M}(X,q;\ell) &= \sum_{j=0}^{\ell}\binom{\ell}{j}\left(-A_q\frac{X}{q}\right)^{\ell-j}\sum_{0<n_1,\dots,n_j\le X}\cdots\sum_{\substack{n_1\equiv\dots\equiv n_j \pmod q\\(n_j,q)=1}}\mu^2(n_1)\dots\mu^2(n_j)\\ &= \sum_{j=0}^{\ell}\binom{\ell}{j}\left(-A_q\frac{X}{q}\right)^{\ell-j}\mathcal{S}_j(X;q),\end{aligned} \tag{4.90}$$

say.

We make the change of variables $n_j = n$ and $n_i = n_j + f_i q$, for $i = 1, \dots, j-1$. Thus, we are allowed to write

$$\mathcal{S}_j(X;q) = \sum_{-\frac{X}{q}\le f_1,\dots,f_{j-1}\le\frac{X}{q}}\cdots\sum\sum_{\substack{n\in I(X,q;\mathbf{f},0)\\(n,q)=1}}\mu^2(n+f_1q)\dots\mu^2(n+f_{j-1}q)\mu^2(n), \tag{4.91}$$

where for every $j-$tuple of integers $\mathbf{h} = (h_1, \dots, h_j)$, we write

$$I(X,q;\mathbf{h}) := \bigcap_{i=1}^{j}(-h_iq, X - h_iq].$$

Note that whenever $I(X, q; \mathbf{h}) \neq \emptyset$, we have $I(X, q; \mathbf{h}) = (X_1, X_2]$, where X_1, X_2 are real numbers satisfying

$$0 \le X_1 + h_iq < X_2 + h_iq \le X,\ i = 1, \dots, j.$$

Hence, we may use Theorem 4.6.1 for the inner sum on the right-hand side of (4.91). After summing over $f_1, \dots, f_{j-1}$, we see that

$$\begin{aligned}\mathcal{S}_j(X;q) &= \sum_{-\frac{X}{q}\le f_1,\dots,f_{j-1}\le\frac{X}{q}}\cdots\sum\left(\frac{\varphi(q)}{q}A_q(\mathbf{f},0)\,|I(X,q;\mathbf{f},0)| + O_{\epsilon,\ell}\left(X^{\frac{j}{j+1}+\epsilon}\right)\right)\\ &= \frac{\varphi(q)}{q}\sum_{\mathbf{f}\in\mathbb{Z}^{j-1}}A_q(\mathbf{f},0)\,|I(X,q;\mathbf{f},0)| + O_{\epsilon,\ell}\left(X^{\frac{j}{j+1}+\epsilon}\left(\frac{X}{q}\right)^{j-1}\right),\end{aligned} \tag{4.92}$$

where, in the second line, we observed that whenever $|f_i| > \frac{X}{q}$ for some $1 \leq i \leq j-1$, then $|I(X,q;\mathbf{f},0)| = 0$.

In what follows next, we evaluate the sum over the f_i above. To this purpose we have the following :

Lemma 4.7.1. *With the above notation, and $\mathfrak{B}_j$ as defined in* (4.26)*, we have for every $X > 0$ and every integer q, the inequality*

$$\sum_{\mathbf{f}\in\mathbb{Z}^{\ell-1}} A_q(\mathbf{f},0)\,|I(X,q;\mathbf{f},0)| = q\mathfrak{B}_j\left(\frac{X}{q};q\right).$$

Démonstration. We first notice that

$$\begin{aligned}
|I(X,q;\mathbf{f},0)| &= \int_{-\infty}^{+\infty} \chi_{(0,X]}(v)\prod_{i=1}^{j-1}\chi_{(-f_iq,X-f_iq]}(v)dv \\
&= q\sum_{f=-\infty}^{\infty}\int_0^1 \chi_{(0,X]}(qu+qf)\prod_{i=1}^{j-1}\chi_{(-f_iq,X-f_iq]}(qu+qf)\,du \\
&= q\sum_{f=-\infty}^{\infty}\int_0^1 \chi_{(-f,\frac{X}{q}-f]}(u)\prod_{i=1}^{j-1}\chi_{\left(-f-f_i,\frac{X}{q}-f-f_i\right]}(u)\,du, \qquad (4.93)
\end{aligned}$$

where for each measurable set $A \subset \mathbb{R}$, χ_A denotes its characteristic function and in the second line we made the change of variables $v = qu + qf$, where $u \in (0,1]$ and $f \in \mathbb{Z}$. Summing over $f_1,\ldots,f_{j-1}$ and making the change of variables

$$\begin{cases} h_i = f + f_i, 1 \leq i \leq j-1, \\ h_j = f, \end{cases}$$

we obtain, since $A_q(\mathbf{f},0) = A_q(\mathbf{h})$ (recall (4.27)),

$$\begin{aligned}
\sum_{\mathbf{f}\in\mathbb{Z}^{j-1}} A_q(\mathbf{f},0)\,|I(X,q;\mathbf{f},0)| &= q\sum_{\mathbf{h}\in\mathbb{Z}^j} A_q(\mathbf{h})\int_0^1\prod_{i=1}^{j}\chi_{(-h_i,\frac{X}{q}-h_i]}(u)\,du \\
&= q\sum_{\mathbf{h}\in\mathbb{Z}^j} A_q(\mathbf{h})\int_0^1\prod_{i=1}^{j}\chi_{(-u,\frac{X}{q}-u]}(h_i)\,du.
\end{aligned}$$

Finally, by interchanging the order of summation and integration, we see that

$$\sum_{\mathbf{f}\in\mathbb{Z}^{j-1}} A_q(\mathbf{f},0)\,|I(X,q;\mathbf{f},0)| = q\int_0^1 \sum_{-u<h_1,\ldots,h_j\leq Y-u}\cdots\sum A_q(\mathbf{h})du,$$

which concludes the proof of Lemma 4.7.1. □

Now, Lemma 4.7.1 when applied in (4.92) gives the equality

$$\mathcal{S}_j(X;q) = \varphi(q)\mathfrak{B}_j\left(\frac{X}{q};q\right) + O_{\epsilon,\ell}\left(X^{\frac{j}{j+1}+\epsilon}\left(\frac{X}{q}\right)^{j-1}\right). \tag{4.94}$$

Thus, by replacing (4.94) in (4.90) one obtains (recall (4.25))

$$\mathcal{M}(X,q;\ell) = \varphi(q)\mathfrak{C}_\ell\left(\frac{X}{q};q\right) + O_{\epsilon,\ell}\left(X^{\frac{\ell}{\ell+1}+\epsilon}\left(\frac{X}{q}\right)^{\ell-1}\right). \tag{4.95}$$

Corollary 4.1.7 now follows from Theorem 4.1.6 and equation (4.95) above.

Bibliographie

[1] W. D. Banks, R. Heath-Brown, and I. E. Shparlinski. On the average value of divisor sums in arithmetic progressions. *Int. Math. Res. Not.*, (1) :1–25, 2005.

[2] V. Blomer. The average value of divisor sums in arithmetic progressions. *Q. J. Math.*, **59**(3) :275–286, 2008.

[3] J. Bourgain. More on the sum-product phenomenon in prime fields and its applications. *Int. J. Number Theory*, **1**(1) :1–32, 2005.

[4] J. Bourgain. A remark on solutions of the Pell equation. *Int. Math. Res. Not.*, page rnu023, 2014.

[5] J. Bourgain and M. Z. Garaev. Sumsets of reciprocals in prime fields and multilinear Kloosterman sums. *Izv. Math. 78 (2014), no. 4, 656-707.*

[6] J. Brüdern, A. Granville, A. Perelli, R. C. Vaughan, and T. D. Wooley. On the exponential sum over k-free numbers. *R. Soc. Lond. Philos. Trans. Ser. A Math. Phys. Eng. Sci.*, **356**(1738) :739–761, 1998.

[7] M. J. Croft. Square-free numbers in arithmetic progressions. *Proc. London Math. Soc. (3)*, **30** :143–159, 1975.

[8] É. Fouvry. On the size of the fundamental solution of the Pell equation. *J. Reine Angew. Math.*, to appear.

[9] É. Fouvry, S. Ganguly, E. Kowalski, and Ph. Michel. Gaussian distribution for the divisor function and Hecke eigenvalues in arithmetic progressions. *Comment. Math. Helv.*, **89**(4) :979–1014, 2014.

[10] É. Fouvry and H. Iwaniec. On a theorem of Bombieri-Vinogradov type. *Mathematika*, **27**(2) :135–152, 1980.

[11] É. Fouvry, E. Kowalski, and Ph. Michel. Algebraic trace functions over the primes. *Duke Math. J.*, **163**(9) :1683–1736, 2014.

[12] É. Fouvry, E. Kowalski, and Ph. Michel. On the exponent of distribution of the ternary divisor function. *Mathematika*, **61** :121–144, 1 2015.

[13] É. Fouvry and Ph. Michel. Sur certaines sommes d'exponentielles sur les nombres premiers. *Ann. Sci. École Norm. Sup. (4)*, **31**(1) :93–130, 1998.

[14] J. B. Friedlander and A. Granville. Limitations to the equi-distribution of primes. I. *Ann. of Math. (2)*, **129**(2) :363–382, 1989.

[15] J. B. Friedlander and H. Iwaniec. The divisor problem for arithmetic progressions. *Acta Arith.*, **45**(3) :273–277, 1985.

[16] J. B. Friedlander and H. Iwaniec. Incomplete Kloosterman sums and a divisor problem. *Ann. of Math. (2)*, **121**(2) :319–350, 1985. With an appendix by Bryan J. Birch and Enrico Bombieri.

[17] J. B. Friedlander and H. Iwaniec. *Opera de cribro*, volume **57** of *American Mathematical Society Colloquium Publications*. American Mathematical Society, Providence, RI, 2010.

[18] R. R. Hall. Squarefree numbers on short intervals. *Mathematika*, **29**(1) :7–17, 1982.

[19] R. R. Hall. The distribution of squarefree numbers. *J. Reine Angew. Math.*, **394** :107–117, 1989.

[20] G. H. Hardy and E. M. Wright. *An introduction to the theory of numbers*. Oxford University Press, Oxford, sixth edition, 2008. Revised by D. R. Heath-Brown and J. H. Silverman, with a foreword by Andrew Wiles.

[21] D. R. Heath-Brown. The least square-free number in an arithmetic progression. *J. Reine Angew. Math.*, **332** :204–220, 1982.

[22] D. R. Heath-Brown. The square sieve and consecutive square-free numbers. *Math. Ann.*, **266**(3) :251–259, 1984.

[23] C. Hooley. A note on square-free numbers in arithmetic progressions. *Bull. London Math. Soc.*, **7** :133–138, 1975.

[24] C. H. Jia. The distribution of squarefree numbers. *Beijing Daxue Xuebao*, (3) :21–27, 1987.

[25] A. A. Karatsuba. The distribution of inverses in a residue ring modulo a given modulus. *Russian Academy of Sciences-Doklady Mathematics-AMS Translation*, **48**(3) :452–454, 1994.

[26] E. Kowalski and G. Ricotta. Fourier coefficients of $GL(N)$ automorphic forms in arithmetic progressions. *Geom. Funct. Anal.*, **24**(4) :1229–1297, 2014.

[27] Y.-K. Lau and L. Zhao. On a variance of Hecke eigenvalues in arithmetic progressions. *J. Number Theory*, **132**(5) :869–887, 2012.

[28] P. Le Boudec. On the distribution of squarefree integers in arithmetic progressions. *preprint arXiv :1411.2360*, 2014.

[29] L. Mirsky. Arithmetical pattern problems relating to divisibility by rth powers. *Proc. London Math. Soc. (2)*, **50** :497–508, 1949.

[30] H. L. Montgomery. Primes in arithmetic progressions. *Michigan Math. J.*, **1** :33–39, 1970.

[31] H. L. Montgomery. *Topics in multiplicative number theory*. Lecture Notes in Mathematics, Vol. **227**. Springer-Verlag, Berlin-New York, 1971.

[32] H. L. Montgomery and R. C. Vaughan. On the distribution of reduced residues. *Ann. of Math. (2)*, **123**(2) :311–333, 1986.

[33] R. M. Nunes. Squarefree numbers in arithmetic progressions. *J. Number Theory*, **153** :1–36, 2015.

[34] K. Prachar. Über die kleinste quadratfreie Zahl einer arithmetischen Reihe. *Monatsh. Math.*, **62** :173–176, 1958. (German).

[35] T. Reuss. Pairs of k-free numbers, consecutive square-full numbers. *preprint arXiv :1212.3150*, 2012.

[36] E. C. Titchmarsh. *The theory of the Riemann zeta-function.* The Clarendon Press, Oxford University Press, New York, second edition, 1986. Edited and with a preface by D. R. Heath-Brown.

[37] K.-M. Tsang. The distribution of r-tuples of square-free numbers. *Mathematika*, **32**(02) :265–275, 1985.

[38] P. Turán. Über die Primzahlen der arithmetischen Progression. *Acta Litt. Sci. Szeged*, **8** :226–235, 1937. (German).

[39] R. C. Vaughan. A variance for k-free numbers in arithmetic progressions. *Proc. London Math. Soc. (3)*, **91**(3) :573–597, 2005.

[40] R. Warlimont. Squarefree numbers in arithmetic progressions. *J. London Math. Soc. (2)*, **22**(1) :21–24, 1980.