CECILE DARTYGE

Propriétés multiplicatives des valeurs de certains polynômes, 1994

ORSAY
n° d'ordre :

63618

UNIVERSITÉ de PARIS–SUD
Centre d'ORSAY

THÈSE

présentée

pour obtenir

le grade de Docteur en Sciences
de l'Université Paris XI Orsay
Spécialité : Mathématiques

par

Cécile DARTYGE

Sujet : **Propriétés multiplicatives des valeurs de certains polynômes**

soutenue le : 9 décembre 1994 devant la Commission d'examen

Renée ELKIK Présidente
Jörg BRÜDERN
Hedi DABOUSSI
Jean-Marc DESHOUILLERS
Etienne FOUVRY
Jean-Louis NICOLAS

Je désire tout d'abord exprimer mon admiration et ma plus profonde gratitude à Étienne Fouvry qui a dirigé cette thèse.
Durant ces trois années de recherche, j'ai énormément profité de la richesse de son savoir mathématique et de son enthousiasme très communicatif pour la théorie analytique des nombres.
Il a par ailleurs avec une patience infinie et une très grande disponibilité redressé de nombreuses démonstrations boîteuses et proposé des suggestions qui ont sensiblement amélioré la qualité et la portée d'importants passages de la thèse.

Renée Elkik m'a initiée à la géométrie algébrique et je la remercie d'avoir accepté de présider le jury.

Je suis très reconnaissante à Jörg Brüdern de l'intérêt qu'il a porté à ce travail, du temps qu'il m'a gentiment consacré, d'avoir accepté d'être rapporteur et de participer au jury.

Une part importante de mes connaissances en théorie analytique des nombres provient de cours donnés par Hedi Daboussi. Je le remercie d'avoir accepté de participer au jury.

Je remercie Jean-Marc Deshouillers, dont les travaux avec Henryk Iwaniec sur les sommes de Kloosterman, ont très fortement influencé l'élaboration de la première partie de la thèse, d'avoir accepté d'être rapporteur et de participer au jury de la thèse.

Je remercie également Jean-Louis Nicolas d'avoir accepté de faire partie du jury.

Je tiens enfin à remercier les doctorants d'Orsay pour leur accueil et leur amitié, notamment Marco Garuti, Philippe Michel et Daniel Naie, avec lesquels j'ai réalisé l'annexe B groupant les résultats de géométrie algébrique.

Je dédie cette thèse à ma famille, mes amis, et tout particulièrement à Magali Barale, Nathalie Biguenet, Frédéric-Maïkel Jourdan, et Hervé Levilain, pour leur soutien.

ABSTRACT

We study some multiplicative properties of the values taken by polynomials in $\mathbf{Z}[x_1, ..., x_n]$. The first part deals with the particular polynomials n^2+1, n^3+2. We show that for $\alpha < 1/12.2$, we can find $h > 0$ so that there is a positive proportion of integers n having no prime divisor less than n^α, and so that the greatest prime divisor of n^2+1 is greater than n^{1+h}. Another result is that for $\beta < 149/179$, there exists a positive proportion of integers n, so that all prime factors of n^2+1 are less than n^β. We give another results for the polynomial n^3+2 based on Hooley's work on this subject.

The second part deals with polynomials in $\mathbf{Z}[x_1, ..., x_n]$, with $n \geq 2$. When $n = 2$, and the degree of f is 2 or 3, we obtain significative lower bounds for the greatest prime factor of $f(p_1, p_2)$, for a positive proportion of (p_1, p_2). This improves and generalises a previous work of Plaksin. The same type of minorations are obtained for polynomials $f(p_1, p_2, n_3)$, where degree of f is 3, and for the polynomial $f(p_1, p_2, n_3, n_4) = 1 + p_1^4 + p_2^4 + n_3^5 + n_4^6$. The proof of all these results follows the Tchebychev-Hooley method. We use classical results concerning arithmetic progressions, sieve methods, and upper bounds of exponential sums in finite fields. Another application of these upper bounds, it is the study of $\omega(f(p_1, p_2))$, the number of distinct prime factors of $f(p_1, p_2)$. We show that $\omega(f(p_1, p_2)) < 6d/7 + 5.28..$, for an infinity of (p_1, p_2), d being the degree of f. When $d > 30$, this result improves a previous work of Greaves.

NOTATIONS

Les variables ε, et parfois η, et h avec ou sans indice sont des réels positifs arbitrairement petits qui ne sont pas toujours les mêmes à chaque occurrence.

La lettre p avec ou sans indice, désigne un nombre premier, et P_r représente un entier ayant au plus r facteurs premiers.

On utilise encore les notations suivantes :

- $P(z) = \prod_{p<z} p$,
- $e(x) = \exp(2i\pi x)$,
- $n \sim N$ pour $N \leq n \leq 2N$, parfois cette notation aura un sens plus large : $AN \leq n \leq BN$,
- $[n]$ est la partie entière de n,
- $\|t\|$ est la distance du réel t à l'entier le plus proche,
- $d|n$ signifie que d divise n, $d \not| n$ signifie que d ne divise pas n, et $p^\alpha \| n$ signifie que $p^\alpha | n$, mais que $p^{\alpha+1} \not| n$,
- $\tau(n)$ est le nombre de diviseurs de n,
- $\omega(n)$ et parfois $\nu(n)$ désignent le nombre de facteurs premiers distincts de n,
- $\Omega(n)$ désigne le nombre de facteurs premiers de n, comptés avec leur multiplicité,
- $P^+(n)$ désigne le plus grand facteur premier de n,
- $\varphi(n)$ est l'indicatrice d'Euler : $\varphi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right)$,
- $\mu(n)$ est la fonction de Möbius, elle est définie par :

$$\mu(n) = \begin{cases} (-1)^{\omega(n)} & \text{si } n \text{ est sans facteur carré,} \\ 0 & \text{sinon,} \end{cases}$$

- $a*b(n)$ est le produit de convolution de a et b et vaut $a*b(n) = \sum_{d|n} a(d)b(n/d)$,
- $x \ll_\varepsilon y$ indique qu'il existe une constante $K(\varepsilon) > 0$ telle que $|x| \leq K(\varepsilon)|y|$. On utilise encore la notation $x = O(y)$ pour signaler qu'il existe une constante $K > 0$ telle que $|x| \leq K|y|$,
- $\zeta(s)$ est la fonction ζ de Riemann,
- $L(s, \chi)$ est la série de Dirichlet associée au caractère χ.

TABLE DES MATIÈRES

INTRODUCTION

L'objet de cette thèse est d'étudier certaines propriétés multiplicatives des suites $f(n_1,...,n_k)$, où f est un polynôme à coefficients entiers.
La question phare est la suivante : pour quels $\lambda > 0$, existe-t-il une proportion positive de k-uplets $(n_1,...,n_k)$, avec $n_i \in [x,2x]$, pour $1 \leq i \leq k$, tels que $P^+(f(n_1,...,n_k)) > x^\lambda$, où on a noté $P^+(m)$ le plus grand facteur premier de m. On traite ici les cas où les entiers n_i sont supposés premiers ou presque premiers.
L'enjeu est d'obtenir une valeur de λ la plus grande possible et ainsi trouver une solution s'approchant le mieux du célèbre problème de théorie analytique des nombres suivant : existe-t-il un infinité de k-uplets $(n_1,...,n_k)$ tels que $f(n_1,...,n_k)$ soit un nombre premier ?

La méthode suivie pour aborder cette question est celle initiée par Tchebychev en 1895, puis développée tout au long du siècle par de nombreux mathématiciens. Dans cette thèse, nous profiterons tout particulièrement des innovations apportées par Hooley.

Cette méthode consiste à évaluer de deux manières différentes, lorsque x tend vers $+\infty$, la quantité $\log(V(x)) = \log\left(\prod_{x\leq n_i\leq 2x} f(n_1,...,n_k)\right)$.
La première estimation est obtenue directement en supposant que f soit positif et se comporte comme ses termes de plus haut degré, quand x tend vers $+\infty$. On a alors $\log(f(n_1,..,n_k)) = d\log x + O(1)$, d étant le degré de f.
En sommant ensuite cette égalité sur les n_i, et en utilisant le théorème des nombres premiers dans le cas où les n_i sont supposés premiers, on trouve très facilement cette première estimation.

La deuxième estimation dépend de P^+, le plus grand facteur premier cherché, et part de l'égalité :

$$\log(V(x)) = \sum_{p,\alpha} |\mathcal{A}_{p^\alpha}| \log p,$$

avec

$$\mathcal{A}_{p^\alpha} = \{(n_1,...,n_k),\ x \leq n_i \leq 2x,\quad f(n_1,...,n_k) \equiv 0 \ (\mathrm{mod}\, p^\alpha)\},$$

où la lettre p représente toujours un nombre premier.

Lorsque p^α est assez petit, inférieur à une certaine quantité D, qui correspond à la limite naturelle de répartition en moyenne dans les progressions arithmétiques, (D est de l'ordre de $x^{1/2-\epsilon}$, lorsque f est un polynôme en une variable et n_1 est supposé premier ou presque premier, dans les autres situations, on a $D = x^{1-\epsilon}$), les cardinaux $|\mathcal{A}_{p^\alpha}|$ sont évalués précisément : si les n_i parcourent la suite des entiers, on peut estimer les $|\mathcal{A}_{p^\alpha}|$ directement, sinon on utilise les résultats classiques de répartition en moyenne des nombres premiers dans les progressions arithmétiques du type le théorème de Bombieri-Vinogradov, ou le théorème de Barban-Davenport-Halberstam.

L'étape suivante consiste à montrer que les cardinaux $|\mathcal{A}_{p^\alpha}|$, avec $\alpha \geq 2$ sont négligeables.
Lorsque f est un polynôme du troisième degré, ceci n'est pas immédiat, et on a recours à des cribles appropriés, comme le crible à carrés de Heath-Brown, qui permettent de résoudre cette difficulté en faisant appel aux majorations de Hasse de sommes de caractères de Legendre le long de cubiques.

Le passage crucial de toutes les démonstrations est l'estimation des quantités $|\mathcal{A}_p|$ pour $p \geq D$, avec des méthodes de crible et de sommes d'exponentielles.

Lorsque les n_i sont supposés premiers ou presque premiers, le crible porte sur les produits $n_1 ... n_k$ et parfois il sera nécessaire d'appliquer des cribles simultanés sur les nombres $n_1 ... n_k$ et sur p. Autrement, si les n_i ne vérifient aucune condition spéciale, on crible seulement la variable p.
Tous ces cribles nécessitent une connaissance précise du cardinal des ensembles du type :

$$\mathcal{B}_m(a) = \big\{(n_1, ..., n_k),\ x \leq n_i \leq 2x,\ n_1 ... n_k \equiv 0 \,(\mathrm{mod}\, a),\ f(n_1, ..., n_k) \equiv 0 \,(\mathrm{mod}\, m)\big\}.$$

A cette fin, on traduit les conditions de congruences portant sur les k-uplets $n_1, ..., n_k$ appartenant aux ensembles $\mathcal{B}_m(a)$ en termes de sommes d'exponentielles, ce qui nous conduit à rechercher des majorations de sommes de la forme :

$$\sum_{M \leq m \leq 2M} \sum_{0 < |h_1|, ..., |h_k| < H} S_f(m, h_1, ..., h_k),$$

avec

$$S_f(m, h_1, ..., h_k) = \sum_{\substack{0 \leq u_1, ..., u_k < m \\ f(u_1, ..., u_k) \equiv 0 \ (\mathrm{mod}\, m)}} e\left(\frac{h_1 u_1 + ... + h_k u_k}{m}\right).$$

Lorsque f est un polynôme en une variable, $k = 1$, la somme $S(m, h)$ comporte au plus $(deg f)^{\omega(m)}$ termes, et on ne dispose pas de majoration directe suffisante.

Hooley, en profitant de la structure particulière des polynômes n^2+1 et n^3+2, et en procédant à d'astucieuses résolutions de congruences, puis en sommant sur la variable m, a fait apparaître des sommes de Kloosterman.
Dans le cas du polynôme n^2+1, ces sommes arrivent dans un contexte *agréable*, et Deshouillers et Iwaniec ont pu y appliquer les remarquables résultats de majorations en moyenne de ces sommes qu'ils avaient obtenus par le biais de la théorie des formes modulaires.

L'objet du théorème 1 de la première partie de ce travail, est alors d'adapter les travaux de Hooley sur n^2+1 à l'étude de $P^+(\tilde{n}^2+1)$ où $\tilde{n}$ est un entier presque premier.
Pour le polynôme n^3+2 les transformations de Hooley sont très compliquées : les sommes de Kloosterman vivent dans un cadre peu naturel et les majorations de Weil ne sont pas suffisantes ; ces sommes sont finalement majorées avec l'hypothèse R^* de majorations de sommes courtes de Kloosterman.
Dans la première partie de la thèse, on aborde alors le problème de l'ordre de grandeur de $P^+(n^3+2p^3)$ avec $x \leq n \leq 2x$ et $x^\tau \leq p \leq 2x^\tau$, avec $0 < \tau < 1$, le rajout de la suite $p \in [x^\tau, 2x^\tau]$ permettant d'avoir un résultat inconditionnel. On y améliore aussi le résultat de Hooley sur $P^+(n^3+2)$ par une meilleure utilisation de l'hypothèse R^* (ce dernier résultat reste donc un résultat conditionnel).

Pour $k \geq 2$, $S_f(m, h_1, ..., h_k)$ est une vraie somme d'exponentielles qui, selon toute vraisemblance comporte des compensations. Si $k=2$ et si f est un polynôme homogène, les sommes $S_f(m, h_1, h_2)$ se ramènent à des sommes géométriques, et sont très faciles à estimer.
Sinon, la géométrie algébrique fournit de remarquables résultats.
Plus précisément en faisant des hypothèses de non dégénérescence convenables sur f, on dispose

-pour $k=2$ des majorations de Weil de sommes d'exponentielles le long d'une courbe,

-pour $k=3$ des majorations de Hooley sur des surfaces, obtenues à partir des travaux de Deligne.

-pour $k=4$ des majorations de Laumon sur des hypersurfaces diagonales, obtenues elles aussi à partir des travaux de Deligne.

Tous ces résultats fournissent alors une minoration significative de l'ordre de grandeur de $P^+(f(p_1,p_2))$ ou $P^+(f(p_1,p_2,n_3))$, $P^+(1+p_1^4+p_2^4+n_3^5+n_4^6)$ pour une *proportion positive* de variables p_i et n_i.

Ils permettent encore d'aborder des questions connexes à cette étude. On a ainsi cherché pour certains polynômes, pour quels $y = x^\alpha > 0$, il existait une proportion positive de k-uplets $n_1, .., n_k$ de la taille de x tels que $P^+(f(n_1, ..., n_k)) < y$, les n_i étant des entiers quelconques ou des nombres premiers. Dans la première partie de la thèse, on obtient, en utilisant, à l'issue d'une préparation délicate, les majorations de Deshouillers et Iwaniec de sommes de Kloosterman en moyenne, un résultat pour le polynôme n^2+1 qui complète certains travaux de Schinzel.

Une autre application est encore d'étudier dans le cas où f est un polynôme en deux variables le nombres de facteurs premiers de $f(p_1, p_2)$. En combinant les poids de Richert à un crible de dimension 2 permettant de détecter les produits $p_1 p_2$, et en y incorporant les nouvelles estimations des quantités $|\mathcal{B}_m(a)|$ obtenues avec des méthodes de sommes d'exponentielles, on obtient, lorsque le degré de f est assez grand, des résultats améliorant notablement certains travaux de Greaves.

Bien que les schémas des démonstrations soient les mêmes pour tous les polynômes considérés, les arguments fournis à chaque étape sont très différents selon que f soit en une ou plusieurs variables. C'est pourquoi, ce travail se divise en deux parties : la première est consacrée aux polynômes $n^2 + 1$ et $n^3 + 2$, et dans la deuxième on étudie les polynômes en deux variables ou plus. Ces deux parties sont indépendantes. Les différents résultats obtenus et les méthodes suivies sont présentés en détail au début de chaque partie où on y développe aussi les idées évoquées dans la présente introduction.

PREMIÈRE PARTIE

AUTOUR DE POLYNÔMES EN UNE VARIABLE PARTICULIERS

Chapitre 0

Introduction

Le problème de l'ordre de grandeur du plus grand facteur premier du polynôme n^2+1 remonte au siècle dernier. En 1895, Tchebychev a montré que si P_x désigne le plus grand facteur premier du produit $\prod_{n\leq x}(n^2+1)$, alors le rapport $\frac{P_x}{x}$ tend vers $+\infty$, quand x tend vers $+\infty$.
Ensuite plusieurs mathématiciens ont étendu ce résultat à d'autres polynômes, et en 1921, Nagell [N1] a généralisé et amélioré le théorème de Tchebychev, en montrant que si f est un polynôme irréductible, et si P_x désigne le plus grand facteur premier du produit $\prod_{n\leq x} f(n)$, alors pour tout $\varepsilon < 1$, et pour x assez grand, on a l'inégalité $P_x > x(\log x)^{\varepsilon}$. Puis en 1952, Erdös [E] a amélioré le résultat de Nagell, en montrant l'inégalité $P_x > x(\log x)^{A_1 \log\log\log x}$, et récemment, en 1990, Tenenbaum [T1] a obtenu la minoration $P_x > xe^{(\log x)^{\alpha}}$, pour x assez grand, et $0 < \alpha < 2 - \log 4 = O.61370...$
En 1967, Hooley [H1] a montré en apportant plusieurs idées nouvelles à la méthode de Tchebychev, que pour tout polynôme irréductible de la forme $n^2 - D$, avec $D \neq 0$, l'on avait $P_x > x^{11/10}$ pour x assez grand.
En particulier, il introduisit du crible pour étudier la somme (pour $D = -1$) :

$$\sum_{x<p\leq P_x} \log p |\{0 \leq n \leq x,\ n^2+1 \equiv 0 \pmod p\}|,$$

ce qui l'a conduit à estimer des sommes d'exponentielles du type

$$\sum_{m\sim M} \sum_{\substack{0\leq v<m \\ v^2+1\equiv 0 \pmod m}} e\left(\frac{-hv}{m}\right).$$

Un point remarquable de sa preuve fut alors de transformer cette somme en une somme de Kloosterman portant sur un petit dénominateur, c'est-à-dire une somme du type

$$S(h,k;s) = \sum_{\substack{0\leq u<s \\ (u,s)=1}} e\left(\frac{h\bar{u}+ku}{s}\right),$$

(le symbole $\bar{u}$ désigne un inverse de u modulo s), où s est inférieur à $2M^{1/2}$, pour appliquer les majorations de Weil :

$$S(h,k;s) \ll (h,k,s)^{1/2} s^{1/2+\varepsilon}.$$

Cette transformation repose sur la correspondance de Gauss entre les solutions $v^2+1 \equiv 0 \bmod m$ et les écritures de m sous la forme $m = r^2+s^2$. Plus précisement, on a le lemme :

LEMME 0 (Gauss). *Pour $m > 1$, il existe une correspondance bijective entre les représentations de m sous la forme $m = r^2 + s^2$, avec $(r,s) = 1$, $|r| < s$ et les solutions de $v^2 + 1 \equiv 0 \bmod m$.*

Cette bijection est donnée par $\dfrac{v}{m} = \dfrac{\bar{r}}{s} - \dfrac{r}{s(r^2+s^2)} \pmod 1$,

où $\bar{r}$ désigne l'inverse de r modulo s.

En 1982, Deshouillers et Iwaniec dans [D-I1], ont repris les idées de Hooley, pour y injecter les remarquables résultats sur les majorations de sommes de Kloosterman en moyenne sur h, k, s, qu'ils avaient établis dans [D-I2] et sont ainsi arrivés à la minoration suivante : pour tout $\varepsilon > 0$ et pour x assez grand $P_x > x^{\theta-\varepsilon}$, avec $\theta = 1.202468...$

En 1991, Pomykala dans [Po], afin d'utiliser toute la puissance des travaux de Deshouillers et Iwaniec, s'est intéressé au problème du plus grand facteur premier du produit $P_x(\beta,\theta) = \prod_{n\le x} \prod_{\substack{q\in\mathbf{B}\\ q<x^\theta}} (n^2+q^2)$, où $\mathbf{B}$ est un ensemble de nombres premiers vérifiant la condition de densité

$$\mathbf{B}(y) = |\{b \in \mathbf{B},\ b \le y\}| \ge y^\beta,$$

pour y assez grand.

Pour $\beta < 1$ et $\theta \le \sqrt{\frac{3}{2}} - 1$, il a obtenu pour tout $\varepsilon > 0$, la minoration $P_x(\beta,\theta) > x^{\gamma(\beta,\theta)-\varepsilon}$, quand x tend vers $+\infty$,
avec $\lim_{\beta\to 1} \gamma(\beta, \sqrt{\frac{3}{2}} - 1) = \sqrt{\frac{3}{2}} = 1.2247..$

Le point de départ de ce travail fut d'étudier ce que devenaient ces résultats lorsque l'on remplaçait n par un nombre premier, c'est à dire d'étudier le plus grand facteur premier du produit $P^+\left(\prod_{p\le x}(p^2+1)\right)$.
Une utilisation directe du théorème de Brun-Titchmarsh pour détecter les $p \equiv \pm v \pmod q$, avec $0 \le v < q$, $v^2+1 \equiv 0 \pmod q$ fournit la minoration $P^+ > x^{0.78-\varepsilon}$, pour tout $\varepsilon > 0$, et x assez grand, et nous ne sommes pas parvenus à aller plus loin.
Il est alors naturel d'étudier le plus grand facteur premier du produit $\prod_{\tilde{n}\sim x}(\tilde{n}^2+1)$, où $\tilde{n}$ est un entier ayant peu de facteurs premiers et la notation $n \sim x$ signifie $n \in [x, 2x]$.

On montre le thérème suivant

THÉORÈME 1. *Soit* $0 < \alpha < \dfrac{1}{12.2}$, *il existe* $\varepsilon > 0$ *tel que pour* x *assez grand, on ait l'inégalité :*

$$|\{n \sim x,\ p|n \Rightarrow p > x^{\alpha},\ P^{+}(n^2+1) > x^{1+\varepsilon}\}| \gg \frac{x}{\log x},$$

où $P^{+}(n)$ *désigne le plus grand facteur premier de* n, *avec la convention* $P^{+}(1) = 0$.

La preuve de ce théorème reprend la méthode de Tchebychev-Hooley, mais le fait de travailler avec des nombres presque premiers modifie sensiblement toutes les étapes de la démonstration. En particulier, lorsque p est supérieur à x, l'estimation de la somme

$$\sum_{x<p<P_x} \log p|\{\tilde{n} \sim x,\ \tilde{n}^2+1 \equiv 0 \pmod p\}|$$

est plus ardue.

On détecte les entiers presque premiers $\tilde{n}$, et les nombres premiers p, avec un crible de dimension 2 appliqué aux produits mn, où $n^2+1 \equiv 0 \pmod m$. Il faut alors estimer les quantités

$$\sum_{\substack{m\sim M \\ m\equiv 0 \pmod d}} \log m|\{n \sim x,\ n \equiv 0 \pmod a,\ n^2+1 \equiv 0 \pmod m\}|.$$

On développe en série de Fourier les congruences sur n, mais la condition $n \equiv 0 \pmod a$, perturbe les transformations des sommes d'exponentielles que l'on rencontre alors. Après quelques transformations utilisant le lemme 0, la somme que l'on obtient est finalement de la forme :

$$\sum_{\delta<\Delta} \sum_{\substack{h\sim H \\ k\sim K \\ d\sim D}} a_{d,h,k} \sum_{\substack{s\sim S \\ (s,d)=1}} g(d,\delta,h,k,s) \sum_{\alpha \bmod \delta}{}^{*} e\left(\frac{F(\alpha,h,k,d,s)}{\delta}\right) \sum_{(u,s)=1} e\left(\frac{h\overline{du}+ku}{s}\right),$$

où g est une fonction "lisse", F est une fraction rationnelle et le symbole $*$ indique que les pôles de F sont exclus de la somme sur α, laquelle dépend de $s \bmod \delta$ et casse ainsi la lissité sur s. Les résultats de Deshouillers et Iwaniec de [D-I2] ne sont plus applicables et on estime finalement les sommes sur α et sur u à l'aide des résultats de Weil de géométrie algébrique.

Dans le deuxième chapitre, on étudie la proportion des entiers n, tels que n^2+1 n'ait pas de grand facteur premier. En 1967, Schinzel [Schin] a montré que pour tout $\varepsilon > 0$, il existe une infinité d'entiers n, tels que n^2+1 ait tous ses facteurs premiers inférieurs à n^{ε}. Cependant le résultat de Schinzel obtenu à partir de méthodes de transcendance ne donne aucune idée de la proportion des entiers n vérifiant cette propriété.

Dans ce travail on montre le

THÉORÈME 2. *Pour $0 < y < x$, on pose $\Xi(x,y) = |\{n \sim x, P^+(n^2+1) < y\}|$.*

Pour $y = x^\alpha$, avec $\alpha > \dfrac{149}{179}$, on a l'inégalité : $\Xi(x,y) \gg x$.

Bien que n'étant valable que pour des valeurs de α assez grandes (nous sommes loin de l'exposant $\alpha = \varepsilon$ du remarquable résultat de Schinzel), ce théorème présente l'intérêt de donner la proportion espérée des entiers n vérifiant la propriété. La preuve de ce résultat s'articule autour des systèmes de poids de Balog [Ba], et de Friedlander [Fr2]. Comme pour le théorème 1, on utilise la correspondance de Gauss énoncée au lemme 0 pour arriver à des sommes de Kloosterman.
L'utilisation des poids de Balog et de Friedlander nécessite l'application de cribles simultanés portant sur des variables qui ne sont pas indépendantes. Il faut alors travailler avec un nombre important de variables ce qui provoque des opérations de lissage ardues pour appliquer les majorations en moyenne de sommes de Kloosterman de [D-I2].

A l'heure actuelle, il n'existe pas encore de résultat effectif du même ordre que ceux concernant le polynôme n^2+1, valables pour des polynômes de degré 3 et plus.
En 1978, Hooley a obtenu le remarquable théorème suivant

THÉORÈME (HOOLEY [H2]). *Sous l'hypothèse R^*, pour x assez grand, le plus grand facteur premier du produit $H(x) = \prod_{n \le x}(n^3+2)$ est supérieur à $x^{31/30}$.*

L'hypothèse R^* étant :

Pour ℓ_1, ℓ_2, s des entiers donnés, et A_1 et A_2 tels que $0 \le A_2 - A_1 \le |s|$, on a :

$$\sum_{\substack{A_1 \le r \le A_2 \\ (r,s)=1}} e\left(\frac{\ell_1 \bar{r} + \ell_2 r}{s}\right) = O((A_2 - A_1 + 1)^{1/2} |s|^\varepsilon (\ell_1, s)^{1/2}).$$

La démonstration de ce théorème est très difficile, elle reprend le schéma de la preuve du plus grand facteur premier de n^2+1, chaque étape étant très compliquée. Hooley y établit une correspondance du type le lemme 0 entre les solutions v de la congruence $0 \le v < m$, $v^3 + 2 \equiv 0 \pmod m$, et les représentations de m par une forme cubique en trois variables φ définie par :

$$\begin{aligned}\varphi(x,y,z) &= (x + \theta y + \theta^2 z)(x + \theta\omega y + \theta^2\omega^2 z)(x + \theta\omega^2 y + \theta^2 \omega z) \\ &= x^3 + 2y^3 + 4z^3 - 6xyz,\end{aligned}$$

où $\theta = \sqrt[3]{2}$, et ω est une racine cubique de l'unité.

Cette correspondance n'apparaît pas sous une forme immédiate comme celle du lemme 0. Après une série d'opérations compliquées, Hooley transforme la somme d'exponentielle

$$\sum_{m\sim M} \sum_{\substack{0\leq v<m \\ v^3+2\equiv 0 \pmod m}} e\left(\frac{hv}{m}\right)$$

en une somme schématiquement du type

$$\sum_{0<|b|,|c|\ll M^{1/3}} \sum_{\substack{0\leq v<\lambda \\ \varphi(v,b,c)\equiv 0 \pmod\lambda}} \sum_{\substack{A_1<a<A_2 \\ (B(a),b^3-2c^3)=1 \\ a\equiv v \pmod\lambda}} e\left(\frac{F(a,b,c,\lambda)}{\lambda H}\right) e\left(\frac{h\bar{B}(a)}{b^3-2c^3}\right),$$

où B est une fonction affine de a dépendant de b et c.
Le dénominateur $H\lambda$ est très petit devant b^3-2c^3, ainsi on bloque la congruence de a modulo $H\lambda$ c'est à dire que l'on réécrit la somme sur a comme :

$$\sum_{\nabla \bmod H\lambda} e\left(\frac{F(\nabla,b,c,\lambda)}{\lambda H}\right) \sum_{\substack{A_1'<a<A_2' \\ (B(a),b^3-2c^3)=1 \\ a\equiv v \pmod\lambda,\ a\equiv\nabla \bmod H\lambda}} e\left(\frac{h\bar{B}(a)}{b^3-2c^3}\right).$$

Cette nouvelle somme sur a est alors une somme de Kloosterman, mais l'intervalle $[A_1', A_2']$ est d'amplitude un $O(M^{1/3})$, tandis que le dénominateur b^3-2c^3 est de l'ordre de M ce qui est bien plus grand. La majoration de Weil donne alors un résultat moins bon qu'une majoration triviale $(A_2-A_1)(H\lambda)^{-1}$, qui n'est cependant pas encore suffisante. La somme sur a est alors majorée avec l'hypothèse R^*.
A partir de l'hypothèse R^*, Hooley a en effet montré pour $s\neq 0$,
pour $0\leq A_2-A_1\leq 2|s|$ et pour tout $\varepsilon>0$ l'inégalité :

$$\sum_{\substack{A_1\leq r\leq A_2 \\ (r,s)=1 \\ r\equiv v \pmod\lambda}} e\left(\frac{\ell\bar{r}}{s}\right) = O((A_2-A_1)+1)^{1/2}|s|^{\varepsilon}(\ell,s)^{1/2}.$$

Mais, comme Fouvry l'a remarqué dans [Fo1], en combinant l'hypothèse R^* avec l'identité de Bezout, on a l'inégalité légèrement plus fine :

$$\sum_{\substack{A_1\leq r\leq A_2 \\ (r,s)=1 \\ r\equiv v \pmod\lambda}} e\left(\frac{\ell\bar{r}}{s}\right) = O\left(1+\frac{(A_2-A_1)^{1/2}(\lambda,s)^{1/2}}{\lambda^{1/2}}\right)|s|^{\varepsilon}(\ell,s)^{1/2}.$$

En injectant alors ce résultat dans la preuve de Hooley, on montre le

THÉORÈME 3. *Sous l'hypothèse R^*, et pour x assez grand, le plus grand facteur premier du produit $H(x)$ est supérieur à $x^{19/18}$.*

On est très loin d'avoir une somme lisse que l'on pourrait estimer avec les résultats de Deshouillers et Iwaniec [D-I2].
Tout d'abord l'exponentielle $e\left(\frac{F(a,b,c,\lambda)}{\lambda H}\right)$ est un obstacle du même type que celui rencontré dans la preuve du théorème 1, et surtout, la suite $b^3 - 2c^3$ est très discrète. On a cependant essayé de séparer les congruences sur a pour ainsi appliquer les résultats de Weil sur une somme d'exponentielles de dénominateur $H\lambda$. Ceci n'a rien apporté car le dénominateur $b^3 - 2c^3$ est beaucoup trop gros.

On s'est alors intéressé au problème de l'inégalité $P^+\left(\prod_{\substack{n\sim x\\ p\sim x^\tau}} (n^3+2p^3)\right) > x^{1+\varepsilon}$, l'injection de la suite $p \sim x^\tau$ permet d'avoir un résultat inconditionnel, la question étant d'avoir une valeur de τ la plus petite possible.

En procédant de façon élémentaire, c'est à dire en faisant de soigneuses intégrations par parties pour se ramener à une somme du type

$$\sum_{p\sim x^\tau} \sum_{\substack{A_1<a<A_2\\ a\equiv\nabla \bmod H}} e\left(\frac{hp\bar{B}(a)}{b^3-2c^3}\right),$$

pour ensuite appliquer l'inégalité de Cauchy-Schwarz et puis majorer quasiment trivialement toutes les sommes obtenues on obtient alors le théorème suivant

THÉORÈME 4. *Pour tout $\varepsilon > 0$, il existe $h > 0$, tel que pour x assez grand, on ait l'inégalité, pour $\tau = 2/3 + \varepsilon$:*

$$|\{n \sim x,\ p \sim x^\tau,\ P^+(n^3+2p^3) > x^{1+h}\}| \gg \frac{x^{1+\tau}}{\log x}.$$

Ce théorème s'apparente au résultat de Pomykala sur n^2+q^2 énoncé précédemment. Il est possible d'obtenir un résultat tout aussi général, c'est à dire valable pour $p \in \mathbf{B}(x^\tau)$, et ainsi chercher $h(\beta) > 0$, tel que

$$|\{n \sim x,\ p \in \mathbf{B}(x^\tau), P^+(n^3+2p^3) > x^{1+h(\beta)}\}| \gg |\mathbf{B}(x^\tau)|x.$$

Cependant, l'enjeu du théorème 4 est d'obtenir une valeur de τ la plus petite possible, quitte à obtenir un h très petit, alors que le rajout du paramètre de densité β sert surtout à améliorer $h(\beta)$, mais ne change pas la valeur minimale de τ.

Il semble difficile d'obtenir une plus petite valeur minimale pour τ. Les quantités A_1 et A_2 et la fonction B sont difficilement contrôlables et les variables a et $p \sim x^\tau$ sont trop petites par rapport au dénominateur $b^3 - 2c^3$ pour apporter *via* par exemple l'identité de Vaughan d'intéressantes compensations. Il paraît donc assez ardu d'obtenir des résultats nouveaux sur le polynôme $n^3 + 2$.

La preuve du théorème 4 et l'amélioration de l'exposant du plus grand facteur premier du produit $H(x)$ suivent pas à pas la démonstration de Hooley, mis à part les modifications présentées dans les lignes précédentes, il ne paraît donc pas nécessaire de les exposer dans ce travail. Les preuves des théorèmes 1 et 2 constituent les deux chapitres de cette partie.

Chapitre 1
Le plus grand facteur premier de n^2+1 où n est presque premier

On démontre dans ce chapitre le théorème 1, en suivant la méthode de Tchebychev-Hooley.

1.1. La méthode de Tchebychev.

Soient $x > 2$ et f une fonction de classe C^∞, positive, à support dans $[x, 2x]$ et telle que $f^{(\ell)}(t) \ll t^{-\ell}$, pour tout $\ell \in \mathbf{N}$,
(la constante dans $\ll$, ne dépendant que de ℓ).

On pose $x_0 = \int f(t)dt$, avec $x_0 \approx x$.

Pour $\alpha > 0$, on définit la quantité :

$$V_\alpha(x) = \sum_{p|n \Rightarrow p > x^\alpha} f(n)\log(n^2+1). \tag{1.1}$$

La méthode de Tchebychev consiste alors à évaluer la quantité $V_\alpha(x)$ de deux manière différentes, dont l'une dépend de P^+, le plus grand facteur premier du produit $V_\alpha(x)$.
L'usage de la fonction f n'est pas nécessaire ici, mais elle le sera pour la preuve du théorème 2. On a préféré adopter cette présentation afin de ne pas changer de notation dans le prochain chapitre.

On commence par estimer $V_\alpha(x)$ pratiquement directement à partir du résultat classique concernant les entiers sans petit facteur premier. Nous en donnons une forme très forte due à Tenenbaum ([T2] théorème 3 p. 445) :

LEMME 1.1.1. *Soit la fonction* $\Phi(x,y) = |\{n \le x,\ tels\ que\ p|n \Rightarrow p > y\}|$. *On pose* $u = \dfrac{\log x}{\log y}$. *On a, alors, uniformément pour* $x \ge y \ge 2$, *l'égalité :*

$$\Phi(x,y) = \frac{xw(u) - y}{\log y} + O\Big(\frac{x}{(\log y)^2}\Big),$$

où w *est la fonction de Buchstab et est solution pour* $u > 1$, *de l'équation différentielle aux différences :*

$$\begin{cases} (uw(u))' = w(u-1) & pour\ u > 2, \\ uw(u) = 1 & pour\ 1 \le u \le 2. \end{cases}$$

Nous n'avons pas besoin de toute la puissance de ce résultat, car dans la suite on prendra $y = x^\alpha$, avec α constant compris entre 0 et 1, mais ce lemme s'applique facilement pour montrer le

LEMME 1.1.2. *Pour $0 < \alpha < 1$, on a l'égalité :*

$$V_\alpha(x) = \frac{2w(\alpha^{-1})}{\alpha} x_0 + O\left(\frac{x}{\log x}\right).$$

Preuve du lemme 1.1.2. Soit χ_α la fonction caractéristique des entiers n ayant tous leurs facteurs premiers $> x^\alpha$.
Comme $n \sim x$, on a l'égalité :

$$\begin{aligned} V_\alpha(x) &= \sum_n f(n)\chi_\alpha(n)\log(n^2+1) \\ &= 2\log x \sum_n f(n)\chi_\alpha(n) + O\Big(\sum_n f(n)\chi_\alpha(n)\Big). \end{aligned}$$

Il s'agit alors d'estimer :

$$\sum_n f(n)\chi_\alpha(n) = \int f(t)d\Phi(t, x^\alpha).$$

On fait une intégration par parties :

$$\sum_n f(n)\chi_\alpha(n) = \Big[f(t)\Phi(t,x^\alpha)\Big]_x^{2x} - \int_x^{2x} f'(t)\Phi(t,x^\alpha)dt.$$

Le premier terme du membre de droite est nul, et on utilise le lemme 1.1.1 pour évaluer le second :

$$\begin{aligned} \sum_n f(n)\chi_\alpha(n) = &-\int_x^{2x} \frac{f'(t)t}{\alpha\log x}\omega\left(\alpha^{-1} + O\left(\frac{1}{\log x}\right)\right)dt \\ &+ O\Big(\int_x^{2x} \frac{t|f'(t)|}{\alpha^2(\log x)^2}dt\Big) + O\Big(\int_x^{2x} \frac{x^\alpha|f'(t)|}{\alpha\log x}dt\Big). \end{aligned}$$

Pour x tendant vers $+\infty$, on a l'égalité :

$$\omega\left(\alpha^{-1} + O\left(\frac{1}{\log x}\right)\right) = \omega(\alpha^{-1}) + O\left(\frac{1}{\log x}\right).$$

De plus, comme $f'(t) \ll t^{-1}$, les termes de reste sont $\ll \frac{x}{(\log x)^2}$.

Puis, en faisant une deuxième intégration par parties, on a :

$$\int_x^{2x} \frac{f'(t)t\omega(\alpha^{-1})}{\alpha \log x}dt = \Big[\frac{f(t)t\omega(\alpha^{-1})}{\alpha \log x}\Big]_x^{2x} - \frac{\omega(\alpha^{-1})}{\alpha}\int_x^{2x}\frac{f(t)}{\log x}dt$$
$$= -\frac{\omega(\alpha^{-1})}{\alpha}\frac{x_0}{\log x}.$$

On obtient finalement :

$$V_\alpha(x) = \frac{2\omega(\alpha^{-1})}{\alpha}x_0 + O\Big(\frac{x}{\log x}\Big), \tag{1.1}$$

ce qui termine la preuve du lemme 1.1.2.

Maintenant, tout le reste de la preuve est consacré à la deuxième estimation de $V_\alpha(x)$. On commence par écrire l'égalité :

$$V_\alpha(x) = \sum_{\substack{r,s \\ r \ premier \\ r^s \le 4x^2+1}} \log r \sum_{\substack{n,p|n\Rightarrow p>x^\alpha \\ n^2+1\equiv 0 \pmod{r^\alpha}}} f(n).$$

Pour $d \in \mathbf{N}$, on définit la quantité :

$$|\mathcal{A}_d| = \sum_{\substack{n,p|n\Rightarrow p>x^\alpha \\ n^2+1\equiv 0 \pmod{d}}} f(n).$$

Pour $h, t, \varepsilon, \theta > 0$, avec $1 > t > 1/2 - \varepsilon$, et $\theta > 2/3$, on procède ensuite au découpage suivant (r désigne toujours un nombre premier) :

$$V_\alpha(x) = \sum_{r^s \le x^{1/2-\epsilon}} \log r|\mathcal{A}_{r^s}| + \sum_{x^{1/2-\epsilon}\le r^s \le x^t} \log r|\mathcal{A}_{r^s}| + \sum_{\substack{x^t \le r^s \\ s\ge 2, r\le x^\theta}} \log r|\mathcal{A}_{r^s}|$$
$$+ \sum_{\substack{x^t \le r^2 \\ r>x^\theta}} \log r|\mathcal{A}_{r^2}| + \sum_{x^t<r<x^{1+h}} \log r|\mathcal{A}_r| + \sum_{r>x^{1+h}} \log r|\mathcal{A}_r|$$
$$= S_0 + S_1 + S_2 + S_3 + S_4 + S_5, \tag{1.2}$$

par définition.

La première somme S_0, est évaluée avec un théorème du type "le théorème de Bombieri-Vinogradov" établi par Wolke [W] ; S_1 est majorée avec un crible sur n, S_2 est majorée directement, S_3 est traitée avec le crible à carrés de Heath-Brown. La somme S_4 est la plus difficile à traiter, on la majorera en utilisant un crible de dimension 2 qui servira à détecter à la fois les entiers n presque premiers et les nombres premiers r. On choisira alors $\alpha > 0$ le plus grand possible tel qu'il existe ε et $h > 0$ assez petits tels que $S_5 = V_\alpha(x) - S_0 - S_1 - S_2 - S_3 - S_4$ soit strictement positive.

1.2. Estimation de S_0.

La quantité S_0 s'évalue de la même manière que $V_\alpha(X)$, mais en utilisant le théorème que Wolke montre dans [W], concernant la répartition en moyenne des progressions arithmétiques portant sur des entiers presque premiers.
C'est le lemme suivant

LEMME 1.2.1. *Soient* $\Phi_k(x,z) = \sum_{\substack{n\le x\\(n,k)=1\\p|n\Rightarrow p>z}} 1$, *et* $\Phi(x,z,k,\ell) = \sum_{\substack{n\le x\\n\equiv \ell \pmod k\\p|n\Rightarrow p>z}} 1$,

avec $2\le x,\ 1\le z\le x$.

Alors, pour tout $A>0$, *il existe* $A_2>0$, *tel que uniformément pour* $z\le x^{1/2}$ *et* $Q = x^{1/2}(\log x)^{-A_2}$, *on ait :*

$$\sum_{k\le Q}\max_{(\ell,k)=1}\max_{y\le x}\left|\Phi(y,z,k,\ell)-\frac{1}{\varphi(k)}\Phi_k(y,z)\right| \ll x(\log x)^{-A}.$$

Ce lemme est la clé de la preuve du résultat suivant :

LEMME 1.2.2. *On a l'égalité :*

$$S_0 = \frac{\omega(\alpha^{-1})x}{2\alpha} + O\left(\frac{x}{\log x}\right).$$

Preuve du lemme 1.2.2.
On écrit S_0 sous la forme :

$$S_0 = \sum_{r^s\le x^{1/2-\epsilon}} \log r \sum_{\substack{0<v<r^s\\ v^2+1\equiv 0 \pmod{r^s}}} \sum_{n\equiv v \pmod{r^s}} f(n)\chi_\alpha(n).$$

Pour exprimer cette somme sous forme intégrale, on définit la fonction Ψ :

$$\Psi(t) = \sum_{r^s\le x^{1/2-\epsilon}} \log r \sum_{\substack{0\le v<r^s\\ v^2+1\equiv 0 \pmod{r^s}}} \sum_{\substack{n\le t\\ n\equiv v \pmod{r^s}}} \chi_\alpha(n).$$

On a alors l'égalité :

$$S_0 = \int f(t)d\Psi(t)$$

$$= -\int_x^{2x} f'(t)\Psi(t)dt. \tag{1.3}$$

On applique alors le lemme 1.2.1 à $\Psi(t)$, pour $x<t<2x$:
(1.4)

$$\Psi(t) = \sum_{r^s<x^{1/2-\epsilon}} \log r \sum_{\substack{v \bmod r^s\\ v^2+1\equiv 0(r^s)}} \frac{1}{\varphi(r^s)} \sum_{\substack{n\le t\\(n,r^s)=1}} \chi_\alpha(n) + O\Big(\frac{x}{(\log x)^{100}}\max\rho(r^s)\Big),$$

avec $\rho(d) = |\{0<v<d,\ tels\ que\ v^2+1\equiv 0 \pmod d\}|$.

Cette fonction ρ interviendra dans toutes les étapes de la démonstration, elle prend les valeurs suivantes :

LEMME 1.2.3. *La fonction ρ est multiplicative, et vérifie :*

i) $\rho(2) = 1$, $\rho(2^k) = 0$ *pour* $k > 1$,

ii) pour $p > 2$, *et* $k \geq 1$, $\rho(p^k) = \rho(p)$,

iii) $\rho(p) = 2$ *si* $p \equiv 1 \pmod 4$, $\rho(p) = 0$ *si* $p \equiv -1 \pmod 4$.

Ainsi, pour r premier, on a $0 \leq \rho(r^s) \leq 2$, on reporte ceci dans (1.4), tout en profitant de l'inégalité $f'(t) \ll t^{-1}$:

$$S_0 = -\sum_{r^s < x^{1/2-\epsilon}} \log r \sum_{\substack{v \bmod r^s \\ v^2+1 \equiv 0 (\bmod r^s)}} \frac{1}{\varphi(r^s)} \int_x^{2x} f'(t) \Phi_{r^s}(t, x^\alpha) dt + O\Big(\frac{x}{(\log x)^{10}}\Big).$$

La fonction Φ_{r^s} vérifie l'équation :

$$\Phi_{r^s}(t, x^\alpha) = \Phi(t, x^\alpha) - \sum_{\substack{n \leq t \\ p|n \Rightarrow p > x^\alpha \\ n \equiv 0 \ (\bmod r^s)}} 1.$$

Le deuxième terme du membre de droite de cette dernière égalité est nul si $r \leq x^\alpha$, sinon, si $r > x^\alpha$, alors tout entier n ayant une contribution positive dans cette somme peut se réécrire comme $n = mr^s$, avec $m < tr^{-s}$ et ayant tous ses facteurs premiers supérieurs à x^α.

On a donc l'égalité :

$$\Phi_{r^s}(t, x^\alpha) = \begin{cases} \Phi(t, x^\alpha) & \text{si } r \leq x^\alpha, \\ \Phi(t, x^\alpha) - \Phi(tr^{-s}, x^\alpha) & \text{si } r > x^\alpha. \end{cases}$$

Cette écriture nous permet d'utiliser une nouvelle fois le lemme 1.1.1, et en faisant les mêmes opérations que celles effectuées pour calculer $V_\alpha(x)$, on a :

$$S_0 = \frac{\omega(\alpha^{-1})}{\alpha} \frac{x_0}{\log x} \sum_{\substack{r^s < x^{1/2-\epsilon} \\ r \equiv 1 (\bmod 4)}} \frac{2 \log r}{\varphi(r^s)} \left(1 + O\left(\frac{1}{\log x}\right)\right)$$

$$+ O\left(\frac{x_0}{\log x} \sum_{\substack{r^s < x^{1/2-\epsilon} \\ r > x^\alpha}} \frac{\log r}{r^{2s}} + \frac{x^\alpha}{\log x} \sum_{\substack{r^s < x^{1/2-\epsilon} \\ r > x^\alpha}} \frac{\log r}{r^s}\right).$$

Le terme d'erreur de cette dernière ligne est pour tout $\eta > 0$, un $O(x^{1-\alpha/3} + x^{\alpha+\eta})$, ce qui est très petit.

Ainsi, on obtient, grâce à l'égalité $\pi(x,4,1) = \dfrac{x}{2\log x} + O\left(\dfrac{x}{\log^2 x}\right)$:

$$S_0 = \frac{\omega(\alpha^{-1})}{\alpha}\frac{x_0}{\log x}\left(1+O\left(\frac{1}{\log x}\right)\right)\int_2^{x^{1/2-\epsilon}}\frac{\log r}{r}\frac{dr}{\log r}$$
$$+ O\left(\frac{\omega(\alpha^{-1})}{\alpha\log x}x_0\sum_{\substack{s\geq 2, r^s\leq x^{1/2-\epsilon}\\ r\equiv 1(\mathrm{mod}\,4)}}\frac{2\log r}{\varphi(r^s)}\right).$$

On a donc $S_0 = \frac{\omega(\alpha^{-1})}{2\alpha}x_0 - \varepsilon x_0 + O\left(\frac{x}{\log x}\right)$.

1.3. Majoration de S_1.

On rappelle la définition de S_1 donnée à la ligne (1.2) :

$$S_1 = \sum_{\substack{x^{1/2-\epsilon}\leq r^s\leq x^t\\ r\equiv 1(\mathrm{mod}\,4)}}\log r \sum_{n^2+1\equiv 0\ (\mathrm{mod}\ r^s)} f(n)\chi_\alpha(n) = \sum_{x^{1/2-\epsilon}\leq r^s\leq x^t}\log r|\mathcal{A}_{r^s}|,$$

avec $1/2-\varepsilon < t < 1$.

Première majoration de S_1.

Cette première majoration consiste en quelque sorte à réécrire la preuve du théorème de Brun-Titchmarsh *facile* $\pi(x,q,a) \leq \dfrac{x(2+o(1))}{\varphi(q)\log(x/q)}$, mais dans un autre contexte et avec des notations différentes.
Pour r^s fixé, $r \geq 3$, on va majorer les quantités $|\mathcal{A}_{r^s}|$ en utilisant un crible de Rosser sur n.
Pour $D(r^s) > 0$, que l'on précisera plus tard, on définit les poids de Rosser (λ_d) de la manière suivante : $\lambda_1 = 1, \lambda_d = 0$ si d a un facteur carré, ou si $(d,r) > 1$, et pour d sans facteur carré et tel que $(d,r) = 1$, $d = p_1p_2...p_k$ avec $p_1 > p_2 > ... > p_k$, on pose :

$$\lambda_d = \begin{cases} (-1)^k & \text{si } p_1p_2...p_{2\ell}p_{2\ell+1}^3 < D(r^s), \text{ pour } 0\leq\ell\leq\frac{k-1}{2},\\ 0 & \text{sinon.}\end{cases}$$

Ces coefficients de Rosser vérifient la propriété fondamentale $\lambda * \mathbb{1} \geq \mu * \mathbb{1}$, et on a donc l'inégalité :

$$|A_{r^s}| \leq \sum_{\substack{d|P(x^\alpha)\\ d<D(r^s)}}\lambda_d \sum_{\substack{n\equiv 0\ (\mathrm{mod}\,d)\\ n^2+1\equiv 0\ (\mathrm{mod}\,r^s)}} f(n)$$
$$\leq \sum_{\substack{d|P(x^\alpha)\\ d<D(r^s)}}\lambda_d \sum_{\substack{0<v<dr^s\\ d|v\\ v^2+1\equiv 0\ (\mathrm{mod}\,r^s)}}\ \sum_{n\equiv v\ (\mathrm{mod}\,dr^s)} f(n).$$

On utilise ensuite la formule sommatoire de Poisson :

LEMME 1.3.1. *Soit g une fonction de classe C^1, à support compact dans $\mathbf{R}$, et soit $\hat{g}$ la transformée de Fourier, alors on a :*

$$\sum_{n\equiv a \pmod q} g(n) = \frac{1}{q}\sum_{h\in\mathbf{Z}} e\left(\frac{-ah}{q}\right)\hat{g}\left(\frac{h}{q}\right).$$

On applique la formule de Poisson pour transformer les congruences sur n, le coefficient en $h=0$ fournit le terme principal :

$$\begin{aligned}|\mathcal{A}_{r^s}| &\le \sum_{\substack{d|P(x^\alpha)\\ d<D(r^s)}} \lambda_d \sum_{h\in\mathbf{Z}} \frac{1}{dr^s}\hat{f}\left(\frac{h}{dr^s}\right) \sum_{\substack{0<v<dr^s\\ d|v,\ v^2+1\equiv 0 \pmod{r^s}}} e\left(\frac{-hv}{dr^s}\right)\\ &\le x_0 \sum_{\substack{d|P(x^\alpha)\\ d<D(r^s)\\ (d,r)=1}} \lambda_d \sum_{\substack{0<v<dr^s\\ d|v\\ v^2+1\equiv 0 \pmod{r^s}}} \frac{1}{dr^s}\\ &+ \sum_{\substack{d|P(x^\alpha)\\ d<D(r^s)\\ (d,r)=1}} \lambda_d \sum_{h\neq 0} \frac{1}{dr^s}\hat{f}\left(\frac{h}{dr^s}\right) \sum_{\substack{0<v<dr^s\\ d|v\\ v^2+1\equiv 0 \pmod{r^s}}} e\left(\frac{-hv}{dr^s}\right).\end{aligned}$$

Pour $h\neq 0$, en faisant ℓ intégrations par parties , on trouve :

$$\begin{aligned}\hat{f}\left(\frac{h}{dr^s}\right) &= \left(\frac{-2i\pi h}{dr^s}\right)^{-\ell}\int f^{(\ell)}(t)e\left(\frac{-2i\pi ht}{dr^s}\right)dt\\ &\ll \left(\frac{dr^s}{|h|x}\right)^{\ell} x.\end{aligned}$$

Pour $\varepsilon>0$, en prenant $\ell=[4\varepsilon^{-1}]$, on montre que $\hat{f}\left(\frac{h}{dr^s}\right)\ll\frac{1}{h^2}$, pour $|h|>H$ avec $H=dr^s x^{-1+\varepsilon}$.
Pour $d<x^{1-\varepsilon}r^{-s}$, on a $H\le 1$ et la somme sur $h\neq 0$ est $\ll\frac{x^\varepsilon}{r^s}$.
On choisit alors $D(r^s)=x^{1-\varepsilon}r^{-s}$ et en appliquant le théorème A1 énoncé dans l'annexe A, issu des travaux d'Iwaniec [I1] sur le crible linéaire on obtient :

$$S_1 \le x_0 \sum_{\substack{x^{1/2-\varepsilon}\le r^s\le x^t\\ r\equiv 1 (\mathrm{mod}\, 4)}} \frac{2\log r}{r^s}\prod_{\substack{p<x^\alpha\\ p\neq r}}\left(1-\frac{1}{p}\right)F\left(\frac{\log(x^{1-\varepsilon}r^{-s})}{\log(x^\alpha)}\right)+O\left(\frac{x}{\log x}\right)+\varepsilon' x,$$

avec $\varepsilon'>0$ arbitrairement petit.

Comme

$$\sum_{\substack{s\geq 2\\ x^{1/2-\epsilon}\leq r^s\leq x^t}} \frac{\log r}{r^s} \prod_{\substack{p<x^\alpha\\ p\neq r}} \left(1-\frac{1}{p}\right) x_0 \ll \frac{x}{\log x},$$

on a, en profitant de l'égalité $\pi(x,4,1) = \dfrac{x}{2\log x} + O\left(\dfrac{x}{\log x}\right)$, l'inégalité :

$$S_1 \leq \frac{x_0 e^{-\gamma}}{\alpha \log x} \int_{x^{1/2-\epsilon}}^{x^t} \frac{\log r}{r} F\left(\frac{\log(x/r)}{\log(x^\alpha)}\right) \frac{dr}{\log r} + O\left(\frac{x}{\log x}\right) + \varepsilon' x,$$

c'est-à-dire :

$$S_1 \leq \frac{x_0 e^{-\gamma}}{\alpha} \int_{1/2-\epsilon}^{t} F\left(\frac{1-\lambda}{\alpha}\right) d\lambda + O\left(\frac{x}{\log x}\right) + \varepsilon' x. \tag{1.5}$$

Deuxième majoration de S_1.
On repart de l'égalité

$$S_1 = \sum_{\substack{x^{1/2}<r^s<x^t\\ r\equiv 1 \pmod 4}} \sum_{n\equiv \pm v \pmod{r^s}} f(n)\chi_\alpha(n),$$

où v est une solution de $v^2+1 \equiv 0 \pmod{r^s}$ (r est premier).
Il s'agit alors de détecter les entiers intervenant dans la somme :

$$|\mathcal{A}^{(r^s)}| = \sum_{n\equiv v \pmod{r^s}} f(n)\chi_\alpha(n).$$

A cette fin, on transpose les résultats d'Iwaniec [I2] concernant le théorème de Brun-Titchmarsh à notre situation.
On commence par appliquer le crible linéaire d'Iwaniec sous la forme précise énoncée au théorème A1 de l'annexe A, avec un terme d'erreur apparaissant sous une forme bilinéaire.
Pour $\varepsilon > 0$, $A = \exp(8\varepsilon^{-3})$, $x > K(\varepsilon)$, $M \geq 1$, $N \geq 1$, $D = MN < x$, on a l'inégalité :

$$|\mathcal{A}^{(r^s)}| \leq \frac{x_0}{r^s} \prod_{\substack{p<x^\alpha\\ p\neq r}} \left(1-\frac{1}{p}\right) \left\{F\left(\frac{\log D}{\log x^\alpha}\right) + c\varepsilon\right\} + \sum_{a<A} R_a(\mathcal{A}^{(r^s)}, M, N),$$

où c est une constante absolue et

$$R_a(\mathcal{A}^{(r^s)}, M, N) = \sum_{\substack{m\leq M\\ n\leq N\\ (mn,r)=1}} a_m b_n r(\mathcal{A}^{(r^s)}, mn).$$

En profitant de cette flexibilité du terme d'erreur, Iwaniec a montré l'inégalité :

LEMME 1.3.2. *([I2] théorème 5 p. 105)*

Soit $\varepsilon' > 0$, $x^{2/5} < r^s \leq x^{2/3-6\varepsilon'}$, $M = \dfrac{x^{1-3\varepsilon'}}{r^s}$, $N = \dfrac{x^{1/2-4\varepsilon'}}{r^{3s/4}}$.

On a alors :

$$\sum_{\substack{m\leq M\\ n\leq N\\ (mn,r)=1}} a_m b_n r(\mathcal{A}^{(r^s)}, mn) \ll \frac{x^{1-\varepsilon'}}{r^s}.$$

Grâce à ce lemme, on peut choisir $D = MN = \dfrac{x^{3/2-7\varepsilon}}{r^{7s/4}}$, pour obtenir alors :

$$|\mathcal{A}^{(r^s)}| \leq \frac{x_0}{r^s} \prod_{p<x^\alpha} \left(1-\frac{1}{p}\right) F\left(\frac{\log(x^{3/2-7\varepsilon} r^{-\frac{7s}{4}})}{\log x^\alpha}\right) + \frac{\varepsilon x}{\log x} + O\left(\frac{x}{\log^2 x}\right).$$

Cette majoration est plus fine que celle qui a servi pour (1.5) lorsque $r^s < x^{2/3}$ et on termine les calculs comme précédemment.
A partir de ceci on a :

LEMME 1.3.3. *Pour tout* $\varepsilon > 0$, *on a l'inégalité :*

$$S_1 \leq \frac{x_0 e^{-\gamma}}{\alpha} \int_{1/2-\varepsilon}^{2/3} F\left(\frac{3/2-7\varepsilon-7\lambda/4}{\alpha}\right) d\lambda + \frac{x_0 e^{-\gamma}}{\alpha} \int_{2/3}^{t} F\left(\frac{1-\lambda}{\alpha}\right) d\lambda + \varepsilon x + O\left(\frac{x}{\log x}\right).$$

1.4. Majoration de S_2.

Cette quantité se majore quasiment directement. On écrit la suite d'inégalités :

$$\begin{aligned} S_2 &= \sum_{\substack{x^t<r^s\\ s\geq 2,\ r<x^\theta}} \log r \sum_{\substack{n^2+1\equiv 0 \pmod{r^s}\\ p|n\Rightarrow p>x^\alpha}} f(n) \\ &\ll \sum_{\substack{x^t<r^s\\ s\geq 2,\quad r<x^\theta}} \log r |\{n\in[x,2x],\quad n^2+1\equiv 0 \pmod{r^s}\}| \\ &\ll x \sum_{\substack{x^t<r^s\leq x\\ s\geq 2,\quad r<x^\theta}} \frac{\log r}{r^s} + \sum_{\substack{x<r^s<4x^2+1\\ s\geq 2,\quad r<x^\theta}} \log r \\ &\ll x^{1-t/2+\varepsilon} \sum_{x^t<r^s\leq x} \frac{1}{r^{s/2}} + \sum_{r<x^\theta} \log r \sum_{s\leq \frac{2\log x}{\log r}} 1. \end{aligned}$$

On a ainsi l'inégalité :

$$S_2 \ll x^{1-t/2+\varepsilon'} + x^{\theta+\eta} \ll x^{1-\varepsilon"},$$

pour ε" assez petit.
Donc pour $0 < \theta < 1$, θ aussi proche de 1 que l'on veut, il existe $\varepsilon > 0$, tel que $S_2 \ll x^{1-\varepsilon}$.

1.5. Majoration de S_3 avec un crible à carrés.

On rappelle la définition de S_3 :

$$S_3 = \sum_{\substack{x^\theta < r \\ r \text{ premier}}} \log r \sum_{\substack{n^2+1 \equiv 0 \pmod{r^2} \\ p|n \Rightarrow p > x^\alpha}} f(n).$$

On va montrer que pour $\theta > 3/4$, $S_3 \ll x^{1-\varepsilon}$ pour $\varepsilon > 0$ assez petit.
On part de l'inégalité :

$$S_3 \ll \log x \sum_{x^\theta < d \leq 2x} |\{n \in [x, 2x], \quad n^2 + 1 \equiv 0 \pmod{d^2}\}|,$$

cette somme portant sur les entiers d non nécesairement premiers.
Pour évaluer ceci on utilise le crible à carrés de Heath-Brown ([HB] théorème 1) :

LEMME 1.5.1. *Soit* $\mathbf{A} = (\omega(n))_n$ *une suite de réels, avec* $\omega(n) \geq 0 \quad \forall n$, *et* $\sum \omega(n) < +\infty$.

On définit $S(\mathbf{A}) = \sum_{n \in \mathbf{N}} \omega(n^2)$.

Soit $\mathbf{P}$ *un ensemble de* P *nombres premiers. On suppose que* $\omega(n) = 0$, *pour* $n = 0$ *ou* $n \geq e^P$.

Alors on a la majoration :

$$S(\mathbf{A}) \ll P^{-1} \sum_n \omega(n) + P^{-2} \sum_{p \neq q \in \mathbf{P}} \left| \sum_n \omega(n) \left(\frac{n}{pq}\right) \right|,$$

où $\left(\frac{n}{pq}\right)$ *est le symbole de Jacobi.*

Il faut détecter les $n^2 + 1 = md^2$, avec $m < 4x^{2-2\theta}$ et $md^2 \leq 4x^2 + 1$,
ainsi, on prend les poids

$$\omega(n) = |\{(m, d),\ x^\theta < d \leq 2x,\ m \leq 4x^{2-2\theta},\ md^2 - 1 \in [x^2, 4x^2],$$
$$tels\ que\ n = md^2 - 1\}|,$$

et $\mathbf{P} = \{2 < p < P\}$ où $P > 0$ sera précisé plus tard.

On applique alors le lemme 1.5.1 :
(1.6)

$$S_3 \ll P^{-1+\varepsilon} \sum_{\substack{m\leq 4x^{2-2\theta}\\ x^\theta<d\leq 2x}} 1 + P^{-2+\varepsilon} \sum_{2<p<q<P} \sum_{m\leq 4x^{2-2\theta}} \left| \sum_{x^\theta<d\leq 2xm^{-1/2}} \left(\frac{md^2-1}{pq}\right)\right|.$$

On impose $P < x^{\theta/2}$, alors pour $p \neq q$ impairs, en développant les congruences vérifiées par d, on a :

$$\sum_{x^\theta<d\leq 2xm^{-1/2}} \left(\frac{md^2-1}{pq}\right) \ll \frac{xm^{-1/2}}{pq} \left| \sum_{1\leq u\leq pq} \left(\frac{mu^2-1}{pq}\right)\right| + pq.$$

Pour $p \neq q$, on a encore :

$$\begin{aligned}\sum_{1\leq u\leq pq} \left(\frac{mu^2-1}{pq}\right) &= \sum_{1\leq u\leq pq} \left(\frac{mu^2-1}{p}\right)\left(\frac{mu^2-1}{q}\right)\\ &= \sum_{1\leq \alpha\leq p} \left(\frac{m\alpha^2-1}{p}\right) \sum_{1\leq \beta\leq q} \left(\frac{m\beta^2-1}{q}\right).\end{aligned}$$

Pour calculer ceci, on établit d'abord le lemme :

LEMME 1.5.2. *Si $p \neq 2$ et ne divise pas m,*

$$\sum_{1\leq \alpha\leq p} \left(\frac{m\alpha^2-1}{p}\right) = -\left(\frac{m}{p}\right).$$

Preuve du lemme 1.5.2.
La preuve de ce lemme consiste à faire des opérations élémentaires sur les caractères de Legendre pour aboutir à des sommes de caractères classiques.
On a l'égalité :

$$\begin{aligned}\sum_{1\leq \alpha\leq p} \left(\frac{m\alpha^2-1}{p}\right) &= \left(\frac{-m}{p}\right) \sum_{1\leq \alpha\leq p} \left(\frac{\bar{m}-\alpha^2}{p}\right)\\ &= \left(\frac{-m}{p}\right) \sum_{1\leq \alpha\leq p} \left(\left(\frac{\bar{m}-\alpha^2}{p}\right)+1\right) - \left(\frac{-m}{p}\right) p.\end{aligned}$$

La somme un peu plus compliquée du membre de droite de la ligne précédente, correspond au nombre de points d'une conique particulière, on a l'égalité :

$$\sum_{1\le\alpha\le p}\left(\left(\frac{\bar{m}-\alpha^2}{p}\right)+1\right) = |\{(x,y)\in \mathbf{F}_p\times\mathbf{F}_p \quad tels \quad que\ x^2+y^2\equiv\bar{m}(\mathrm{mod}\,p)\}|$$

$$= \sum_{x+y\equiv\bar{m}(p)}\left(1+\left(\frac{x}{p}\right)\right)\left(1+\left(\frac{y}{p}\right)\right)$$

$$= p+\sum_{x+y\equiv\bar{m}(p)}\left(\frac{x}{p}\right)\left(\frac{y}{p}\right)$$

$$= p+\sum_{x}\left(\frac{x}{p}\right)\left(\frac{\bar{m}-x}{p}\right).$$

Maintenant, pour $x\neq 0$, on a $\left(\frac{x}{p}\right)=\left(\frac{\bar{x}}{p}\right)$,
et ainsi $\left(\frac{x}{p}\right)\left(\frac{\bar{m}-x}{p}\right)=\left(\frac{\bar{x}(\bar{m}-x)}{p}\right)=\left(\frac{\bar{x}\bar{m}-1}{p}\right)$.
C'est à dire :

$$\sum_{1\le\alpha\le p}\left(\left(\frac{\bar{m}-\alpha^2}{p}\right)+1\right)=p+\sum_{x\neq 0}\left(\frac{\bar{x}\bar{m}-1}{p}\right),$$

ensuite on pose $c=\bar{x}\bar{m}-1$, pour arriver à une somme toute simple :

$$\sum_{1\le\alpha\le p}\left(\left(\frac{\bar{m}-\alpha^2}{p}\right)+1\right)=p+\sum_{c\neq -1}\left(\frac{c}{p}\right)$$

$$= p-\left(\frac{-1}{p}\right),$$

ce qui termine la démonstration du lemme 1.5.2.
On aurait pu aussi obtenir ce résultat à partir du théorème 8.2 du livre de Hua [H] p. 174.

En appliquant ce lemme à la majoration de S_3 écrite dans (1.6), on a :

$$S_3 \ll P^{-1+\varepsilon}x^{3-2\theta}+P^{-2+\varepsilon_1}\sum_{2<p<q<P}\sum_{m<x^{2-2\theta}}\left(\frac{x}{pq}\frac{(m,pq)}{\sqrt{m}}+pq\right)$$

$$\ll P^{-1+\varepsilon_1}x^{3-2\theta}+P^{-2}x^{2-\theta+\varepsilon}+P^2x^{2-2\theta+\varepsilon_1}.$$

En prenant $P=x^{\theta/3}$, on obtient $S_3\ll x^{3-\frac{7\theta}{3}}+x^{2-4\theta/3+\varepsilon_1}$.
Pour $\theta>3/4$, il existe $\varepsilon>0$ tel que $S_3\ll x^{1-\varepsilon}$.

Il reste maintenant à majorer la somme S_4 définie dans (1.2).

1.6. Découpage de S_4.

On découpe l'intervalle $[x^t, x]$ en intervalles de la forme $[P_k, P_{k+1}]$, avec $P_k = 2^k \frac{x^t}{2}$, puis on partage la somme S_4 en :

$$S_4 = \sum_{0 \le k \le K} W_k, \tag{1.7}$$

avec

$$W_k = \sum_r C_k(r) \log r |\mathcal{A}_r|,$$

où les C_k sont des fonctions positives de classe C^∞, à support dans $[P_k, 4P_k]$, telles que $C_k^{(\ell)}(t) \ll P_k^{-\ell}$, uniformément sur t et vérifiant :

$$\sum_{0 \le k \le K} C_k(z) = \begin{cases} 1 & \text{si } x^t < z < x^{1+h}, \\ O(1) & \text{si } \frac{x^t}{2} < z < x^t \text{ ou si } x^{1+h} < z < 2x^{1+h}, \\ 0 & \text{sinon .} \end{cases}$$

Il apparaîtra à la fin de la majoration de S_4, que la perte de précision de l'inégalité (1.7), correspondant à la somme sur les r avec $x^t/2 < r < x^t$, ou $x^{1+h} < r < 2x^{1+h}$ est négligeable de l'ordre de $\dfrac{x}{\log x}$.
Le découpage dyadique de $[x^t, x]$ garantit un bon contrôle de r, par contre il n'est pas nécessaire de lisser cette variable, mais on a préféré adopter cette notation, car elle sera reprise lors de la preuve du théorème 2 où il faudra travailler dans un contexte lisse pour être en mesure d'appliquer les majorations en moyenne de sommes de Kloosterman.

Ainsi, on est amené à estimer des sommes de la forme :

$$W_P = \sum_{P < r < 4P} \log r . C(r) \sum_{\substack{n^2+1 \equiv 0 \pmod r \\ p|n \Rightarrow p > x^\alpha}} f(n), \tag{1.8}$$

ce qui se fera avec un crible de dimension 2 sur r et sur n.

1.7. Préparation au crible.

Pour $P \in [x^t/2, 2x^{1+h}]$, fixé, on pose :

$$S_P(d_1, d_2) = \sum_{\substack{m \in [P, 4P] \\ m \equiv 0 \pmod{d_2}}} C(m) \log m \sum_{\substack{n \equiv 0 \pmod{d_1} \\ n^2+1 \equiv 0 \pmod m}} f(m).$$

En reprenant les idées de Hooley [H1], nous allons établir la proposition suivante :

PROPOSITION 1.7. *Pour d_1 et d_2 sans facteur carré on a :*

$$S_P(d_1,d_2) = x_0 \frac{L(1,\chi_4)}{\zeta(2)} \frac{\omega(d_1,d_2)}{d_1 d_2} \int \frac{C(t)\log t}{t} dt + O\left(\frac{x\tau^2(d_2)P^{-1/2}\log P}{d_1 d_2^2}\right) + R(P,d_1,d_2),$$

$\omega(d_1,d_2)$ étant la fonction multiplicative définie par :

$$\omega(d_1,d_2) = \begin{cases} \rho(d_2) \prod_{\substack{p\equiv 1\ (4)\\ p\mid d_1 d_2}} \left(1+\frac{1}{p}\right)^{-1} \prod_{\substack{p\mid d_1\\ p\equiv 1\ (4)}} \left(1-\frac{1}{p}\right) \prod_{2\mid d_1 d_2} \left(1+\frac{1}{2}\right)^{-1} & \text{si } (d_1,d_2)=1, \\ 0 & \text{si } (d_1,d_2)>1, \end{cases}$$

avec $\rho(d) = |\{0 < v < d\ ,\ v^2+1 \equiv 0 \pmod d\}|$.

Le terme d'erreur $R(P,d_1,d_2)$ vérifie :

si $P < D^{-1}x$

$$\sum_{d<D} \mu^2(d) \sum_{d_1 d_2 = d} |R(P,d_1,d_2)| \ll x^\varepsilon \qquad \forall \varepsilon > 0,$$

si $P > xD^{-1}$:

$$\sum_{d<D} \mu^2(d) \sum_{d_1 d_2 = d} |R(P,d_1,d_2)| \ll P^{3/4} D^{3/2} x^\varepsilon \qquad \forall \varepsilon > 0.$$

Démonstration de la proposition 1.7.
Comme pour la majoration de S_1, on commence par appliquer la formule sommatoire de Poisson énoncée au lemme 1.3.1 :

$$S_P(d_1,d_2) = \sum_{m\equiv 0 \pmod{d_2}} C(m)\log m \sum_{\substack{0\le v<d_1 m\\ d_1\mid v\\ v^2+1\equiv 0 \pmod m}} \sum_{n\equiv v \pmod{d_1 m}} f(n)$$

$$= \sum_{m\equiv 0 \pmod{d_2}} C(m)\log m \sum_{h\in\mathbf{Z}} \hat f\left(\frac{h}{d_1 m}\right) \frac{1}{d_1 m} \sum_{\substack{0\le v<d_1 m\\ d_1\mid v\\ v^2+1\equiv 0 \pmod m}} e\left(\frac{-hv}{d_1 m}\right). \tag{1.9}$$

Le terme principal est donné par $h=0$, $\hat f(0) = x_0$ et dans le paragraphe suivant, on montrera que :

(1.10)

$$\sum_{m\equiv 0 \pmod{d_2}} C(m)\log m \frac{x_0}{d_1 m} \sum_{\substack{0\le v<d_1 m\\ d_1\mid v\\ v^2+1\equiv 0 \pmod m}} 1 = \frac{\omega(d_1,d_2)}{d_1 d_2} x_0 \frac{L(1,\chi_4)}{\zeta(2)} \int \frac{C(t)\log t}{t} dt + E_0,$$

où E_0 est une erreur assez petite.

Pour $h \neq 0$, comme pour S_1, on montre que $\hat{f}\left(\frac{h}{d_1 m}\right) \ll \frac{1}{h^2}$, pour $|h| > H$, avec $H = P d_1 x^{-1+\varepsilon}$.

Ainsi, pour $d_1 \leq D < x^{1-\varepsilon} P^{-1}$, on a $H \leq 1$ et $\sum_{d<D} \mu^2(d) \sum_{d_1 d_2 = d} |R(P, d_1, d_2)| \ll x^{\varepsilon}$, ce qui prouve le premier résultat annoncé (cas $P < xD^{-1}$).

Pour P grand, $P > xD^{-1}$, on va améliorer ce résultat en faisant intervenir des sommes d'exponentielles. On compte profiter d'éventuelles compensations sur la somme $\sum_m \sum_v e\left(\frac{-hv}{d_1 m}\right)$ que l'on transforme avec le lemme 0 énoncé dans l'introduction.
Le problème est que lorsqu'on écrit $m = r^2 + s^2$, on a souvent $(s, d_1) > 1$, ce qui nous empêche d'inverser $d_1 \bmod s$. Il faut donc tenir compte de ce pgcd, ce qui rend les opérations plus délicates.
On doit estimer pour $H = PDx^{-1+\varepsilon}$:

$$R'_P(d_1, d_2) = \sum_{0<|h|<H} \sum_{m \equiv 0 \pmod{d_2}} C(m) \log m \hat{f}\left(\frac{h}{d_1 m}\right) \frac{1}{d_1 m} \sum_{\substack{0<v<d_1 m \\ d_1 | v \\ v^2+1 \equiv 0 \pmod m}} e\left(\frac{-hv}{d_1 m}\right).$$

Le lemme de Gauss (le lemme 0) nous permet d'écrire que :

$$R'_P \ll \sum_{\sigma | d_1} \sum_{0<|h|<H} \sum_{\substack{r^2+s^2 \equiv 0 \pmod{d_2} \\ (r,s)=1\ ,\ |r|<s \\ \sigma=(s,d_1) \\ (r^2+s^2, d_1)=1}} C(r^2+s^2) \log(r^2+s^2)$$

$$\times \hat{f}\left(\frac{h}{d_1(r^2+s^2)}\right) \frac{1}{d_1(r^2+s^2)} e\left(\frac{-hv\{r,s\}}{d_1(r^2+s^2)}\right), \tag{1.11}$$

avec $v\{r,s\} = d_1 w\{r,s\}$ et $w\{r,s\} = \bar{d}_1 \left(\frac{\bar{r}}{s}(r^2+s^2) - \frac{r}{s}\right)$,
où $\bar{r}$ est un inverse de $r \bmod s$ et $\bar{d}_1$ un inverse de $d_1 \mod (r^2+s^2)$.
Bien que m ait parfois plusieurs écritures sous la forme $m = r^2 + s^2$, on n'a rien rajouté dans la ligne (1.11), car d'après le lemme 0, ces écritures sont en bijection avec les solutions v de la congruence $v^2 + 1 \equiv 0 \pmod m$.

Transformation de $e\left(\frac{-hv\{r,s\}}{d_1(r^2+s^2)}\right) = e\left(\frac{-h\bar{d}_1}{(r^2+s^2)}\left(\frac{\bar{r}}{s}(r^2+s^2) - \frac{r}{s}\right)\right)$.
On voudrait développer directement l'intérieur de l'exponentielle, mais ce n'est pas possible car d_1 n'est *a priori* pas inversible $\bmod s$, et on doit utiliser le lemme d'inversion suivant :

LEMME 1.7.1. *(réécriture de Bezout).*

Pour $(n_1, n_2) = 1$, *on a :* $\frac{\bar{n}_1}{n_2} + \frac{\bar{n}_2}{n_1} = \frac{1}{n_1 n_2} \pmod 1$.

On écrit $d_1 = \delta\sigma$, avec $\sigma = (s, d_1)$; on a alors $(\delta, \sigma) = 1$, car d_1 est sans facteur carré. Dans le lemme 0, le choix de $\bar{r} \bmod s$ est libre, plus précisément, si a et a' sont deux inverses de $r \bmod s$, alors,

$$\frac{a'}{s}(r^2+s^2) - \frac{r}{s} \equiv \frac{a}{s}(r^2+s^2) - \frac{r}{s} \ (\mathrm{mod}\, r^2+s^2).$$

On prend alors dans l'expression de $v\{r,s\}$, $\bar{r}^{(\sigma s)}$, la place de $\bar{r}$, $\bar{r}^{(\sigma s)}$ désignant un inverse de $r \bmod \sigma s$.
On pose $\Omega = \dfrac{\bar{r}^{(\sigma s)}}{s}(r^2+s^2) - \dfrac{r}{s}$. Soit $\bar{\delta}$ un inverse de δ modulo $\sigma s(r^2+s^2)$, ceci est cohérent car d_1 est sans facteur carré.
En appliquant le lemme 1.7.1 à $n_1 = \sigma$, $n_2 = r^2+s^2$ on a :

$$\begin{aligned} e\left(\frac{-h\bar{d}_1\Omega}{r^2+s^2}\right) &= e\left(\frac{-h\bar{\delta}\Omega\bar{\sigma}}{r^2+s^2}\right) \\ &= e\left(\frac{-h\bar{\delta}\Omega}{\sigma(r^2+s^2)} + \frac{h\bar{\delta}\Omega\overline{(r^2+s^2)}^{(\sigma s)}}{\sigma}\right), \end{aligned} \tag{1.12}$$

où, $\overline{r^2+s^2}^{(\sigma s)}$ est un inverse de r^2+s^2 modulo σs.
En développant la formule définissant Ω, en utilisant le fait que $\sigma | s$, on a :

$$e\left(\frac{\Omega}{\sigma}\right) = e\left(\frac{\bar{r}^{(\sigma s)}r^2}{\sigma s} - \frac{r}{\sigma s}\right) = 1.$$

L'égalité (1.12) se simplifie donc pour devenir :

$$\begin{aligned} e\left(\frac{-h\bar{d}_1\Omega}{r^2+s^2}\right) &= e\left(\frac{-h\bar{\delta}\Omega}{\sigma(r^2+s^2)}\right) \\ &= e\left(\frac{-h\bar{\delta}\bar{r}}{\sigma s} + \frac{h\bar{\delta}r}{\sigma s(r^2+s^2)}\right). \end{aligned}$$

L'exponentielle $e\left(\dfrac{-h\bar{\delta}\bar{r}}{\sigma s}\right)$ créera une somme de Kloosterman. Par contre on ne peut pas traiter directement $e\left(\dfrac{h\bar{\delta}r}{\sigma s(r^2+s^2)}\right)$.
Pour se débarrasser du $\bar{\delta}$, dans cette dernière exponentielle on réapplique le lemme d'inversion à $n_1 = \delta$, $n_2 = \sigma s(r^2+s^2)$:

$$e\left(\frac{h\bar{\delta}r}{\sigma s(r^2+s^2)}\right) = e\left(\frac{hr}{\delta\sigma s(r^2+s^2)} - \frac{hr\overline{\sigma s(r^2+s^2)}}{\delta}\right).$$

On obtient finalement :

$$e\left(\frac{-hv\{r,s\}}{d_1(r^2+s^2)}\right) = e\Bigg(\underbrace{\frac{-h\bar{\delta}\bar{r}}{\sigma s}}_{\substack{\text{terme de somme} \\ \text{de Kloosterman}}} + \underbrace{\frac{hr}{d_1 s(r^2+s^2)}}_{\substack{\text{terme} \\ \text{lisse}}} - \underbrace{\frac{hr\overline{\sigma s(r^2+s^2)}}{\delta}}_{\substack{\text{terme constant} \\ \text{lorque les congruences} \\ \text{de } r \text{ et } s \bmod \delta \\ \text{sont fixées}}}\Bigg).$$

Les variables de sommation importantes sont r et s.

Dans ces deux dernières lignes, et dans toute la suite, les barres $\bar{}$ d'inverses ont maintenant le sens habituel relatif au dénominateur. Le terme lisse ne pose aucun problème, on s'en débarasse en faisant une intégration par partie. Par contre, l'exponentielle de dénominateur δ est un terme fortement oscillant, et même lorque δ est petit, ce terme nous empêche d'utiliser les majorations de Deshouillers et Iwaniec [D-I2] de sommes de sommes de Kloosterman.

Estimation de la somme sur r de (1.11).
Pour alléger l'écriture , on pose :

$$F(r,s) = e\left(\frac{hr}{d_1 s(r^2+s^2)}\right)\frac{C(r^2+s^2)\log(r^2+s^2)}{d_1(r^2+s^2)}\hat{f}\left(\frac{h}{d_1(r^2+s^2)}\right).$$

Pour $0 < |h| < H$ et $P^{1/2} < s < 2P^{1/2}$, $(\sigma, s) = 1$, fixés, on étudie :

$$\Sigma_s = \sum_{\substack{r^2+s^2\equiv 0 \pmod{d_2}\\ |r|<s\ ,\ (r,s)=1}} e\left(\frac{-hr\bar{\sigma}\bar{s}\overline{(s^2+r^2)}}{\delta}\right) e\left(\frac{-h\bar{\delta}\bar{r}}{\sigma s}\right) F(r,s). \tag{1.13}$$

On développe les congruences sur r en somme d'exponentielles :

$$\begin{aligned}
\Sigma_s &= \frac{1}{d_2\sigma s\delta}\sum_{\ell=1}^{d_2\sigma s\delta}\sum_{\substack{\rho \bmod d_2\sigma s\delta\\ \rho^2+s^2\equiv 0 \pmod{d_2}\\ (\rho,s)=1}}\sum_{|r|<s} e\left(\frac{\ell(r-\rho)}{d_2\delta\sigma s}\right)F(r,s)\\
&\quad\times e\left(\frac{-h\bar{\delta}\bar{\rho}}{\sigma s}\right)e\left(\frac{-h\rho\bar{\sigma}\bar{s}\overline{(s^2+\rho^2)}}{\delta}\right)\\
&= \frac{1}{d_1 d_2 s}\sum_{\ell=1}^{d_1 d_2 s}\sum_{|r|<s} F(r,s)e\left(\frac{\ell r}{d_1 d_2 s}\right)\\
&\quad\times\sum_{\substack{\rho \bmod d_2\sigma s\delta\\ \rho^2+s^2\equiv 0 \pmod{d_2}\\ (\rho,s)=1}} e\left(\frac{-h\bar{\delta}\bar{\rho}}{\sigma s}\right)e\left(\frac{-h\rho\bar{\sigma}\bar{s}\overline{(s^2+\rho^2)}}{\delta}\right)e\left(\frac{-\ell\rho}{d_1 d_2 s}\right)\\
&= \frac{1}{d_1 d_2 s}\sum_{\ell=1}^{d_1 d_2 s}\Sigma_r^{(2)}\Sigma_\rho,
\end{aligned} \tag{1.14}$$

par définition.

• Pour la somme sur r on fait une transformation d'Abel :

$$\Sigma_r^{(2)} \ll \left(\sum_{|r|<s} e\left(\frac{\ell r}{d_1 d_2 s}\right)\right) F(s,s) - \int_{-s}^{s} \left(\sum_{-s<r<t} e\left(\frac{\ell r}{d_1 d_2 s}\right)\right) \frac{\partial F}{\partial t}(t,s)dt$$

$$\ll \min\left(s, \left\|\frac{\ell}{d_1 d_2 s}\right\|^{-1}\right) \frac{x^{1+\epsilon}}{d_1 P}$$

$$+ \min\left(s, \left\|\frac{\ell}{d_1 d_2 s}\right\|^{-1}\right) \int_{-s}^{s} \left(\frac{x^{1+\epsilon} t}{d_1 (t^2+s^2)^2} + \frac{x^{2+\epsilon} th}{d_1^2 (t^2+s^2)^3}\right) dt.$$

Pour écrire ceci on a fait les calculs suivants : comme $\hat{f}\left(\frac{h}{d_1(r^2+s^2)}\right) \ll x$,on a l'inégalité : $F(r,s) \ll x^{1+\epsilon}/(d_1 P)$.
On étudie ensuite la dérivée de F à partir de l'écriture :

$$F(r,s) = e\left(\frac{hr}{d_1 s(r^2+s^2)}\right) \frac{C(r^2+s^2)\log(r^2+s^2)}{d_1(r^2+s^2)} \hat{f}\left(\frac{h}{d_1(r^2+s^2)}\right).$$

Pour s fixé , lorsqu'on dérive par rapport à r les dérivées de C , du log donnent un terme du type $\frac{x^{1+\epsilon} r}{d_1(r^2+s^2)^2}$,
celle de l'exponentielle, donne un terme de l' ordre de :

$$\frac{x^{1+\epsilon}}{d_1(r^2+s^2)} \left|\frac{\partial}{\partial r} e\left(\frac{hr}{d_1 s(r^2+s^2)}\right)\right| \ll \frac{x^{1+\epsilon}}{d_1(r^2+s^2)} \frac{hs}{d_1(r^2+s^2)^2}.$$

Enfin, pour le terme $\hat{f}$, on a :

$$\frac{\partial}{\partial r} \hat{f}\left(\frac{h}{d_1(r^2+s^2)}\right) \ll \frac{x^{2+\epsilon} hr}{d_1(r^2+s^2)^2},$$

ce qui donne :

$$\frac{\partial F}{\partial t}(t,s) \ll \frac{x^{1+\epsilon} s}{d_1(t^2+s^2)^2} + \frac{x^{2+\epsilon} hs}{d_1^2(t^2+s^2)^3}.$$

On a donc

$$\sum_{|r|<s} F(r,s) e\left(\frac{\ell r}{d_1 d_2 s}\right) \ll \left(\frac{x^{1+\epsilon}}{d_1 P} + \frac{x^{2+\epsilon} h}{d_1^2 P^2}\right) \min\left(s, \left\|\frac{\ell}{d_1 d_2 s}\right\|^{-1}\right).$$

Pour $0 < |h| < H$, le premier terme du membre de droite l'emporte sur le deuxième.
On en déduit que

$$\Sigma_r^{(2)} = \sum_{|r|<s} F(r,s) e\left(\frac{\ell r}{d_1 d_2 s}\right) \ll \frac{x^{1+\epsilon}}{d_1 P} \min\left(s, \left\|\frac{\ell}{d_1 d_2 s}\right\|^{-1}\right). \tag{1.15}$$

• *Estimation de la somme sur ρ.*
D'après (1.14), on a :

$$\Sigma_\rho = \sum_{\substack{\rho \bmod d_2\sigma s\delta \\ \rho^2+s^2\equiv 0 \pmod{d_2} \\ (\rho,s)=1}} e\left(\frac{-h\bar{\delta}\bar{\rho}}{\sigma s}\right) e\left(\frac{-h\rho\bar{\sigma}\bar{s}\overline{(s^2+\rho^2)}}{\delta}\right) e\left(\frac{-\ell\rho}{d_1 d_2 s}\right).$$

Comme $(d_2, d_1 s) = 1$, grâce au théorème de Bezout, on peut écrire $\rho = ud_2 + vd_1 s$, ce qui donne :

$$\Sigma_\rho = \sum_{\substack{v \bmod d_2 \\ d_1^2 v^2+1\equiv 0 (\bmod d_2)}} e\left(\frac{-lv}{d_2}\right)$$

$$(1.16) \quad \times \sum_{\substack{u \bmod d_1 s \\ (u,s)=1 \\ (d_2^2u^2+s^2,\delta)=1}} e\left(\frac{-h\bar{\delta}\bar{d}_2\bar{u}}{\sigma s}\right) e\left(\frac{-hd_2u\bar{\sigma}\bar{s}\overline{(s^2+d_2^2u^2)}}{\delta}\right) e\left(\frac{-\ell u}{d_1 s}\right).$$

• la somme sur v est un $O(2^{\nu(d_2)})$.
En utilisant à nouveau Bezout et en profitant du fait que $(\delta, \sigma s) = 1$, on écrit $u = \alpha\sigma s + \beta\delta$, on obtient alors pour la somme sur u :
(1.17)

$$\Sigma_u = \sum_{\substack{(\beta,s)=1 \\ \beta \bmod \sigma s}} e\left(\frac{-h\overline{d_2\delta^2}\bar{\beta} - \ell\beta}{\sigma s}\right) \sum_{\alpha \bmod \delta}{}^{*} e\left(\frac{-hd_2\alpha\overline{(\alpha^2 d_2^2\sigma^2 s^2 + s^2)} - \ell\alpha}{\delta}\right),$$

où $*$ indique que la somme porte sur les α tels que l'exponentielle soit définie (ici sur les α tels que $(\alpha^2 d_2^2\sigma^2 + 1, \delta) = 1$).
• la somme sur β est une somme de Kloosterman et d'après la majoration classique de Weil cette somme est un $O\left((\sigma s)^{1/2+\varepsilon}(\sigma s, h, \ell)^{1/2}\right)$.
• il reste à estimer

$$\Sigma_\alpha = \sum_{\alpha \bmod \delta}{}^{*} e\left(\frac{-hd_2\alpha\overline{(\alpha^2 d_2^2\sigma^2 s^2 + s^2)} - \ell\alpha}{\delta}\right).$$

Comme δ est sans facteur carré on peut établir le résultat suivant :

LEMME 1.7.2. *La somme Σ_α se décompose en :*

$$\Sigma_\alpha = \prod_{p|\delta} \sum_{\alpha \bmod p}{}^{*} e\left(\frac{-hd_2\overline{(\delta/p)}\bar{s}^2\alpha\overline{(d_2^2\sigma^2\alpha^2+1)} - \ell\overline{(\delta/p)}\alpha}{p}\right).$$

Il suffit de prouver ceci pour $\delta = p_1 p_2$ où p_1 et p_2 sont 2 nombres premiers distincts, ce qui se fait en écrivant $\alpha = \alpha_1 p_2 + \alpha_2 p_1$ puis en séparant les deux nouvelles sommes ainsi obtenues.
Grâce au lemme 1.7.2 , il nous suffit d'évaluer :

$$\sum_{\alpha \bmod p}{}^{*} e\left(\frac{-hd_2\overline{(\delta/p)}\bar{s}^2\alpha\overline{(d_2^2\sigma^2\alpha^2+1)} - \ell\overline{(\delta/p)}\alpha}{p}\right).$$

Si $p|(h,\ell)$, cette somme vaut à peu près p, elle est quasiment nulle si $p|h$ mais $p \not| \ell$, ces deux résultats étant exacts à 0, 1 ou 2 près selon le nombre pôles α exclus par la condition $*$.
Lorsque $(p,h) = 1$, on estime cette somme avec le lemme suivant qui est un cas particulier d'un résultat énoncé par Deligne dans [D], et qui traite de la majoration d'une somme d'exponentielle d'une fraction rationnelle, dans l'esprit du théorème de Weil :

LEMME 1.7.3. *Soit* $\mathbf{P}^1$ *la droite projective sur* $\mathbf{F}_p$, *et soit* f *un morphisme* $f : \mathbf{P}^1 \longrightarrow \mathbf{P}^1$, *non identiquement égal à* ∞.

Soit

$$S_f = \sum_{\substack{x \in \mathbf{P}^1 \\ f(x) \neq \infty}} e\left(\frac{f(x)}{p}\right).$$

Pour tout point x *de* $\mathbf{P}^1$, *on pose* $v_x(f) =$ *ordre du pôle de* f *en* x *si* $f(x) = \infty$, $v_x(f) = 0$ *sinon. Alors on a :*

$$|S_f| \leq \sum_{v_x(f) \neq 0} (1 + v_x(f)) p^{1/2}.$$

Dans notre situation, on a $f(x) = ax + \dfrac{bx}{c^2x^2+1}$ avec $a = -\ell\overline{(\delta/p)}$,
$b = -hd_2\overline{(\delta/p)}\bar{s}^2$ et $c = d_2\sigma$.
Si $p \equiv 1 \bmod 4$, f a 3 pôles ∞, $\bar{c}\sqrt{-1}$, $-\bar{c}\sqrt{-1}$ et $v_x(f) = 1$, en ces pôles.
Si $p \equiv -1 \bmod 4$ f a un seul pôle ∞ et $v_\infty(f) = 1$.
On a donc

$$|S_f| \leq 6p^{1/2}.$$

Ce qui donne

$$\Sigma_\alpha \ll 6^{\nu(\delta)}\delta^{1/2}(\delta,h,\ell)^{1/2},$$

et en reportant dans (1.17), on a $\Sigma_u \ll (d_1 s)^{1/2+\varepsilon}(d_1 s, h)^{1/2}$, puis dans (1.16), on obtient pour Σ_ρ :

$$\Sigma_\rho \ll (sd_1)^{1/2+\varepsilon}(d_1 s, h)^{1/2}.$$

En injectant ceci avec (1.15), dans (1.14), on trouve :

$$\Sigma_s \ll \frac{x^{1+\varepsilon}}{d_1 P} d_1^{1/2} s^{1/2} (d_1 s, h)^{1/2}.$$

On reporte ceci dans (1.11), et en faisant le changement de variables $s \leftrightarrow \sigma s$, on a la majoration :

$$R'(P,d_1,d_2) \ll \sum_{\sigma\delta=d_1} \sum_{P^{1/2}<s\sigma<2P^{1/2}} \frac{x^{1+\varepsilon} d_1^{1/2} s^{1/2} \sigma^{1/2}}{d_1 P} \sum_{0<|h|<H} (\sigma s, h)^{1/2}.$$

La somme sur h dans le terme de droite est un $O(H^{1+\varepsilon})$.
Comme $H = d_1 P x^{-1+\varepsilon}$, on a :

$$\begin{aligned} R'(P,d_1,d_2) &\ll \sum_{\sigma\delta=d_1} x^{\varepsilon} \sum_{P^{1/2}<\sigma s<2P^{1/2}} (\sigma s)^{1/2} d_1^{1/2} \\ &\ll P^{3/4} x^{\varepsilon} \sum_{\sigma\delta=d_1} d_1^{1/2} \sigma^{-1/2} \ll P^{3/4} x^{\varepsilon} d_1^{1/2}. \end{aligned}$$

Ce qui donne

$$\begin{aligned} \sum_{d<D} \mu^2(d) \sum_{d_1 d_2=d} |R(P,d_1,d_2)| &\ll \sum_{d<D} P^{3/4} x^{\varepsilon} d^{1/2} \\ &\ll P^{3/4} x^{\varepsilon} D^{3/2}, \end{aligned}$$

ce qui correspond au résultat annoncé dans la proposition 1.7.

• *Évaluation du terme principal.*
Il s'agit d'évaluer :

$$T_P(d_1,d_2) = x \sum_{m\equiv 0 \pmod{d_2}} \frac{\log m . C(m)}{d_1 m} \sum_{\substack{0<v<d_1 m \\ d_1|v \\ v^2+1\equiv 0 \pmod m}} 1.$$

On va montrer le lemme suivant :

LEMME 1.7.4. *On a l'égalité :*

$$T_P(d_1,d_2) = \frac{xL(1,\chi_4)}{\zeta(2)} \frac{\omega(d_1,d_2)}{d_1 d_2} \int \frac{C(t)\log t}{t} dt + O\left(x \frac{\tau^2(d_2) P^{-1/2} \log P}{d_1 d_2^2}\right),$$

avec

$$\omega(d_1,d_2) = \begin{cases} 0 & \text{si } (d_1,d_2) > 1, \\ \rho(d_2) \displaystyle\prod_{\substack{p|d_1 d_2 \\ p\equiv 1 (\mathrm{mod}\, 4)}} \left(1+\frac{1}{p}\right)^{-1} \prod_{\substack{p|d_1 \\ p\equiv 1 \pmod 4}} \left(1-\frac{1}{p}\right) \prod_{2|d_1 d_2} \left(1+\frac{1}{2}\right)^{-1} & \text{sinon.} \end{cases}$$

La démonstration de ce lemme est calquée sur celles de Hooley [H1], Deshouillers et Iwaniec [D-I1]. On commence par utiliser des séries génératrices. Soit

$$h_{a,\ell}(s) = \sum_{d\geq 1} \frac{\rho(a,\ell d)}{d^s},$$

avec $\rho(a,d) = |\{n \in \{0,...,d-1\},\ a^2n^2+1 \equiv 0 \pmod d\}|$.
Pour $a = 1$ on a $\rho(1,\ell d) = \rho(\ell d)$,
si $(a,d) = 1$, $\rho(a,d) = \rho(d)$,
si $(a,\ell) > 1$, $h_{a,\ell}(s) = 1$ pour tout s.
Dans la suite, on suppose que $(a,\ell) = 1$ et que ℓ et a sont sans facteur carré, et on va établir que :
(1.19)

$$h_{a,\ell}(s) = \rho(\ell)\frac{\zeta(s)L(s,\chi_4)}{\zeta(2s)} \prod_{\substack{p|a\ell \\ p\equiv 1 \pmod 4}} \left(1+\frac{1}{p^s}\right)^{-1} \prod_{\substack{p|a \\ p\equiv 1 \pmod 4}} \left(1-\frac{1}{p^s}\right) \prod_{2|a\ell} \left(1+\frac{1}{2^s}\right)^{-1}$$

En effet, on a l'égalité :

$$h_{a,\ell}(s) = \prod_{(p,a\ell)=1} \left(\sum_{k\in\mathbb{N}} \frac{\rho(p^k)}{p^{ks}}\right) \prod_{\substack{p|\ell \\ p\neq 2}} \left(\sum_{k\in\mathbb{N}} \frac{\rho(p^{k+1})}{p^{ks}}\right)$$

$$= \rho(\ell) \prod_{(p,a\ell)=1} \left(\sum_{k\in\mathbb{N}} \frac{\rho(p^k)}{p^{ks}}\right) \prod_{\substack{p|\ell \\ p\equiv 1 \pmod 4}} \left(1-\frac{1}{p^s}\right)^{-1},$$

car d'après le lemme 1.2.3, $\dfrac{\rho(p^{k+1})}{p^{ks}} = \dfrac{\rho(p)}{p^{ks}}$, pour $p \neq 2$,
$\rho(p) = 0$ si $p \equiv -1 \pmod 4$
$\rho(2) = 1$,et $\rho(2^k) = 0$ pour $k > 1$.
Donc $\displaystyle\sum_{k\in\mathbb{N}} \frac{\rho(2^{k+1})}{2^{ks}} = 1$

Soit $h(s) = \displaystyle\sum_{d\in\mathbb{N}} \frac{\rho(d)}{d^s} = h_{1,1}(s)$; on a encore $h(s) = \dfrac{\zeta(s)L(s,\chi_4)}{\zeta(2s)}$.

On évalue alors le rapport $\dfrac{h_{a,\ell}(s)}{h(s)}$:

$$\frac{h_{a,\ell}(s)}{h(s)} = \rho(\ell)\frac{\prod_{(p,a\ell)=1}\left(\sum_{k\in\mathbb{N}} \frac{\rho(p^k)}{p^{ks}}\right)}{\prod_{p}\left(\sum_{k\in\mathbb{N}} \frac{\rho(p^k)}{p^{ks}}\right)} \prod_{\substack{p|\ell \\ p\equiv 1 \pmod 4}} \left(1-\frac{1}{p^s}\right)^{-1}$$

$$= \rho(\ell) \prod_{p|a\ell} \left(\sum_{k\in\mathbb{N}} \frac{\rho(p^k)}{p^{ks}}\right)^{-1} \prod_{\substack{p|\ell \\ p\equiv 1 \pmod 4}} \left(1-\frac{1}{p^s}\right)^{-1}.$$

Lorsque $\rho(\ell) \neq 0$ cela donne :

$$\frac{h_{a,\ell}(s)}{h(s)} = \rho(\ell) \prod_{\substack{p|a\ell \\ p\equiv 1 (\mathrm{mod}\, 4)}} \left(1+\frac{1}{p^s}\right)^{-1} \prod_{\substack{p|a\ell \\ p\equiv 1 (\mathrm{mod}\, 4)}} \left(1-\frac{1}{p^s}\right) \times \prod_{\substack{p|\ell \\ p\equiv 1 (\mathrm{mod}\, 4)}} \left(1-\frac{1}{p^s}\right)^{-1} \prod_{2|a\ell} \left(1+\frac{1}{2^s}\right)^{-1}.$$

Après quelques simplifications, et en profitant du fait que $(a,\ell)=1$, on trouve :

$$h_{a,\ell}(s) = \rho(\ell)h(s) \prod_{\substack{p|a\ell \\ p\equiv 1 (\mathrm{mod}\, 4)}} \left(1+\frac{1}{p^s}\right)^{-1} \prod_{\substack{p|a \\ p\equiv 1 \ (\mathrm{mod}\, 4)}} \left(1-\frac{1}{p^s}\right) \prod_{2|a\ell} \left(1+\frac{1}{2^s}\right)^{-1}.$$

Pour finir, on recopie Deshouillers et Iwaniec [D-I1].
On écrit

$$\frac{C(m)\log m}{m} = \frac{1}{2i\pi}\int_{(\sigma)} \frac{R(s)}{m^s} ds$$

avec $\sigma > 0$, et $R(s)$ est la transformée de Mellin de la fonction $u \mapsto \dfrac{C(u)\log u}{u}$.
D'après la formule d'inversion de Mellin, en faisant 2 intégrations par parties , on montre que :

$$R(s) = \int C(y)\frac{\log y}{y} y^{s-1} dy \ll (|s|+1)^{-2} P^{\sigma-1}\log P.$$

Soit $\sigma > 1$, on a l'égalité :

$$\sum_{m\equiv 0 (\mathrm{mod}\, d_2)} \frac{C(m)\log m}{m}\rho(d_1,m) = \frac{1}{2i\pi}\int_{(\sigma)} \frac{R(s)h_{d_1,d_2}(s)}{d_2^s} ds.$$

Ensuite, suivant Deshouillers et Iwaniec [D-I1] p. 9, on décale cette intégrale à

$\Re = 1/2$ et en reprenant leurs résultats :

$$\sum_{m\equiv 0(\mathrm{mod}\, d_2)} \frac{C(m)\log m}{m}\rho(d_1,m) = \frac{R(1)\rho(d_2)}{d_2}\frac{L(1,\chi_4)}{\zeta(2)}$$
$$\times \prod_{\substack{p|d_1d_2\\ p\equiv 1 \pmod 4}} \left(1+\frac{1}{p}\right)^{-1} \prod_{\substack{p|d_1\\ p\equiv 1 \pmod 4}} \left(1-\frac{1}{p}\right) \prod_{2|d_1d_2} \left(1+\frac{1}{2}\right)^{-1}$$
$$+ \frac{1}{2i\pi}\int_{(1/2)} \frac{R(s)h_{d_1,d_2}(s)}{d_2^s}ds$$
$$= \frac{\rho(d_2)}{d_2}\frac{L(1,\chi_4)}{\zeta(2)}\int \frac{C(y)\log y}{y}dy$$
$$\times \prod_{\substack{p|d_1d_2\\ p\equiv 1 \pmod 4}} \left(1+\frac{1}{p}\right)^{-1} \prod_{\substack{p|d_1\\ p\equiv 1 \pmod 4}} \left(1-\frac{1}{p}\right) \prod_{2|d_1d_2} \left(\frac{2}{3}\right)$$
$$+ \underbrace{O\left(\frac{P^{-1/2}\log P}{d_2^{1/2}}\int (|s|+1)^{-2}2^{\nu}(d_2)\left|\frac{\zeta(s)L(s,\chi_4)}{\zeta(2s)}\right|ds\right)}_{O\left(\frac{\tau^2(d_2)P^{-1/2}\log P}{d_2^{1/2}}\right)},$$

ce qui termine la preuve du lemme 1.7.4 et ainsi celle de la proposition 1.7.

1.8. Majoration de S_4.

On part de l'inégalité (les quantités W_P étant celles définies à la ligne (1.8)) :

$$W_P \leq \sum_{\substack{n^2+1\equiv 0 \pmod m\\ p|mn\Rightarrow p>x^\alpha}} \log m C(m) f(n).$$

Soient $(\lambda)_d$ les poids de Selberg correspondant à ce problème de crible.(Pour une définition précise, on peut consulter le livre d'Halberstam et Richert [H-R] chapitre 3 p. 97.)
On a alors la majoration :

$$W_P \leq \sum_{\substack{m,n\\ n^2+1\equiv 0 \pmod m}} \log m C(m) f(n) \left(\sum_{\substack{d|P(x^\alpha)\\ d|mn}} \lambda_d\right)^2.$$

On développe ensuite ce carré, et en reprenant les notations du tout début du paragraphe 1.7, on a l'inégalité :

$$W_P \leq \sum_{d_1,d_2|P(x^\alpha)} \lambda_{d_1}\lambda_{d_2} \sum_{ab=[d_1,d_2]} S_P(a,b),$$

car $S_P(d_1,d_2) = 0$ dès que $(a,b) = 1$.

On applique alors la proposition 1.7 :

$$W_p \leq \sum_{d_1,d_2|P(x^\alpha)} \lambda_{d_1}\lambda_{d_2} x_0 \frac{L(1,\chi_4)}{\zeta(2)} \int \frac{C(t)\log t}{t} dt. \frac{\Omega([d_1,d_2])}{[d_1,d_2]}$$
$$\sum_{d_1,d_2|P(x^\alpha)} \lambda_{d_1}\lambda_{d_2} \sum_{ab=[d_1,d_2]} R(P,a,b),$$

avec $\Omega([d_1,d_2]) = \sum_{ab=[d_1,d_2])} \omega(a,b)$, car $\omega(a,b) = 0$ si $(a,b) > 1$.
D'après les valeurs de ω données dans la proposition 1.7, on a :

$$\Omega(p) = \begin{cases} 4/3 & \text{si } p = 2, \\ \dfrac{3p-1}{p+1} & \text{si } p \equiv 1 \pmod 4, \\ 1 & \text{si } p \equiv -1 \pmod 4. \end{cases}$$

Les conditions d'application du théorème A2 sont remplies, et en appliquant ce résultat de Selberg sur les cribles de dimension 2, puis en sommant sur P, on obtient pour S_4 la majoration :

$$S_4 \leq \prod_{p<x^\alpha} \left(1 - \frac{\Omega(p)}{p}\right) \frac{L(1,\chi_4)}{\zeta(2)} \int \frac{du}{u\sigma_2\left(\frac{\log D(u)}{\log x^\alpha}\right)} + O\left(\varepsilon x + \frac{x}{\log x}\right),$$

avec d'après la formule du terme d'erreur de la proposition 1.7, $D(u) = x^{2/3-\varepsilon}t^{-1/2}$.
A partir des valeurs de Ω données ci-dessus, on a l'égalité :

$$\prod_{p<x^\alpha} \left(1 - \frac{\Omega(p)}{p}\right) = \frac{\zeta(2)}{L(1,\chi_4)} \prod_{p<x^\alpha} \left(1 - \frac{1}{p}\right)^2 \left(1 + O\left(\frac{1}{\log x}\right)\right).$$

Grâce à tout ceci, on a le

LEMME 1.8. *On a la majoration :*

$$S_4 \leq \frac{x_0 e^{-2\gamma}}{\alpha^2} \int_t^{1+h} \frac{\lambda d\lambda}{\sigma_2\left(\frac{2/3-\lambda/2}{\alpha}\right)} + O\left(\varepsilon x + \frac{x}{\log x}\right).$$

1.9. Conclusion.

En revenant à l'égalité (1.2), puis en y reportant (1.1), les lemmes 1.2.2, 1.3.3, 8.1, et les résultats des paragraphes 1.4, et 1.5, on a :

$$\begin{aligned} S_5 &= V_\alpha(x) - S_0 - S_1 - S_2 - S_3 - S_4 \\ &\geq x_0\left(\frac{3w(\alpha^{-1})}{2\alpha} - \frac{e^{-\gamma}}{\alpha}\int_{1/2-\varepsilon}^{2/3} F\left(\frac{3/2-7\varepsilon-7\lambda/4}{\alpha}\right)d\lambda - \frac{e^{-\gamma}}{\alpha}\int_{2/3}^{t} F\left(\frac{1-\lambda}{\alpha}\right)d\lambda\right) \\ &\quad - x_0\frac{e^{-2\gamma}}{\alpha^2}\int_t^{1+h} \frac{\lambda d\lambda}{\sigma_2\left(\frac{2/3-\lambda/2}{\alpha}\right)} + O(\varepsilon x_0) + O\left(\frac{x}{\log x}\right) \\ &\geq x_0\left(\frac{3w(\alpha^{-1})}{2\alpha} - I_1 - I_2 - I_3\right) + O(\varepsilon x_0) + O\left(\frac{x}{\log x}\right), \end{aligned}$$

par définition.

On cherche alors α le plus grand possible tel que la minoration ci dessus soit strictement positive.

Pour $\alpha^{-1} > 5.5$, on a $w(\alpha^{-1}) = e^{-\gamma} \pm 10^{-5}$, on approximera donc la fonction w par $e^{-\gamma}$.
Le réel t correspond au raccord des deux intégrales I_2 et I_3, c'est à dire que t est solution de

$$\frac{2}{1-\lambda} = \frac{e^{-2\gamma}\lambda}{\alpha^2 \sigma_2(u(\lambda))},$$

avec $u(\lambda) = \dfrac{2/3 - \lambda/2}{\alpha}$.
Mais pour $1/12 > \alpha > 1/24$, et $t > 14/15$, on a $u(\lambda) \in [2,4]$, et

$$\sigma_2(u(\lambda)) = e^{-2\gamma}[(1/2 + \frac{\log 2}{4} - \frac{\log(u(\lambda))}{4})u^2(\lambda) - u(\lambda) + 1/2],$$

et le réel t ne peut être déterminé directement.

Calcul de I_1.
Comme $\varepsilon > 0$ et $h > 0$ sont arbitrairement petits, on n'en tient pas compte dans tous les calculs qui vont suivre. Pour $u \geq 2$, on a l'égalité : $(uf(u))' = F(u-1)$.
Cette égalité s'applique ici pour $\dfrac{3/2 - 7\lambda/4}{\alpha} \geq 1$, ce qui est vérifié pour tout $1/2 < \lambda < 2/3$, lorsque $\alpha \leq 1/3$, ce qui sera le cas.
On fait alors le changement de variables adéquat $u = (3/2 - 7\lambda/4)1/\alpha + 1$ pour obtenir

$$\begin{aligned} I_1 &= -\frac{4e^{-\gamma}}{7} \int_{1+5/(8\alpha)}^{1+1/(3\alpha)} F(u-1)du \\ &= \frac{4e^{-\gamma}}{7} \left(\left(1 + \frac{5}{8\alpha}\right) f\left(1 + \frac{5}{8\alpha}\right) - \left(1 + \frac{1}{3\alpha}\right) f\left(1 + \frac{1}{3\alpha}\right) \right). \end{aligned}$$

Calcul de I_2.
On a $\frac{1-\lambda}{\alpha} \leq 2$, pour $\lambda \geq 1 - 2\alpha$ et $1 - 2\alpha \geq 2/3$, pour $\alpha \leq 1/6$. Dans ce cas, on a le découpage :

$$\begin{aligned} I_2 &= \int_{2/3}^{1-2\alpha} \frac{e^{-\gamma}}{\alpha} F\left(\frac{1-\lambda}{\alpha}\right) d\lambda + \int_{1-2\alpha}^{t} \frac{e^{-\gamma}}{\alpha} F\left(\frac{1-\lambda}{\alpha}\right) d\lambda \\ &= J_1 + J_2, \end{aligned}$$

par définition.
L'intégrale J_1 se calcule de la même manière que que I_1, on pose $w = \dfrac{1-\lambda}{\alpha} + 1$:

$$J_1 = -\int_{1+1/(3\alpha)}^{3} e^{-\gamma} F(w-1)dw = e^{-\gamma} \left(\left(1 + \frac{1}{3\alpha}\right) f\left(1 + \frac{1}{3\alpha}\right) - 3f(3) \right).$$

Pour J_2, on a $\frac{e^{-\gamma}}{\alpha} F\left(\frac{1-\lambda}{\alpha}\right) = \frac{2}{1-\lambda}$ pour $1-2\alpha < \lambda < t$.
Ainsi $J_2 = 2\log(2\alpha) - 2\log(1-t)$. Donc on a

$$I_2 = e^{-\gamma}\left(\left(1+\frac{1}{3\alpha}\right) f\left(1+\frac{1}{3\alpha}\right) - 3f(3)\right) + 2\log(2\alpha) - 2\log(1-t).$$

Calcul de I_3.

$$I_3 = \int_t^1 \frac{e^{-2\gamma}}{\alpha^2} F\left(\frac{2/3-\lambda/2}{\alpha}\right) d\lambda.$$

Lorsque $\alpha < 1/12$, l'argument de F_2 est supérieur à 2, on a donc en reprenant la notation $u(\lambda) = 2/(3\alpha) - \lambda/(2\alpha)$:

$$I_3 = \int_t^1 \frac{\lambda}{\alpha^2[(1/2 + \frac{\log 2 - \log(u(\lambda))}{4})u(\lambda)^2 - u(\lambda) + 1/2]} d\lambda.$$

Conclusion. Pour $\alpha = 1/12.2$, et $t = 0.9926$, on a :

$$\frac{3\omega(\alpha^{-1})}{2\alpha} - I_1 - I_2 - I_3 > 0.$$

Cela termine la preuve du théorème 1.

Chapitre 2
Entiers de la forme n^2+1 sans grand facteur premier

2.0. Introduction.

La démonstration du théorème 2 s'organise autour du système de poids de Balog-Friedlander (cf [Ba] et [Fr2]), défini de la manière suivante :

$$g(n) = |\{(a,b);\ n^2+1 = ab,\ P^+(ab) < y,\ x^{1+\delta} < b < x^{1+2\delta},\ et\ p|b \Rightarrow p > z\}|,$$

avec $z = x^\beta$, et δ, β sont positifs et arbitrairement petits. Ainsi, on a l'inégalité $g(n) \leq 2^{2/\beta}$, ce qui donne la majoration :

$$\sum_{n\sim x} g(n) \ll_\beta \Xi(x,y).$$

Soit f une fonction positive et inférieure à 1, C^∞, à support dans $[x,2x]$, telle que $f^{(\ell)}(t) \ll t^{-\ell}$, uniformément sur t et pour tout $\ell \geq 1$, et vérifiant encore :

$$f(t) = \begin{cases} 1 & \text{si } t \in [5x/4, 7x/4], \\ \in [0,1] & \text{si } t \in [x,2x], \\ 0 & \text{sinon.} \end{cases}$$

On a alors $\sum_n g(n)f(n) \ll \sum_{n\sim x} g(n)$.

On pose encore $X = \int f(t)dt$. On a donc $X \approx x$.

On part du découpage suivant :

$$\begin{aligned} \sum_n g(n)f(n) \geq \sum_n f(n)|\{(a,b)\ ;\ & n^2+1 = ab,\ P^+(a) < y, \\ & x^{1+\delta} < b < x^{1+2\delta},\ p|b \Rightarrow p > z\}| \\ - \sum_n f(n)|\{(a,b,p)\ ;\ & p > y,\ n^2+1 = abp, \\ & x^{1+\delta} < pb < x^{1+2\delta},\ q|b \Rightarrow q > z\}| \\ \geq S_1 - S_2. & \end{aligned}$$

Les estimations des sommes S_1 et S_2 sont liées à la connaissance des cardinaux des ensembles :

$$C_m = \{n \sim x,\ n^2+1 \equiv 0 \ (\mathrm{mod}\, m)\},$$

où m est un nombre entier sans grand facteur premier pour S_1, et est de la forme pb où b est un entier sans petit facteur premier pour S_2. Lorsque $m < x^{1-\epsilon}$, ces cardinaux sont faciles à estimer, et on a assez rapidement un résultat exact. Par contre, lorsque $m = pb$ et est supérieur à $x^{1-\epsilon}$, ces estimations sont plus difficiles, et on a recours à des méthodes de crible.

L'intérêt du sytème de poids de Friedlander, est de réduire le plus possible la taille de l'intervalle où il faut obtenir de telles estimations,
on a en effet $x^{1+\delta} < pb < x^{1+2\delta}$, où δ est extrêmement petit, tandis qu'une approche naïve, par exemple du type $\Xi(x,y) \geq x - \sum_{y<p<x^2} |C_p|$, aurait fourni un résultat moins précis.
Balog [Ba], fut le premier à utiliser un système de poids, pour la résolution de $p+a$ sans grand facteur premier. Cependant, son système de poids ne donnait pas une minoration du bon ordre de grandeur de $\Xi(x,y)$.
Friedlander [Fr2] a amélioré le système de poids de Balog en ajoutant la condition $p|n \rightarrow p > x^{\beta}$. Cette condition permet de borner uniformément les poids $g(n)$, et ainsi d'obtenir une minoration de $\Xi(x,y)$ sans passer par l'inégalité de Cauchy-Schwarz. C'est pourquoi, on obtient une minoration de $\Xi(x,y)$ de l'ordre de x, tandis qu'avec un système de poids du type celui de Balog, on aurait obtenu une minoration de l'ordre de $\frac{x}{\log x}$. De plus, le choix de β étant libre, la valeur de α que l'on obtient est inchangée.

Lors de la minoration et de la majoration des quantités S_1 et S_2, respectivement nous utiliserons fréquemment la fonction ρ définie par :

$$\rho(d) = |\{0 \leq v < d,\ v^2 + 1 \equiv 0 \pmod d\}|.$$

Les propriétés de cette fonction ont déja étées énoncées dans le chapitre précédent, au lemme 1.3.3, mais on préfère les rappeler ici :

LEMME 2.0. *La fonction ρ est multiplicative et vérifie*

i) $\rho(2) = 1$ *et* $\rho(2^k) = 0$ *pour* $k > 1$,

ii) pour $p > 2$, *et* $k \geq 1$, $\rho(p^k) = \rho(p)$,

iii) $\rho(p) = 2$ *si* $p \equiv 1 \pmod 4$, $\rho(p) = 0$ *si* $p \equiv -1 \pmod 4$.

2.1.Minoration de S_1.

On va établir la proposition suivante :

PROPOSITION 2.1. *Pour* $0 < z < D$, *avec* $D = x^{\delta/2}$ *et* $\delta < 1/100$, *on a la minoration :*

(2.1)

$$S_1 \geq \frac{Xe^{-\gamma}}{\log z}\left(f\left(\frac{\log D}{\log z}\right) + O(\delta) + O_\delta\left(\frac{1}{\log z}\right)\right)\left(1 - \log\left(\frac{\log x}{\log y}\right)\right)\log x^{\delta},$$

où f est l'habituelle fonction de minoration des cribles linéaires, et non la fonction introduite au paragraphe 2.0.

2.1.1. Application du crible.

Dans l'écriture de S_1, nous allons détecter la condition $p|b \Rightarrow p > z$ par le crible. On écrit donc :

$$S_1 \geq \sum_{\substack{4x^{1-2\delta}<m<x^{1-\delta} \\ P^+(m)<y}} \sum_{\substack{n^2+1\equiv 0 \pmod m \\ p|\frac{n^2+1}{m} \Rightarrow p>z}} f(n).$$

On a ainsi $m < x^{1-\delta} < x$, de plus, comme z sera très petit, de l'ordre de x^{δ^2}, la minoration que l'on obtiendra alors avec le crible sera très précise.
Soient λ_d^- les poids de Rosser-Iwaniec correspondant à un crible linéaire de niveau D pour cribler jusqu'à z. Ils vérifient entre autres les propriétés suivantes :
$\lambda_1^- = 1$, $\lambda_d^- = 0$ pour $d > D$, ou si d a un facteur carré, $|\lambda_d^-| \leq 1$, $\lambda^- * \mathbb{1} \leq \mu * \mathbb{1}$.
Grâce à ces propriétés, on a la minoration :

$$S_1 \geq \sum_{d<D} \lambda_d^- \sum_{\substack{4x^{1-2\delta}<m<x^{1-\delta} \\ P^+(m)<y}} \sum_{n^2+1\equiv 0 \pmod{md}} f(n).$$

On applique ensuite la formule sommatoire de Poisson énoncée au lemme 1.2.3 :

$$\begin{aligned} S_1 &\geq \sum_{d<D} \lambda_d^- \sum_{\substack{4x^{1-2\delta}<m<x^{1-\delta} \\ P^+(m)<y}} \sum_{\substack{0\leq v<md \\ v^2+1\equiv 0 \pmod{md}}} \sum_{n\equiv v \pmod{md}} f(n) \\ &\geq \sum_{d<D} \lambda_d^- \sum_{\substack{4x^{1-2\delta}<m<x^{1-\delta} \\ P^+(m)<y}} \frac{1}{md} \sum_{h\in\mathbb{Z}} \hat{f}\left(\frac{h}{dm}\right) \sum_{\substack{0\leq v<md \\ v^2+1\equiv 0 \pmod{md}}} e\left(\frac{-hv}{md}\right). \\ &\geq \sum_{h=0} \cdots + \sum_{h\neq 0} \cdots \\ &\geq TP + E, \end{aligned}$$

par définition.

2.1.2. Majoration du terme d'erreur.

Pour $h \neq 0$, en faisant deux intégrations par parties, on montre que

$$\hat{f}\left(\frac{h}{dm}\right) \ll h^{-2}x^{-1}(dm)^2.$$

De plus, d'après le lemme 2.0, la somme sur v est $O(x^\epsilon)$ avec $\epsilon > 0$ arbitrairement petit.
Le terme d'erreur est donc majoré par :

$$\begin{aligned} E &\ll \sum_{d<D} \sum_{4x^{1-2\delta}<m<x^{1-\delta}} dmx^{-1+\epsilon} \\ &\ll D^2x^{1-2\delta+\epsilon}. \end{aligned} \tag{2.2}$$

Pour $D = x^{\delta/2}$, on a $E \ll x^{1-\epsilon'}$, pour $\epsilon' > 0$ assez petit.

2.1.3. Évaluation du terme principal TP.

Il reste à calculer

$$TP = X \sum_{\substack{4x^{1-2\delta} < m < x^{1-\delta} \\ P^+(m) < y}} \sum_{d<D} \lambda_d^- \frac{\rho(dm)}{dm}.$$

Pour se ramener à des fonctions multiplicatives par rapport à d, on écrit : $\rho(dm) = \rho(m)\rho_m(d)$, avec

$$\begin{cases} \rho_m(2) = 0 & \text{si } 2|m, \\ \rho_m(p) = 1 & \text{si } p|m \text{ et si } p > 2, \\ \rho_m(2^\alpha) = 0 & \text{si } \alpha > 1, \\ \rho_m(p^\alpha) = \rho_m(p) & \text{si } \alpha > 1, \text{ et } p > 2, \\ \rho_m(p) = \rho(p) & \text{si } p \not| m. \end{cases}$$

Puis en appliquant les résultats d'Iwaniec [I1] sur les cribles linéaires, énoncé dans le théorème A1 de l'annexe A, pour m fixé, on a :

$$\sum_{d<D} \lambda_d^- \frac{\rho(dm)}{dm} = \frac{\rho(m)}{m} \prod_{p<z} \left(1 - \frac{\rho_m(p)}{p}\right) \left[f\left(\frac{\log D}{\log z}\right) + O_\delta\left(\frac{1}{\log x}\right)\right],$$

avec

$$\prod_{p<z} \left(1 - \frac{\rho_m(p)}{p}\right) = \prod_{\substack{p|m \\ 2<p<z}} \left(1 - \frac{1}{p}\right) \prod_{\substack{(p,m)=1 \\ 2<p<z}} \left(1 - \frac{\rho(p)}{p}\right) \eta_2(m),$$

où

$$\begin{aligned} \eta_2(m) &= 1 - \frac{\rho_m(2)}{2} \\ &= \begin{cases} 1 & \text{si } 2|m, \\ 1/2 & \text{sinon.} \end{cases} \end{aligned}$$

A partir de ceci, on a l'égalité :

(2.3)

$$TP = X \frac{1}{2} \left[f\left(\frac{\log D}{\log z}\right) + O_\delta\left(\frac{1}{\log x}\right)\right] \prod_{p<z} \left(1 - \frac{\rho(p)}{p}\right) \sum_{\substack{4x^{1-2\delta} < m < x^{1-\delta} \\ P^+(m) < y}} \frac{\omega_z(m)}{m},$$

où pour des commodités d'écriture on a posé :

$$\omega_z(m) = \rho(m) \prod_{2<p<z, p|m} \left(1 - \frac{1}{p}\right) \left(1 - \frac{\rho(p)}{p}\right)^{-1} 2\eta_2(m).$$

Le facteur 2 devant $\eta_2(m)$, est destiné à rendre la fonction ω_z multiplicative.

Nous allons établir le

LEMME 2.1.1. *Pour tout $\varepsilon > 0$, on a l'égalité :*

$$\sum_{m<M} \omega_z(m) = \frac{L(1,\chi_4)}{\zeta(2)} \tilde{H}(1) M + O(M^{1/2+\varepsilon}) + O\left(\frac{M}{z}\right),$$

où $\tilde{H}(1)$ est le produit convergent défini par :

$$\tilde{H}(1) = \frac{4}{3} \prod_{p \equiv 1 \pmod 4} \left(1 + \frac{2}{(p+1)(p-2)}\right).$$

Preuve du lemme 2.1.1.
On commence par étudier la série génératrice liée à cette somme, soit :

$$H_z(s) = \sum_{m \geq 1} \frac{\omega_z(m)}{m^s}.$$

On écrit cette fonction sous forme de produit eulérien :

$$\begin{aligned} H_z(s) &= (1+2^{1-s}) \prod_{2<p<z} \left(1 + \rho(p)\left(1-\frac{1}{p}\right)\left(1-\frac{\rho(p)}{p}\right)^{-1} \frac{1}{p^s\left(1-\frac{1}{p^s}\right)}\right) \\ &\quad \times \prod_{p \geq z} \left(1 + \frac{\rho(p)}{p^s\left(1-\frac{1}{p^s}\right)}\right) \\ &= \zeta(s)(1-2^{-s})(1+2^{1-s}) \prod_{2<p<z} \left(1 - \frac{1}{p^s} + \frac{\rho(p)}{p^s}\left(\frac{p-1}{p-\rho(p)}\right)\right) \\ &\quad \times \prod_{p \geq z} \left(1 - \frac{1}{p^s} + \frac{\rho(p)}{p^s}\right) \\ &= \frac{\zeta(s)L(s,\chi_4)}{\zeta(2s)} \left(1 + \frac{1}{2^s+1}\right) \prod_{\substack{p<z \\ p \equiv 1 \bmod 4}} \left(1 + \frac{1}{p^s} + \frac{2}{p^s(p-2)}\right)\left(1+\frac{1}{p^s}\right)^{-1}. \end{aligned}$$

On définit alors une fonction $\tilde{H}_z$ par,

$$H_z(s) = \frac{\zeta(s)L(s,\chi_4)}{\zeta(2s)} \tilde{H}_z(s). \tag{2.4}$$

Dans la suite nous utiliserons le fait que :

$$\begin{aligned} \tilde{H}_z(s) &= \left(1 + \frac{1}{2^s+1}\right) \prod_{p \equiv 1 \pmod 4} \left(1 + \frac{1}{p^s} + \frac{2}{p^s(p-2)}\right)\left(1+\frac{1}{p^s}\right)^{-1}\left(1 + O\left(\frac{1}{z^\sigma}\right)\right) \\ &= \tilde{H}(s)\left(1 + O\left(\frac{1}{z^\sigma}\right)\right), \end{aligned} \tag{2.5}$$

par définition, avec $\sigma = \Re s$.

Le produit définissant $\tilde{H}(s)$ est normalement convergent sur $\sigma \geq \sigma_0$, avec $\sigma_0 > 0$.

Soient $1 < c < 2$, et $M, T \geq 1$ que l'on précisera plus tard. Sans perte de généralité on peut supposer que M est un demi-entier.En appliquant la formule de Perron, on a :

$$\sum_{m<M} \omega_z(m) = \int_{c-iT}^{c+iT} \frac{H_z(s)M^s}{s} ds + O\left(\frac{M^c}{T} \sum_{n=1}^{\infty} \frac{|\omega_z(n)|}{n^c} |\log(M/n)|^{-1}\right).$$

Le terme d'erreur est pour tout $\varepsilon > 0$, un $O(M^{1+c+\varepsilon}T^{-1})$,
et pour $T \geq M^{1/2+c+2\varepsilon}$, cette erreur est assez petite. Ensuite, on décale cette intégrale à gauche de la droite $\Re s = 1$, cela donne, en reprenant les notations de (2.4) :

$$\sum_{m<M} \omega_z(m) = M\frac{L(1,\chi_4)\tilde{H}_z(1)}{\zeta(2)} - \int_{1/2-iT}^{1/2+iT} \frac{H_z(s)M^s}{s} ds$$
$$\pm \int_{1/2\pm iT}^{c\pm iT} \frac{H_z(s)M^s}{s} ds + O(M^{1/2+\varepsilon}).$$

Majoration des branches horizontales.
D'après (2.5), le produit $\tilde{H}$ se majore uniformément sur les segments $[1/2 \pm iT, c \pm iT]$.
De plus, pour $1/2 \leq \Re s \leq c$, on a les inégalités $\dfrac{1}{|\zeta(2s)|} \ll \log T$,
et $|L(s,\chi_4)| \ll T^{1/6+\varepsilon}$.

Il reste alors à majorer une intégrale sur ζ. On utilise le fait que pour tout $T \geq 2$, on ait l'inégalité :

$$\int_T^{2T} \int_{1/2}^{c} |\zeta(\sigma + it)| d\sigma dt = O(T \log T),$$

pour en déduire que pour tout $T \geq 2$, il existe $T_1 \in [T, 2T]$ tel que

$$\int_{1/2}^{c} |\zeta(\sigma + iT_1)| d\sigma = O(\log T_1). \tag{2.6}$$

En prenant $T = T_1$, et en tenant compte de toutes ces remarques, on a l'inégalité suivante :

$$\int_{1/2}^{c} \frac{|H_z(\sigma + iT_1)M^{\sigma+iT_1}|}{|\sigma + iT_1|} d\sigma \ll T_1^{1/6+\varepsilon} T_1^{-1} M^c (\log T_1)^2. \tag{2.7}$$

Comme $T_1 = M^{1/2+c+\varepsilon}$, avec $c = 1 + \eta$, $\eta > 0$ pouvant être choisi aussi petit que l'on veut, l'intégrale ci-dessus est majorée par un $O(M^{-1/4+\eta/6)+\varepsilon})$.

Majoration de la branche verticale.
En faisant un découpage dyadique de l'intervalle $[1/2-iT, 1/2+iT]$ pour majorer $1/s$, on se ramène à majorer $O(\log M)$ intégrales du type :

$$\int_{1/2+iK}^{1/2+2iK} \frac{H_z(s)M^s}{s} ds.$$

En profitant du fait que $\tilde{H}$ soit normalement convergent sur $\Re s > 1/4$, et que pour $\Re s \geq 1/2$, on ait $\dfrac{1}{|\zeta(2s)|} \ll \log T$,
puis en appliquant l'inégalité de Cauchy-Schwarz, on a l'inégalité :

$$\int_{1/2+iK}^{1/2+2iK} \frac{H_z(s)M^s}{s} ds \ll \frac{M^{1/2+\varepsilon}}{K} \left| \int_{1/2+iK}^{1/2+2iK} |L(s,\chi_4)|^2 ds \right|^{1/2} \left| \int_{1/2+iK}^{1/2+2iK} |\zeta(s)|^2 ds \right|^{1/2}.$$

Les deux intégrales du membre de droite sont respectivement des $O(K(\log K)^2)$, $O(K \log K)$, (on n'a pas besoin d'utiliser les majorations les plus précises), et ainsi, la branche verticale vérifie la majoration :

$$\int_{1/2+iK}^{1/2+2iK} \frac{H_z(s)M^s}{s} ds \ll M^{1/2+\varepsilon'}.$$

Toutes ces inégalités conduisent à :

$$\sum_{m<M} \omega_z(m) = \frac{ML(1,\chi_4)\tilde{H}(1)}{\zeta(2)} + O\left(\frac{M}{z} + M^{1/2+\varepsilon}\right).$$

Ce qui finit la preuve du lemme 2.1.1.

Grâce à ce lemme nous avons presque terminé la preuve de la proposition 2.1.
Pour $M^{1/2} < y < M$, on a :

$$\sum_{\substack{m<M \\ P^+(m)<y}} \omega_z(m) = \sum_{m<M} \omega_z(m) - \sum_{y<p<M} \omega_z(p) \sum_{m<Mp^{-1}} \omega_z(m).$$

La première somme du membre de droite se calcule directement avec le lemme 2.1.1.
On utilise encore ce lemme pour évaluer la somme portant sur les $m < Mp^{-1}$.
La deuxième somme vaut alors :

$$\sum_{y\leq p<M} \frac{L(1,\chi_4)\tilde{H}(1)}{\zeta(2)} \frac{M}{p} \omega_z(p)$$
$$+ O\left(M^{1/2+\varepsilon} \sum_{y\leq p<M} \frac{\omega_z(p)}{p^{1/2+\varepsilon}} + \frac{M}{z} \sum_{y\leq p<M} \frac{\omega_z(p)}{p} \right),$$

avec pour $p \geq y > 2$,

$$\omega_z(p) = \begin{cases} 2\left(1-\frac{1}{p}\right)\left(1-\frac{2}{p}\right)^{-1} & \text{si } p \equiv 1 \pmod 4, \\ 0 & \text{si } p \equiv -1 \pmod 4 \end{cases}$$

Ainsi, grâce à l'égalité $\pi(x,4,1) = \dfrac{x}{2\log x} + O\left(\dfrac{x}{(\log x)^2}\right)$,
on obtient l'égalité :

$$\sum_{\substack{m<M \\ P^+(m)<y}} \omega_z(m) = \frac{L(1,\chi_4)\tilde{H}_z(1)}{\zeta(2)} M\left(1 - \log\left(\frac{\log M}{\log y}\right)\right) + O\left(\frac{M}{\log M}\right).$$

En faisant une intégration par partie, on a :
(2.8)

$$\sum_{\substack{x^{1-2\delta}<m<x^{1-\delta} \\ P^+(m)<y}} \frac{\omega_z(m)}{m} = \frac{L(1,\chi_4)\tilde{H}(1)}{\zeta(2)} \log x^{\delta}\left(1 - \log\left(\frac{\log x}{\log y}\right) + O(\delta) + O_\delta\left(\frac{1}{\log x}\right)\right).$$

On reporte ensuite (2.8), dans (2.3), les produits eulériens se simplifient alors, en effet, on a l'égalité :

$$\frac{1}{2}\tilde{H}_z(1)\prod_{p<z}\left(1-\frac{\rho(p)}{p}\right) = \frac{\zeta(2)}{L(1,\chi_4)}\prod_{p<z}\left(1-\frac{1}{p}\right)\left(1+O\left(\frac{1}{\log z}\right)\right).$$

En profitant de ceci, tout en tenant compte de (2.2), on obtient le résultat annoncé dans la proposition 2.1.

2.2. Majoration de S_2.

On rappelle la définition de S_2 :

$$S_2 = \sum_n f(n)|\{(a,b,p);\ p>y,\ n^2+1 = pab,\ x^{1+\delta} < bp < x^{1+2\delta},\ et\ q|b \Rightarrow q > z\}|$$

(2.9) $$= \sum_{y<p<x^{1+2\delta}} \sum_{\substack{x^{1+\delta}<bp<x^{1+2\delta} \\ q|b\Rightarrow q>z}} |C_{bp}|,$$

avec $|C_{bp}| = \sum_{n^2+1\equiv 0 \pmod{bp}} f(n).$

Dans cette partie, on établit la proposition :

PROPOSITION 2.2. *Pour $D = x^{\delta/2}$, et pour tout $\varepsilon > 0$, on a la majoration :*

$$S_2 \leq \frac{Xe^{-\gamma}\log(x^\delta)}{\log z}\left(1+O\left(\frac{1}{\log z}\right)\right)(2+\varepsilon)F\left(\frac{\log D}{\log z}\right)$$
$$\times\left(\log\left(\frac{1}{2\alpha-1}\right)+O(\delta)+O_{\delta,\varepsilon}\left(\frac{1}{\log x}\right)\right). \tag{2.10}$$

Cette démonstration utilisera les majorations en moyenne de sommes de Kloosterman établies par Deshouillers et Iwaniec [D-I2].
Pour être en mesure d'appliquer ces résultats, il faut rendre les variables b et p indépendantes et lisser p. Ceci nécessite un découpage assez précis de l'ensemble :
$S = \{(p,b);\ y < p < x^{1+2\delta};\ x^{1+\delta} < pb < x^{1+2\delta}\}$.

2.2.1 Découpage et lissage de S.

Pour cette opération, on utilise des techniques classiques qu'on retrouve par exemple chez Fouvry dans [Fo2]. Plus particulièrement on a besoin du lemme :

LEMME 2.2.1. *Soit $\Delta > 1$, il existe une suite $b_{\ell,\Delta}$, $\ell \geq 0$, de fonctions C^∞ à support dans $[\Delta^{\ell-1}, \Delta^{\ell+1}]$ vérifiant les conditions*

$$\forall \xi \geq 1,\ \sum_{\ell=0}^{\infty} b_{\ell,\Delta}(\xi) = 1,$$

$$\forall \xi \geq 1,\ \forall \nu \geq 1,\ b_{\ell,\Delta}^{(\nu)}(\xi) \ll_\nu \xi^{-\nu}\Delta^\nu(\Delta-1)^{-\nu}.$$

Pour utiliser ce lemme, il est commode de connaître une famille explicite de fonctions $b_{\ell,\Delta}$ vérifiant ces proriétés.
On reprend la suite de fonctions donnée par Fouvry.
Soit h une fonction de classe C^∞, définie sur $[0,1]$, positive, vérifiant :
$h(0) = 1$, $h(1) = 0$, $h^{(\nu)}(0^+) = h^{(\nu)}(0^-) = 0$ pour $\nu \geq 1$.
La suite $b_{\ell,\Delta}$ est alors définie par

$$b_{\ell,\Delta}(\xi) = \begin{cases} 0 & \text{si } \xi \leq \Delta^{\ell-1} \text{ ou si } \xi \geq \Delta^{\ell+1}, \\ 1 - h(1-(\Delta^\ell-\xi)(\Delta^\ell-\Delta^{\ell-1})^{-1}) & \text{si } \Delta^{\ell-1} < \xi \leq \Delta^\ell, \\ h((\xi-\Delta^\ell)(\Delta^{\ell+1}-\Delta^\ell)^{-1}) & \text{si } \Delta^\ell \leq \xi < \Delta^{\ell+1}. \end{cases}$$

A partir de ces fonctions nous en déduisons le corollaire

LEMME 2.2.2. *Pour $\Delta = x^{1+\delta}(x^{1+\delta}-x^{1-2\delta})^{-1} = (1-x^{-3\delta})^{-1}$, les deux assertions suivantes sont vérifiées :*

i) Il existe une famille de fonctions $g_{\ell,\Delta}$ *avec* $L_0 \leq \ell \leq L$, *avec* $L \ll x^{3\delta}\log x$ *à support dans* $[x^{1+\delta}\Delta^{\ell-1}, x^{1+\delta}\Delta^{\ell+1}]$, *telles que*

$$\forall \xi \geq 1,\ \forall \nu \geq 1,\ g_{\ell,\delta}^{(\nu)}(\xi) \ll_\nu \xi^{-\nu} x^{3\delta\nu},$$

et vérifiant encore

$$\sum_{L_0\leq\ell\leq L} g_{\ell,\Delta}(\xi) = \begin{cases} 1 & si\ \xi \in [x^{1+\delta}, x^{1+2\delta}], \\ O(1) & si\ \xi \in [x^{1+\delta} - x^{1-2\delta}, x^{1+2\delta}\Delta], \\ 0 & sinon\ . \end{cases}$$

ii) Il existe une deuxième famille $\gamma_{j,\Delta}$, $J_0 \leq j \leq J$ *avec* $J \ll x^{3\delta}\log x$, *vérifiant les mêmes propriétés de lissité que les* $g_{\ell,\Delta}$, *mais cette fois-ci les supports sont inclus dans* $[y\Delta^{j-1}, y\Delta^{j+1}]$ *et on a :*

$$\sum_{J_0\leq j\leq J} \gamma_{j,\Delta}(\xi) = \begin{cases} 1 & si\ \xi \in [y, x^{1+2\delta}], \\ O(1) & si\ \xi \in [y\Delta^{-1}, x^{1+2\delta}\Delta], \\ 0 & sinon. \end{cases}$$

Preuve du lemme 2.2.2.
Les fonctions $g_{\ell,\Delta}$ pour $L_0 \leq \ell \leq L$ sont celles définies par

$$g_{\ell,\Delta}(u) = b_{\ell,\Delta}\left(\frac{u}{x^{1+\delta}}\right),$$

L vérifie alors $x^{1+\delta}\Delta^L = x^{1+2\delta}$, c'est à dire $L = \dfrac{\delta\log x}{\log\Delta} = O(x^{3\delta}\log x)$.

De même, pour $J_0 \leq j \leq J$, on définit les fonctions $\gamma_{j,\Delta}$ par

$$\gamma_{j,\Delta} = b_{\ell,\Delta}\left(\frac{u}{y}\right),$$

avec $J = \dfrac{\log(x/y)}{\log\Delta}$.

Ces nouvelles familles g et γ vérifient bien (i) et (ii).

En appliquant successivement la première puis la deuxième assertion du lemme 2.2.2, on a l'egalité :

$$S_2 = \sum_{\substack{L_0\leq\ell\leq L \\ J_0\leq j\leq J}} \sum_{\substack{p,b \\ q|b\Rightarrow q>z}} g_{\ell,\Delta}(bp)\gamma_{j,\Delta}(p)|C_{pb}| + E,$$

avec

$$E \ll \sum_{x^{1+\delta}\Delta^{-1}\leq pb\leq x^{1+\delta}} |C_{pb}| + \sum_{x^{1+2\delta}\leq pb\leq x^{1+2\delta}\Delta} |C_{bp}|$$
$$+ \sum_{\substack{y\Delta^{-1}\leq p\leq y \\ x^{1+\delta}\Delta^{-1}<bp<x^{1+2\delta}\Delta}} |C_{bp}| + \sum_{\substack{x^{1+2\delta}\leq p\leq x^{1+2\delta}\Delta \\ x^{1+\delta}\Delta^{-1}<pb<x^{1+2\delta}\Delta}} |C_{pb}|.$$

Et on écrit :

$$E \ll E_1 + E_2 + E_3 + E_4.$$

Les quantités $|C_{bp}|$ sont des $O(x^{\varepsilon/10})$, car $pb \geq \frac{1}{2}x^{1+\delta}$, pour x assez grand.
La première somme E_1 vérifie donc :

$$\begin{aligned} E_1 &\ll x^{\varepsilon/10} \sum_{x^{1+\delta}\Delta^{-1}<pb<x^{1+\delta}} 1 \\ &\ll x^{\varepsilon} \sum_{x^{1+\delta}\Delta^{-1}<m<x^{1+\delta}} 1 \\ &\ll x^{\varepsilon}(x^{1+\delta} - x^{1+\delta}\Delta^{-1}) \\ &\ll x^{1+\delta+\varepsilon}(1-\Delta^{-1}) \ll x^{1-2\delta+\varepsilon}. \end{aligned}$$

De la même manière, on montre que la deuxième somme E_2 est un $O(x^{1-\delta+\varepsilon})$.
La troisième somme E_3, vérifie :

$$\begin{aligned} E_3 &\ll x^{\varepsilon/10} \sum_{\substack{y\Delta^{-1}<p<y \\ x^{1+\delta}y^{-1}\Delta^{-1}<b<x^{1+2\delta}y^{-1}\Delta^2}} 1 \\ &\ll (y - y\Delta^{-1})(x^{1+2\delta}y^{-1}\Delta^2 - x^{1+\delta}y^{-1}\Delta^{-1}) \\ &\ll (1-\Delta^{-1})\Delta^2 x^{1+2\delta} \\ &\ll x^{1-\delta+\varepsilon}, \end{aligned}$$

car $\Delta = O(1)$.
De même, la dernière somme est un $O(x^{1-\delta+\varepsilon})$.

Ainsi, il reste à estimer $O(x^{6\delta}(\log x)^2)$ sommes du type :

$$S(P,B) = \sum_{p\in[P,4P]} \sum_{\substack{b\in[B,4B] \\ q|b\Rightarrow q>z}} g(bp)\gamma(p)|C_{pb}|,$$

où les fonctions g et γ sont celles des assertions i) et ii) du lemme 2.2.2, et le produit PB vérifie : $x^{1+\delta} \ll PB \ll x^{1+2\delta}$, et $y \ll P \ll x^{1+2\delta}$.

2.2.2. Préparation au crible.

Nous allons majorer avec des méthodes de crible les conditions p premier et $q|b \Rightarrow q > z$.
Cependant, comme z sera très petit (on choisira $z = x^{\delta^2}$), nous ne criblerons pas de la même façon ces deux conditions.
Nous utiliserons donc un crible vectoriel, en transposant les travaux de Brüdern et Fouvry sur ce sujet (cf [B-F]) à notre situation (qui est bien plus simple que la leur).

Pour cela on établit la proposition :

PROPOSITION 2.2.3. *Soient d_1 et d_2 deux entiers sans facteur carré, premiers entre eux. On définit les quantités :*

$$S(P,B,d_1,d_2) = \sum_{\substack{m\in[P,4P]\\ m\equiv 0 \pmod{d_1}}} \sum_{\substack{b\in[B,4B]\\ b\equiv 0 \pmod{d_2}}} |C_{mb}| g(mb)\gamma(m),$$

les fonctions g et γ étant les fonctions de lissage provenant du lemme 2.2.2.

On a alors l'égalité :

(2.11)

$$S(P,B,d_1,d_2) = X\tilde{K}(1)\left(\frac{L(1,\chi_4)}{\zeta(2)}\right)^2 \frac{\omega(d_1,d_2)}{d_1d_2}\iint \frac{\gamma(u)g(uv)}{uv}dudv + R(P,B,d_1,d_2),$$

où $\tilde{K}(1)$ est le produit eulérien :

$$\tilde{K}(1) = \frac{8}{9}\prod_{p\equiv 1 \pmod 4}\left(1-\frac{2}{(p+1)^2}\right). \tag{2.12}$$

La fonction de crible $\omega(d_1,d_2)$ vaut :

$$\omega(d_1,d_2) = \tilde{\eta}(d_1d_2)\rho(d_1d_2)\prod_{\substack{p|d_1d_2\\ p\equiv 1 \pmod 4}}\left(1+\frac{2}{p}-\frac{1}{p^2}\right)^{-1}, \tag{2.13}$$

avec

$$\tilde{\eta}(d_1d_2) = \begin{cases} \frac{1}{2} & \text{si } 2|d_1d_2,\\ 1 & \text{sinon.}\end{cases}$$

Le terme d'erreur $R(P,B,d_1,d_2)$ vérifie pour tous poids $\{\lambda\}$, $\{\mu\}$, tels que $|\lambda|\leq 1$ et $|\mu|\leq 1$, l'inégalité :

$$\sum_{\substack{d_1<D_1\\ d_2<D_2}} \lambda_{d_1}\mu_{d_2}R(P,B,d_1,d_2) \ll D_2^{200}P^{3/4}B^{5/4}D_1^{1/2}.$$

Nous n'avons pas du tout cherché à donner une puissance de D_2 dans le terme d'erreur la plus petite possible, cela était en effet inutile, puisque dans les applications, D_2 sera une puissance minuscule de x.

Pour démontrer la proposition 2.2.3, on part de l'expression :

$$S(P,B,d_1,d_2) = \sum_{\substack{b\in[B,4B]\\ b\equiv 0 \pmod{d_2}}} \sum_{m\equiv 0 \pmod{d_1}} g(mb)\gamma(m)|C_{bm}|.$$

Comme au paragraphe 1, on applique la formule sommatoire de Poisson :

$$S(P,B,d_1,d_2) = \sum_{\substack{b\in[B,4B]\\ b\equiv 0 \pmod{d_2}}} \sum_{m\equiv 0 \pmod{d_1}} \frac{g(mb)\gamma(m)}{mb}$$
$$\times \sum_{h\in\mathbf{Z}} \hat{f}\left(\frac{h}{bm}\right) \sum_{v^2+1\equiv 0 \pmod{bm}} e\left(\frac{-hv}{bm}\right)$$
$$= T(P,B,d_1,d_2) + E(P,B,d_1,d_2),$$

avec

$$T(P,B,d_1,d_2) = X \sum_{\substack{b\in[B,4B]\\ b\equiv 0 \pmod{d_2}}} \sum_{m\equiv 0 \pmod{d_1}} \frac{g(mb)\gamma(m)\rho(bm)}{mb}, \tag{2.14}$$

et,

$$E(P,B,d_1,d_2) = \sum_{\substack{b\in[B,4B]\\ b\equiv 0 \pmod{d_2}}} \sum_{m\equiv 0 \pmod{d_1}} \frac{g(mb)\gamma(m)}{mb}$$
$$\times \sum_{h\neq 0} \hat{f}\left(\frac{h}{bm}\right) \sum_{v^2+1\equiv 0 \pmod{bm}} e\left(\frac{-hv}{bm}\right). \tag{2.15}$$

2.2.3. Transformation du terme d'erreur.

Pour $h \neq 0$, en faisant $[4\varepsilon^{-1}]$ intégrations par parties, on montre que $\hat{f}\left(\frac{h}{bm}\right) \ll \frac{1}{h^2}$, pour $|h| > H$, avec $H = PBx^{-1+\varepsilon}$.

Ainsi, la contribution des termes en $|h| > H$ dans $\sum_{\substack{d_1<D_1\\ d_2<D_2}} E(P,B,d_1,d_2)$ est

$$\ll \sum_{\substack{d_1<D_1\\ d_2<D_2}} \sum_{\substack{b\in[B,4B]\\ b\equiv 0 \pmod{d_2}}} \sum_{m\equiv 0 \pmod{d_1}} \frac{\gamma(m)\rho(bm)}{bm} \ll x^{\varepsilon}. \tag{2.16}$$

Il reste à majorer

$$R(P,B) = \sum_{0<|h|<H} \sum_{\substack{d_1<D_1\\ d_2<D_2}} \lambda^+_{d_1}\mu^+_{d_2}$$
$$\sum_{\substack{b\in[B,4B]\\ b\equiv 0 \pmod{d_2}}} \sum_{m\equiv 0 \pmod{d_1}} \frac{g(mb)\gamma(m)}{bm} \hat{f}\left(\frac{h}{bm}\right) \sum_{v^2+1\equiv 0 \pmod{bm}} e\left(\frac{-hv}{bm}\right).$$

Pour cela, on utilise les formules explicites des solutions de $v^2+1 \equiv 0 \pmod{bm}$ données au lemme 0 de l'introduction de cette partie, mais que l'on préfère réénoncer ici sous une forme légèrement différente :

LEMME 2.2.4. *(Gauss) Pour $m > 1$, il existe une correspondance bijective entre les représentations de m sous la forme $m = r^2 + s^2$, avec $(r,s) = 1$, $r, s > 0$, et les solutions de $v^2 + 1 \equiv 0 \pmod{m}$.*

Cette bijection est donnée par : $\dfrac{v}{m} = \dfrac{\bar{r}}{s} - \dfrac{r}{s(r^2+s^2)} \pmod 1$.

Grâce à ce lemme, en faisant quasiment les mêmes opérations que celles effectuées au paragraphe 1.7, on a :

$$R(P,B) = \sum_{0<|h|<H} \sum_{\substack{d_1<D_1 \\ d_2<D_2}} \lambda^+_{d_1}\mu^+_{d_2} \sum_{\substack{b\in[B,4B] \\ b\equiv 0 \bmod d_2}}$$

$$\times \sum_{\substack{(r,s)=1 \\ r,s>0 \\ r^2+s^2\equiv 0 \pmod{bd_1}}} F(r^2+s^2,b,h)e\left(\frac{-h\bar{r}}{s}\right)\left(1+O\left(\frac{r|h|}{s(r^2+s^2)}\right)\right), \tag{2.17}$$

où on a posé

$$F(r^2+s^2,b,h) = \frac{1}{r^2+s^2}g(r^2+s^2)\gamma\left(\frac{r^2+s^2}{b}\right)\hat{f}\left(\frac{h}{r^2+s^2}\right). \tag{2.18}$$

La fonction $A(r,s,b,h) = F(r^2+s^2,b,h)$ est presque lisse, plus précisement, on a le lemme

LEMME 2.2.5. *Pour tous ν_1, ν_2, ν_3, $\nu_4 \geq 0$, avec $\nu = \nu_1+\nu_2+\nu_3+\nu_4$, on a les inégalités :*

$$(i) \qquad \frac{\partial^\nu A(r,s,b,h)}{\partial r^{\nu_1}\partial s^{\nu_2}\partial b^{\nu_3}\partial h^{\nu_4}} \ll \frac{x(PB)^{-1}x^{3\delta\nu}}{r^{\nu_1}s^{\nu_2}b^{\nu_3}h^{\nu_4}},$$

$$(ii) \qquad \frac{\partial^\nu A(r,s,b,h)}{\partial r^{\nu_1}\partial s^{\nu_2}\partial b^{\nu_3}\partial h^{\nu_4}} \ll \frac{x(PB)^{-1}x^{3\delta\nu}}{(PB)^{\nu_1/2}s^{\nu_2}b^{\nu_3}h^{\nu_4}}.$$

Preuve du lemme 2.2.5.
Pour vérifier ceci, il suffit de le faire sur chaque fonction $\gamma\left(\frac{r^2+s^2}{b}\right)$,

$g(r^2+s^2)$, $\frac{1}{r^2+s^2}$, $\hat{f}\left(\frac{h}{r^2+s^2}\right)$.

Par construction, les dérivées partielles des fonctions g et γ amènent une erreur de $x^{3\delta}$. La fonction $(r,s,h) \to \frac{h}{r^2+s^2}$ étant une fonction lisse pour $0 < |h| < PBx^{-1+\varepsilon}$, et $r^2+s^2 \sim PB$, et la composée de fonctions lisses étant lisse, pour montrer que $(r,s,h) \to \hat{f}\left(\frac{h}{r^2+s^2}\right)$ est lisse, il suffit de vérifier que $x^{-1}\hat{f}$ est lisse, ce qui est le cas car f est lisse à support compact dans $[x,2x]$. Le point (ii) se vérifie directement à partir du fait que $r^2+s^2 \sim PB$.

Ce lemme n'est pas utile dans l'immédiat, mais servira plus tard lors de discussions préparatoires aux majorations de sommes de Kloosterman en moyenne.

Auparavant, il faut évaluer dans (2.17) la contribution à $R(P,B)$ du terme en $O\left(\frac{r|h|}{s(r^2+s^2)}\right)$.
D'après (2.18), on peut majorer $F(r^2+s^2,b,h)$ par $x^{1+\varepsilon}(PB)^{-1}$ et donc par $H^{-1}x^{2\varepsilon}$, cette contribution est ainsi d'un ordre de grandeur inférieur à :

$$\sum_{0<|h|<H} \sum_{\substack{d_1<D_1\\ d_2<D_2}} \sum_{\substack{b\in[B,4B]\\ b\equiv 0 \pmod{d_2}}} \sum_{0<s\ll(PB)^{1/2}} \sum_{\substack{0<r\ll(PB)^{1/2}\\ r^2\equiv -s^2 \pmod{bd_1}}} \frac{r}{s}(PB)^{-1}x^{\varepsilon_2}$$

$$\ll \sum_{0<|h|<H} \sum_{\substack{d_1<D_1\\ d_2<D_2}} \sum_{\substack{b\in[B,4B]\\ b\equiv 0 \pmod{d_2}}} \sum_{0<s\ll(PB)^{1/2}} \frac{x^{\varepsilon_2}}{sbd_1} \ll Hx^{\varepsilon_3},$$

ce qui est assez petit.

Ensuite, on réapplique la formule de Poisson dans la somme sur r.
Pour $s>0$ fixé on a :

$$\sum_{\substack{(r,s)=1\\ r>0\\ r^2+s^2\equiv 0 \pmod{bd_1}}} F(r^2+s^2,b,h)e\left(\frac{-h\bar{r}}{s}\right) = \sum_{\substack{0\le u<d_1bs\\ (u,s)=1\\ u^2+s^2\equiv 0 \pmod{d_1b}}} e\left(\frac{-h\bar{u}}{s}\right) \times \sum_{r\equiv u \pmod{d_1bs}} F(r^2+s^2,b,h)$$

$$= \frac{1}{d_1bs}\sum_{k\in\mathbf{Z}} \sum_{\substack{u \bmod d_1bs\\ (u,s)=1\\ u^2+s^2\equiv 0 \pmod{d_1b}}} e\left(\frac{-h\bar{u}}{s}+\frac{-ku}{d_1bs}\right) G(s,b,d_1,h,k),$$

avec

$$G(s,b,d_1,h,k) = \int F(\rho^2+s^2,b,h)e\left(\frac{k\rho}{bd_1s}\right)d\rho. \tag{2.19}$$

Les conditions $(u,s)=1$ et $u^2+s^2\equiv 0 \pmod{bd_1}$ entraînent que $(bd_1,s)=1$. En écrivant alors $u=\alpha s+\beta d_1 b$, avec $\alpha^2+1\equiv 0 \pmod{d_1 b}$, on a :

$$R(P,B) \ll \sum_{0<|h|<H} \sum_{\substack{d_1<D_1\\ d_2<D_2}} \lambda^+_{d_1}\mu^+_{d_2} \sum_{k\in\mathbb{Z}} \sum_{\substack{b\in[B,4B]\\ b\equiv 0 \pmod{d_2}}} \rho(d_1 b,k)$$
$$\times \sum_{(s,bd_1)=1} \frac{G(s,b,d_1,h,k)}{bd_1 s} S(-h\overline{bd_1},-k;s),$$

avec

$$\rho(d_1 b,k) = \sum_{\substack{\alpha \bmod d_1 b\\ \alpha^2+1\equiv 0 \pmod{d_1 b}}} e\left(\frac{-k\alpha}{d_1 b}\right),$$

et,

$$S(-h\overline{d_1 b},-k;s) = \sum_{\substack{u \bmod s\\ (u,s)=1}} e\left(\frac{-h\overline{d_1 b}\bar{u}-ku}{s}\right).$$

Pour $k=0$, la somme de Kloosterman se ramène à une somme de Ramanujan : $|S(-h\overline{d_1 b},0;s)|\le (h,s)$.

Ainsi, en majorant $|G(s,b,d_1,h,k)|$ par un $O(x(PB)^{-1/2+\varepsilon})$, la contribution des termes en $k=0$ est inférieure à :

$$x(PB)^{-1/2} \sum_{0<|h|<H} \sum_{\substack{d_1<D_1\\ d_2<D_2}} \sum_{\substack{b\in[B,4B]\\ b\equiv 0 \pmod{d_2}}} \frac{\rho(d_1 b)}{d_1 b} \sum_s \frac{(h,s)}{s} \ll D_2 H (BP)^{-1/2} x^{1+\varepsilon}$$
$$\ll D_2 x^{1/2+\delta+2\varepsilon},$$

d'après l'inégalité $PB\ll x^{1+2\delta}$.

Dans la suite on supposera qu'il existe $\varepsilon>0$ assez petit, tel que :

$$D_2 \ll x^{1/2-\delta-2\varepsilon}. \tag{2.20}$$

Il reste donc à majorer

$$R_2 = \sum_{0<|h|<H} \sum_{k\neq 0} \sum_{\substack{d_1<D_1\\ d_2<D_2}} \lambda^+_{d_1}\mu^+_{d_2} \sum_{\substack{b\in[B,4B]\\ b\equiv 0 \pmod{d_2}}} \rho(d_1 b,k)$$
$$\times \sum_{(s,bd_1)=1} \frac{G(s,b,d_1,h,k)}{bd_1 s} S(-h\overline{bd_1},-k;s).$$

On découpe les sommes sur s et sur d_1 en $O((\log x)^2)$ sommes du type

$$R_2(L,S) = \sum_{d_1} \dots \sum_{(s,d_1 b)=1} \frac{\ell(d_1)a(s)}{s} G(s,b,d_1,h,k) S(-h\overline{bd_1},-k;s),$$

où $a(s)$, $\ell(d_1)$ sont des fonctions C^∞, positive, à support dans $[S,2S]$, $[L,2L]$ respectivement, avec $S\ll (BP)^{1/2}$, et $1<L<D_1$ les fonctions $a(s)$, $\ell(d_1)$ vérifiant de plus : $a^{(\nu)}(s)\ll s^{-\nu}$ et $\ell^{(\nu)}(d_1)\ll d_1^{-\nu}$, uniformément sur s et d_1, pour tout $\nu\ge 1$.

Il n'y a pas de problème de bord pour s, car $G(s,b,d_1,h,k)$ est déja à support compact pour s. Pour d_1, il n'y en n'a pas non plus, car $\lambda^+_{d_1}=0$ pour $d_1>D_1$.

Pour $k\neq 0$ en faisant $\nu=[4\varepsilon^{-1}]$ intégrations par parties, on a :

$$G(s,b,d_1,h,k)=\left(\frac{-d_1bs}{2i\pi k}\right)^{\nu}\int\frac{\partial^{\nu}}{\partial\rho^{\nu}}F(\rho^2+s^2,b,h)e\left(\frac{k\rho}{d_1bs}\right)d\rho.$$

D'après le lemme 2.2.5, on a :

$$\frac{\partial^{\nu}}{\partial\rho^{\nu}}F(\rho^2+s^2,b,h)\ll\frac{x^{3\delta\nu}x(PB)^{-1}}{(PB)^{\nu/2}},$$

et ainsi la majoration :

$$G(s,b,d_1,h,k)\ll x(PB)^{-1/2}\left(\frac{d_1bsx^{3\delta}}{(PB)^{1/2}k}\right)^{\nu}. \tag{2.21}$$

Donc, pour $|k|\geq LBS(PB)^{-1/2}x^{3\delta+3\varepsilon}=K$, on a :

$$G(s,b,d_1,h,k)\ll\frac{1}{xk^2}.$$

La contribution des termes $|k|>K$ est alors $\ll HS^{1/2}x^{-1+\varepsilon'}$
et donc $\ll x^{3/4+3\delta/2+\varepsilon'}$, ce qui est assez petit.
On a donc :

$$\begin{aligned}R_2(L,S)=&\sum_{\substack{0<|h|<H\\0<|k|<K}}\sum_{\substack{d_1\\d_2<D_2}}\lambda^+_{d_1}\mu^+_{d_2}\sum_{\substack{b\in[B,4B]\\b\equiv 0\pmod{d_2}}}\rho(d_1b,k)\\&\times\sum_{(d_1b,s)=1}\frac{G(s,b,d_1,h,k)}{bd_1s}\ell(d_1)a(s)S(-h\overline{bd_1},-k;s)\\&+O(x^{3/4+3\delta/2+\varepsilon'}).\end{aligned} \tag{2.22}$$

2.2.4. Majorations de sommes de Kloosterman multilinéaires.

Le reste $R_2(L,S)$ va être majoré à l'aide du lemme suivant qui est une légère généralisation du théorème 11 de [D-I2], analogue au lemme 5 de [Fo2].

LEMME 2.2.6. *Soient $D, H, K, S \geq 1$ et Φ une fonction de classe C^∞ à support compact dans $[D, 2D] \times [H, 2H] \times [K, 2K] \times [S, 2S]$, dont les dérivées partielles vérifient :*

il existe $\eta > 0$, tel que :

$$\frac{\partial^{\nu_1+\nu_2+\nu_3+\nu_4}}{\partial d^{\nu_1}\partial h^{\nu_2}\partial k^{\nu_3}\partial s^{\nu_4}}\Phi(d,h,k,s) \ll (DHKS)^{\eta(\nu_1+\nu_2+\nu_3+\nu_4)} d^{-\nu_1} h^{-\nu_2} k^{-\nu_3} s^{-\nu_4},$$

uniformément sur d, h, k, s, pour tout $\nu_1, \nu_2, \nu_3, \nu_4 \geq 0$.

(On dit alors que le défaut de lissité de Φ est inférieur à η.)

Alors il existe une constante absolue c_0 telle que pour toute suite de nombres complexes $b_{d,k}$, on ait :

$$\sum_{D\leq d<2D} \sum_{\substack{0<h\leq H\\ 0<k\leq K}} b_{d,k} \sum_{(s,d)=1} \Phi(d,h,k,s) S(h\bar{d},k,s) \ll (DHKS)^{c_0\eta+\varepsilon} \|b\| H^{1/2}(L+M),$$

avec

$$L = \frac{\sqrt{D}(S\sqrt{D}+\sqrt{HK}+S\sqrt{H})(S\sqrt{D}+\sqrt{HK}+S\sqrt{K})}{S\sqrt{D}+\sqrt{HK}},$$

$M = S^{3/2}(D(D+K))^{1/4}$,

et $\|b\|$ est la norme ℓ^2 de la suite b, c'est à dire $\|b\| = \left(\sum_{d,k} |b_{d,k}|^2\right)^{1/2}$.

La fonction "presque lisse" intervenant dans R_2 est $\dfrac{G(s,b,d_1,h,k)}{bd_1 s} a(s)\ell(d_1)$ et elle vérifie :
$\dfrac{G(s,b,d_1,h,k)}{bd_1 s} \ll \dfrac{x(PB)^{-1/2}}{SBL}$, son défaut de lissité est inférieur à 3δ d'après le lemme 2.2.5.

On va donc travailler avec $\Phi(s,b,d_1,h,k) = Z^{-1}\dfrac{G(s,b,d_1,h,k)a(s)\ell(d_1)}{bd_1 s}$,

avec $Z = \dfrac{x(PB)^{-1/2}}{SBL}$.
Cela donne

$$R_2(L,S) \ll Z \sum_{\substack{d_1\\ d_2<D_2}} \lambda^+_{d_1}\mu^+_{d_2} \sum_{\substack{0<|h|<H\\ 0<|k|<K}} \sum_{\substack{b\in[B,4B]\\ b\equiv 0 \pmod{d_2}}} \rho(bd_1,k) \sum_{(s,bd_1)=1} \Phi(s,b,d_1,h,k) S(-h\overline{bd_1},-k,s).$$

Nous ne sommes pas encore en mesure d'appliquer le lemme 8, il faut regrouper les variables b et d_1.
Pour cela, comme l'avait fait Pomykala dans [Po], on suit le procédé de [D-I2] p. 269 qui utilise la formule d'inversion de Fourier.
On écrit :

$$\Phi(s,b,d_1,h,k) = \iint \Theta(s,t_1,t_2,h,k)e(t_1b+t_2d_1)dt_1dt_2, \tag{2.23}$$

avec,

$$\Theta(s,t_1,t_2,h,k) = \iint \Phi(s,y_1,y_2,h,k)e(-t_1y_1-t_2y_2)dy_1dy_2. \tag{2.24}$$

Dans la suite on utilisera le

LEMME 2.2.7. *Pour $t_1t_2 \neq 0$, et pour $\sigma = \sigma_1+\sigma_2+\sigma_3$ avec $\sigma_i \geq 1$, pour $i = 1,2,3$,on a :*

$$\begin{aligned}\frac{\partial^\sigma}{\partial s^{\sigma_1}\partial h^{\sigma_2}\partial k^{\sigma_3}}\Theta(s,t_1,t_2,h,k) &= (2i\pi t_1)^{-\nu_1}(2i\pi t_2)^{-\nu_2}\\ &\times \iint \frac{\partial^{\nu_1+\nu_2+\sigma}}{\partial s^{\sigma_1}\partial y_1^{\nu_1}\partial y_2^{\nu_2}\partial h^{\sigma_2}\partial k^{\sigma_3}}\Phi(s,y_1,y_2,h,k)e(-t_1y_1-t_2y_2)dy_1dy_2\\ &\ll (t_1B)^{-\nu_1}(t_2L)^{-\nu_2}x^{3\delta(\sigma+\nu_1+\nu_2)}s^{-\sigma_1}h^{-\sigma_2}k^{-\sigma_3}BL. \qquad (2.25)\end{aligned}$$

Pour obtenir ce lemme, on différentie σ fois la fonction Θ et on intègre ν_1 fois par parties par rapport à y_1, ν_2 fois par rapport à y_2 l'expression (2.24).

On prend $\nu_1 = 0$ si $|t_1B| \leq 1$, $\nu_1 = 2$ sinon, et $\nu_2 = 0$ si $|t_2D_1| \leq 1$, $\nu_2 = 2$ sinon, ceci pour avoir

$$\iint D_1B(t_1B)^{-\nu_1}(t_2D_1)^{-\nu_2}dt_1dt_2 \ll O(1) \tag{2.26}$$

On a ainsi en réinterprétant les différentes variables et en posant $J = LB$:

$$\begin{aligned}R_2(L,S) \ll \iint \frac{ZBLX^{3\delta(\nu_1+\nu_2)}}{(t_1B)^{\nu_1}(t_2D_1)^{\nu_2}} \sum_{\substack{0<|h|<H\\0<|k|<K}} \sum_{J<j<8J} a_{j,k}(t_1,t_2)\\ \times \sum_{(s,j)=1} \tilde{\Theta}(s,t_1,t_2,h,k)S(-h\bar{j},-k;s)dt_1dt_2, \qquad (2.27)\end{aligned}$$

avec

$$\tilde{\Theta}(s,t_1,t_2,h,k) = \frac{(t_1B)^{\nu_1}(t_2L)^{\nu_2}}{BLX^{3\delta(\nu_1+\nu_2)}}\Theta(s,t_1,t_2,h,k), \tag{2.28}$$

et

$$a_{j,k}(t_1,t_2) = \sum_{\substack{b\in[B,4B]\\d_1\in[L,2L]\\bd_1=j}} \sum_{\substack{d_2<D_2\\b\equiv 0 \pmod{d_2}}} \lambda_{d_1}^+\mu_{d_2}^+\rho(j,k)e(t_1b+t_2d_1). \tag{2.29}$$

Les entiers ν_1 et ν_2 dépendent de t_1 et t_2 suivant (2.26).

2.2.5. Évaluation du terme d'erreur.

On applique le lemme 2.2.6 à (2.27).
Le D de ce lemme correspond à $J = LB$, sinon toutes les autres variables h, k, s ont la même signification dans ce lemme, et dans la ligne (2.27). La fonction presque lisse est $\tilde{\Theta}$. D'après le lemme 2.2.7, son défaut de lissité est inférieur à 3δ, et elle ne dépend pas de j.

A partir de l'expression de $|a_{j,k}|$ donnée dans (2.29) on trouve la majoration triviale suivante :

$$\sum_{j,k} |a_{j,k}|^2 \ll LBKx^{\varepsilon}, \tag{2.30}$$

avec $\varepsilon < \delta$.

Par ailleurs $H = PBx^{-1+\varepsilon}$, donc H vérifie $H \ll x^{2\delta}$ et aura une très faible contribution car δ sera extrêmement petit.

Précédemment, on a choisi (cf (2.21)), $K = LB^{1/2}SP^{-1/2}x^{3\delta+3\varepsilon}$,
avec $S \ll (PB)^{1/2}$, donc $K \ll LBx^{3\delta+3\varepsilon}$.
De plus on a encore, $BPx^{-1} \ll x^{2\delta}$ ce qui est aussi très petit.

En appliquant le lemme 2.2.6 tout en tenant compte de ces remarques, on a la majoration :

$$\begin{aligned} R_2(L,S) &\ll x^{100\delta}\frac{(D_1BK)^{1/2}}{D_1B}(D_1BS + S^{3/2}(D_1B)^{1/2} \\ &\ll x^{100\delta}(P^{1/2}B^{3/2}D_1 + P^{3/4}B^{5/4}D_1^{1/2}). \end{aligned} \tag{2.31}$$

Puisqu'on veut $R_2 \ll x^{1-\varepsilon}$, cela impose pour le niveau du crible D_1 les majorations $D_1 \leq xP^{-1/2}B^{-3/2}x^{-100\delta}$, et $D_1 \leq x^2P^{-3/2}B^{-5/2}x^{-50\delta}$.

Lorsque $PB > x^{1+\delta}$ cela donne $D_1 = x^2P^{-3/2}B^{-5/2}x^{-50\delta}$. Pour $D_2 = x^{\delta/2}$, la condition (2.20) est alors largement vérifiée.

(On pourra remarquer que si à la place du lemme 2.2.6, on avait utilisé les majorations de Weil sur les sommes de Kloosterman on aurait obtenu un niveau de crible $D_1 \ll xP^{-3/4}B^{-7/4}$ à des puissances de x^{δ} près.)

2.2.6. Evaluation du terme principal.

On rappelle l'expression de ce terme obtenue précédemment :

$$\begin{aligned} T(P,B,d_1,d_2) &= X \sum_{b\equiv 0 \pmod{d_2}} \sum_{m\equiv 0 \pmod{d_1}} \frac{g(bm)\gamma(m)\rho(bm)}{bm} \\ &= X \sum_{b\equiv 0 \pmod{d_2}} \sum_{m\equiv 0 \pmod{d_1 b}} \frac{g(m)\gamma(mb^{-1})\rho(m)}{m}. \end{aligned}$$

Deshouillers et Iwaniec ont montré dans [D-I1] p. 9 l'égalité :

$$\sum_{m\equiv 0 \pmod{d_1 b}} \frac{g(m)\gamma(mb^{-1})\rho(m)}{m} = \frac{\rho(d_1 b)}{d_1 b} \prod_{p|d_1 b} \left(1+\frac{1}{p}\right)^{-1} \frac{L(1,\chi_4)}{\zeta(2)} \int \frac{g(u)\gamma(ub^{-1})}{u} du$$

$$+ O\left(\frac{\tau^2(d_1 b)x^{6\delta}}{\sqrt{d_1 b P}\log P}\right), \tag{2.32}$$

l'erreur $x^{6\delta}$ provient des défauts de lissité des fonctions g et γ.
Il reste alors à estimer pour u fixé dans le support de g,

$$\sum_{b\equiv 0 \pmod{d_2}} \frac{\theta(d_1 b)}{d_1 b}\gamma(ub^{-1}),$$

où θ est la fonction définie par

$$\theta(n) = \rho(n)\prod_{p|n}\left(1+\frac{1}{p}\right)^{-1}. \tag{2.33}$$

Alors comme au paragraphe 1, on étudie la série

$$K(s) = \sum_{m\geq 1} \frac{\theta(md_1 d_2)}{m^s} \tag{2.34}$$

Pour d_1, d_2, sans facteur carré donnés, on écrit : $\theta(md_1 d_2) = \theta(d_1 d_2)\theta_{d_1 d_2}(m)$.
La fonction $\theta_{d_1 d_2}$ prend donc les valeurs suivantes :

$$\begin{cases} \theta_{d_1 d_2}(2^\alpha) = 0 & \text{si } \alpha > 1, \\ \theta_{d_1 d_2}(2) = 2/3 & \text{si } 2 \not| d_1 d_2, \\ \theta_{d_1 d_2}(2) = 0 & \text{si } 2|d_1 d_2, \\ \theta_{d_1 d_2}(p^\alpha) = \theta_{d_1 d_2}(p) & \text{pour } \alpha > 1 \text{ et si } p > 2, \\ \theta_{d_1 d_2}(p) = 1 & \text{si } p|d_1 d_2, \text{ et si } p > 2, \\ \theta_{d_1 d_2}(p) = \frac{2p}{p+1} & \text{si } p \equiv 1 \pmod 4 \text{ et si } p \not| d_1 d_2, \\ \theta_{d_1 d_2}(p) = 0 & \text{si } p \equiv -1 \pmod 4 \text{ et si } p \not| d_1 d_2. \end{cases}$$

Ensuite, on écrit K sous forme de produit eulérien :

$$K(s) = \theta(d_1 d_2)\eta_2(d_1 d_2, s)\prod_{p>2}\left(1+\frac{\theta_{d_1 d_2}(p)}{p^s(1-\frac{1}{p^s})}\right),$$

avec

$$\eta_2(d_1 d_2, s) = \begin{cases} 1 & \text{si } 2|d_1 d_2, \\ 1+\frac{2^{1-s}}{3} & \text{sinon.} \end{cases}$$

Et d'après les valeurs prises par $\theta_{d_1 d_2}$, on a :

$$K(s) = \theta(d_1 d_2)\eta_2(d_1 d_2, s) \prod_{\substack{p \equiv 1 \pmod 4 \\ p | d_1 d_2}} \left(1 - \frac{1}{p^s} + \frac{2p}{(p+1)p^s}\right)^{-1}$$
$$\times \prod_{\substack{p \equiv -1 \pmod 4 \\ p | d_1 d_2}} \left(1 - \frac{1}{p^s}\right)^{-1} \prod_{p \equiv 1 \pmod 4} \left(1 - \frac{1}{p^s} + \frac{2p}{(p+1)p^s}\right)\left(1 - \frac{1}{p^s}\right)^{-1}.$$

Le produit $\prod_{\substack{p \equiv -1 \pmod 4 \\ p | d_1 d_2}} (...)$ n'a aucune contribution, car d'après (2.33), $\theta(d) = 0$, si d a un facteur premier congru à $-1 \pmod 4$.

En poursuivant encore un peu ces calculs, on arrive à :

$$K(s) = \frac{\zeta(s)L(s, \chi_4)}{\zeta(2s)} \Omega(d_1 d_2, s)\tilde{K}(s),$$

avec

$$\tilde{K}(s) = \left(1 + \frac{2^{1-s}}{3}\right)\left(1 + \frac{1}{2^s}\right)^{-1} \prod_{p \equiv 1 \pmod 4} \left(1 - \frac{1}{p^s} + \frac{2p}{(p+1)p^s}\right)\left(1 + \frac{1}{p^s}\right)^{-1},$$

et,

$$\Omega(d_1 d_2, s) = \tilde{\eta}(d_1 d_2, s)\theta(d_1 d_2) \prod_{\substack{p | d_1 d_2 \\ p \equiv 1 \pmod 4}} \left(1 - \frac{1}{p^s} + \frac{2p}{(p+1)p^s}\right)^{-1},$$

avec

$$\tilde{\eta}(d_1 d_2, s) = \begin{cases} \left(1 + \frac{2^{1-s}}{3}\right)^{-1} & \text{si } 2 | d_1 d_2, \\ 1 & \text{sinon.} \end{cases}$$

Maintenant, pour calculer $T(P, B, d_1, d_2)$ on utilise la formule d'inversion de Mellin. D'après (2.32), on a :

$$T(P, B, d_1, d_2) = X \frac{L(1, \chi_4)}{\zeta(2)} \sum_{b \equiv 0 \pmod{d_2}} \frac{\theta(d_1 b)}{d_1 b} \int \frac{g(u)\gamma(ub^{-1})}{u} du + O\left(\frac{x^{15\delta+\varepsilon} B^{1/2}}{\sqrt{d_1 P}}\right).$$

Soit $Q(b) = \int \frac{g(u)\gamma(ub^{-1})}{u} du$, où g est à support dans $[x^{1+\delta}\Delta^{\ell-1}, x^{1+\delta}\Delta^{\ell+1}]$ et γ dans $[y\Delta^{k-1}, y\Delta^{k+1}]$.
(On a alors $PB = x^{1+\delta}\Delta^{\ell-1}$.)
On écrit

$$\frac{Q(b)}{b} = \frac{1}{2i\pi}\int_{(\sigma)} \frac{R(s)b^{-s}}{s} ds,$$

avec,

$$R(s) = \int \frac{Q(v)}{v} v^{s-1} dv.$$

D'après les supports de γ et de g, la fonction Q est à support dans :

$$[x^{1+\delta}y^{-1}\Delta^{\ell-k-2}, x^{1+\delta}y^{-1}\Delta^{\ell-k+2}] = [B_1, B_2].$$

On intègre alors R par parties :

$$R(s) = \left[\frac{v^s}{s}\frac{Q(v)}{v}\right]_{B_1}^{B_2} - \int_{B_1}^{B_2} \frac{v^s}{s}\frac{d}{dv}\left(\frac{Q(v)}{v}\right) dv,$$

mais $Q(B_1) = 0$, car la condition uB_1^{-1} appartient au support de γ, impose $u \leq x^{1+\delta}\Delta^{\ell-1}$, et ainsi $g(u) = 0$. De même, on a $Q(B_2) = 0$.
Ainsi, on a l'égalité :

$$R(s) = -\int_{B_1}^{B_2} \frac{v^s}{s}\frac{d}{dv}\left(\frac{Q(v)}{v}\right) dv,$$

et après une nouvelle intégration par parties, on a :
(2.35)

$$R(s) = \int_{B_1}^{B_2} \frac{v^{s+1}}{s(s+1)}\frac{d^2}{dv^2}\left(\frac{Q(v)}{v}\right) dv \ll (|s|+1)^{-2}x^{6\delta\sigma}(|B_1|^{\sigma-1} + |B_2|^{\sigma-1}).$$

En sommant alors sur b, on a :

$$\frac{L(1,\chi_4)}{\zeta(2)} \sum_{b\equiv 0 \pmod{d_2}} \frac{\theta(d_1 b)}{d_1 b} \int \frac{g(u)\gamma(ub^{-1})}{u} du = \frac{L(1,\chi_4)}{\zeta(2)}\frac{1}{2i\pi}\int_{(\sigma)} \frac{R(s)K(s)}{(d_1 d_2)^s} ds,$$

où $K(s)$ dépend de d_1 et d_2 et $\sigma > 1$ et a été définie dans (2.34). On déplace alors cette intégrale à gauche de la droite $\Re s = 1$ et en utilisant (2.35), et en reprenant les arguments basés sur des propriétés des fonctions $\zeta(s)$, $\zeta(2s)$, $L(s,\chi_4)$ exposés lors de la preuve du lemme 2.1.1, ou bien en appliquant directement le résultat de [D-I1] p. 9, on a l'égalité :

$$\sum_{b\equiv 0 \pmod{d_2}} \frac{\theta(d_1 b)}{d_1 b} \int \frac{g(u)\gamma(ub^{-1})}{u} du = \frac{L(1,\chi_4)}{\zeta(2)}\tilde{K}(1)\frac{\omega(d_1,d_2)}{d_1 d_2} \iint \frac{g(u)\gamma(uv^{-1})}{uv} du dv$$

$$+ O\left(\frac{x^{15\delta}}{\sqrt{d_1 d_2 B}}\right). \tag{2.36}$$

(Pour des raisons esthétiques, on a écrit $\omega(d_1, d_2)$, à la place de $\Omega(d_1 d_2, 1)$.) Les différents termes d'erreur de (2.35) et (2.36) imposent

$$\sqrt{D_1 D_2} \ll x\sqrt{B}x^{-\varepsilon},$$

ce qui est plus faible que les conditions de la fin du paragraphe 2.2.5.
Tout ceci termine la démonstration de la proposition 2.2.3.

2.2.7. Application du crible vectoriel.

Grâce à la proposition 2.2.3, on est maintenant en mesure d'appliquer un crible en deux variables pour majorer les cardinaux $|C_{pb}|$.
La difficulté est que la fonction de crible ω de cette proposition ne vérifie pas d'égalité de la forme $\omega(a_1, a_2) = \omega_1(a_1)\omega_2(a_2)$, mais dépend du pgcd de (a_1, a_2), et le cas le plus délicat est quand ce pgcd est composé de nombreux petits facteurs premiers. Pour écarter cette difficulté, on reprend les idées de Brüdern et Fouvry [B-F], on commence par cribler très faiblement ces deux variables.
Pour cela nous utilisons le lemme fondamental pour un crible de dimension 2, tel qu'il est énoncé dans Iwaniec [I1].

LEMME 2.2.8. *Soient $u \geq 2$, $D \geq 2$, on pose $s = \dfrac{\log D}{\log u}$. Il existe alors deux suites $\lambda_d^{\pm}$, telles que $\lambda_1^{\pm} = 1$, $|\lambda_d^{\pm}| \leq 1$, $\lambda_d^{\pm} = 0$ pour $d > D$,*

$\lambda^- * \mathbb{1} \leq \mu * \mathbb{1} \leq \lambda^+ * \mathbb{1}$, *et*

$$\sum_{d|P(u)} \frac{\lambda_d^{\pm}\Omega(d)}{d} = V(u)\{1 + O(e^{-s}(\log D)^{-1/3})\},$$

avec $V(u) = \prod_{p<u}\left(1 - \dfrac{\Omega(p)}{p}\right)$, *$\Omega$ étant la fonction multiplicative définie par*

$$\frac{\Omega(p)}{p} = \frac{\omega(1,p)}{p} + \frac{\omega(p,1)}{p} - \frac{\omega(p,p)}{p^2}.$$

A partir de ce lemme on en déduit le corollaire :

COROLLAIRE 2.2.9. *On garde les notations du lemme 2.2.8. Etant donnés a_1, a_2 deux entiers sans facteur carré, avec tous leur facteur premier $> u$ on définit:*

$$S(a_1, a_2, u) = \sum_{\substack{b,m \\ m\equiv 0 \pmod{a_1} \\ b\equiv 0 \pmod{a_2} \\ p|bm \Rightarrow p>u}} g(bm)\gamma(m)|C_{bm}|.$$

Alors on a l'égalité :

$$S(a_1,a_2,u) = X\tilde{K}(1)\left(\frac{L(1,\chi_4)}{\zeta(2)}\right)^2 V(u)\frac{\omega(a_1,a_2)}{a_1a_2} \times \iint \frac{g(vw)\gamma(v)}{vw}dvdw\left\{1+O\left(\frac{e^{-s}}{(\log D)^{1/3}}\right)\right\} + O\left(\sum_{\substack{d|P(u)\\ d<D}}\mu^2(d)\sum_{d_1d_2=d}R(P,B,a_1d_1,a_2d_2)\right),$$

avec $V(u) = \prod_{p<u}\left(1-\frac{\Omega(p)}{p}\right)$.

Preuve du corollaire.
On commence par utiliser la suite λ^+ pour obtenir la majoration :

$$\begin{aligned} S(a_1,a_2,u) &\leq \sum_{d|P(u)}\lambda_d^+ \sum_{\substack{bm\equiv 0 \pmod d\\ b\equiv 0 \pmod{a_2}\\ m\equiv 0 \pmod{a_1}}} g(bm)\gamma(m)|C_{bm}| \\ &\leq \sum_{d|P(u)}\lambda_d^+ \sum_{d_1d_2=d}\sum_{\substack{m\equiv 0 \pmod{a_1d_1}\\ b\equiv 0 \pmod{a_2d_2}}} g(bm)\gamma(m)|C_{bm}|. \end{aligned}$$

D'après la proposition 2.2.3, on a :

$$\begin{aligned} S(a_1,a_2,u) &\leq X\tilde{K}(1)\left(\frac{L(1,\chi_4)}{\zeta(2)}\right)^2 \frac{\omega(a_1,a_2)}{a_1a_2}\iint\frac{g(vw)\gamma(v)}{vw}dvdw\sum_{d|P(u)}\frac{\lambda_d^+\Omega(d)}{d} \\ &\quad + \sum_{\substack{d|P(u)\\ d<D}}\lambda_d^+\sum_{d_1d_2=d}R(P,d_1a_1,d_2a_2) \\ &\leq X\tilde{K}(1)\left(\frac{L(1,\chi_4)}{\zeta(2)}\right)^2 \frac{\omega(a_1,a_2)}{a_1a_2}V(u) \\ &\quad \times\iint\frac{g(vw)\gamma(v)}{vw}dvdw\left(1+O\left(\frac{e^{-s}}{(\log D)^{1/3}}\right)\right) \\ &\quad + \sum_{\substack{d|P(u)\\ d<D}}\lambda_d^+\sum_{d_1d_2=d}R(P,d_1a_1,d_2a_2), \end{aligned}$$

ce qui prouve la majoration. De même en utilisant la suite λ_d^- on obtient la minoration.

• *Retour à la majoration de* $S(P,B)$.
Pour $z_1 < z_2$, on définit $P(z_1,z_2) = \prod_{z_1<p<z_2} p$, et on part de la majoration :

$$S(P,B) \leq \sum_{p|mb \Rightarrow p>u} \mu * \mathbb{1}(m,P(u,w))\mu * \mathbb{1}(b,P(u,z))g(mb)\gamma(m)|C_{mb}|.$$

On majore ensuite ces convolutions à l'aide des poids de Rosser-Iwaniec λ^+, μ^+ définis comme suit :
$\lambda_1^+ = \mu_1^+ = 1$, $\lambda_{d_1}^+ = 0$ si $d_1 > D_1$ et $\mu_{d_2}^+ = 0$ si $d_2 > D_2$,
$\lambda_d^+ = \mu_d^+ = 0$ si d a un facteur carré,
et pour $d = p_1...p_r$ avec $p_1 > p_2 > ..... > p_r$:

$$\lambda_d^+ = \begin{cases} (-1)^r & \text{si } p_1...p_{2\ell}p_{2\ell+1}^3 < D_1, \text{ pour tout } 0 \leq \ell \leq \dfrac{r-1}{2}, \\ 0 & \text{sinon,} \end{cases}$$

$$\mu_d^+ = \begin{cases} (-1)^r & \text{si } p_1...p_{2\ell}p_{2\ell+1}^3 < D_2, \text{ pour tout } 0 \leq \ell \leq \dfrac{r-1}{2}, \\ 0 & \text{sinon.} \end{cases}$$

A partir de ces poids on a :

$$\begin{aligned} S(P,B) &\leq \sum_{d_1|P(u,w)} \sum_{d_2|P(u,z)} \lambda_{d_1}^+ \mu_{d_2}^+ S(d_1,d_2,u) \\ &\leq A\tilde{K}(1)V(u)\left(1 + O\left(\frac{e^{-s}}{(\log D)^{1/3}}\right)\right) \sum_{\substack{d_1|P(u,w) \\ d_2|P(u,z)}} \lambda_{d_1}^+ \mu_{d_2}^+ \frac{\omega(d_1,d_2)}{d_1 d_2} \\ &\quad + O\left(\sum_{\substack{d_1|P(u,w) \\ d_2|P(u,z)}} |\lambda_{d_1}^+||\mu_{d_2}^+| \sum_{\substack{\ell<D \\ \ell|P(u)}} \mu^2(\ell) \sum_{\ell_1\ell_2=\ell} R(P,B,\ell_1 d_1, \ell_2 d_2) \right), \end{aligned}$$

d'après le corollaire 2.2.9.
Pour $\varepsilon > 0$ petit, on choisit $D = x^\varepsilon$, et $u = x^{\varepsilon^2}$ le terme d'erreur de la ligne précédente peut être réarrangé en :

$$\sum_{d_1<DD_1} \sum_{d_2<DD_2} |\lambda_{d_1}'^+||\mu_{d_2}'^+| R(P,B,d_1,d_2),$$

où les $\lambda_{d_1}'^+$, $\mu_{d_2}'^+$ sont en valeur absolue respectivement inférieurs à $\tau(d_1)$, $\tau(d_2)$ et sont nuls pour $d_1 > DD_1$, respectivement pour $d_2 > DD_2$, et ainsi cette erreur est d'après la proposition 2.2.3 majorée par $(D^2D_2)^{200}D_1^{1/2}B^{5/4}P^{3/4}$.

• *Traitement du terme principal.*

Dans un premier temps on écarte les entiers d_1 et d_2, tels que le pgcd $(d_1, d_2) > 1$, c'est à dire que l'on écrit :

$$\begin{aligned}\sum_{\substack{d_1|P(u,w)\\ d_2|P(u,z)}} \lambda^+_{d_1}\mu^+_{d_2}\frac{\omega(d_1,d_2)}{d_1d_2} &= \sum_{\substack{d_1|P(u,w)\\ d_2|P(u,z)\\ (d_1,d_2)=1}} \lambda^+_{d_1}\mu^+_{d_2}\frac{\omega(d_1,d_2)}{d_1d_2}\\ &\quad + \sum_{\substack{d_1|P(u,w)\\ d_2|P(u,z)\\ (d_1,d_2)>1}} \lambda^+_{d_1}\mu^+_{d_2}\frac{\omega(d_1,d_2)}{d_1d_2}\\ &= T_1 + T_2.\end{aligned}$$

Le terme T_2 est petit. Pour vérifier ceci, on commence par majorer les $\omega(d_1, d_2)$; d'après la ligne (2.13) de la proposition 2.2.3, on a $\omega(d_1, d_2) = O(x^\eta)$ pour tout $\eta > 0$, et en particulier pour $\eta = \varepsilon^3$ (où ε est extrêmement petit).
Les d_1 et d_2 étant de plus sans facteur carré, on peut alors profiter de l'inégalité :

$$T_2 \ll \sum_{\beta>u}\frac{1}{\beta^2}\sum_{\substack{d_1<\frac{DD_1}{\beta}\\ d_2<\frac{DD_2}{\beta}}}\frac{x^{\varepsilon^3}}{d_1d_2}.$$

En sommant directement, on obtient alors :

$$T_2 \ll x^{2\varepsilon^3}\log(DD_1)\log(DD_2)u^{-1} \ll x^{-\varepsilon^2/2}.$$

Maintenant, afin d'être en mesure d'appliquer les résultats d'Iwaniec sur les cribles linéaires, nous allons séparer les variables d_1 et d_2 dans la somme T_1.
Nous utiliserons la notation suivante :
$\omega_1(p) = \omega(p, 1)$ et $\omega_2(p) = \omega(1, p)$. (en fait, on a $\omega_1 = \omega_2$!)

On a alors l'égalité

$$\begin{aligned}T_1 &= \sum_{d_1|P(u,w)}\lambda^+_{d_1}\frac{\omega_1(d_1)}{d_1}\sum_{d_2|P(u,z)}\mu^+_{d_2}\frac{\omega_2(d_2)}{d_2}\\ &\quad + O\left(\sum_{\delta>u}\frac{\mu^2(\delta)}{\delta^2}\sum_{\substack{d_1<\frac{D_1}{\delta}\\ d_2<\frac{D_2}{\delta}}}\lambda^+_{d_1}\mu^+_{d_2}\frac{\omega_1(d_1\delta)\omega_2(d_2\delta)}{d_1d_2}\right)\\ &= T_1' + O(T_2').\end{aligned}$$

On montre de la même manière que pour T_2, que le terme d'erreur T_2' est un $O(x^{-\varepsilon^2/2})$.

Ensuite, en appliquant les résultats d'Iwaniec [I1] énoncés au théorème A1, on a :

$$T_1' \leq \prod_{u<p<w}\left(1-\frac{\omega_1(p)}{p}\right)\prod_{u<p<z}\left(1-\frac{\omega_2(p)}{p}\right)\left(F\left(\frac{\log D_1}{\log w}\right)F\left(\frac{\log D_2}{\log u}\right)+\varepsilon\right).$$

En faisant des raisonnements analogues à ceux du paragraphe 1, on montre :

$$\prod_{p<Q}\left(1-\frac{\omega_1(p)}{p}\right)=\prod_{p<Q}\left(1-\frac{1}{p}\right)\left(C+O\left(\frac{1}{\log Q}\right)\right),$$

avec :

$$C=\prod_{p}\left(1-\frac{1}{p}\right)^{-1}\left(1-\frac{\omega_1(p)}{p}\right).$$

On montre encore, après des calculs peu intéressants sur les produits eulériens :

$$V(u)=\prod_{p<u}\left(1-\frac{\Omega(p)}{p}\right)\prod_{p<u}\left(1-\frac{1}{p}\right)^2\left(\frac{\zeta(2)}{L(1,\chi_4)}\right)^2\left(\tilde{K}(1)^{-1}+O((\log u)^{-1})\right),$$

$\tilde{K}(1)$ étant le produit défini dans la proposition 2.2.3.

Enfin, en prenant $w=D_1^{1/2}$, avec $D_1=x^2P^{-1/2}B^{-5/2}$ et $z=x^{\delta^2}$, $D_2=x^{\delta/2}$ on trouve la majoration :

$$S(P,B)\leq\frac{A}{\log z}(1+O((\log u)^{-1}))F\left(\frac{1}{2\delta}\right)\left(\frac{2+\varepsilon}{\log D_1}\right)\iint\frac{g(v_1v_2)\gamma(v_1)}{v_1v_2}dv_1dv_2.$$

2.2.8. Conclusion pour S_2.

Il reste à évaluer :

$$S_2=\sum_{P,B}S(P,B),$$

ce qui revient en fait à calculer l'intégrale :

$$\begin{aligned}I&=\int_y^x\int_{x^{1+\delta}u^{-1}}^{x^{1+2\delta}u^{-1}}\frac{dudv}{uv\log(x^2u^{-3/2}v^{-5/2})}\\&=\int_\alpha^1\int_{1-\mu+\delta}^{1-\mu+2\delta}\frac{\log x\,d\nu d\mu}{2-3\mu/2-5\nu/2}.\end{aligned}$$

En calculant la valeur de cette intégrale on a la majoration :

$$S_2 \leq \frac{Ae^{-\gamma}}{\log z} F\left(\frac{1}{2\delta}\right)(2+\varepsilon)\delta \log x \left(-\log(\alpha - 1/2) - \log 2 + O(\delta) + O_{\delta,\varepsilon}\left(\frac{1}{\log x}\right)\right).$$

2.3.Conclusion.

D'après les propositions 2.1 et 2.2, δ, ε pouvant être choisis arbitrairement petits, l'inégalité $S_1 - S_2 > 0$ est réalisée dès que

$$1 - \log\frac{1}{\alpha} + 2\log 2 + 2\log(\alpha - 1/2) > 0.$$

C'est à dire α doit vérifier :

$$\alpha(\alpha - 1/2)^2 > \frac{1}{4e},$$

ce qui fournit $\alpha > \dfrac{149}{179} = 0.8324...$

DEUXIÈME PARTIE

PROPRIÉTÉS MULTIPLICATIVES DES VALEURS DE CERTAINS POLYNÔMES EN PLUSIEURS VARIABLES

Chapitre 0

Introduction

Les résultats du précédent travail laissent deux questions ouvertes : existe-t-il $\varepsilon > 0$, tel que $P^+\left(\prod_{p\sim x}(p^2+1)\right) > x^{1+\varepsilon}$, pour $x \to +\infty$? Peut-on obtenir un résultat inconditionnel concernant le polynôme n^3+2 ?
Pour le moment, nous ne sommes pas en mesure d'y répondre, et l'objectif de cette deuxième partie est de montrer que ces inégalités sont vérifiées en moyenne et ainsi d'étudier les propriétés multiplicatives de polynômes à coefficients entiers et en plusieurs variables tels par exemple $f(p_1,p_2) = 1+p_1^2+p_2^2$, ou $f(p_1,p_2,n_3) = 1+p_1^3+p_2^3+n_3^3$, etc.
Pour mener à bien ces recherches, il faut évaluer le comportement asymptotique des cardinaux des ensembles du type :

$$\mathcal{A}_m = \{(p_1,p_2),\ p_1,p_2 \sim x,\ f(p_1,p_2) \equiv 0 \pmod m\}$$

où p_1, p_2 sont des nombres premiers et la notation $n \sim N$, signifie $n \in [N,2N]$.

Lorsque m est petit, c'est à dire $m < x^{1-\varepsilon}$, le cardinal de ces ensembles est donné en moyenne grâce à un résultat du type le théorème de Bombieri-Vinogradov, obtenu à partir du classique théorème de Barban-Davenport-Halberstam pour la suite des nombres premiers.

Quand m est grand, on évalue ces ensembles individuellement à l'aide de méthodes de cribles, qui conduisent à des majorations de sommes d'exponentielles du type :

$$S_f(m,g,h) \sum_{\substack{0\le u,v<m \\ f(u,v)\equiv 0 \pmod m}} e\left(\frac{gu+hv}{m}\right).$$

Si f est un polynôme homogène, cette somme est facile à évaluer.
En effet, comme Greaves l'a montré dans [G1], pour $(uv,m)=1$, la congruence $f(u,v) \equiv 0 \pmod m$ se transforme en $v \equiv wu \pmod m$, avec $f(1,w) \equiv 0 \pmod m$. La somme $S_f(m,g,h)$ se comporte donc comme une somme géométrique, et on bénéficie d'importantes compensations.

En faisant alors l'hypothèse de positivité suivante :

(H1) : Il existe $A > 0$, et $x_0 > 0$, tels que pour $x,y > x_0$, on ait $f(x,y) > A(x^d+y^d)$, d étant le degré de f,

on montre le résultat suivant

THÉORÈME 1. *Soit f un polynôme irréductible, homogène, dont les coefficients sont premiers entre eux, et vérifiant l'hypothèse (H1).*

i) Si f est un polynôme du deuxième degré, alors pour $\lambda_2 < 10/9$, on a l'inégalité suivante :

$$|\{(p_1,p_2)\ ;\ p_1,p_2 \sim x,\ P^+(f(p_1,p_2)) > x^{\lambda_2}\}| \gg \frac{x^2}{\log^2 x}.$$

ii) Si f est un polynôme du troisième degré, alors pour $\lambda_3 < 6/5$, on a l'inégalité :

$$|\{(p_1,p_2)\ ;\ p_1,p_2 \sim x,\ P^+(f(p_1,p_2)) > x^{\lambda_3}\}| \gg \frac{x^2}{\log^2 x}.$$

L'hypothèse (H1) n'a aucun caractère crucial, elle sert seulement à définir $\log(f(p_1,p_2))$, et avec quelques modifications, on pourrait obtenir un résultat valable par exemple pour le polynôme $x^3 - 2y^3$.

Lorsque le polynôme f n'est pas homogène, les sommes $S_f(m,g,h)$ ne se majorent plus aussi facilement, et il faut faire appel aux résultats pointus de géométrie algébrique sur les majorations de sommes d'exponentielles sur des corps finis.
Dans le cas où f est un polynôme en deux variables, les majorations de Weil sont valables dans un cadre général, il faut seulement écarter les situations dégénérées comme par exemple les cas où la fonction $\Phi(u,v) = gu + hv$ est constante sur les courbes $C_p = \{(u,v) \in \mathbf{F}_p^2,\ f(u,v) \equiv 0 \pmod p\}$.
Plus précisement, pour $(g,h,t) \in \mathbf{Z}^3$, on définit les diviseurs de la courbe C_p suivants :

$$D(g,h,t) = \sum_{\substack{P=(u,v)\in C_p \\ gu+hv-t\equiv 0 \pmod p}} P.$$

Les résultats de Weil [Bo] sont alors applicables dès que l'on fait l'hypothèse :

(H2) Pour tout $t \in \mathbf{Z}$, tous $(g,h) \in \mathbf{Z}^2$, tels que $(g,h,p) = 1$,
on a $\mathrm{Deg}\ D(g,h,t) = O(1)$, la constante implicite ne dépend que du polynôme f.

L'hypothèse (H2) exclue les cas aberrants comme les "faux polynômes en deux variables" c'est à dire les $f(x,y) = \sum_{k=0}^{d} c_k(ax+by+c)^k$.
Parmi les polynômes vérifiant l'hypothèse (H2), on trouve les polynômes absolument irréductibles sur $\mathbf{Q}$, par exemple les polynômes du genre $f(x,y) = y^d - g(x)$, où le degré de g est premier à d.

Ces polynômes sont très commodes à étudier, du fait de leur *stabilité* algébrique, et on aurait pu restreindre notre étude à cette famille de polynômes et éviter bien des complications dans les premiers chapitres de ce travail, mais il était dommage de laisser tomber des polynômes du type par exemple $x^4 + y^2$, $x^3 - 7y^{15}$, ou plus compliqué,

$$27y^6 + 2x^3y^3 + 27y^4x + 27y^4 + 9x^2y^2 + 18y^2x + x^3 + 9y^2 + 3x^2 + 3x + 1$$

$$= (3y^2 + \sqrt[3]{2}xy + x + 1)(3y^2 + j\sqrt[3]{2}xy + x + 1)(3y^2 + j^2\sqrt[3]{2}xy + x + 1)!!!$$

Plus sérieusement, il est difficile de déterminer si un polynôme est absolument irréductible ou ne l'est pas (On peut trouver des critères dans le livre de Schmidt [Schm] p.190), tandis que les hypothèses des théorèmes qui suivront seront aisées à vérifier.

En incorporant ceci dans la méthode de Tchebychev-Hooley, on montre le

THÉORÈME 2. *Soit f un polynôme irréductible en deux variables, dont les coefficients sont premiers entre eux et vérifiant les conditions (H1) et (H2).*

Les deux assertions suivantes sont alors vérifiées :

i) Dans le cas où f est un polynôme du second degré, pour $\lambda_2 < 36/35$, on a l'inégalité :

$$|\{(p_1, p_2)\ ;\ p_1, p_2 \sim x,\ P^+(f(p_1, p_2)) > x^{\lambda_2}\}| \gg \frac{x^2}{\log^2 x}.$$

ii) Si f est un polynôme du troisième degré, alors pour $\lambda_3 < 20/19$, on a l'inégalité :

$$|\{(p_1, p_2)\ ;\ p_1, p_2 \sim x,\ P^+(f(p_1, p_2)) > x^{\lambda_3}\}| \gg \frac{x^2}{\log^2 x}.$$

Le point (i) est une amélioration et une généralisation d'un résultat de Plaksin [Pl]. Celui-ci avait en effet obtenu pour le polynôme $f(p_1, p_2) = p_1^2 + p_2^2 + 1$ un exposant $\lambda_2 = 71/70$. Cette amélioration résulte du fait que les variables p_1 p_2 jouent un rôle symétrique, il est donc plus intéressant de les détecter avec un crible de dimension 2 sur les produits correspondants n_1n_2, que de cribler séparément ces variables n_1, n_2 à l'aide de cribles linéaires.

La méthode de Tchebychev-Hooley suivie pour démontrer le théorème 1 s'étend aux polynômes en trois variables, mais en utilisant les majorations de sommes d'exponentielles données par Deligne et en faisant les hypothèses suivantes :

(H3) Il existe $x_0 > 0$ et $A > 0$, tels que $f(x_1, x_2, x_3) > A(x_1^d + x_2^d + x_3^d)$ pour tous $x_1, x_2, x_3 > x_0$.

(H4) Pour tous les entiers, (g,h,k,t) on définit les variétés

$$W(g,h,k,t) = \{(u,v,w) \in \mathbf{F}_p^3,\ f(u,v,w) \equiv 0 \,(\mathrm{mod}\, p),\ gu+hv+kw-t \equiv 0 \,(\mathrm{mod}\, p).$$

On suppose que W vérifie les conditions suivantes pour tous g,h,k, tels que $(g,h,k,p) = 1$:

(i) $W(g,h,k,t)$ est une courbe, ou la variété vide.

(ii) Pour tout t sauf un nombre fini ne dépendant pas de p, $W(g,h,k,t)$ est une courbe absolument irréductible.

et on a alors le théorème suivant

THÉORÈME 3. *Soit f un polynôme irréductible de $\mathbf{Z}[x_1,x_2,x_3]$, de degré 3, dont les coefficients sont premiers entre eux et vérifiant les conditions (H3) et (H4):*

Alors, pour $\tau < 7/6$ on a l'inégalité :

$$|\{(p_1,p_2,n_3)\ ;\ p_1,p_2,n_3 \sim x,\ P^+(f(p_1,p_2,n_3) > x^\tau\}| \gg \frac{x^3}{\log^2 x}.$$

L'hypothèse (H4) est d'un caractère tout aussi général que l'hypothèse (H2), elle exclut les polynômes du type

$$f(u,v,w) = \sum_{\substack{0\le i,j\le d \\ 0\le i+j\le d}} a_{i,j}(\alpha u+\beta v+\gamma w+\delta)^i(\alpha' u+\beta' v+\gamma' w+\delta')^j.$$

Bien que les résultats de Deligne apportent d'importantes compensations dans les sommes d'exponentielles rencontrées dans la démonstration, la méthode suivie ne permet pas d'obtenir un résultat intéressant concernant $P^+(f(p_1,p_2,p_3))$, f étant un polynôme de degré 3.
En effet on obtient seulement $P^+(f(p_1,p_2,p_3)) > x^{\lambda_3'}$ pour une proportion positive de p_1,p_2,p_3, avec $\lambda_3' < 3/2 - \sqrt{3/14}$, mais $3/2 - \sqrt{3/14} < 20/19 = \lambda_3$, l'exposant obtenu au point (ii) du théorème 2.
Toutes les compensations gagnées dans les sommes d'exponentielles n'ont pas suffi à combler la perte de précision causée par l'application d'un crible de dimension 3 pour détecter les produits $p_1p_2p_3$.

Lorsque f est un polynôme homogène (en trois variables), on peut majorer les sommes d'exponentielles sans faire appel aux résultats de géométrie algébrique de Deligne, mais avec des méthodes élémentaires du type de celles qui ont servi à la preuve du théorème 1, cependant, les résultats que l'on trouve sont du même ordre que ceux du cas général.
L'étude des polynômes homogènes en trois variables reste donc un problème ouvert peut-on dans certains cas trouver des compensations en moyenne sur les sommes d'exponentielles du type de celles qu'on obtenues Deshouillers et Iwaniec dans [D-I1] pour le polynôme n^2+1 ?

A notre connaissance, il n'existe pas encore de résultat systématique du type celui de Hooley donnant une majoration de $S_f(p, h_1, ..., h_k)$ lorsque f est un polynôme en quatre variables et plus.
Katz et Laumon [K-L] ont obtenu un résultat général annonçant la majoration espérée $O(p^{(k-1)/2})$ pour presque tous les $(h_1, ..., h_k)$, mais ce résultat n'est pas applicable dans ce contexte, car les h_i peuvent être petits. Laumon [Lau] a obtenu des résultats précis sur des sommes d'exponentielles le long d'hypersurfaces diagonales et il nous a semblé intéressant de donner un exemple de polynôme pour lequel ce résultat s'appliquait agréablement. Ce polynôme est de degré supérieur à 4, c'est pourquoi, le résultat que l'on trouve n'est pas tout à fait aussi précis que les précédents théorèmes.
Dans le prolongement du théorème 3, on montre le

THÉORÈME 3 BIS. *Pour* $\lambda < \dfrac{16248}{13725} = 1.18...$, *on définit les ensembles* $\mathcal{C}(\lambda)$ *suivants :*

$$\mathcal{C}(\lambda) = \{(p_1, p_2, n_3, n_4),\ p_1, p_2 \sim x,\ n_3 \sim x^{4/5},\ n_4 \sim x^{2/3},\ \textit{et vérifiant } (i) \textit{ ou} (ii)\},$$

avec

(i) il existe $p > x(\log x)^{-3}$ *tel que* $p^2 | 1 + p_1^4 + p_2^4 + n_3^5 + n_4^6$,

(ii) $P^+(1 + p_1^4 + p_2^4 + n_3^5 + n_4^6) > x^\lambda$.

Les ensembles $\mathcal{C}(\lambda)$ *vérifient la minoration :* $|\mathcal{C}(\lambda)| \gg \dfrac{x^{52/15}}{\log^2 x}$.

On ne peut pas comparer directement ce théorème avec le résultat issu du théorème 3 car dans ce théorème, les variables n'ont pas toutes le même poids. En appliquant la méthode suivie pour démontrer le théorème 3 à la suite $1+p_1^4+p_2^4+n_3^5$, avec $p_1 \sim x$, $p_2 \sim x$, et $n_3 \sim x^{4/5}$, on montre que pour une proportion positive de (p_1, p_2, n_3), le nombre $1 + p_1^4 + p_2^4 + n_3^5$ admet soit un facteur carré supérieur à $x^2(\log x)^{-6}$, soit un facteur premier supérieur à $x^{\lambda'}$, avec $\lambda' < 1.15 < \lambda$.
On peut obtenir des résultats de ce genre pour une très large famille de polynômes. On a choisi le polynôme $1 + t_1^4 + t_2^4 + t_3^5 + t_4^6$, car tous arguments de la preuve correspondant à ce polynôme s'enchaînent très bien. Dans la fin du chapitre 6 on indique quelles situations critiques ont été évitées par ce choix de polynôme, laissant ainsi ouvertes plusieurs questions de géométrie algébrique qui sortent du cadre de cette thèse.

Nous avons ensuite repris les travaux de Plaksin [Pl] sur le polynôme $1 + x_1^2 + x_2^2$ pour obtenir des majorations précises du cardinal des ensembles :

$$\{(n_1, n_2),\ n_1, n_2 \sim x,\ n_1 n_2 \equiv 0 \pmod a,\ n_1^2 + n_2^2 + 1 \equiv 0 \pmod m\}.$$

Les résultats de Plaksin ne sont valables que dans le cas où m est un nombre premier, mais en ajoutant la condition $(n_1 n_2, m) = 1$, ils se généralisent à des entiers m quelconques.

Ceci sert à la démonstration du théorème suivant qui est pour ainsi dire dual au théorème 2 :

THÉORÈME 4. *Pour $1 < y < x$, soit Ψ, la fonction définie par*

$$\Psi(x,y) = |\{(p_1,p_2)\ ;\ p_1,p_2 \sim x,\ P^+(p_1^2+p_2^2+1) < y\}|,$$

où $P^+(n)$ est le plus grand facteur premier de n.

Pour $y > x^\alpha$, avec $\alpha = \exp(-1/33) = 0.97..$, on a alors l'inégalité :

$$\Psi(x,y) \gg \frac{x^2}{\log^2 x}.$$

Comme dans la preuve du théorème 2 de la première partie de cette thèse concernant le polynôme n^2+1, on adapte les poids de Balog-Friedlander ([Ba], [Fr2]) au polynôme $p_1^2+p_2^2+1$.
On peut obtenir des résultats de ce type valables pour n'importe quel polynôme f en deux variables irréductible vérifiant l'hypothèse (H2), mais au prix de discussions fastidieuses sur la nature des points singuliers des courbes

$$\{(x_1,x_2) \in \mathbf{C^2}\ ;\ f(x_1,x_2) = 0\}$$

que l'on a préféré éviter.

Dans l'esprit des travaux de Greaves ([G2] et [G3]), et de Richert [H-R], nous nous sommes intéressé au problème de représentation de nombres presque premiers par des polynômes en deux variables et nous montrons le

THÉORÈME 5. *Soit f un polynôme irréductible de degré 3 en deux variables dont les coefficients sont premiers entre eux et vérifiant l'hypothèse (H2). On a alors l'inégalité :*

$$|\{(n_1,n_2) \sim x\ ;\ f(n_1,n_2) = P_3\}| \gg \frac{x^2}{\log x}.$$

Pour démontrer ce résultat, on applique le crible pondéré de Richert (cf par exemple le théorème 9.3 p.253 du livre de [H-R]), que nous pouvons utiliser directement grâce aux lemmes intermédiaires qui ont servi à la preuve du théorème 2.

Pour mieux saisir l'intérêt du théorème 5, il est utile de rappeler les résultats suivants (tous les polynômes considérés sont primitifs et irréductibles) :

-si f est un polynôme de degré 3, l'équation $f(p_1,p_2) = P_4$ a une infinité de solutions (p_1,p_2), (Greaves [G3]).

-si f est un polynôme homogène de degré 3, il existe une infinité de (n_1,n_2), tels que $f(n_1,n_2) = P_2$. (Greaves [G2]).

-si f est un polynôme toujours de degré 3, mais en une seule variable, il existe une infinité d'entiers n tels que $f(n)$ ait au plus quatre facteurs premiers. (Richert [H-R])

Par contre, nous ne sommes pas parvenus à obtenir un théorème de ce type intéressant pour un polynôme en trois variables. Les méthodes utilisées ne suffisent pas pour montrer que $f(n_1, n_2, n_3) = P_2$ pour une infinité de n_1, n_2, n_3.

Nous regrettons encore que les théorèmes 1, 3, 5, ne s'étendent pas à des polynômes de degré 4 et plus. On est bloqué par le fait que lorsque le degré du polynôme est supérieur ou égal à 4, on n'ait pas trouvé de majoration satisfaisante du nombre de (p_1, p_2) tels que $f(p_1, p_2) \equiv 0 \pmod{p^2}$, où p est un nombre premier supérieur à x. On peut cependant faire le parallèle entre cette difficulté et le fait que l'on ne sait pas si il existe un polynôme (irréductible) de degré 4 prenant une infinité de valeurs sans facteur carré.

Le premier résultat de Greaves [G3] évoqué ci-dessus concerne en fait des polynômes de degré d quelconque. Il a en effet montré que si f est de degré d, alors $f(p_1, p_2) = P_{d+1}$ pour une infinité de nombres premiers p_1, p_2. Pour obtenir ceci, il se sert du théorème de Richert qui est la clé de la preuve du théorème 5, et des estimations en moyenne des quantités $\mathcal{A}_m$ pour $m < x^{1-\epsilon}$ obtenues à partir du théorème de Barban-Davenport-Halberstam.

Cependant, en revenant à la définition des poids de Richert, et en y combinant un crible de dimension 2, on peut repousser le niveau général du crible de $m < x^{1-\epsilon}$, à $m < x^{2-\epsilon}$, lorsque f est un polynôme homogène, à $m < x^{4/3-\epsilon}$, lorsque f vérifie la condition (H2).

En profitant de ceci, dans le cas où f est un polynôme homogène, nous apportons l'amélioration du résultat de Greaves suivante :

THÉORÈME 6. *Soit f un polynôme irréductible homogène en deux variables de degré d, dont les coefficients sont premiers entre eux. On a alors l'inégalité :*

$$|\{(p_1, p_2) \sim x \ ; \ \Omega(f(p_1, p_2)) < \frac{2d}{3} + 8.24\}| \gg \frac{x^2}{\log^3 x}.$$

Ce résultat est intéressant pour $2d/3 + 8.24 < d + 1$, c'est à dire pour $d \geq 22$.
En fait, pour chaque d on peut obtenir un meilleur résultat, mais après de longs calculs d'optimisation qui sont sans intérêt.

L'utilisation des poids de Richert nécessite non seulement une connaissance précise des quantités $|\mathcal{A}_m|$, lorsque m est sans facteur carré, mais encore une inégalité du type :

$$\sum_{z<p<y} |\mathcal{A}_{p^2}| = o\left(\frac{x^2}{\log^3 x}\right).$$

Lorsque f est homogène, Greaves a obtenu ceci dans [G4], en profitant astucieusement de l'homogénéité de f pour traduire en terme de réseaux, la congruence $f(n_1, n_2) \equiv 0 \pmod{p^2}$.

Lorsque le polynôme n'est pas homogène, ce raisonnement ne tient plus, et quand le degré de f est supérieur à 4, on ne peut obtenir une majoration satisfaisante de $|\mathcal{A}_{p^2}|$, pour $p > x$.
Ainsi le résultat que l'on obtient pour un polynôme f non homogène concerne seulement la quantité $\omega(f(p_1, p_2))$, la fonction $\omega(n)$ étant le nombre de facteurs premiers distincts de n :

THÉORÈME 7. *Soit f un polynôme irréductible en deux variables de degré d, dont les coefficients sont premiers entre eux et vérifiant l'hypothèse (H2). Pour $x \geq 1$, et pour tout $\varepsilon > 0$, on définit l'ensemble $\mathcal{E}$ suivant :*

$$\mathcal{E} = \{(p_1, p_2)\ ;\ p_1, p_2 \sim x \text{ et vérifiant } (i),\ (ii) \text{et } (iii)\},$$

avec (i) : $p|f(p_1, p_2) \Rightarrow p > x^{1/4}$,

(ii) : $p^2|f(p_1, p_2) \Rightarrow p > x^{1-\varepsilon}$,

(iii) : $\omega(f(p_1, p_2)) < k(d)$.

Lorsque $k(d) > 6d/7 + 5.278$, on a la minoration :

$$|\mathcal{E}| \gg \frac{x^2}{\log^3 x}.$$

Ce résultat apprend quelque chose de nouveau pour $d > 30$, mais la remarque faite après le théorème 6 est valable pour ce théorème, si on le désire, pour chaque d fixé, on peut améliorer la valeur $k(d)$.
Plus le degré de f est grand, plus ce théorème est intéressant. Par exemple, si f est un polynôme de degré 1000, alors nous savons d'après Greaves que pour une infinité de p_1, p_2, $f(p_1, p_2) = P_{1001}$, mais le théorème 7 dit que $\omega(p_1, p_2) \leq 862...$

Quand on cherche une estimation des cardinaux $|\mathcal{A}_m|$, on écrit l'approximation classique :

$$|\mathcal{A}_m| = |\mathcal{A}|\frac{r(m)}{\varphi(m)^2} + R_m,$$

avec $\mathcal{A} = \{(p_1, p_2); p_1, p_2 \sim x\}$,

$r(m) = |\{(u, v); 0 \leq u, v < m,\ (uv, m) = 1,\ f(u, v) \equiv 0 \pmod m\}|$, et R_m est un terme d'erreur que l'on espère rendre acceptable.

(On adopte des notations analogues lorsque f est un polynôme en trois variables.)

Le premier chapitre de ce travail fournit des estimations de la fonction r, avec des arguments algébriques, géométriques et combinatoires parfois assez ardus car nous travaillons dans un cadre très général.
Dans le deuxième, on donne des majorations de sommes d'exponentielles résultant des travaux de Weil et de Deligne qui seront reprises dans le chapitre trois où on établira des estimations asymptotiques des cardinaux d'ensembles du type :

$$\{(n_1, n_2),\ n_1, n_2 \sim x,\ n_1 n_2 \equiv 0 \ (\mathrm{mod}\, a),\ f(n_1, n_2) \equiv 0 \ (\mathrm{mod}\, m)\},$$

où m et a sont des entiers sans facteur carré pour alors être en mesure d'estimer les ensembles $\mathcal{A}_m$, lorsque m est supérieur à $x^{1-\epsilon}$. Les quantités $|\mathcal{A}_m|$, pour $m < x^{1-\epsilon}$ sont estimées en moyenne dans le chapitre 4, à l'aide du théorème de Barban-Davenport-Halberstam.

Enfin, les cinq derniers chapitres correspondent aux preuves des différents théorèmes annoncés.

Chapitre 1
Résultats préliminaires sur les fonctions r

La fonction r est jumelée avec la fonction ρ définie par :

$$\rho(m) = |\{(u,v),\ 0 \leq u,v < m,\ f(u,v) \equiv 0 \pmod m\}|,$$

avec une définition analogue lorsque f est un polynôme en trois variables. Ces fonctions ρ et r dépendent bien sûr du polynôme f, mais dans toute la suite il n'y aura pas de problème d'ambiguïté, si ce n'est dans quelques passages des paragraphes 1.4, 2.3 et 6.3, où on notera alors ces fonction ρ_f et r_f.

1.1. Les résultats de Plaksin.

Dans le cas où f est le polynôme $f(x,y) = x^2 + y^2 - k$, avec $k \in \mathbf{Z}$, Plaksin a déterminé (dans [Pl], lemme 14 p. 282) les valeurs prises par la fonction ρ. Il a montré le lemme :

LEMME 1.1.1. *La fonction ρ est multiplicative, et vérifie :*

$$\rho(p) = \begin{cases} p - \chi_4(p) & \text{si } p \nmid k \\ p(1+\chi_4(p)) - \chi_4(p) & \text{si } p|k, \end{cases}$$

où χ_4 est le caractère non trivial modulo 4.

De plus, lorsque $p \nmid k$, on a : $\rho(p^\alpha) = p^{\alpha-1}\rho(p)$, pour $\alpha \geq 1$.

Plaksin a encore étudié les valeurs de la fonction r, définie dans l'introduction nous utiliserons le résultat ([Pl] lemme 15 p. 282) :

LEMME 1.1.2. *La fonction r est multiplicative et prend les valeurs suivantes :*

si $p > 2$, et $\alpha \geq 1$, $r(p^\alpha) = p^{\alpha-1}r(p)$,

pour $p > 2$, on a :

$$r(p) = \begin{cases} \varphi(p)(1+\chi_4(p)) & \text{si } p|k, \\ \varphi(p) - 1 - \chi_4(p) - 2\left(\frac{k}{p}\right) & \text{sinon.} \end{cases}$$

Enfin, pour $p = 2$, on a :

$r(2^\alpha) = 2^{\alpha-3}r(8)$, *pour* $\alpha \geq 3$,

$$r(2) = \begin{cases} 1 & \text{si } 2|k, \\ 0 & \text{sinon,} \end{cases}$$

$$r(4) = \begin{cases} 4 & \text{si } k \equiv 2 \pmod 4, \\ 0 & \text{sinon,} \end{cases}$$

$$r(8) = \begin{cases} 16 & \text{si } k \equiv 2 \pmod 8, \\ 0 & \text{sinon.} \end{cases}$$

1.2. Évaluation des fonctions r et ρ dans le cas où f est un polynôme homogène.

Si $(uv, m) = 1$, l'équation $f(u, v) \equiv 0 \pmod m$, se réécrit comme
$u \equiv wv \pmod m$, avec $f(1, w) \equiv 0 \pmod m$.
En profitant de cette idée, Greaves a montré dans [G2], le résultat :

LEMME 1.2. *(i) On a l'inégalité $\rho(p) = O(p)$, la constante du O ne dépend que de f.*

(ii) Pour $Q > 2$, on a l'égalité :

$$\sum_{p<Q} \frac{\rho(p) \log p}{p^2} = \log Q + O(1),$$

(iii) Pour $\alpha \geq 3$, on a $\rho(p^\alpha) = O(p^{\alpha+[\alpha(1-2/d)]})$, et pour $\alpha = 2$, on a : $\rho(p^2) = O(p^2)$.

(iv) La fonctions r associée vérifie des propriétés similaires.

1.3. Étude des fonctions r et ρ dans le cas où f est un polynôme en 2 variables : cas général.

D'après le théorème chinois ces fonctions sont multiplicatives.
Lorsque f est un polynôme absolument irréductible sur $\mathbf{F}_p$, Weil a prouvé que $\rho(p) = p + O(\sqrt{p})$. Puis, Greaves [G3] a étendu ce résultat au cas qui nous intéresse, c'est à dire lorsque f est un polynôme irréductible non homogène, mais pas nécessairement absolument irréductible sur $\mathbf{Q}$.
Dans ce cas, il existe une extension algébrique K de $\mathbf{Q}$, dans laquelle f se factorise en produit de facteurs absolument irréductibles

$$f = g_1 \cdots g_m.$$

Les coefficients de g_1 engendrent une extension $\mathbf{Q}(\theta_1)$ de $\mathbf{Q}$.
Soit O_{θ_1} l'anneau des entiers de $\mathbf{Q}(\theta_1)$.
On a le résultat ([G3])

LEMME 1.3.1. *Pour tout p, sauf un nombre fini, on a :*

$$\rho(p) = ps_p + O(\sqrt{p}),$$

où s_p est le nombre d'idéaux premiers P de O_{θ_1}, tels que $Norm(P) = p$.

Ensuite en utilisant le corollaire de Nagell [N1] du théorème des idéaux premiers, on a :

$$\sum_{p \leq Q} \frac{s_p \log p}{p} = \log Q + O(1),$$

et ainsi,

$$\sum_{p \leq Q} \frac{\rho(p) \log p}{p^2} = \log Q + O(1). \tag{1.1}$$

Cette dernière égalité est une condition d'application des cribles de Selberg, et de Rosser-Iwaniec.

Pour évaluer $\rho(p^\alpha)$, lorsque $\alpha \geq 2$, il est intéressant de tenir compte des singularités sur f, ou plus précisement de F, le polynôme homogène associé.
Soit $\mathbf{P}^2_{\mathbf{Q}}$ l'espace projectif de dimension 2 sur $\mathbf{Q}$. On définit alors la courbe Y associée à F :

$$Y = \{(x_1, x_2, t) \in \mathbf{P}^2_{\mathbf{Q}},\ F(x_1, x_2, t) = 0\},$$

On dit qu'une courbe est lisse, lorsqu'elle n'admet aucun point singulier, c'est à dire ici, quand le sytème d'équations :

$$F(x_1, x_2, t) = \frac{\partial F}{\partial x_1}(x_1, x_2, t) = \frac{\partial F}{\partial x_2}(x_1, x_2, t) = 0,$$

n'a pas de solution (x_1, x_2, t) sur $\mathbf{P}^2_{\mathbf{Q}}$.
On montre la proposition suivante

PROPOSITION 1.3.2. *Les deux assertions suivantes sont vérifiées :*

i) si Y est une courbe lisse sur $\mathbf{P}^2_{\mathbf{Q}}$, alors pour tout p, sauf un nombre fini, pour tout $\alpha \geq 2$, on a l'égalité : $\rho(p^\alpha) = p^{\alpha-1}\rho(p)$, et a fortiori la majoration $\rho(p^\alpha) = O(p^\alpha)$,

ii) dans le cas général, on a pour tout $\alpha \geq 2$, la majoration :

$$\rho(p^\alpha) = O(\alpha p^{\frac{4\alpha}{3}}),$$

les constantes implicites ne dépendent que de f.

Le résultat (ii) n'est pas optimal mais est de caractère général, ce qui sera très utile dans la suite.
On aurait pu obtenir par récurrence des formules précises, mais de syntaxe plus lourde, et au prix de discussions fastidieuses sur la nature des singularités de f.

Preuve de (i).
Pour p premier, on appelle X_p la courbe sur $\mathbf{F}_p^2$, définie par

$$X_p = \{(x,y) \in \mathbf{F}_p^2,\ f(x,y) \equiv 0 \ (\mathrm{mod}\, p)\}.$$

Alors d'après le lemme B2, énoncé dans l'annexe B, il existe P, tel que pour tout $p > P$, les courbes X_p soient lisses sur $\mathbf{F}_p$.
La démonstration du point (i) est du même type que celle du lemme de Hensel. Pour $\alpha \geq 2$, et pour $p > P$, on écrit $x = u + \lambda p^{\alpha-1}$, $y = v + \mu p^{\alpha-1}$, avec $0 \leq u, v < p^{\alpha-1}$, et $0 \leq \lambda, \mu < p$.

En appliquant la formule de Taylor, on a l'égalité

$$f(x,y) \equiv f(u,v) + p^{\alpha-1}\left(\lambda \frac{\partial f}{\partial u}(u,v) + \mu \frac{\partial f}{\partial v}(u,v)\right) \ (\mathrm{mod}\, p^\alpha).$$

Comme la courbe X_p est lisse, on ne peut avoir en un point où $f(u,v) \equiv 0 \ (\mathrm{mod}\, p)$,

$$\frac{\partial f}{\partial u}(u,v) \equiv \frac{\partial f}{\partial v}(u,v) \equiv 0 \ (\mathrm{mod}\, p).$$

Ainsi, chaque solution (u,v) comptée dans $\rho(p^{\alpha-1})$, fournit exactement p solutions de $\rho(p^\alpha)$, ce qui revient à écrire $\rho(p^\alpha) = p\rho(p^{\alpha-1})$.

Preuve de (ii).
Le principe de cette démonstration consiste à fixer une variable, par exemple la première u, puis d'appliquer les résultats généraux de Nagell [N2] sur le nombre de solutions de la congruence $g(v) \equiv 0 \ \mathrm{mod}\, p^\alpha$ au polynôme $g(v) = f(u,v)$. La difficulté est que ces résultats dépendent du discriminant de g et donc de la variable u.
Le lemme suivant est un récapitulatif des théorèmes 42, 52, 53, 54 des pages 80 à 90 du livre de Nagell [N2].

LEMME 1.3.3. *Soit g un polynôme primitif de degré d et de discriminant D.*

La fonction $\sigma_g(n) = |\{0 \leq u < n,\ g(u) \equiv 0 \ (\mathrm{mod}\, n)\}|$ est multiplicative, et vérifie les propriétés suivantes :

i) pour tout p premier, on a $\sigma_g(p) \leq d$,

ii) si $p \not| D$, alors pour tout $\alpha \geq 1$, on a l'égalité

$$\sigma_g(p^\alpha) = \sigma_g(p),$$

iii) si $p|D$, et plus précisément si $p^\mu \| D$, alors pour α tel que $\alpha \geq 2\mu + 1$, on a l'égalité :

$$\sigma_g(p^\alpha) = \sigma_g(p^{2\mu+1}) \leq dp^{2\mu},$$

iv) plus généralement, pour tout $p \geq 2$ et tout $\alpha \geq 1$, on a l'inégalité :

$$\sigma_g(p^\alpha) \leq dD^2.$$

Pour a mod p^α donné, on définit les polynômes g_a et h_a par $g_a(b) = f(a,b)$, et $h_a(b) = f(b,a)$. On note $D(g_a)$, $D(h_a)$ leur discriminant respectif.

On part de l'égalité :

$$\rho(p^\alpha) = \sum_{0 \le \beta \le \alpha} \Psi(\beta),$$

avec

$$\Psi(\beta) = \sum_{\substack{0 \le u,v < p^\alpha \\ f(u,v) \equiv 0 \pmod{p^\alpha} \\ p^\beta = (D(g_u), D(h_v), p^\alpha)}} 1.$$

Nous allons établir deux majorations de $\Psi(\beta)$. La première est intéressante lorsque β est grand. On oublie la contrainte $f(u,v) \equiv 0 \pmod{p^\alpha}$, et on a la majoration :

$$\Psi(\beta) \le \sum_{\substack{0 \le u < p^\alpha \\ D(g_u) \equiv 0 \pmod{p^\beta}}} \sum_{\substack{0 \le v < p^\alpha \\ D(h_v) \equiv 0 \pmod{p^\beta}}} 1.$$

Les sommes sur u et sur v sont alors des $O(p^{\alpha-\beta})$, d'après le point (iv) du lemme 1.3.3 appliqué aux polynômes $u \to D(g_u)$, et $v \to D(h_v)$. La constante du "O" ne dépend que de f. Ainsi on a la première majoration :

$$\Psi(\beta) = O(p^{2(\alpha-\beta)}).$$

Pour la deuxième majoration, lorsque β est petit inférieur à $\alpha/2$, on écrit :

$$\Psi(\beta) \le \sum_{\substack{0 \le u < p^\alpha \\ p^\beta \| (D(g_u), p^\alpha)}} \sigma_{g_u}(p^\alpha) + \sum_{\substack{0 \le v < p^\alpha \\ p^\beta \| (D(h_v), p^\alpha)}} \sigma_{h_v}(p^\alpha).$$

D'après les points (iii) et (iv) du lemme 1.2.4, on a $\sigma_{g_u}(p^\alpha) = O(p^{2\beta})$, la somme sur u est un $O(p^{\alpha-\beta+2\beta})$, celle sur v se majore de la même manière, et on a ainsi la majoration :

$$\Psi(\beta) \ll p^{\alpha+\beta}.$$

En comparant ces deux majorations, on trouve $\Psi(\beta) = O(p^{4\alpha/3})$, ce qui finit le preuve du point (ii) de la proposition 1.3.2.

A partir des lemmes 1.3.1 et 1.3.2 et de l'égalité (1.1), nous avons facilement le corollaire suivant

COROLLAIRE 1.3.4. *La fonction multiplicative r vérifie les propriétés :*

i) $r(p) = O(p)$,

ii) pour $P > 2$, *on a :*

$$\sum_{p \le P} \frac{r(p) \log p}{\varphi(p)^2} = \log P + O(1),$$

iii) pour $\alpha \ge 2$, *on a l'inégalité* $r(p^\alpha) = O(\alpha p^{4\alpha/3})$.

1.4. Étude du cas à 3 variables.

Dans ce paragraphe, f est un polynôme irréductible en 3 variables dont les coefficients sont premiers entre eux, et on rappelle que ρ est alors la fonction multiplicative définie par :

$$\rho(m) = |\{(u,v,w),\ 0 \leq u,v,w < m,\ f(u,v,w) \equiv 0 \mod m\}|$$

• Si f est un polynôme homogène, alors pour p un nombre premier, on a l'égalité

$$\rho(p) = \sigma(0,p) + (p-1)\sigma(1,p),$$

où $\sigma(k,p) = |\{0 \leq v,w < p,\ f(k,v,w) \equiv 0 \pmod p\}|$. En effet on a :

$$\rho(p) = \sum_{k=0}^{p-1} \sigma(k,p),$$

et pour $(k,p) = 1$, on a : $\sigma(k,p) = \sigma(1,p)$. Le polynôme $f(0,y,z)$ est homogène et d'après le lemme 1.2, on a : $\sigma(0,p) = O(p)$.

On applique ensuite le lemme 1.3.1 au polynôme $g(v,w) = f(1,v,w)$, pour obtenir, en reprenant les notations de ce lemme,

$$\rho(p) = s_p p^2 + O(p^{3/2}).$$

• Cas où f n'est pas un polynôme homogène.

Nous suivons la démarche de Greaves évoquée au paragraphe 1.3.
Si f est un polynôme absolument irréductible, alors Lang et Weil [L-W] ont montré que $\rho(p) = p^2 + O(p^{3/2})$, la constante sous-entendue dans le O, ne dépend que du degré de f.

Dans le cas plus général, on reprend les notations du paragraphe 1.3,
$f = g_1 ... g_m$ dans K, une extension algébrique de $\mathbf{Q}$, les g_i étant absolument irréductibles, et $\mathbf{Q}(\theta_1)$ est l'extension de $\mathbf{Q}$ engendrée par les coefficients de g_1. Le polynôme f étant irréductible, les facteurs g_i sont conjugués entre eux, et pour $i \neq 1$, on note θ_i l'image de θ_1 par l'automorphisme fixant $\mathbf{Q}$, et envoyant le polynôme g_1 sur g_i.
Soit Φ le polynôme minimal de θ_1, sur $\mathbf{Z}$. Soit f_p, la réduction de f sur $\mathbf{F}_p$. On suppose que cette réduction se factorise en

$$f_p = h_1 ... h_s,$$

et que celle de Φ s'écrit : $\Phi \equiv \Phi_1 ... \Phi_t \pmod p$, les h_i et les Φ_i étant irréductibles sur $\mathbf{F_p}$.

En reprenant la démonstration de Greaves [G3] et en l'adaptant à un polynôme en trois variables on montre le

LEMME 1.4.1. *Pour tout p sauf un nombre fini, le nombre de facteurs h_i absolument irréductibles est s_p le nombre de Φ_j linéaires.*

Le fait de travailler avec une variable supplémentaire n'entraîne pas de grosse modification dans la preuve de Greaves, mais on a préféré refaire ici la démonstration car certains arguments de la preuve seront repris dans la suite.

Preuve du lemme 1.4.1.
Soit O_K l'anneau des entiers de K, et pour p fixé, soit $\wp$ un idéal premier de O_K contenant p. On note $\mathbf{F}_\wp$ le corps résiduel correspondant, $\bar{f}$, $\bar{g}_1$, ...,$\bar{g}_m$, $\bar{\theta}_i$, les réductions respectives sur $\mathbf{F}_\wp$ de f, g_1, ..., g_m, et θ_i.
Les coefficients de g_1, et θ_1 peuvent s'exprimer les uns en fonction des autres à partir de polynômes à coefficients rationnels. Si p ne divise pas les dénominateurs de ces coefficients, alors les coefficients de $\bar{g}_1$ génèrent $\mathbf{F}_p[\bar{\theta}_1]$.
D'après le lemme B1, lorque p est assez grand, les $\bar{g}_1$,..., $\bar{g}_m$ sont irréductibles sur $\bar{\mathbf{F}}_p$.

Les polynômes $\bar{g}_i$ étant conjugués entre eux (car f est irréductible sur $\mathbf{Q}$), et l'homomorphisme envoyant $\bar{g}_i$ sur $\bar{g}_j$, envoie $\bar{\theta}_i$ sur $\bar{\theta}_j$, et vice versa, $h = \bar{g}_1...\bar{g}_s$ est un polynôme irréductible à coefficients dans $\mathbf{F}_p$, si et seulement si $(x-\bar{\theta}_1)...(x-\bar{\theta}_s)$ est irréductible à coefficients dans $\mathbf{F}_p$.

On a ainsi établi une correspondance entre les facteurs irréductibles h_i de f_p, et les facteurs Φ_j de Φ. Le lemme 1.4.1 est ainsi prouvé.

Lorsque $p \not| D$, D étant le discriminant de Φ, le nombre s_p est égal au nombre d'idéaux premiers P de l'anneau des entiers de $\mathbf{Q}(\theta_1)$, tels que $Norm(P) = p$, d'après un résultat de Dedekind ([A] chap. 11).

• Si h_i est absolument irréductible, alors comme on l'a dit plus haut, le nombre de solutions (u, v, w) tels que $f(u, v, w) \equiv 0 \mod p$ est $p^2 + O(p^{3/2})$.

• Si h_i n'est pas absolument irréductible, alors tous les zéros de h_i sont des points singuliers de la variété definie par h_i, car h_i dans une extension K_i de $\mathbf{F_p}$ se factorise en

$$h_i = \tilde{h}_{i,1}...\tilde{h}_{i,s}.$$

Si $h_i(u, v, w) \equiv 0 \pmod p$, alors, il existe j_0 tel que $\tilde{h}_{i,j_0}(u, v, w) \equiv 0 \pmod p$. Comme les $\tilde{h}_{i,l}$ sont conjugués, on en déduit que $\tilde{h}_{i,j}(u, v, w) \equiv 0 \pmod p$, pour tout $1 \leq j \leq s$. Les polynômes h_i sont irréductibles donc d'après le lemme B4, ils admettent seulement un $O(p)$ de points (u, v, w) singuliers, et ainsi, on a :

$$|\{(u, v, w) \mod p,\ h_i(u, v, w) \equiv 0 \pmod p\}| = O(p).$$

• Pour $i \neq j$, le nombre de solutions (u,v,w) des congruences
$h_i(u,v,w) \equiv h_j(u,v,w) \equiv 0 \pmod p$ est d'un ordre de grandeur inférieur à p. On peut en effet tout d'abord supposer que les polynômes sont absolument irréductibles.
D'après la correspondance établie au lemme 1.4.1 entre les facteurs h_k, et les Φ_k, si h_i et h_j ne sont pas premiers entre eux, alors les Φ_k ne le sont pas non plus et p divise alors le discriminant de Φ. Pour p assez grand les polynômes h_i et h_j sont donc premiers entre eux.
L'ensemble $E_{i,j} = \{(u,v,w) \in \mathbf{F}_p^3,\ h_i(u,v,w) \equiv h_j(u,v,w) \equiv 0 \pmod p\}$ est alors une variété de dimension au plus 1 et ainsi, d'après le lemme B3, on a $|E_{i,j}| \ll p$.

En assemblant toutes ces remarques et en appliquant le corollaire de Nagell [N1] du théorème des idéaux premiers évoqué au paragraphe 1.2, nous avons le lemme :

LEMME 1.4.2. *Les propriétés suivantes sont vérifiées :*

i) $\rho(p) = O(p^2)$, *la constante sous-jacente ne dépend que de* f,

ii) on a l'égalité pour $P \geq 2$:

$$\sum_{p<P} \frac{\rho(p)\log p}{p^3} = \log P + O(1).$$

Il reste encore à établir un résultat du type la proposition 1.3.2, valable pour un polynôme en trois variables. Comme au paragraphe 1.3, on a un résultat plus précis et plus facile à obtenir lorsque la surface projective Y associée à f définie par (F étant le polynôme homogène associé à f) :

$$Y = \{(x_1,x_2,x_3,t) \in \mathbf{P}^3_{\mathbf{Q}},\ F(x_1,x_2,x_3,t) = 0\},$$

est lisse.
Pour p premier, on note encore X_p la surface réduite associée à f définie par :

$$X_p = \{(x_1,x_2,x_3) \in \mathbf{F}_p^3,\ f(x_1,x_2,x_3) \equiv 0 \pmod p\}.$$

On montre la proposition suivante

PROPOSITION 1.4.3. *Les trois assertions suivantes sont vérifiées :*

i) $\rho(p^2) = O(p^4)$,

ii) si Y *est une lisse sur* $\mathbf{P}^3_{\mathbf{Q}}$, *alors pour tout* p, *sauf un nombre fini, et pour tout* $\alpha \geq 2$, *on a :* $\rho(p^\alpha) = p^2\rho(p^{\alpha-1})$,

et on a alors la majoration $\rho(p^\alpha) = O(p^{2\alpha})$.

iii) dans le cas général, on a : $\rho(p^\alpha) = O(\alpha^3 p^{18\alpha/7})$.

(Les constantes implicites ne dépendent que de f.*)*

L'estimation (iii) est vérifiée pour $\alpha = 2$, mais n'est pas assez fine pour les applications futures.
Nous commençons donc par prouver le point (i).
• Dans un premier temps, on suppose que f est irréductible sur $\mathbf{F}_p$. On écrit $u_1 = u + \lambda_1 p$, $v_1 = v + \lambda_2 p$ et $w_1 = w + \lambda_3 p$,
avec $0 \leq u, v, w, \lambda_1, \lambda_2, \lambda_3 < p$.
En remplaçant dans ρ, cela donne :

$$\rho(p^2) = \sum_{\substack{u,v,w \bmod p \\ f(u,v,w) \equiv 0 \pmod p}} |\{(\lambda_1, \lambda_2, \lambda_3) \bmod p,$$
$$f(u,v,w) + p\left(\lambda_1 \frac{\partial f}{\partial u}(u,v,w) + \lambda_2 \frac{\partial f}{\partial v}(u,v,w) + \lambda_3 \frac{\partial f}{\partial w}(u,v,w)\right) \equiv 0 \pmod{p^2}\}|.$$

Si (u, v, w) est un point singulier de X_p, alors la somme sur λ_1,λ_2, λ_3 vaut p^3, sinon elle vaut p^2.

On a donc la majoration :

$$\rho(p^2) \ll |S_p| p^3 + |X_p| p^2,$$

où S_p est l'ensemble des points singuliers de la surface X_p.
Comme f est irréductible sur $\mathbf{F}_p$, S_p est d'après le lemme B4 de l'annexe B, une variété de dimension inférieure à 1 et vérifie de plus : $|S_p| = O(p)$; en outre, d'après le lemme 1.4.2, $|X_p| = O(p^2)$. On a donc la majoration désirée : $\rho(p^2) = O(p^4)$.

• On ne suppose plus que f soit irréductible sur $\mathbf{F}_p$.
Dans ce cas, f se décompose dans $\mathbf{F}_p$ en

$$f \equiv f_1^{\alpha_1} \ldots . f_r^{\alpha_r} \pmod p,$$

où les f_i sont irréductibles.
Mais en revenant à la preuve du lemme 1.4.1 et à la définition du polynôme Φ, on vérifie avec la correspondance établie entre les facteurs irréductibles de $f \bmod p$, et ceux de $\Phi \bmod p$, que l'un des exposants α_i est supérieur à 2 seulement dans le cas où p divise D, le discriminant de Φ. On suppose alors que $p > D$, ainsi tous les α_i sont égaux à 1.

Soit (u, v, w) compté dans $\rho_f(p^2)$, alors, il existe $1 \leq i, j \leq r$
tels que $f_i(u,v,w) f_j(u,v,w) \equiv 0 \pmod{p^2}$, et $f_i(u,v,w) \equiv f_j(u,v,w) \equiv 0 \pmod p$.
Ceci revient à écrire la majoration :

$$\rho_f(p^2) \leq \sum_{1 \leq i \leq r} \rho_{f_i}(p^2) + \sum_{1 \leq i < j \leq r} \rho_{f_i}(p) \rho_{f_j}(p).$$

Les f_i étant irréductibles, on a $\rho_{f_i}(p^2) = O(p^4)$, et d'après le lemme 1.4.2,
$\rho_{f_i}(p) = O(p)$, on a donc $\rho_f(p^2) = O(p^4)$.

Ce type de raisonnement ne s'étend pas facilement à l'étude de $\rho(p^\alpha)$ dans le cas général, car u, v, w seraient donnés $\bmod p^{\alpha-1}$, mais il est valable dans le cas (ii).

Preuve de (ii). D'après le lemme B2, il existe P tel que pour $p > P$, la variété X_p soit lisse sur $\mathbf{F}_p$. En faisant les mêmes opérations que celles de la preuve de la proposition (i) du lemme 1.3.2, mais pour trois variables au lieu de deux, on montre que $\rho(p^\alpha) = p^2\rho(p^{\alpha-1})$, et ainsi que (ii) est vérifié pour $p > P$.

Preuve de (iii).
La preuve de ce point est dans le même esprit que celle de l'assertion (ii) de la proposition 1.3.2, et reprend d'ailleurs les résultats de ce lemme, mais hélas, le fait de travailler avec une variable supplémentaire alourdit sensiblement la démonstration de ce point.

On fixe deux variables, par exemple a et b, pour appliquer les résultats de Nagell énoncés au lemme 1.3.3 au polynôme $c \to g_{a,b}(c) = f(a,b,c)$, mais la difficulté est que le discriminant du polynôme $g_{a,b}$ dépend des variables a et b.
Pour $a, b \bmod p^\alpha$ on définit les polynômes $g_{a,b}$, $h_{a,b}$, $k_{a,b}$ par $g_{a,b}(t) = f(a,b,c)$, $h_{a,b}(t) = f(a,t,b)$, $k_{a,b}(t) = f(t,a,b)$. On définit encore $D(g_{a,b})$, $D(h_{a,b})$, $D(k_{a,b})$ les discriminants respectifs des polynômes $g_{a,b}$, $h_{a,b}$, $k_{a,b}$.
On découpe alors $\rho(p^\alpha)$ suivant la valuation p adique du pgcd des trois discriminants définis ci-dessus.
On part de l'écriture :

$$\rho(p^\alpha) = \sum_{0 \le \beta \le \alpha} \Psi_3(\beta),$$

avec

$$\Psi_3(\beta) = \sum_{\substack{u,v,w \bmod p^\alpha \\ f(u,v,w) \equiv 0 \bmod p^\alpha \\ p^\beta = (p^\alpha, D(g_{u,v}), D(h_{u,w}), D(k_{v,w}))}} 1.$$

On établit ensuite deux majorations pour $\Psi_3(\beta)$. La première, celle qui s'obtient le plus directement, est valable lorsque β est petit, inférieur à $\alpha/2$.
On utilise l'inégalité :

$$\Psi_3(\beta) \ll \sum_{\substack{0 \le u,v < p^\alpha \\ p^\beta \| D(g_{u,v})}} \sum_{\substack{0 \le w < p^\alpha \\ f(u,v,w) \equiv 0 \pmod{p^\alpha}}} 1.$$

D'après l'assertion (iii) du lemme 1.3.3, la somme sur w est $O(p^{2\beta})$, puis avec l'inégalité (ii) de la proposition 1.3.2, on montre que celle sur u et v, est un $O(p^{2(\alpha-\beta)+4\beta/3})$.
Ainsi on a comme première majoration :

$$\Psi_3(\beta) \ll p^{2\alpha+4\beta/3}. \tag{1.2}$$

Pour la deuxième majoration on ignore la condition $f(u,v,w) \equiv 0 \pmod{p^\alpha}$, pour se consacrer aux congruences $D(g_{u,v}) \equiv D(h_{u,w}) \equiv D(k_{v,w}) \equiv 0 \pmod{p^\beta}$ qui portent sur des polynômes en deux variables, et on fait quasiment les mêmes opérations que celles effectuées pour établir le point (ii) de la proposition 1.3.2.

Nous définissons alors les polynômes suivants : $D^{(1)}_{g,a}$ est le discriminant du polynôme $b \to D(g_{a,b})$, vu comme un polynôme à coefficients dans $\mathbf{Z}[a]$, $D^{(2)}_{g,b}$ est le discriminant de $a \to D(g_{a,b})$, vu comme un polynôme à coefficients dans $\mathbf{Z}[b]$, et on définit de la même manière les polynômes $D^{(1)}_{h,a}$, $D^{(2)}_{h,b}$, $D^{(1)}_{k,a}$, $D^{(2)}_{k,b}$.

Ensuite, pour $0 \leq \gamma \leq \beta$ on définit l'ensemble $C(\beta,\gamma)$, par :

$$C(\beta,\gamma) = \{(u,v,w) \mod p^\alpha, (u,v,w) \in C_1(\beta) \cap C_2(\beta,\gamma)\},$$

avec

$$C_1(\beta) = \{(u,v,w) \mod p^\alpha,\ p^\beta = (p^\alpha, D(g_{u,v}), D(h_{u,w}), D(k_{v,w}))\},$$

et,

$$C_2(\beta,\gamma) = \{(u,v,w) \mod p^\alpha,$$
$$p^\gamma = \left(p^\beta, D(D^{(1)}_{g,u}), D(D^{(2)}_{g,v}), D(D^{(1)}_{h,u}), D(D^{(2)}_{h,w}), D(D^{(1)}_{k,v}), D(D^{(2)}_{k,w})\right)\},$$

où comme au paragraphe 1.3, on a noté $D(P)$ le discriminant du polynôme P.

En utilisant toutes ces notations on écrit,

$$\Psi(\beta) \leq \sum_{0 \leq \gamma \leq \beta} |C(\beta,\gamma)|.$$

On établit deux estimations de $|C(\beta,\gamma)|$. Parmi les six discriminants intervenant dans $C_2(\beta,\gamma)$, il en existe au moins un, par exemple $D^{(1)}_{h,u}$, qui ne soit pas divisible par $p^{\gamma+1}$. Lorsque γ est petit, inférieur à $\beta/2$, on profite alors du fait que $|C(\beta,\gamma)|$ est majoré par un nombre fini de sommes du type :

$$\sum_{\substack{u,v \bmod p^\alpha \\ D(g_{u,v}) \equiv 0 \pmod{p^\beta} \\ (D^{(1)}_{h,u}, p^\beta) = p^\gamma}} \ \sum_{\substack{w \bmod p^\alpha \\ D(h_{u,w}) \equiv 0 \bmod p^\beta}} 1.$$

D'après l'assertion (iii) du lemme 1.3.3, la somme sur w est un $O(p^{(\alpha-\beta)+2\gamma})$, ensuite on majore la somme sur u et v par un $O(\beta p^{2(\alpha-\beta)+4\beta/3})$, grâce à la proposition 1.3.2.

Nous avons donc comme première majoration :

$$C(\beta,\gamma) = O(\beta p^{3(\alpha-\beta)+2\gamma+4\beta/3}). \tag{1.3}$$

Lorsque γ est grand, nous ne tenons compte que des conditions définissant $|C_2(\beta,\gamma)|$,

$$\begin{aligned} |C(\beta,\gamma)| &\ll |C_2(\beta,\gamma)| \\ &\ll \sum_{\substack{u,v,w \bmod p^\alpha \\ D^{(1)}_{g,u} \equiv D^{(2)}_{g,v} \equiv D^{(2)}_{h,w} \equiv 0 \pmod{p^\gamma}}} 1. \end{aligned}$$

Chacun des polynômes $D^{(1)}_{g,u}$, $D^{(2)}_{g,v}$, $D^{(2)}_{h,w}$ est un polynôme en une seule variable, dont les coefficients dépendent seulement des coefficients de f, et grâce au lemme 1.3.3, on a la majoration : $|C(\beta,\gamma)| \ll p^{3(\alpha-\gamma)}$.

Cette dernière majoration est plus précise que (1.3), pour $\gamma \geq \beta/3$, on a donc : $|C(\beta,\gamma)| \ll \beta^2 p^{3\alpha-\beta}$.

En comparant ceci avec (1.2), on a :

$$\Psi_3(\beta) \ll \min(\beta p^{(2\alpha+4\beta/3)}, \beta^2 p^{3\alpha-\beta}).$$

C'est à dire, $\Psi_3(\beta) \ll \alpha^2 p^{18\alpha/7}$. Cela fournit alors la majoration de $\rho(p^\alpha)$ annoncée pour $\alpha \geq 3$.

A partir de la proposition 1.4.3, on a directement le

COROLLAIRE 1.4.4. *Pour p premier, la fonction r vérifie les majorations :*

i) $r(p^2) = O(p^4)$

ii) pour $\alpha \geq 3$, $r(p^\alpha) = O(\alpha^3(p^{18\alpha/7}))$.

Chapitre 2
Quelques résultats sur les sommes d'exponentielles

Dans ce chapitre, on donne des estimations des sommes d'exponentielles qui interviennent lorsque l'on développe les conditions de congruences définissant les quantités $|\mathcal{A}_d|$ en série de Fourier.

2.1. Sommes d'exponentielles en deux variables.

Soit f un polynôme irréductible en deux variables. Soient $m \geq 1$ un entier sans facteur carré, et g, h deux autres entiers. Il s'agit alors d'étudier la somme

$$S_f(m,g,h) = \sum_{\substack{0\leq x,y<m \\ f(x,y)\equiv 0 \pmod m}} e\left(\frac{gx+hy}{m}\right).$$

On commence par observer le lemme suivant

LEMME 2.1.1. *Soient m et n deux entiers premiers entre eux. On a l'égalité :*

$$S_f(mn,g,h) = S_f(m,g\bar{n},h\bar{n})S_f(n,g\bar{m},h\bar{m}),$$

Preuve du lemme 2.1.1.
Pour $(x,y) \bmod mn$, en profitant du fait que $(m,n)=1$,
on écrit $x = mx_1 + nx_2$, et $y = my_1 + ny_2$.
La somme devient alors :

$$S_f(mn,g,h) = \sum_{\substack{0\leq x_1,y_1<n \\ 0\leq x_2,y_2<m \\ f(x_1m+x_2n,y_1m+y_2n)\equiv 0 \pmod{mn}}} e\left(\frac{gx_1+hy_1}{n}\right) e\left(\frac{gx_2+hy_2}{m}\right).$$

La condition $f(x_1m + x_2n, y_1m + y_2n) \equiv 0 \pmod{mn}$ se scinde en

$$\begin{cases} f(x_1m, y_1m) \equiv 0 \pmod n, \\ f(x_2n, y_2n) \equiv 0 \pmod m, \end{cases}$$

ce qui après le changement de variables adéquat, termine la preuve du lemme.

Grâce à ce lemme on peut se restreindre à étudier des sommes du type $S_f(p,g,h)$, p étant un nombre premier.

a) *On suppose que f est un polynôme homogène.*

La somme $S_f(p,g,h)$ peut se réécrire comme :

$$S_f(p,g,h) = \sum_{0 \leq k < p} e\left(\frac{k}{p}\right) w(k),$$

avec $w(k) = |\{(u,v),\ 0 \leq u,v < p, f(u,v) \equiv 0 \pmod p,\ gu + hv \equiv k \pmod p\}|$.

Grâce à l'homogénéité de f, on a l'égalité $w(k) = w(1)$, pour $(k,p) = 1$, et ainsi, on a $S_f(m,g,h) = w(0) - w(1)$. De plus, on a $w(1) = O(1)$, et $w(0) = O(p, f(-h,g))$. Les arguments que l'on vient de donner sont ceux mis au point par Greaves dans [G1] pour montrer le

LEMME 2.1.2. *Soit f un polynôme irréductible homogène. On a l'inégalité : $S_f(p,g,h) = O(p, f(-h,g))$. La constante implicite ne dépend que de f.*

b) *Cas des polynômes non homogènes.*

On suppose maintenant que f est un polynôme irréductible non homogène, vérifiant l'hypothèse (H2). La somme $S_f(p,g,h)$ ne s'évalue alors plus aussi facilement, mais à l'aide de résultats puissants de géométrie algébrique, on montre le

LEMME 2.1.3. *Soit f un polynôme irréductible, vérifiant la condition (H2). On a l'inégalité :*

$$S_f(p,g,h) = O(p^{1/2}(p,g,h)^{1/2}).$$

La constante sous-entendue ne dépend que de f.

Preuve du lemme 2.1.3.

Lorsque $p|(g,h)$, ce résultat est contenu dans le lemme 1.3.1. Dans la suite on suppose donc que $(p,g,h) = 1$.

On estime alors cette somme à l'aide d'un résultat de Bombieri [Bo], qui, en reprenant les travaux de Weil, a obtenu un résultat général sur les sommes d'expo nentielles le long d'une courbe.

On a la proposition suivante

PROPOSITION 2.1.4. *Soit X une courbe projective de degré d_1 définie sur $\mathbf{F}_p$, incluse dans $\mathbf{P}^2$, le plan projectif sur $\mathbf{F}_p$.*

Soit $R(x_1,x_2,x_3)$ une fraction rationnelle homogène de $\mathbf{P}^2$ à valeurs dans $\mathbf{F}_p$, et soit d_2, le degré de son numérateur.

On définit alors la somme

$$S(R,X) = \sum_{x \in X}^{*} e\left(\frac{R(x)}{p}\right),$$

où $*$ indique que les pôles de R sont exclus de la somme.

Soient $\Gamma_1, \Gamma_2, ..., \Gamma_s$, *les composantes absolument irréductibles de* X.

On suppose que la condition suivante est vérifiée :

(A) Pour toute fraction rationnelle homogène $h = h(x_1, x_2, x_3)$, *définie sur la clôture algébrique* $\bar{\mathbf{F}}_p$ *de* $\mathbf{F}_p$, *la fonction* $R - h^p + h$ *n'est pas identiquement nulle sur toute composante absolument irréductible* Γ_i *de* X.

On a alors :

$$|S(R, X)| \leq (d_1^2 + 2d_1d_2 - 3d_1)\sqrt{p} + d_1^2.$$

(En particulier, (A) est vérifiée quand $d_1d_2 < p$, *et* R *n'est pas constant sur chaque composante absolument irréductible* Γ_i *de* X.*)*

Cet énoncé est contenu dans le théorème 6 p. 97 de [Bo]. Ce dernier théorème est bien plus général que la version présentée ici, mais celle-ci est suffisante pour la preuve du lemme 2.1.3.

Soit $F(x, y, z)$, le polynôme homogène associé à f. La courbe X est alors celle définie par

$$X = \{(x_1, x_2, x_3) \in \mathbf{P}^2,\ F(x_1, x_2, x_3) \equiv 0 \pmod p\},$$

et en prenant comme application rationnelle R, celle qui à $x \in \mathbf{P}^2$, $x = (x_1, x_2, x_3)$, associe

$$R(x) = \frac{gx_1 + hx_2}{x_3}.$$

On a alors $S(R, X) = S_f(p, g, h)$, de plus la condition (A) est remplie lorsque f vérifie l'hypothèse (H1). L'inégalité annoncée au lemme 2.1.3 est donc vérifiée, d'après la proposition 2.1.4.

Grâce à ce lemme nous sommes en mesure de donner une majoration de la somme

$$\tilde{S}_f(p, g, h) = \sum_{\substack{0 < x_1, x_2 < p \\ f(x_1, x_2) \equiv 0 \pmod p}} e\left(\frac{gx_1 + hx_2}{p}\right).$$

On a le corollaire suivant

COROLLAIRE 2.1.5. *Soit* f *un polynôme irréductible, vérifiant l'hypothèse (H2). On a la majoration :*

$$\tilde{S}_f(p, g, h) = O(p^{1/2}(p, g, h)^{1/2}).$$

La constante du O *ne dépend que de* f.

Preuve du corollaire.
On part de l'égalité :

$$\tilde{S}_f(p,g,h) = S_f(p,g,h) - \sum_{\substack{0\le x_2<p \\ f(0,x_2)\equiv 0 \pmod p}} e\left(\frac{hx_2}{p}\right) - \sum_{\substack{0\le x_1<p \\ f(x_1,0)\equiv 0 \pmod p}} e\left(\frac{gx_1}{p}\right) + 1(0,0),$$

avec $1(0,0) = \begin{cases} 1 & \text{si } f(0,0) \equiv 0 \pmod p, \\ 0 & \text{sinon.} \end{cases}$

Lorsque p est assez grand, les polynômes $f(0,x_2)$, et $f(x_1,0)$ ne sont pas identiquement nuls sur $\mathbf{F}_p$, la deuxième et la troisième somme sont donc des $O(1)$. Le lemme 2.1.3 permet de conclure.

Lorsque le polynôme f est homogène, de la même manière, mais plus facilement on montre que $\tilde{S}_f(p,g,h) = O((p, f(-h,g))$.

2.2. Étude d'une somme d'exponentielles particulière.

Dans la suite du paragraphe 1.1 nous étudions les sommes définies par :

$$S_m(d,g,h) = \sum_{\substack{0\le u,v<d \\ au^2+bv^2+m\equiv 0 \pmod d}} e\left(\frac{gu+hv}{d}\right),$$

et,

$$\tilde{S}_m(d,g,h) = \sum_{\substack{0\le u,v<d \\ (uv,d)=1 \\ au^2+bv^2+m\equiv 0 \pmod d}} e\left(\frac{gu+hv}{d}\right),$$

où d, a, b, m sont des entiers tels que $(mab, d) = 1$. Pour alléger la notation, nous avons préféré ne pas faire apparaître a et b dans les désignations des sommes ci-dessus.
Dans cette partie, on ne suppose plus que d est sans facteur carré.
En appliquant le théorème chinois on montre les propriétés multiplicatives suivantes : pour $(d_1, d_2) = 1$, on a les égalités :

$$S_m(d_1d_2,g,h) = S_m(d_1, \bar{d}_2 g, \bar{d}_2 h) S_m(d_2, \bar{d}_1 g, \bar{d}_1 h),$$

et,

$$\tilde{S}_m(d_1d_2,g,h) = \tilde{S}_m(d_1, \bar{d}_2 g, \bar{d}_2 h) \tilde{S}_m(d_2, \bar{d}_1 g, \bar{d}_1 h).$$

Il suffit donc d'étudier des sommes su type $S_m(p^\alpha, g, h)$ et $\tilde{S}_m(p^\alpha, g, h)$, où p est un nombre premier.
Plaksin a établi le lemme ([Pl] lemme 18 p. 286)

LEMME 2.2.1. *Pour $\alpha \ge 1$, et $(m,p) = 1$, on a l'inégalité :*

$$S_m(p^\alpha, g, h) = O(p^{\alpha/2}(p^\alpha, g, h)^{1/2}).$$

Nous allons démontrer la même majoration pour la somme $\tilde{S}(p^\alpha, g, h)$, c'est à dire le lemme

LEMME 2.2.2. *Pour $\alpha \geq 1$, $p > 2$, et $(m,p) = 1$ on a la majoration :*

$$\tilde{S}_m(p^\alpha, g, h) = O(p^{\alpha/2}(p^\alpha, g, h)^{1/2}).$$

Preuve du lemme 2.2.2.

La preuve de ce lemme repend la démonstration de Plaksin (cf [Pl] p.286-289), qui consiste à développer les congruences sur u et v en sommes d'exponentielles, pour arriver à des sommes de Gauss et de Kloosterman. Le rajout de la condition $(uv, d) = 1$, rend cependant les calculs plus longs.

Le cas $\alpha = 1$, a déja été traité dans le paragraphe précédent. Dans la suite on suppose donc que $\alpha \geq 2$.

• On suppose que $p|(g,h)$.

On écrit alors $g = pg_1$, $h = ph_1$, $u = u_1 + \lambda p^{\alpha-1}$, et $v = v_1 + \mu p^{\alpha-1}$, avec $0 \leq u_1, v_1 < p^{\alpha-1}$, et $0 \leq \lambda, \mu < p$.

Notre somme devient alors :

$$\tilde{S}_m(p^\alpha, g, h) = \sum_{\substack{0<u_1,v_1<p^\alpha \\ (u_1v_1,p)=1 \\ au_1^2+bv_1^2+m\equiv 0 \pmod{p^{\alpha-1}}}} \sum_{\substack{0\leq\lambda,\mu<p \\ 2au_1\lambda+2bv_1\equiv 0 \pmod{p}}} e\left(\frac{g_1u_1 + h_1v_1}{p^{\alpha-1}}\right).$$

Donc si $p|(g,h)$, alors $\tilde{S}_m(p^\alpha, g_1, h_1) = p\tilde{S}_m(p^{\alpha-1}, g, h)$, et de proche en proche, si $p^t|(g,h)$, avec $t < \alpha$, alors, on a :

$$\tilde{S}_m(p^\alpha, g, h) = p^t\tilde{S}_m(p^{\alpha-t}, gp^{-t}, hp^{-t}).$$

• On suppose maintenant que $(g,h,p) = 1$ et $\alpha \geq 2$.

On part de l'égalité :

$$\tilde{S}_m(p^\alpha, g, h) = \frac{1}{p^\alpha}\sum_{k=0}^{p^\alpha-1} \sum_{\substack{u,v \bmod p^\alpha \\ (uv,p)=1}} e\left(\frac{k(au^2+bv^2+m)+gu+hv}{p^\alpha}\right).$$

On sépare alors ces sommes suivant le pgcd (k, p^α) :

$$\tilde{S}_m(p^\alpha, g, h) = \frac{1}{p^\alpha}\sum_{t=0}^{\alpha} \sum_{\substack{k=1 \\ (k,p)=1}}^{p^{\alpha-t}} e\left(\frac{km}{p^{\alpha-t}}\right)\Sigma_u(k,t,g)\Sigma_v(k,t,h), \tag{2.1}$$

avec

$$\Sigma_u(k,t,g) = \sum_{\substack{u \bmod p^\alpha \\ (u,p)=1}} e\left(\frac{akp^tu^2+gu}{p^\alpha}\right),$$

et $\Sigma_v(k,t,h))$ est définie similairement.

On a alors le

LEMME 2.2.3. *Pour $t < \alpha$, on a l'égalité :*

$$\Sigma_u(k,t,g) = \begin{cases} p^t \displaystyle\sum_{0<w<p^{\alpha-t}} e\left(\frac{akw^2}{p^{\alpha-t}} + \frac{gw}{p^\alpha}\right) & \text{si } p^t | g, \\ 0 & \text{sinon.} \end{cases}$$

Preuve du lemme 2.2.3.
On écrit $u = w + \lambda p^{\alpha-t}$, avec $0 < w < p^{\alpha-t}$, $(w,p) = 1$ et $0 \leq \lambda < p^t$.
La somme devient alors :

$$\sum_{\substack{0<w<p^{\alpha-t} \\ (w,p)=1}} e\left(\frac{akw^2}{p^{\alpha-t}} + \frac{gw}{p^\alpha}\right) \sum_{\lambda=0}^{p^t} e\left(\frac{g\lambda}{p^t}\right) = \begin{cases} p^t \displaystyle\sum_{\substack{0<w<p^{\alpha-t} \\ (w,p)=1}} e\left(\frac{amw^2}{p^{\alpha-t}} + \frac{gw}{p^\alpha}\right) & \text{si } p^t | g \\ 0 & \text{sinon.} \end{cases}$$

Suite de la preuve du lemme 2.2.2.
Comme $(p,g,h) = 1$, on peut supposer par exemple, que $(p,g) = 1$. On remarque que dans (2.1), seules les sommes correspondant à $t = 0$ et $t = \alpha$ peuvent ne pas être nulles. On a donc :

$$\tilde{S}_m(p^\alpha, g, h) = \frac{1}{p^\alpha} \sum_{\substack{0 \leq k < p^\alpha \\ (k,p)=1}} e\left(\frac{km}{p^\alpha}\right) \Sigma_u(k,0,g)\Sigma_v(k,0,h) + \frac{1}{p^\alpha} \sum_{\substack{u,v \bmod p^\alpha \\ (uv,p)=1}} e\left(\frac{gu+hv}{p^\alpha}\right).$$

La deuxième somme est un produit de deux sommes de Ramanujan, et comme $(g,p) = 1$, et $\alpha \geq 2$, cette somme est nulle car :

$$\sum_{\substack{u \bmod p^\alpha \\ (u,p)=1}} e\left(\frac{gu}{p^\alpha}\right) = \mu(p^\alpha) = 0.$$

Pour évaluer la première somme, on calcule précisément les quantités $\sum_v(k,0,h)$. On a le lemme

LEMME 2.2.4. *On a l'égalité :*

$$\Sigma_v(k,0,h) = \begin{cases} 0 & \text{si } p|h \text{ et } \alpha \geq 2, \\ \left(\frac{bk}{p^\alpha}\right) p^{\alpha/2} i^{\left(\frac{p^\alpha-1}{2}\right)^2} e\left(\frac{-\overline{4bk}h^2}{p^\alpha}\right) & \text{si } p \not| h, \text{ et } \alpha \geq 2, \\ \left(\frac{bk}{p}\right) \sqrt{p} i^{\left(\frac{p-1}{2}\right)^2} e\left(\frac{-\overline{4bk}h^2}{p}\right) - 1 & \text{si } \alpha = 1. \end{cases}$$

Preuve du lemme 2.2.4.
On reprend la formule :

$$\begin{aligned}\Sigma_v(k,0,h) &= \sum_{\substack{v \bmod p^\alpha \\ (v,p)=1}} e\left(\frac{bkv^2+hv}{p^\alpha}\right) \\ &= \sum_{v \bmod p^\alpha} e\left(\frac{bkv^2+hv}{p^\alpha}\right) - \sum_{\substack{v \bmod p^\alpha \\ p|v}} e\left(\frac{bkv^2+hv}{p^\alpha}\right) \\ &= \Sigma_1 - \Sigma_2.\end{aligned}$$

La somme Σ_1 se ramène à une somme de Gauss qui est estimée dans [Lan] :

$$\begin{aligned}\Sigma_1 &= \sum_{v \bmod p^\alpha} e\left(\frac{bk(v+\overline{2bk}h)^2}{p^\alpha}\right) e\left(\frac{-\overline{4bk}h^2}{p^\alpha}\right) \\ &= \left(\frac{bk}{p^\alpha}\right) p^{\alpha/2} i^{\left(\frac{p^\alpha-1}{2}\right)^2} e\left(\frac{-\overline{4bk}h^2}{p^\alpha}\right).\end{aligned}$$

Pour Σ_2, la technique est la même, mais le traitement est un peu plus long. On écrit pour $\alpha \geq 2$:

$$\begin{aligned}\Sigma_2 &= \sum_{v \bmod p^{\alpha-1}} e\left(\frac{bkp^2v^2+hpv}{p^\alpha}\right) \\ &= \sum_{v \bmod p^{\alpha-1}} e\left(\frac{bkpv^2+hv}{p^{\alpha-1}}\right).\end{aligned}$$

Si $\alpha = 2$, alors

$$\Sigma_2 = \begin{cases} p & \text{si } p|h, \\ 0 & \text{sinon.}\end{cases}$$

Pour $\alpha > 2$, on recommence, on écrit : $v = v_1 + \lambda p^{\alpha-2}$, avec $0 \leq \lambda < p$, $0 \leq v_1 < p^{\alpha-2}$, et ainsi on a l'égalité

$$\Sigma_2 = \sum_{v_1 \bmod p^{\alpha-2}} e\left(\frac{bkv_1^2}{p^{\alpha-2}} + \frac{hv_1}{p^{\alpha-1}}\right) \sum_{\lambda=0}^{p-1} e\left(\frac{\lambda h}{p}\right),$$

cette somme est alors nulle si $(p,h) = 1$.
Si $p|h$, i.e $h = ph_1$, elle vaut alors :

$$\begin{aligned}p \sum_{v \bmod p^{\alpha-2}} e\left(\frac{bkv_1^2+h_1v_1}{p^{\alpha-2}}\right) &= \left(\frac{bk}{p^{\alpha-2}}\right) p^{\alpha/2} i^{\left(\frac{p^{\alpha-2}-1}{2}\right)^2} e\left(\frac{-\overline{4bk}h_1^2}{p^{\alpha-2}}\right) \\ &= \Sigma_1,\end{aligned}$$

ce qui termine la preuve du lemme 2.2.4.

Avec ce dernier résultat nous sommes enfin en mesure d'achever la preuve du lemme 2.2.2.
Pour $\alpha \geq 2$, d'après les lemmes 2.2.3 et 2.2.4, on a :

$$\tilde{S}_m(p^\alpha, g, h) = \begin{cases} \left(\frac{ab}{p^\alpha}\right) \sum_{\substack{0<k<p^\alpha \\ (k,p)=1}} e\left(\frac{km - (\overline{4a}g^2 + \overline{4b}h^2)\bar{k}}{p^\alpha}\right) & \text{si } (p,h)=1, \\ 0 & \text{si } p|h, \end{cases}$$
$$= O(p^{\alpha/2}).$$

La preuve du lemme 2.2.2 est alors terminée.

2.3. Sommes d'exponentielles en trois variables.

Dans ce paragraphe, on établit des résultats analogues à ceux du paragraphe 2.1, mais concernant des sommes en trois variables. On considère un polynôme f, irréductible, en trois variables, vérifiant l'hypothèse (H4), et nous étudions :

$$S_f(m, h_1, h_2, h_3) = \sum_{\substack{0 \leq x_1, x_2, x_3 < m \\ f(x_1,x_2,x_3) \equiv 0 \pmod m}} e\left(\frac{h_1x_1 + h_2x_2 + h_3x_3}{m}\right),$$

où m est un entier sans facteur carré.

Comme au début du paragraphe 2.2, on commence par remarquer que pour $(m,n) = 1$, on a l'égalité :

$$S_f(mn, h_1, h_2, h_3) = S_f(m, h_1\bar{n}, h_2\bar{n}, h_3\bar{n}) S_f(n, h_1\bar{m}, h_2\bar{m}, h_3\bar{m}).$$

Il nous suffit donc d'étudier des sommes du type $S_f(p, h_1, h_2, h_3)$.
On a le résultat

LEMME 2.3.1. *On suppose que f est irréductible et vérifie l'hypothèse (H4); les sommes S_f vérifient alors l'inégalité :*

$$S_f(p, h_1, h_2, h_3) = O(p(p, h_1, h_2, h_3)),$$

où la constante sous-jacente ne dépend que de f.

Lorsque $h_1 \equiv h_2 \equiv h_3 \equiv 0 \pmod p$, on retrouve le lemme 1.3.2, sinon, ce résultat est un cas particulier du théorème 5 p.117 de Hooley [H3] obtenu à partir des travaux de Deligne dont on rappelle l'énoncé ci-dessous :

LEMME 2.3.2. *Soient f et g deux polynômes en trois variables vérifiant les conditions :*

Pour $t \in \mathbf{F_p}$, on note $W(t)$ la variété définie par :

$$W(t) = \{(x_1, x_2, x_3) \in \mathbf{F_p},\ f(x_1, x_2, x_3) \equiv 0 \,(\mathrm{mod}\, p),\ g(x_1, x_2, x_3) - t \equiv 0 \,(\mathrm{mod}\, p)\}.$$

On suppose que W vérifie les conditions :

i) Pour tout t sauf un nombre fini ne dépendant pas de p, $W(t)$ est une courbe absolument irréductible.

ii) $W(t)$ est une courbe (éventuellement réductible), ou la variété vide.

Alors, on a la majoration :

$$\sum_{\substack{x_1, x_2, x_3 \bmod p \\ f(x_1, x_2, x_3) \equiv 0 \ (\mathrm{mod}\, p)}} e\left(\frac{g(x_1, x_2, x_3)}{p}\right) \ll p,$$

où la constante ne dépend que des degrés de f et de g.

Lorsque $(p, h_1, h_2, h_3) = 1$ les conditions (i) et (ii) sont clairement vérifiées d'après (H4), et on a ainsi le lemme 2.3.1.
On a encore le

COROLLAIRE 2.3.3. *Soit $\tilde{S}_f(m, h_1, h_2, h_3)$ la somme définie par*

$$\tilde{S}_f(m, h_1, h_2, h_3) = \sum_{\substack{x_1, x_2, x_3 \ mod m \\ (m, x_1 x_2 x_3) = 1 \\ f(x_1, x_2, x_3) \equiv 0 \ (\mathrm{mod}\, m)}} e\left(\frac{h_1 x_1 + h_2 x_2 + h_3 x_3}{m}\right).$$

Pour m sans facteur carré, on a la majoration :

$$\tilde{S}_f(m, h_1, h_2, h_3) = O(m(m, h_1, h_2, h_3)).$$

Preuve du corollaire
On a l'égalité :

$$\tilde{S}_f(p, h_1, h_2, h_3) = S_f(p, h_1, h_2, h_3) - \sum_{\substack{x_1, x_2, x_3 \bmod p \\ x_1 x_2 x_3 \equiv 0 \ (\mathrm{mod}\, p) \\ f(x_1, x_2, x_3) \equiv 0 (\mathrm{mod}\, p)}} e\left(\frac{h_1 x_1 + h_2 x_2 + h_3 x_3}{p}\right).$$

La deuxième somme se décompose en un nombre fini de sommes des trois types suivants :

a) des sommes du type $S_g(p, h_2, h_3)$, où g est le polynôme défini par $g(x_2, x_3) = f(0, x_2, x_3)$,

b) des sommes en une variable comme $\displaystyle\sum_{\substack{0 \le x_3 < p \\ f(0,0,x_3) \equiv 0 \ (\mathrm{mod}\, p)}} e\left(\frac{h x_3}{p}\right)$.

c) ± 1 dans le cas où $f(0, 0, 0) \equiv 0 \,(\mathrm{mod}\, p)$.

Les termes du type b) et c) sont trivialement des $O(p)$.
Pour la somme du type a), lorsque p est assez grand, le polynôme g n'est pas identiquement nul sur $\mathbf{F}_p$, et on a l'inégalité triviale $|S_g(p, h_2, h_3)| \leq \rho_g(p)$. En transposant alors les résultats du lemme 1.3.1 à des polynômes non nécessairement irréductibles, on a facilement la majoration $\rho_g(p) = O(p)$, la constante ne dépendant que de g. On a donc bien $\tilde{S}_f(p, h_1, h_2, h_3) = O(p(p, h_1, h_2, h_3))$.

Chapitre 3
Préparations aux cribles

Dans cette partie, on obtient des estimations asymptotiques des quantités

$$(3.1) \qquad |\mathcal{A}_m| = |\{(n_1, n_2),\ x \leq n_1, n_2 \leq 2x, f(n_1, n_2) \equiv 0 \pmod m\}|,$$

pour $x \geq 1$ assez grand, et m sans facteur carré supérieur à $x^{1-\varepsilon}$, où ε est un réel positif minuscule, qui serviront à la preuve du théorème 5. (Ces ensembles $\mathcal{A}_m$ n'ont aucun rapport avec ceux présentés dans l'introduction).
Nous étudierons encore les ensembles

$$(3.2) \qquad \mathcal{A}_m(a) = \{(n_1, n_2) \in C(a, m),\ x \leq n_1, n_2 \leq 2x\},$$

où $C(a, m)$ est l'ensemble des conditions

$$\begin{cases} (n_1 n_2, m) = 1, \\ n_1 n_2 \equiv 0 \pmod a, \\ f(n_1, n_2) \equiv 0 \pmod m. \end{cases}$$

Pour démontrer le théorème 3 concernant un polynôme en trois variables, nous évaluerons ensuite le cardinal de l'ensemble

$$(3.3) \qquad \mathcal{B}_m(a) = \{(n_1, n_2, n_3) \in D(a, m),\ x \leq n_1, n_2, n_3 \leq 2x\},$$

où $D(a, m)$ est l'ensemble des conditions

$$\begin{cases} (n_1 n_2 n_3, m) = 1, \\ n_1 n_2 \equiv 0 \pmod a, \\ f(n_1, n_2, n_3) \equiv 0 \pmod m. \end{cases}$$

Les démonstrations des théorèmes 6 et 7 passent par l'étude des ensembles :

$$(3.4) \quad \mathcal{C}_m(a) = \{(n_1, n_2),\ n_1, n_2 \sim x,\ n_1 n_2 \equiv 0 \pmod a,\ f(n_1, n_2) \equiv 0 \pmod m\},$$

où a et m sont des entiers sans facteur carré, mais pas nécessairement premiers entre eux.

Pour obtenir ces estimations, on traduit en termes de sommes d'exponentielles, les systèmes de congruences définissant ces ensembles, pour arriver à des sommes du type celles étudiées dans les deux paragraphes précédents.

3.1.Estimation de $|\mathcal{A}_m|$.

Ce paragraphe est consacré à la démonstration du lemme

LEMME 3.1. *Soit f un polynôme irréductible en deux variables dont les coefficients sont premiers entre eux, et vérifiant l'hypothèse (H2). Pour m sans facteur carré, on a l'égalité :*

$$|\mathcal{A}_m| = \frac{x^2\rho(m)}{m^2} + R_m,$$

où pour tout $\varepsilon > 0$, le terme d'erreur R_m vérifie la majoration :

$$R_m = O\left(\frac{x^{1+\varepsilon}}{\sqrt{m}} + x^{\varepsilon}\sqrt{m}\right).$$

Preuve du lemme 3.1. En reprenant la définition (3.1), on a l'égalité :

$$|\mathcal{A}_m| = \sum_{\substack{u,v \bmod m \\ f(u,v)\equiv 0 \pmod m}} \sum_{\substack{n_1,n_2\sim x \\ n_1\equiv u \pmod m \\ n_2\equiv v \pmod m}} 1.$$

On développe ensuite les sommes sur n_1 et n_2 en sommes d'exponentielles :

$$|\mathcal{A}_m| = \frac{1}{m^2}\sum_{k,\ell=0}^{m-1}\sum_{n_1,n_2\sim x}\sum_{\substack{u,v \bmod m \\ f(u,v)\equiv 0 \pmod m}} e\left(\frac{k(u-n_1)+\ell(v-n_2)}{m}\right).$$

On réarrange alors cette somme en reprenant les notations des précédents paragraphes :

$$|\mathcal{A}_m| = \frac{1}{m^2}\sum_{k,\ell=0}^{m-1}\sum_{n_1,n_2\sim x} e\left(\frac{-kn_1-\ell n_2}{m}\right) S_f(m,k,\ell).$$

Le terme en $k=\ell=0$ fournit le terme principal, et les sommes sur x_1 et x_2 sont des séries géométriques qui se majorent facilement :

$$|\mathcal{A}_m| = x^2\frac{\rho(m)}{m^2} + O\left(\sum_{k=1}^{m/2}\frac{x}{mk}(|S_f(m,\pm k,0)|+|S_f(m,0,\pm k)|) + \sum_{0<k,\ell<m/2}\frac{|S_f(m,\pm k,\pm\ell)|}{k\ell}\right).$$

Le terme d'erreur se majore avec le lemme 2.1.2 :

$$|\mathcal{A}_m| = x^2\frac{\rho(m)}{m^2} + O\left(\frac{x}{\sqrt{m}}\sum_{0<k<m}\frac{(k,m)^{1/2}}{k} + \sum_{0<k,\ell<m}\frac{\sqrt{m}(m,k,\ell)^{1/2}}{k\ell}\right).$$

Etant donné que pour tout $\varepsilon > 0$, on a la majoration :

$$\sum_{0<k<m} \frac{(k,m)^{1/2}}{k} = O(x^{\varepsilon}),$$

on a le résultat annoncé.

3.2. Estimation de $|\mathcal{A}_m(a)|$

En suivant une démarche analogue à celle du paragraphe précédent nous montrons le

LEMME 3.2. *Soit f un polynôme irréductible en deux variables dont les coefficients sont premiers entre eux, et vérifiant l'hypothèse (H2). Soient a et m deux entiers sans facteur carré et premiers entre eux. Pour tout $\varepsilon > 0$, on a l'égalité :*

$$|\mathcal{A}_m(a)| = x^2 \frac{r(m)\lambda(a)}{m^2 a^2} + O\left(\frac{x^{1+\varepsilon}}{\sqrt{m}} + x^{\varepsilon}\sqrt{m}\right),$$

où λ est la fonction multiplicative définie par : $\lambda(p) = 2p - 1$.

Preuve du lemme 3.2.

D'après la définition de $|\mathcal{A}_m(a)|$ donnée dans (3.2), nous avons l'égalité :

$$|\mathcal{A}_m(a)| = \sum_{\substack{0\le u,v<am \\ (u,v)\in C(a,m)}} \sum_{\substack{n_1,n_2\sim x \\ n_1\equiv u \pmod{am} \\ n_2\equiv v \pmod{am}}} 1.$$

On développe ensuite les sommes sur n_1, n_2 en sommes d'exponentielles :

$$|\mathcal{A}_m(a)| = \frac{1}{a^2m^2} \sum_{0\le k,\ell<am} \sum_{n_1,n_2\sim x} e\left(\frac{-kn_1 - \ell n_2}{am}\right) \sum_{\substack{0\le u,v<am \\ (u,v)\in C(a,m)}} e\left(\frac{ku+\ell v}{am}\right).$$

Comme $(a,m) = 1$, en écrivant $u = au_1 + mu_2$, $v = av_1 + mv_2$, la somme sur u, v devient :

$$\sum_{\substack{u_2,v_2 \pmod a \\ u_2v_2\equiv 0 \pmod a}} e\left(\frac{ku_2+\ell v_2}{a}\right) \sum_{\substack{0<u_1,v_1<m \\ (u_1v_1,m)=1 \\ f(au_1,av_1)\equiv 0 \pmod m}} e\left(\frac{ku_1+\ell v_1}{m}\right).$$

La somme sur u_1 et v_1 correspond à la somme d'exponentielles $\tilde{S}_f(m, \bar{a}k, \bar{a}\ell)$ étudiée au chapitre 2.

On pose

$$\lambda(a,k,\ell) = \sum_{\substack{0\le u,v<a \\ uv\equiv 0 \pmod a}} e\left(\frac{ku+\ell v}{a}\right).$$

Cette fonction s'évalue facilement avec des méthodes élémentaires. Lorsque a est sans facteur carré, on montre le

LEMME 3.2.1. *La fonction $\lambda(a,k,\ell)$ est multiplicative par rapport à a, et vérifie pour $a = p$ premier :*

$$\lambda(p,k,\ell) = \begin{cases} -1 & \text{si } (p,k\ell) = 1, \\ \varphi(p) & \text{si } p|k\ell, \text{ mais } (p,k,\ell) = 1, \\ 2p-1 & \text{si } p|(k,\ell). \end{cases}$$

Preuve du lemme 3.2.1.
La multiplicativité se vérifie avec le théorème chinois. Pour $a = p$ premier, on a l'égalité :

$$\lambda(p,k,\ell) = \sum_{0\le u<p} e\left(\frac{ku}{p}\right) + \sum_{0\le v<p} e\left(\frac{\ell v}{p}\right) - 1,$$

ce qui correspond au résultat annoncé.
Dans toute la suite nous écrirons $\lambda(a)$ pour $\lambda(a,0,0)$

Retour à la preuve du lemme 3.2.
On isole le terme en $k = \ell = 0$:

$$\begin{aligned} |\mathcal{A}_m(a)| &= x^2 \frac{\lambda(a)r(m)}{a^2m^2} \\ &\quad + O\left(\sum_{1<k<am/2} \frac{x}{akm}(|\lambda(a,\pm k,0)||\tilde{S}_f(m,\pm k,0)| + |\lambda(a,0,\pm k)||\tilde{S}_f(m,0,\pm k)|)\right) \\ &\quad + O\left(\sum_{0<k,\ell<am/2} \frac{1}{k\ell}|\lambda(a,\pm k,\pm\ell)||\tilde{S}_f(m,\pm k,\pm\ell)|\right). \end{aligned} \tag{3.5}$$

D'après le lemme 3.2.1, on a la majoration $\lambda(a,k,\ell) = O((a,k\ell))$ tandis que le corollaire 2.1.5 fournit la majoration $\tilde{S}_f(m,k,\ell) = O(m^{1/2+\varepsilon}(m,k,\ell)^{1/2})$.
Le terme d'erreur de la formule (3.5) est donc majoré par

$$\frac{x^{1+\varepsilon}}{am} \sum_{0<k<am} \frac{a\sqrt{m(m,k)}}{k} + x^{\varepsilon} \sum_{0<k,\ell<am} \frac{(a,k\ell)}{k\ell}\sqrt{m(m,k,\ell)},$$

et une majoration directe de ces sommes donne le résultat annoncé dans le lemme 3.2.

Dans le cas particulier où f est le polynôme $f(n_1, n_2) = n_1^2+n_2^2+1$, la démonstration ci-dessus est valable pour tout entier m non nécessairement sans facteur carré. On utilise alors le lemme 2.2.2 pour estimer les sommes $\tilde{S}_f(m, k, \ell)$. Nous avons donc le lemme

LEMME 3.2.2. *Pour a sans facteur carré, et pour tout entier m tel que $(a, m) = 1$, dans le cas où f est le polynôme $f(n_1, n_2) = n_1^2 + n_2^2 + 1$, on a l'égalité :*

$$|\mathcal{A}_m(a)| = x^2 \frac{r(m)\lambda(a)}{a^2 m^2} + O(\frac{x^{1+\varepsilon}}{\sqrt{m}} + x^{\varepsilon}\sqrt{m}).$$

Lorsque f est un polynôme homogène, on majore les sommes $\tilde{S}_f(m, k, \ell)$ avec le lemme 2.1.2, ce qui donne $\tilde{S}_f(m, k, \ell) = O(x^{\varepsilon}((m, f(-\ell, k))$. Le terme d'erreur de (3.5) devient alors :

$$R_1(a,m) + R_2(a,m) = \frac{x^{1+\varepsilon}}{am} \sum_{0<k<am} \frac{a}{k}((m, f(-k,0) + (m, f(0,k))$$
$$+ x^{\varepsilon} \sum_{0<k,\ell<am} \frac{(a, k\ell)}{k\ell}(m, f(-\ell, k)).$$

Ces sommes s'évaluent plus facilement en moyenne sur m et sur a. On admet provisoirement que l'équation $f(n_1, n_2) = 0$ a pour seul couple solution sur $\mathbf{Z}^2$ $(0, 0)$. On a l'inégalité :

$$\sum_{\substack{0<m<M \\ 0<a<A}} R_2(a,m) \ll x^{\varepsilon} \sum_{0<k,\ell<AM} \sum_{\substack{0<m<M \\ 0<a<A \\ \max(k,\ell)<am}} \frac{(a, k\ell)(f(-\ell, k), m)}{k\ell}$$
$$\ll x^{\varepsilon} \sum_{0<k,\ell<AM} AM \frac{\tau(kl)\tau(f(-\ell, k))}{k\ell}$$
$$\ll AMx^{\varepsilon},$$

on a noté $\tau(n)$, le nombre de diviseurs de n.
De la même manière on montre l'inégalité :

$$\sum_{\substack{0<m<M \\ 0<a<A}} R_1(a,m) \ll x^{1+\varepsilon}A.$$

On ne peut en effet avoir $f(-\ell, k) = 0$, avec $(k, \ell) \neq 0$. Si par exemple $\ell \neq 0$, alors $f(-\ell, k) = (-\ell)^d f\left(1, \frac{-k}{\ell}\right)$, et si le polynôme $g(t) = f(1, t)$ a une racine rationnelle, il admet une factorisation sur $\mathbf{Q}[t]$ du type $g(t) = g_1(t)g_2(t)$. En notant alors d_i le degré de g_i, on a pour $x \neq 0$, l'écriture $f(x, y) = f_1(x, y)f_2(x, y)$, avec $f_i(x, y) = x^{d_i} g_i(y/x)$, ce qui contredit le fait que f soit irréductible.
Donc $f(-k, \ell)$ a comme seule solution $(0, 0)$ sur $\mathbf{Z}^2$.

On a ainsi le

LEMME 3.2.3. *Soit f un polynôme irréductible, homogène, dont les coefficients sont premiers entre eux. Pour tous entiers a et m sans facteur carré et premiers entre eux, on a l'égalité :*

$$|\mathcal{A}_m(a)| = x^2 \frac{r(m)\lambda(a)}{a^2 m^2} + R(a,m),$$

où le terme d'erreur $R(a,m)$ vérifie pour tout $\varepsilon > 0$ l'inégalité :

$$\sum_{\substack{0<a<A \\ 0<m<M \\ (a,m)=1}} |R(a,m)| \ll x^{1+\varepsilon} A + x^{\varepsilon} AM.$$

3.3. Estimation de $|\mathcal{C}_m(a)|$.

On estime ces quantités quasiment de la même manière que les $|\mathcal{A}_m(a)|$, seulement, il faut tenir compte des pgcd (a,m). On définit ainsi la fonction suivante :

$$\rho_0(d) = |\{(u,v),\ 0 \le u,v < d,\ uv \equiv 0 \pmod d,\ f(u,v) \equiv 0 \pmod d\}|.$$

Cette fonction est multiplicative, et on a l'égalité : $\rho_0(p) = \rho(p) - r(p)$.
On montre ici le lemme :

LEMME 3.3. *Soit f un polynôme irréductible en deux variables dont les coefficients sont premiers entre eux, et vérifiant la condition (H2). Soient a et m deux entiers sans facteur carré. Soit $\delta = (a,m)$. On écrit alors $a = a_1\delta$ et $m = m_1\delta$. Pour tout $\varepsilon > 0$ on a l'égalité :*

$$|\mathcal{C}_m(a)| = x^2 \frac{\rho(m_1)\lambda(a_1)\rho_0(\delta)}{a_1^2 m_1^2 \delta^2} + O\left(\frac{x^{1+\varepsilon}}{\delta\sqrt{m_1}} + x^{\varepsilon}\sqrt{m_1}\right).$$

Preuve du lemme 3.3
La seule différence par rapport à la preuve du lemme 3.2 est que la somme d'exponentielles à étudier est de la forme :

$$\Sigma(a_1, m_1, \delta, g, h) = \sum_{\substack{0 \le u,v < am \\ uv \equiv 0 \pmod a \\ f(u,v) \equiv 0 \pmod m}} e\left(\frac{gu+hv}{am}\right) = \sum_{\substack{0 \le u,v < a_1 m_1 \delta^2 \\ uv \equiv 0 \pmod{a_1\delta} \\ f(u,v) \equiv 0 \pmod{m_1\delta}}} e\left(\frac{gu+hv}{a_1 m_1 \delta^2}\right).$$

On commence par appliquer l'identité de Bezout pour séparer les conditions de congruence sur a_1, m_1, δ, ce qui donne l'égalité :

$$\Sigma(a_1, m_1, \delta, g, h) = \lambda(a_1, g, h) S_f(m_1, \overline{a_1\delta^2}g, \overline{a_1\delta^2}h) T_f(\delta, \overline{a_1 m_1}g, \overline{a_1 m_1}h),$$

avec

$$T_f(\delta, \overline{a_1 m_1}g, \overline{a_1 m_1}h) = \sum_{\substack{0 \le u,v < \delta^2 \\ f(u,v) \equiv 0 \pmod{\delta} \\ uv \equiv 0 \pmod{\delta}}} e\left(\frac{\overline{a_1 m_1}(gu + hv)}{\delta^2}\right).$$

En appliquant une seconde fois l'identité de Bezout, et en profitant du fait que δ soit un entier sans facteur carré, on a la formule

$$T_f(\delta, \overline{a_1 m_1}g, \overline{a_1 m_1}h) = \prod_{p \mid \delta} T_f(p, \overline{a_1 m_1 \hat{p}^2}g, \overline{a_1 m_1 \hat{p}^2}h),$$

avec la notation $\hat{p} = \delta/p$.

Il suffit donc d'étudier des sommes du type $T_f(p, g, h) = \sum_{\substack{0 \le u,v < p^2 \\ uv \equiv 0 \pmod{p} \\ f(u,v) \equiv 0 \pmod{p}}} e\left(\frac{gu + hv}{p^2}\right)$.

En écrivant $u = u_0 + \lambda p$, $v = v_0 + \mu p$, avec $0 \le u_0, v_0, \lambda, \mu < p$, on a l'égalité :

$$T_f(p, g, h) = \sum_{\substack{0 \le u_0, v_0 < p \\ u_0 v_0 \equiv 0 \pmod{p} \\ f(u_0, v_0) \equiv 0 \pmod{p}}} e\left(\frac{gu_0 + hv_0}{p^2}\right) \sum_{0 \le \lambda, \mu < p} e\left(\frac{g\lambda + h\mu}{p}\right)$$

$$= \begin{cases} p^2 \rho_0(p) & \text{si } g \equiv h \equiv 0 \pmod{p^2}, \\ O(p^2) & \text{si } g \equiv h \equiv 0 \pmod{p}, \\ 0 & \text{sinon.} \end{cases}$$

En utilisant ceci et en appliquant les lemmes 2.1.3 et 3.2.1, on a les inégalités :

$$\Sigma(a_1, m_1, \delta, g, h) = O((a_1, gh) m_1^{1/2+\varepsilon} (m_1, g, h)^{1/2} (\delta, g, h)^2),$$

et

$$\frac{\Sigma(a_1, m_1, \delta, 0, 0)}{a^2 m^2} = \frac{\lambda \rho(m_1) \rho_0(\delta)}{a_1^2 m_1^2 \delta^2}.$$

La preuve de ce lemme se termine alors exactement comme celle du lemme 3.2.

Lorsque f est un polynôme homogène, la somme critique correspondante est majorée par

$$\Sigma(a_1, m_1, \delta, g, h) = O((a_1, gh)(m_1, (f(-h, g))(\delta, g, h)^2),$$

et le raisonnement qui a servi pour le lemme 3.2.3, s'applique ici.

On a donc le lemme

LEMME 3.3.1. *Soit f un polynôme irréductible, homogène, dont les coefficients sont premiers entre eux. Soient a et m deux entiers sans facteur carré. On adopte l'écriture $a = a_1\delta$, $m = m_1\delta$, avec $(a_1, m_1) = 1$. On a alors l'égalité :*

$$|\mathcal{C}_m(a)| = x^2 \frac{\rho(m_1)\lambda(a_1)\rho_0(\delta)}{a_1^2 m_1^2 \delta^2} + R(a,m),$$

où le terme d'erreur $R(a,m)$ vérifie pour tout $\varepsilon > 0$ l'inégalité :

$$\sum_{\substack{0<a<A \\ 0<m<M}} |R(a,m)| \ll x^{1+\varepsilon}A + x^{\varepsilon}AM.$$

3.4. Estimation de $|\mathcal{B}_m(a)|$.

Maintenant, f est un polynôme en trois variables irréductible, dont les coefficients sont premiers entre eux, vérifiant l'hypothèse (H4), et nous nous occupons des ensembles $|\mathcal{B}_m(a)|$ définis dans (3.3).
On montre le lemme

LEMME 3.4. *Soient a et m deux entiers sans facteur carré et premiers entre eux. On a l'égalité :*

$$|\mathcal{B}_m(a)| = x^3 \frac{\lambda(a)r(m)}{a^2 m^3} + R_m(a).$$

Pour tout $\varepsilon > 0$, le terme d'erreur vérifie la majoration :

$$R_m(a) = O(x^{2+\varepsilon}m^{-1} + x^{1+\varepsilon} + x^{\varepsilon}m).$$

preuve du lemme 3.4.
Comme dans les paragraphes précédents nous partons de l'égalité :

$$|\mathcal{B}_m(a)| = \sum_{\substack{n_1,n_2,n_3 \sim x \\ (n_1,n_2,n_3)\in D(a,m)}} 1.$$

On développe ensuite ceci en sommes d'exponentielles puis en profitant du fait que $(a,m) = 1$ et en reprenant les notations du chapitre 2, nous avons l'égalité :

$$|\mathcal{B}_m(a)| = \frac{1}{a^2m^3} \sum_{0\le h_1,h_2<am} \sum_{0\le h_3<m} \sum_{n_1,n_2,n_3\sim x} e\left(\frac{-h_1n_1 - h_2n_2 - ah_3n_3}{am}\right)$$

$$\times \lambda(a,h_1,h_2)\tilde{S}_f(m, h_1\bar{a}, h_2\bar{a}, h_3), \tag{3.6}$$

Dans l'expression (3.6), on isole le terme principal donné par $h_1 = h_2 = h_3 = 0$:

$$|\mathcal{B}_m(a)| = x^3 \frac{r(m)\lambda(a)}{a^2 m^3}$$
$$+ O\left(\frac{x^2}{a^2m^2} \sum_{0<h<m/2} \frac{\lambda(a)}{h} |\tilde{S}_f(m,0,0,\pm h\bar{a})|\right)$$
$$+ O\left(\frac{x^2}{am^2} \sum_{0<h<am/2} \frac{|\lambda(a,\pm h,0)|}{h} [|\tilde{S}_f(m,\pm h\bar{a},0,0)| + |\tilde{S}_f(m,0,\pm h\bar{a},0)|]\right)$$
$$+ O\left(\frac{x}{am} \sum_{\substack{0<h_1<am/2 \\ 0<h_2<m/2}} \frac{|\lambda(a,\pm h_1,0)|}{h_1 h_2} [|\tilde{S}_f(m,\pm h_1\bar{a},0,\pm h_2)| + |\tilde{S}_f(m,0,\pm h_1\bar{a},\pm h_2)|]\right)$$
$$+ O\left(\frac{x}{m} \sum_{0<h_1,h_2<am/2} |\frac{\lambda(a,\pm h_1,\pm h_2)|}{h_1 h_2} |\tilde{S}_f(m,\pm h_1\bar{a},\pm h_2\bar{a},0)|\right)$$
$$+ O\left(\sum_{\substack{0<h_1,h_2<am/2 \\ 0<h_3<m/2}} \frac{|\lambda(a,\pm h_1,\pm h_2)|}{h_1 h_2 h_3} |\tilde{S}_f(m,\pm h_1\bar{a},\pm h_2\bar{a},\pm h_3)|\right).$$

Nous appliquons alors le lemme 3.2.1 et le corollaire 2.3.3 pour majorer les différents termes d'erreur.
Les deux premières lignes de termes d'erreur sont majorées par :

$$\frac{x^2}{a^2m^2} \sum_{0<h<am/2} \frac{a}{h} m(m,h) + \frac{x^2}{am^2} \sum_{0<h<am} \frac{am(m,h)}{h}$$
$$\ll \frac{x^{2+\varepsilon}}{m}.$$

Les troisièmes et quatrièmes lignes de terme d'erreur sont inférieures à :

$$\frac{x}{am} \sum_{\substack{0<h_1<am \\ 0<h_2<m}} \frac{am(m,h_1,h_2)}{h_1 h_2} \ll \frac{x}{m} \sum_{0<h_1,h_2<am} \frac{(a,h_1h_2))}{h_1 h_2} m(m,h_1,h_2) \ll \frac{x^{1+\varepsilon}}{m}.$$

Enfin le dernier terme d'erreur est majoré par :

$$\sum_{\substack{0<h_1,h_2<am \\ 0<h_3<m}} (a,h_1h_2h_3) \frac{m(m,h_1,h_2,h_3)}{h_1h_2h_3} \ll x^\varepsilon m.$$

Dans toutes ces dernières majorations, ε est bien entendu un réel positif aussi petit que l'on veut. Tout ceci finit alors la preuve du lemme 3.4.

Chapitre 4
Théorèmes de valeur moyenne sur des progressions arithmétiques simultanées

4.1. Cas des polynômes en deux variables.

Dans ce paragraphe, f est un polynôme irréductible, non nécessairement homogène. Soit $\mathcal{E}$ la collection d'entiers contenant d'éventuelles répétitions définie par

$$\mathcal{E} = \{f(p_1, p_2), p_1, p_2 \sim x\}.$$

Pour $m \geq 2$ on note $\mathcal{E}_m$ les ensembles $\mathcal{E}_m = \{a \in \mathcal{E},\ a \equiv 0 \pmod m\}$.
A partir du théorème de Barban-Davenport-Halberstam, on montre ici le

LEMME 4.1. *i) Pour $x \geq 2$, et pour tout $\varepsilon > 0$, on a l'inégalité :*

$$\sum_{\substack{m<x^{1-\epsilon} \\ \mu^2(m)=1}} \left| |\mathcal{E}_m| - \frac{r(m)}{\varphi(m)^2}|\mathcal{E}| \right| \ll_\varepsilon \frac{x^2}{(\log x)^{10}}.$$

ii) Lorsque le polynôme homogène F associé à f (dans le cas où f n'est pas un polynôme homogène) est lisse sur $\mathbf{P}^2_{\mathbf{Q}}$, il existe un ensemble fini de nombres premiers P_f, tel que pour $x \geq 2$, pour tout $\varepsilon > 0$, on ait l'inégalité :

$$\sum_{\substack{m<x^{1-\epsilon} \\ p|m \Rightarrow p \notin P_f}} \left| |\mathcal{E}_m| - \frac{r(m)}{\varphi(m)^2}|\mathcal{E}| \right| \ll_\varepsilon \frac{x^2}{(\log x)^{10}}.$$

Le point (i) a déja été démontré par Greaves dans [G3], mais on a préféré réécrire la démonstration pour alors en déduire facilement le point (ii).
Ce lemme n'apparaît pas sous une forme optimale, on pourrait par exemple étendre la somme sur m à $m < x(\log x)^{-A}$, avec $A > 0$ assez grand, mais la version donnée ici sera suffisante pour la suite. Pour démontrer le théorème 2 énoncé dans l'introduction, on utilise seulement la condition m est un nombre premier inférieur à $x^{1-\epsilon}$, la condition plus génerale $\mu^2(m) = 1$ sert aux preuves des théorèmes 6 et 7. Le point (ii) sert à la preuve du théorème 4 concernant le polynômes $x^2 + y^2 + 1$.

Preuve du lemme 4.1.
On commence par montrer l'assertion (i), puis on en déduira (ii).
On met tout d'abord de coté les entiers m ayant un grand nombre de facteurs premiers distincts, c'est à dire les entiers m tels que $\omega(m) \geq 20 \log\log x$.

Greaves a montré dans [G3], relation (7), l'inégalité :

$$(4.1) \qquad \sum_{\substack{m\le x^{1-\epsilon}\\ \omega(m)\ge 20\log\log x}} \mu^2(m)\left||\mathcal{E}_m| - \frac{r(m)}{\varphi(m)^2}|\mathcal{E}|\right| \ll \frac{x^2}{(\log x)^{20\log 2-6}}.$$

Pour m tel que $\omega(m) < 20\log\log x$, on réécrit les quantités $|\mathcal{E}_m| - \frac{r(m)}{\varphi(m)^2}|\mathcal{E}|$ sous la forme :

$$|\mathcal{E}_m| - \frac{r(m)}{\varphi(m)^2}|\mathcal{E}| = \sum_{\substack{0\le u,v<m\\ (uv,m)=1\\ f(u,v)\equiv 0 \pmod m}} \Big(\sum_{\substack{p_1\sim x\\ p_1\equiv u \pmod m}} \sum_{\substack{p_2\sim x\\ p_2\equiv v \pmod m}} 1 - \frac{1}{\varphi(m)^2} \sum_{p_1,p_2\sim x} 1\Big).$$

On a rajouté la condition $(uv, m) = 1$, car p_1 et p_2 sont des nombres premiers tels que $m < x^{1-\epsilon} < x \le \min(p_1, p_2)$. Cette condition est nécessaire pour appliquer les résultats sur les progressions arithmétiques.
A partir de ceci, on applique l'inégalité triangulaire pour obtenir l'écriture :

$$\left||\mathcal{E}_m| - \frac{r(m)}{\varphi(m)^2}|\mathcal{E}|\right| \le \sum_{\substack{0\le u,v<m\\ (uv,m)=1\\ f(u,v)\equiv 0 \pmod m}} \left| \sum_{\substack{p_1\sim x\\ p_1\equiv u \pmod m}} \sum_{\substack{p_2\sim x\\ p_2\equiv v \pmod m}} 1 - \frac{1}{\varphi(m)} \sum_{p_2\sim x} 1 \right|$$

$$+ \sum_{\substack{0\le u,v<m\\ (uv,m)=1\\ f(u,v)\equiv 0 \pmod m}} \frac{1}{\varphi(m)} \sum_{p_2\sim x} \left| \sum_{\substack{p_1\sim x\\ p_1\equiv u \pmod m}} 1 - \frac{1}{\varphi(m)} \sum_{p_1\sim x} 1 \right|.$$

Etant donné l'inégalité $\sum_{\substack{p_1\sim x\\ p_1\equiv v \pmod m}} 1 = O\left(\frac{x}{m}\right)$, on est amené à majorer deux sommes du type :
(4.2)

$$S = \sum_{\substack{m<x^{1-\epsilon}\\ \omega(m)<20\log\log x}} \frac{x}{\varphi(m)}\mu^2(m) \sum_{\substack{0\le u<m\\ (u,m)=1}} \sigma_{f_u}(m) \left| \sum_{\substack{p_1\sim x\\ p_1\equiv u \pmod m}} 1 - \frac{1}{\varphi(m)} \sum_{p_1\sim x} 1 \right|,$$

avec,

$$\sigma_{f_u}(m) = \sum_{\substack{0\le v<m\\ (v,m)=1\\ f(u,v)\equiv 0 \pmod m}} 1.$$

Comme Greaves [G3] l'a expliqué, en écrivant f sous la forme

$$f(u,v) = \sum_{0\le i\le d} g_i(u)v^i = f_u(v),$$

le polynôme f_u est identiquement nul si et seulement si $g_i(u) \equiv 0 \pmod p$ pour tout $0 \le i \le d$, ceci ne peut être vérifié que par un nombre fini de p car f est un polynôme irréductible sur $\mathbf{Z}$.
Pour prouver ceci, on raisonne avec des résultants. Certains g_i peuvent être identiquement nuls, et on préfère réécrire le polynôme f sous la forme :

$$f(u,v) = \sum_{0\le k\le \kappa} g_{i_k}(u)v^{i_k},$$

où $\{i_k,\ 0 \le k \le \kappa\} = \{0 \le j \le d,\ g_j \ne 0\}$.
On considère alors le système de résultants suivants :
on prend $P_0 = (g_{i_0}, g_{i_1})$, le résultant R_0 des polynômes $g_{i_0}P_0^{-1}$ et $g_{i_1}P_0^{-1}$ est alors un entier non nul.
On définit ensuite par récurrence pour $0 < k < \kappa$,
le polynôme $P_{i_k} = (P_{i_{k-1}}, g_{i_k})$, puis R_{i_k} le résultant de $P_{i_{k-1}}P_{i_k}^{-1}$, et $g_{i_{k+1}}P_{i_k}^{-1}$, ainsi, $R_{i_k} \in \mathbf{Z}^*$. On a alors $P_{i_{\kappa-1}} | (g_{i_0}, \dots, g_{i_{\kappa-1}})$, mais le polynôme f étant irréductible, le résultant R_{i_κ} des polynômes $P_{i_{\kappa-1}}$ et g_{i_κ} est un entier non nul.
Pour $p > R = \max\limits_{0\le k\le\kappa} |R_{i_k}|$, les polynômes g_{i_0}, g_{i_1},..,g_{i_κ} n'ont pas de racine commune dans $\bar{\mathbf{F}}_p$.
On en déduit que pour u fixé, on a l'inégalité :

$$\sigma_{f_u}(m) \ll_R d^{\omega(m)} \ll (\log x)^{20\log d},$$

lorsque $m < x$, et $\omega(m) < 20\log\log x$.
En tenant compte de ceci, on applique l'inégalité de Cauchy-Schwarz dans l'expression de S de la ligne (4.2) :

$$S \ll x \left\{ \sum_{\substack{m<x^{1-\epsilon}\\ \omega(m)<20\log\log x}} \mu^2(m) \sum_{\substack{0<u<m\\(u,m)=1}} \left| \sum_{\substack{p_1\sim x\\ p_1\equiv u \pmod m}} 1 - \frac{1}{\varphi(m)} \sum_{p_1\sim x} 1 \right|^2 \right\}^{1/2}$$
$$\times \left\{ \sum_{\substack{m<x^{1-\epsilon}\\ \omega(m)<20\log\log x}} \mu^2(m) \sum_{\substack{0<u<m\\(u,m)=1}} \left(\frac{\sigma_{f_u}(m)}{\varphi(m)}\right)^2 \right\}^{1/2}.$$

La deuxième accolade est majorée trivialement par un $O((\log x)^{20\log d+1})$, grâce aux discussions sur les congruences que l'on vient de faire,
tandis que la première est majorée par $\dfrac{x}{(\log x)^{101+20\log d}}$,
d'après le théorème de Barban-Davenport-Halberstam.
On a ainsi la majoration $S \ll \dfrac{x^2}{(\log x)^{100}}$, ce qui finit la preuve du point (i).

Preuve du point (ii).
La condition $\mu^2(m) = 1$ dans la preuve de l'assertion (i) a servi à majorer uniformément sur $u \bmod m$, et sur m, les quantités $\sigma_{f_u}(m)$ et à établir l'égalité (4.1). D'après le lemme B2, si le polynôme homogène F associé à f est lisse sur $\mathbf{P}^2_{\mathbf{Q}}$, alors pour tout p sauf un nombre fini, f_p, la réduction de f est lisse sur $\mathbf{F}_p$. Il existe alors P_f tel que pour $p > P_f$, on ait : $\sigma_{f_u}(p^\alpha) \leq \deg f_u \leq \deg f$, pour tous p, α et $u \bmod p^\alpha$ et tel qu'on ait aussi $r(p^\alpha) = p^{\alpha-1} r(p)$, et ainsi tous les arguments de la preuve sont valables pour ce polynôme.

Plus particulièrement, si $f(x,y) = x^2 + y^2 + 1$ on peut choisir $P_f = \emptyset$.

4.2. Progressions sur trois variables.

On suppose que f est un polynôme irréductible en trois variables et tel que $f(x,y,0)$ ne soit pas identiquement nul sur $\mathbf{C}$ (cette condition est contenue dans l'hypothèse (H4)). Soit $\mathcal{G}$ la collection d'entiers contenant d'éventuelles répétitions, définie par

$$\mathcal{G} = \{f(p_1, p_2, n_3),\ p_1, p_2, n_3 \sim x\}.$$

Pour tout entier $m \geq 2$, on note $\mathcal{G}_m = \{a \in \mathcal{G},\ a \equiv 0 \pmod m\}$.

Le rajout d'une troisième variable parcourant la suite des entiers, permet d'obtenir facilement un résultat en moyenne, c'est le

LEMME 4.2. *Pour $x \geq 2$, et pour tout $\varepsilon > 0$, on a l'inégalité :*

$$\sum_{p < x^{1-\varepsilon}} \log p \left| |\mathcal{G}_p| - \frac{r(p)}{\varphi(p)^3} |\mathcal{G}| \right| \ll_\varepsilon x^{3-\varepsilon/2}.$$

On a préféré donner un résultat juste suffisant pour la preuve du théorème 3 plutot qu'une version plus générale, mais plus longue à démontrer.

Preuve du lemme 4.2.
En appliquant l'inégalité triangulaire de la même façon qu'au début de la preuve du lemme 4.1, on est amené à estimer des sommes du type :
(4.3)

$$\sum_{p < x^{1-\varepsilon}} \log p \sum_{\substack{0 \leq u,v,w < p \\ f(u,v,w) \equiv 0 \pmod p}} \sum_{\substack{p_1 \sim x \\ p_1 \equiv u \pmod p}} \sum_{\substack{p_2 \sim x \\ p_2 \equiv v \pmod p}} \left| \sum_{\substack{n_3 \sim x \\ n_3 \equiv w \pmod p}} 1 - \frac{1}{\varphi(p)} \sum_{n_3 \sim x} 1 \right|.$$

Le terme entre $|\ |$ est un $O(x^{\varepsilon/2})$, et les sommes sur p_1 et p_2 sont trivialement des $O(xp^{-1})$.

Le terme (4.3) est alors majoré par :

$$O\left(x^{\varepsilon/2} \sum_{p < x^{1-\varepsilon}} p^2 \left(\frac{x}{p}\right)^2 \log p \right) = O(x^{3-\varepsilon/3}).$$

Le lemme 4.2 est donc prouvé.

Chapitre 5

Étude du plus grand facteur premier de polynômes en deux variables, de degré deux ou trois, pris en des valeurs premières

Cette partie est consacrée à la preuve du théorème 2.
Soit f un polynôme irréductible non homogène dont les coefficients sont premiers entre eux, et vérifiant les hypothèses (H1) et (H2). Dans le dernier paragraphe de ce chapitre, on traitera le cas où f est un polynôme homogène.

La preuve du théorème 2 reprend la méthode de Tchebychev-Hooley développée dans la première partie de la thèse lors de l'étude du plus grand facteur premier de $\tilde{n}^2+1$.
Elle consiste à estimer de deux manières différentes (dont l'une dépendra de $P^+(f(p_1,p_2))$, le produit

$$V(x)=\prod_{\substack{p_1\sim x\\ p_2\sim x}} f(p_1,p_2).$$

La première façon est directe, on calcule :

$$\log V(x)=\sum_{p_1,p_2\sim x}\log f(p_1,p_2).$$

On note d le degré de f. D'après la condition (H1), on a pour $p_1,p_2\sim x$ l'égalité $\log f(p_1,p_2)=d\log x+O(1)$. En appliquant le théorème des nombres premiers on obtient l'estimation suivante :

$$\log V(x)=\frac{dx^2}{\log x}+O\left(\frac{x^2}{(\log x)^2}\right). \tag{5.1}$$

Par ailleurs, on a encore :

$$\log V(x)=\sum_{\substack{p,\alpha\\ p^\alpha\ll x^d}}\log p|\mathcal{E}_{p^\alpha}|,$$

avec

$$\mathcal{E}_{p^\alpha}=\{(p_1,p_2),\ p_1,p_2\sim x,\ f(p_1,p_2)\equiv 0\ (\mathrm{mod}\,p^\alpha)\}.$$

Pour $\varepsilon>0$, on procède alors au découpage suivant :

$$\begin{aligned}\log V(x)&=\sum_{p^\alpha<x^{1-\varepsilon}}\log p|\mathcal{E}_{p^\alpha}|+\sum_{\substack{\alpha\geq 2\\ p^\alpha\geq x^{1-\varepsilon}}}\log p|\mathcal{E}_{p^\alpha}|+\sum_{x^{1-\varepsilon}\leq p<P}\log p|\mathcal{E}_p|\\ &=S_1+S_2+S_3,\end{aligned}$$

par définition. On a noté P le plus grand facteur premier du produit $V(x)$.

5.1. Évaluation de S_1.

On part de l'écriture :

$$\begin{aligned} S_1 &= \sum_{p<x^{1-\epsilon}} \log p|\mathcal{E}_p| + \sum_{p^\alpha<x^{1-\epsilon},\ \alpha\geq 2} \log p|\mathcal{E}_{p^\alpha}| \\ &= S_1' + S_1'', \end{aligned}$$

par définition. La somme S_1' fournit le terme principal. Elle est estimée avec l'assertion (i) du lemme 4.1.
Grâce à ce lemme, on a l'égalité :

$$S_1' = \frac{x^2}{(\log x)^2} \sum_{p<x^{1-\epsilon}} \log p \frac{r(p)}{\varphi(p)^2} + O\left(\frac{x^2}{(\log x)^2}\right).$$

D'après le point (ii) du corollaire 1.3.4, on a l'estimation :

$$S_1' = (1-\varepsilon)\frac{x^2}{\log x} + O\left(\frac{x^2}{(\log x)^2}\right).$$

La somme S_1'' est, par contre, négligeable. En effet, d'après le théorème de Brun-Titchmarsh, pour $p^\alpha < x^{1-\epsilon}$, on a l'inégalité :

$$|\mathcal{E}_{p^\alpha}| \ll \left(\frac{x}{\varphi(p^\alpha)\log x}\right)^2 r(p^\alpha).$$

De plus, d'après le corollaire 1.3.4, on a $r(p^\alpha) = O(\alpha p^{4\alpha/3})$, ce qui permet d'écrire l'inégalité :

$$S_1'' \ll \frac{x^2}{\log^2 x} \sum_{\substack{p^\alpha<x^{1-\epsilon} \\ \alpha\geq 2}} \frac{\alpha \log p}{p^{2\alpha/3}} \ll \frac{x^2}{\log^2 x}.$$

Ainsi, on vient d'établir le lemme

LEMME 5.1. *On a l'égalité :*

$$S_1 = (1-\varepsilon)\frac{x^2}{(\log x)} + O\left(\frac{x^2}{(\log x)^2}\right).$$

5.2. Majoration de S_2 dans le cas où f est un polynôme de degré deux.

Lorsque f est un polynôme de degré deux, la somme S_2 s'évalue directement, à partir de la majoration :

$$S_2 \ll \sum_{\substack{\alpha\geq 2 \\ p^\alpha\geq x^{1-\epsilon}}} \sum_{\substack{m\sim x^2 \\ m\equiv 0 \pmod{p^\alpha}}} v_f(m),$$

où $v_f(m)$ est le nombre de solutions entières (a,b) à l'équation $m = f(a,b)$. Dans cette dernière ligne, la notation $m \sim x^2$ signifie qu'il existe deux entiers A_1 et A_2 tels que $A_1 x^2 \leq m \leq A_2 x^2$.

On montre ensuite que pour tout $\eta > 0$, on a $v_f(n) = O(n^\eta)$.
Comme f vérifie les hypothèses (H1) de positivité et (H2) de non dégénérescence, on a l'écriture :

$$Mf(x,y) = A(ax+by+c)^2 + B(dy+e)^2 + C,$$

avec $a,b,c,d,e,A,B,C,M \in \mathbf{Z}$, et les entiers M,A,B sont strictement positifs.
Il s'agit alors de montrer que l'on a uniformément pour tout n l'inégalité :

$$|\{(x,y) \in \mathbf{Z}^2,\ n = Ax^2 + By^2\}| = O(n^\varepsilon).$$

Or ce cardinal est inférieur à $2|\{0 \leq v < n,\ v^2 + AB \equiv 0 \pmod n\}|$ (c.f par exemple [Sm] Art 86 p. 172), on a donc bien l'inégalité annoncée.

Ceci donne la majoration :

$$\begin{aligned} S_2 &\ll x^{2+\eta} \sum_{\substack{\alpha \geq 2 \\ p^\alpha > x^{1-\varepsilon}}} \frac{1}{p^\alpha} \\ &\ll x^{1,9}. \end{aligned} \tag{5.2}$$

Lorsque f est un polynôme du troisième degré, la somme S_2 est bien plus difficile à estimer. On évalue séparément les $f(p_1,p_2)$ ayant un gros facteur carré ou un gros facteur cubique.

Pour $\eta > 0$, minuscule, on découpe la somme S_2 de la manière suivante :

$$\begin{aligned} S_2 &= \sum_{\substack{p < x^{1-\eta}, \alpha \geq 2 \\ p^\alpha > x^{1-\varepsilon}}} \log p |\mathcal{E}_{p^\alpha}| + \sum_{p > x^{1-\eta}} \log p |\mathcal{E}_{p^2}| + \sum_{p > x^{1-\eta}} \log p |\mathcal{E}_{p^3}| \\ &= R_1 + R_2 + R_3, \end{aligned} \tag{5.3}$$

par définition. On peut déja remarquer que $R_3 \leq R_2$.

5.3. Majoration de la somme R_1.

Dans ce paragraphe, on montre le

LEMME 5.2. *On a la majoration :* $R_1 \ll \dfrac{x^2}{(\log x)^{10}}$.

Preuve du lemme 5.2.

Pour travailler avec une somme en moins et ainsi rendre les discussions plus claires, on écrit :

$$R_1 \ll \log x \sum_{2 \leq \alpha \ll \log x} R(\alpha),$$

avec

$$R(\alpha) = \sum_{x^{(1-\epsilon)\frac{1}{\alpha}} < p < x^{1-\eta}} |\mathcal{E}_{p^\alpha}|.$$

Pour majorer $R(\alpha)$, on bloque comme au paragraphe 1 une variable, par exemple p_1, puis on résoud $f(p_1, p_2) \equiv 0 \pmod{p^\alpha}$. Le problème est lorsque p divise Δ_{p_1}, le discriminant du polynôme $t \to f(p_1, t)$, les solutions p_2 peuvent alors être nombreuses, surtout lorsque α est de la taille de $\log x$. On définit encore Δ_{p_2} le discriminant du polynôme $t \to f(t, p_2)$, puis on découpe la somme $R(\alpha)$ suivant la taille du pgcd $(\Delta_{p_1}, \Delta_{p_2}, p^\alpha)$.

On écrit donc l'égalité :

$$\begin{aligned} R(\alpha) &= \sum_{x^{(1-\epsilon)\frac{1}{\alpha}} < p < x^{1-\eta}} \sum_{\substack{p_1, p_2 \sim x \\ f(p_1,p_2) \equiv 0 \pmod{p^\alpha} \\ (p^\alpha, \Delta_{p_1}, \Delta_{p_2}) < (\log x)^{100}}} 1 + \sum_{x^{(1-\epsilon)\frac{1}{\alpha}} < p < x^{1-\eta}} \sum_{\substack{p_1, p_2 \sim x \\ f(p_1,p_2) \equiv 0 \pmod{p^\alpha} \\ (p^\alpha, \Delta_{p_1}, \Delta_{p_2}) \geq (\log x)^{100}}} 1 \\ &= R_1(\alpha) + R_2(\alpha), \end{aligned}$$

par définition.

• Majoration de $R_1(\alpha)$.

La condition $(p^\alpha, \Delta_{p_1}, \Delta_{p_2}) < (\log x)^{100}$, entraîne que $(p^\alpha, \Delta_{p_1}) < (\log x)^{100}$, ou $(p^\alpha, \Delta_{p_2}) < (\log x)^{100}$. Les sommes sur p_1 et sur p_2 se majorent alors par

$$\sum_{\substack{p_1 \sim x \\ (p^\alpha, \Delta_{p_1}) < (\log x)^{100}}} \sum_{\substack{0 \leq v < p^\alpha \\ f(p_1, v) \equiv 0 \pmod{p^\alpha}}} \sum_{\substack{p_2 \sim x \\ p_2 \equiv v \pmod{p^\alpha}}} 1$$

$$+ \sum_{\substack{p_2 \sim x \\ (p^\alpha, \Delta_{p_2}) < (\log x)^{100}}} \sum_{\substack{0 \leq v < p^\alpha \\ f(v, p_2) \equiv 0 \pmod{p^\alpha}}} \sum_{\substack{p_1 \sim x \\ p_1 \equiv v \pmod{p^\alpha}}} 1.$$

Ces deux sommes se traitent de la même façon.

Pour la première, comme $(\Delta_{p_1}, p^\alpha) < (\log x)^{100}$, d'après le point (iii) du lemme 1.3.3, on a :

$$|\{0 \leq v < p^\alpha,\ f(u, v) \equiv 0 \pmod{p^\alpha}\}| = O((\Delta_{p_1}, p^\alpha)^2) = O((\log x)^{200}).$$

Les deux sommes ci-dessus sont donc majorées par : $O\left(x(\log x)^{200}\left(\frac{x}{p^\alpha} + 1\right)\right)$.

En reportant ce résultat dans $R_1(\alpha)$, cela donne la majoration :

$$\begin{aligned} R_1(\alpha) &\ll x(\log x)^{200} \sum_{x^{(1-\epsilon)\frac{1}{\alpha}} < p < x^{1-\eta}} \left(\frac{x}{p^\alpha} + 1\right) \\ &\ll x^{5/3+\epsilon/3}(\log x)^{200} \sum_{x^{\frac{1-\epsilon}{\alpha}} < p < x^{1-\eta}} \frac{x}{p^{2\alpha/3}} + x^{2-\eta}(\log x)^{200} \\ &\ll x^{2-h}, \end{aligned}$$

pour $h > 0$ assez petit.

• Majoration de $R_2(\alpha)$.
On oublie la condition $f(p_1, p_2) \equiv 0 \pmod{p^\alpha}$, mais pour tout $p < x^{1-\eta}$, on profite de l'inclusion :

$$\{p_1, p_2 \sim x, (p^\alpha, \Delta_{p_1}, \Delta_{p_2}) \geq (\log x)^{100}\} \subset \bigcup_{\substack{\beta > 0 \\ p^\beta \geq (\log x)^{100}}} \{p_1, p_2 \sim x, \Delta_{p_1} \equiv \Delta_{p_2} \equiv 0 \pmod{p^\beta}\}.$$

A partir de ceci on a la majoration

$$\begin{aligned} R_2(\alpha) &\ll \sum_{(\log x)^{100} \leq p^\beta,\ p < x^{1-\eta}} \sum_{\substack{p_1 \sim x \\ \Delta_{p_1} \equiv 0 \pmod{p^\beta}}} \sum_{\substack{p_1 \sim x \\ \Delta_{p_1} \equiv 0 \pmod{p^\beta}}} 1 \\ &\ll \sum_{(\log x)^{100} \leq p^\beta,\ p < x^{1-\eta}} \left(\frac{x^2}{p^{2\beta}} + 1\right), \end{aligned}$$

et ainsi, $R_2(\alpha) \ll \frac{x^2}{(\log x)^{20}}$.
Ces deux majorations de $R_1(\alpha)$, et $R_2(\alpha)$ sont largement suffisantes pour prouver le lemme 5.2.

5.4. Majoration de R_2.

Dans ce paragraphe, on s'occupe de la somme R_2 définie dans (5.3), on établit le

LEMME 5.3. *Pour tout $\varepsilon > 0$, il existe $\eta > 0$ assez petit, tel qu'on ait la majoration : $R_2 \ll x^{1.9+\varepsilon}$.*

Comme dans la première partie de la thèse, on détecte en utilisant le crible à carrés de Heath-Brown [HB], les grands facteurs carrés de l'ensemble contenant d'éventuelles répétitions :

$$\{f(p_1, p_2),\ p_1, p_2 \sim x\}.$$

On rappelle le lemme

LEMME 5.4. *Soit* $\mathbf{A} = (\omega(n))_n$ *une suite d'entiers, avec* $\omega(n) \geq 0$ $\forall n$, *et tel que* $\sum \omega(n) < +\infty$. *On définit* $S(\mathbf{A}) = \sum_1^\infty \omega(n^2)$.

Soit $\mathbf{P}$ *un ensemble de* P *nombres premiers. On suppose que* $\omega(n) = 0$ *pour* $n = 0$, *ou pour* $|n| \geq e^P$.

On a alors l'inégalité :

$$S(\mathbf{A}) \ll P^{-1} \sum_n \omega(n) + P^{-2} \sum_{p \neq q \in \mathbf{P}} \left| \sum_n \omega(n) \left(\frac{n}{pq}\right) \right|,$$

où $\left(\frac{n}{pq}\right)$ *est le symbole de Jacobi.*

Avant d'appliquer ce lemme, il faut procéder à quelques transformations préparatoires sur la somme R_2. On commence par ignorer les conditions p_1, p_2 premiers, et en reprenant la notation $|\mathcal{A}_d|$ définie au troisième chapitre cf (3.1), on écrit la majoration :

$$\begin{aligned} R_2 &\leq \sum_{p > x^{1-\epsilon}} \log p |\mathcal{A}_{p^2}| \\ &\ll \log x \sum_{m > x^{1-\epsilon}} |\mathcal{A}_{m^2}|. \end{aligned}$$

Si n_1 et n_2 vérifient $f(n_1, n_2) = m^2 d$, avec $m > x^{1-\epsilon}$, on a encore l'écriture : $f(n_1, n_2) = m'^2 d'$, avec toujours $m' > x^{1-\epsilon}$, mais d' est alors un entier sans facteur carré, ce qui nous permettra d'utiliser les majorations des sommes $S_f(d', h, k)$ établies au chapitre 2.
On part donc de la majoration :

$$R_2 \ll x^{\epsilon'} \sum_{d < x^{1+\epsilon}} \mu^2(d) R_2(d),$$

avec

$$R_2(d) = \sum_{m^2 > x^{2-2\epsilon}} \omega_d(m^2),$$

et

$$\omega_d(m) = |\{(n_1, n_2),\ n_1, n_2 \sim x,\ \frac{f(n_1, n_2)}{d} = m\}|.$$

On applique alors le lemme 5.4 sur chaque quantité $R_2(d)$, en choisissant $\mathbf{P_d} = \{p < x^\theta,\ (p, d) = 1\}$, où θ est un réel positif que l'on précisera plus tard. Ainsi P, le cardinal $|\mathbf{P_d}|$ est de l'ordre de $\frac{x^\theta}{\log x}$.

On a donc la majoration :

$$R_2(d) \ll x^{\varepsilon'} P^{-1} \sum_{\substack{n_1,n_2 \sim x \\ f(n_1,n_2)\equiv 0 \pmod d}} 1 + x^{\varepsilon'} P^{-2} \sum_{p\neq q\in \mathbf{P}} \left| \sum_{\substack{n_1,n_2\sim x \\ f(n_1,n_2)\equiv 0 \pmod d}} \left(\frac{\frac{f(n_1,n_2)}{d}}{pq}\right)\right|.$$

On écrit alors :

$$R_2(d) \ll x^{\varepsilon'}(P^{-1}\Sigma_1 + P^{-2}\Sigma_2).$$

La somme Σ_1 s'évalue directement car d est sans facteur carré, l'équation $f(n_1,n_2) \equiv 0 \pmod d$ se résoud alors facilement :

$$\Sigma_1 \ll \left(\frac{x}{d} + O(1)\right)^2 d \ll \frac{x^2}{d} + d.$$

La somme Σ_2 est plus difficile à évaluer, pour des commodités d'écriture, on la réécrit sous la forme :

$$\Sigma_2 = \sum_{p\neq q\in \mathbf{P}_d} |T(p,q,d)|,$$

avec évidemment :

$$T(p,q,d) = \sum_{\substack{n_1,n_2\sim x \\ f(n_1,n_2)\equiv 0 \pmod d}} \left(\frac{\frac{f(n_1,n_2)}{d}}{pq}\right).$$

Pour évaluer les quantités $T(p,q,d)$, on développe les sommes sur n_1 et n_2 en sommes d'exponentielles, pour être en mesure d'utiliser les résultats du chapitre 2, et des résultats de Hasse sur les sommes de caractères le long de cubiques.

On part de l'égalité :

$$T(p,q,d) = \frac{1}{p^2q^2d^2} \sum_{g,h \bmod pqd} \sum_{\substack{0\leq u,v<pqd \\ f(u,v)\equiv 0 \pmod d}} \left(\frac{d}{pq}\right)\left(\frac{f(u,v)}{pq}\right)$$

$$\times \sum_{n_1,n_2\sim x} e\left(\frac{g(u-n_1)+h(v-n_2)}{pqd}\right). \tag{5.4}$$

Ensuite on sépare ces différentes sommes, ce qui est permis d'après le théorème chinois car $(pq,d) = 1$:

$$T(p,q,d) = \frac{1}{p^2q^2d^2}\left(\frac{d}{pq}\right) \sum_{0\leq g,h<pqd} \sum_{n_1\sim x} e\left(\frac{-gn_1}{pqd}\right) \sum_{n_2\sim x} e\left(\frac{-hn_2}{pqd}\right)$$

$$\times H_f(p,g,h)H_f(q,g,h)S_f(d,g,h), \tag{5.5}$$

où $S_f(d,g,h)$ est la somme d'exponentielles étudiée au chapitre 2, et $H_f(p,g,h)$ est la somme de caractères suivante :

$$H_f(p,g,h) = \sum_{0\leq u,v<p} \left(\frac{f(u,v)}{p}\right) e\left(\frac{gu+hv}{p}\right).$$

Lorsque $(g,h) \neq (0,0)$ on majore trivialement les sommes $H_f(p,g,h)$ par p^2 (ce qui est loin de la majoration que l'on peut obtenir grâce au lemme de Hooley), tandis que d'après le lemme 2.1.3, on a la majoration :

$$S_f(d,g,h) = O(d^{1/2+\varepsilon}(d,g,h)^{1/2}).$$

Ainsi la contribution des termes en $(g,h) \neq (0,0)$ est inférieure à :

$$Q_1 = \frac{x^{1+\varepsilon}}{pqd} \sum_{0<g<pqd} \frac{p^2q^2}{g}\sqrt{d(d,g)} + x^{\varepsilon} \sum_{0<g,h<pqd} \frac{p^2q^2}{gh}\sqrt{d(d,g,h)}.$$

Un calcul direct fournit alors la majoration :

$$Q_1 \ll \frac{x^{1+\varepsilon_1}pq}{\sqrt{d}} + p^2q^2\sqrt{d}x^{\varepsilon_1}.$$

Il reste à majorer le terme en $g = h = 0$ qui correspond à :

$$Q_2 = \frac{x^2\rho(d)}{d^2p^2q^2} \sum_{0\leq u,v<p} \left(\frac{f(u,v)}{p}\right) \sum_{0\leq u,v<q} \left(\frac{f(u,v)}{q}\right). \tag{5.6}$$

Ici, une estimation triviale des sommes de caractères de Legendre n'est pas suffisante et on établit le

LEMME 5.5. *On suppose que f vérifie l'hypothèse (H2). On a alors la majoration :*

$$\sum_{0\leq u,v<p} \left(\frac{f(u,v)}{p}\right) = O(p^{3/2}),$$

la constante implicite ne dépendant que de f.

L'exposant 3/2 n'est pas optimal, on peut le ramener à 1, mais il convient à notre situation, et cette majoration s'obtient directement à partir du résultat de Hasse suivant [Si] :

LEMME 5.6. *Soit $g(x) \in \mathbf{F}_p[x]$ un polynôme de degré 3, non constant. On a alors l'inégalité :*

$$\left|\sum_{x\in\mathbf{F}_p} \left(\frac{g(x)}{p}\right)\right| \ll \sqrt{p}.$$

Preuve du lemme 5.5
On réécrit le polynôme f sous la forme

$$f(u,v) = \sum_{0\leq k\leq 3} g_k(u)v^k.$$

Comme f vérifie l'hypothèse (H2), f ne peut se ramener à un polynôme en une seule variable, les polynômes g_1, g_2 et g_3 ne sont donc pas tous identiquement nuls sur $\mathbf{F}_p$ lorsque p est assez grand. On désire alors fixer la variable u pour appliquer le lemme 5.6 au polynôme $f_u : v \mapsto f(u,v)$, mais il faut mettre de côté les u tels que les polynômes f_u soient constants sur $\mathbf{F}_p$. Ils appartiennent à l'ensemble $S_p = \{0 \leq u < p,\ g_1(u) \equiv g_2(u) \equiv g_3(u) \equiv 0 \pmod p\}$.
On a ainsi l'égalité :

$$\sum_{0\leq u,v<p} \left(\frac{f(u,v)}{p}\right) = \sum_{\substack{0\leq u<p \\ u\notin S_p}} \sum_{0\leq v<p} \left(\frac{f(u,v)}{p}\right) + O(p|S_p|).$$

Comme les g_i, pour $i = 1,2,3$ ne sont pas tous identiquement nuls, on a $|S_p| = O(1)$, tandis que d'après le théorème 5.6 la somme sur les $u \notin S_p$ est un $O(p^{3/2})$. L'inégalité annoncée au lemme 5.5 est donc vérifiée.

On reporte alors le résultat du lemme 5.5 dans (5.6) :

$$Q_2 \ll \frac{x^2\rho(d)}{d^2\sqrt{pq}}.$$

Au chapitre 1, on a vu que $\rho(d) = O(d)$, et on a donc finalement :

$$T(p,q,d) \ll \frac{x^{1+\epsilon_1}pq}{\sqrt{d}} + p^2q^2\sqrt{d}x^{\epsilon_1} + \frac{x^2}{d\sqrt{pq}}.$$

On reporte ceci dans Σ_2 :

$$\Sigma_2 \ll \frac{P^4x^{1+\epsilon_1}}{\sqrt{d}} + P^6x^{\epsilon_1}\sqrt{d} + \frac{Px^{2+\epsilon_1}}{d}. \tag{5.7}$$

Ainsi on a l'inégalité pour tout d sans facteur carré :

$$R_2(d) \ll x^{\epsilon'}\left(P^{-1}\frac{x^2}{d} + dP^{-1} + \frac{P^2x^{1+\epsilon_2}}{\sqrt{d}} + P^4\sqrt{d}x^{\epsilon_2} + \frac{P^{-1}x^2}{d}\right),$$

c'est-à-dire :

$$\begin{aligned} R_2 &\ll \sum_{d<x^{1+\epsilon}} R_2(d) \\ &\ll x^2P^{-1}x^{\epsilon_3} + P^4x^{3/2+\epsilon_3}. \end{aligned}$$

En choisissant $P = x^\theta = x^{1/10}$, on a l'inégalité : $R_2 \ll x^{1,9+\epsilon}$.

5.5. Estimations de S_3.

D'après les lignes (5.1) et (5.2), les lemmes 5.1, 5.2, 5.3, nous avons les égalités :
-lorsque f est un polynôme du second degré :

$$\begin{aligned} S_3 &= \log V(x) - S_1 - S_2 \\ &= \frac{(1+\varepsilon)x^2}{\log x} + O\left(\frac{x^2}{(\log x)^2}\right), \end{aligned} \tag{5.8}$$

-lorsque le degré de f est trois :

$$S_3 = \frac{(2+\varepsilon)x^2}{\log x} + O\left(\frac{x^2}{(\log x)^2}\right). \tag{5.9}$$

Le principe de la méthode de Tchebychev consiste alors à chercher une majoration de S_3 qui dépende de P le plus grand facteur premier du produit $V(x)$ et d'en déduire ensuite une minoration de P.
On rappelle la définition de S_3 :

$$S_3 = \sum_{p > x^{1-\epsilon}} \log p |\mathcal{E}_p|.$$

On écarte les (p_1, p_2) de $\mathcal{E}_p$ tels que $p | p_1 p_2$:

$$S_3 = \sum_{p > x^{1-\epsilon}} \log p |\mathcal{F}_p| + O(x^{1+\epsilon}),$$

où $\mathcal{F}_p$ est l'ensemble contenant d'éventuelles répétitions :

$$\mathcal{F}_p = \{p_1 p_2,\ p_1, p_2 \sim x,\ (p_1 p_2, p) = 1,\ f(p_1, p_2) \equiv 0 \pmod p\}.$$

Avec des méthodes de crible qui reprennent des résultats du chapitre 3, on montre le lemme :

LEMME 5.7. *Pour p assez grand, et pour $z \geq 1$, on a la majoration :*

$$|\mathcal{F}_p| \leq \frac{2x^2}{(\log z)^2} \frac{r(p)}{p^2} + O\left(\frac{z^2 x^{1+\epsilon}}{\sqrt{p}} + \sqrt{p} z^2 x^{\epsilon}\right).$$

Preuve du lemme 5.7.
On détecte les nombres premiers p_1, p_2 par du crible, pour $z \geq 1$, on écrit la majoration :

$$|\mathcal{F}_p| \leq \sum_{\substack{n_1, n_2 \sim x \\ q | n_1 n_2 \Rightarrow q > z \\ (n_1 n_2, p) = 1 \\ f(n_1, n_2) \equiv 0 \pmod p}} 1.$$

Les familles d'entiers correspondant à ce problème de crible, sont exactement les ensembles $\mathcal{A}_p(a)$ étudiés au chapitre 3, définis par (3.2) ; d'après le lemme 3.2, on a l'égalité pour a sans facteur carré, et premier à p :

$$|\mathcal{A}_p(a)| = x^2 \frac{r(p)\lambda(a)}{p^2 a^2} + O\left(\frac{x^{1+\epsilon}}{\sqrt{p}} + x^{\epsilon}\sqrt{p}\right),$$

avec $\lambda(q) = 2q - 1$ lorsque q est un nombre premier.

Les conditions (1) et (2) du théorème A2 sont vérifiées, et d'après ce théorème, on a la majoration (on prend $z < x^{1+\varepsilon}$) :

$$|\mathcal{F}_p| \leq \frac{x^2 r(p)}{p^2} 2e^{2\gamma} \prod_{q<z} \left(1 - \frac{\lambda(q)}{q^2}\right) \left(1 + O\left(\frac{1}{\log z}\right)\right)$$

$$+ \sum_{a<z^2} 3^{\nu(a)} \mu^2(a) \left(\frac{x^{1+\varepsilon}}{\sqrt{p}} + x^{\varepsilon}\sqrt{p}\right). \tag{5.10}$$

Le produit eulérien vaut exactement $\prod_{q<z} \left(1 - \frac{1}{p}\right)^2$, en appliquant la formule de Mertens et en majorant directement le terme d'erreur on trouve le résultat annoncé au lemme 5.7.

On reporte ce résultat dans S_3 :

$$S_3 \leq 2x^2 \sum_{x^{1-\varepsilon}<p<P} \log p \frac{r(p)}{p^2 (\log z_p)^2} \left(1 + O\left(\frac{1}{\log z}\right)\right)$$

$$+ O\left(\sum_{x^{1-\varepsilon}<p<P} \log p \left(\frac{z_p^2 x^{1+\varepsilon}}{\sqrt{p}} + \sqrt{p} z_p^2 x^{\varepsilon}\right)\right). \tag{5.11}$$

On choisit ensuite $z_p = x^{1-2\varepsilon} p^{-3/4}$ de telle sorte que le terme d'erreur de (5.11) soit un $O(x^{2-\varepsilon})$ (la limite est alors $P < x^{4/3-10\varepsilon}$, pour que $z_p > 1$), ce qui fournit la majoration :

$$S_3 \leq 2x^2 \sum_{x^{1-\varepsilon}<p<P} \frac{\log p}{\log^2 (x^{1-2\varepsilon} p^{-3/4})} \frac{r(p)}{p^2} + O\left(x^{2-\varepsilon} + \frac{x^2}{(\log x)^2}\right).$$

On applique le point (ii) du corollaire 1.3.4, ce qui donne l'inégalité :

$$S_3 \leq 2x^2 \int_{x^{1-\varepsilon}}^{P} \frac{dt}{t \log^2 (x^{1-2\varepsilon} t^{-3/4})} + O\left(\frac{x^2}{\log^2 x} + x^{2-\varepsilon}\right).$$

En écrivant alors $P = x^{\Lambda}$, (avec $\Lambda < 4/3 - 10\varepsilon$), puis en calculant l'intégrale ci-dessus on aboutit à la majoration :

$$S_3 \leq \frac{x^2}{\log x} \left(\frac{8}{3(1 - 3\Lambda/4)} - \frac{32}{3} + \varepsilon\right) + O\left(\frac{x^2}{\log^2 x}\right). \tag{5.12}$$

5.6. Conclusion dans le cas où f est un polynôme du second degré.

En comparant (5.8) et (5.12), le plus grand facteur $P_2 = x^{\lambda_2}$ de $V(x)$ doit vérifier

$$1 \leq \frac{8}{3(1 - 3\lambda_2/4)} - \frac{32}{3},$$

c'est à dire $\lambda_2 \geq 36/35$.

5.7. Conclusion dans le cas où f est un polynôme du troisième degré.

A partir de (5.9) et (5.12), le plus grand facteur premier $P_3 = x^{\lambda_3}$ doit alors vérifier :

$$2 \leq \frac{8}{3(1-3\lambda_3/4)} - \frac{32}{3},$$

c'est à dire $\lambda_3 \geq 20/19$.

5.8. Cas des polynômes homogènes.

On garde les mêmes notations, mais f est maintenant un polynôme homogène, irréductible en deux variables, dont les coefficients sont premiers entre eux, et vérifiant l'hypothèse (H1). On a toujours l'égalité :

$$\begin{aligned}\log V(x) &= \frac{dx^2}{\log x} + O\left(\frac{x^2}{(\log x)^2}\right) \\ &= S_1 + S_2 + S_3.\end{aligned}$$

D'après le point (ii) du lemme 4.1, et les estimations de $\rho(p^\alpha)$ données au paragraphe 1.2, on a l'égalité :

$$\begin{aligned}S_1 &= \sum_{p^\alpha < x^{1-\epsilon}} \log p |\mathcal{E}_{p^\alpha}| \\ &= (1-\varepsilon)\frac{x^2}{\log x} + O\left(\frac{x^2}{\log x}\right).\end{aligned}$$

Les majorations des paragraphes 5.2, 5.3, 5.4, ont utilisé principalement les estimations de $\rho(p^\alpha)$, et $\tilde{S}_f(p,g,h)$. Étant donné que lorsque f est homogène les estimations correspondantes sont plus fines, on a donc toujours :

$$S_2 \ll \frac{x^2}{(\log x)^2}.$$

Pour S_3, l'homogénéité de f permet d'avoir une majoration plus fine que celle du paragraphe 5.5, en utilisant le lemme 3.2.3 à la place du lemme 3.2. Le z_p correspondant vaut alors $z_p = x^{1-\epsilon}p^{-1/2}$, pour $p < x^{2-\epsilon}$, et on obtient la majoration

$$S_3 \leq \int_{x^{1-\epsilon}}^{P} \frac{2x^2}{t(\log(x^{1-\epsilon}t^{-1/2}))^2} dt + O\left(\frac{x^2}{\log^2 x}\right).$$

En écrivant $P = x^H$, puis en calculant cette intégrale, on a la majoration :

$$S_3 \leq \frac{x^2}{\log x}\left(4\left(\frac{1}{1-H/2}\right) - 8 + \varepsilon\right) + O\left(\frac{x^2}{\log^2 x}\right).$$

Lorsque le degré de f est 2, le plus grand facteur $P_2 = x^{H_2}$ doit vérifier :

$$1 \leq \frac{8}{2 - H_2} - 8,$$

c'est à dire $H_2 \geq 10/9$.

Si le degré de f est 3, le plus grand facteur $P_3 = x^{H_3}$ correspondant vérifie alors :

$$\frac{8}{2 - H_3} - 8 \geq 2,$$

c'est à dire $H_3 \geq 6/5$.

Chapitre 6

Étude du plus grand facteur premier de polynômes de degré 3, en trois variables, pris en des valeurs premières

Dans ce chapitre, f est un polynôme irréductible en trois variables, du troisième degré, dont les coefficients sont premiers entre eux et vérifiant les hypothèses (H3) et (H4) définies dans l'introduction.

La méthode de Tchebychev consiste ici à étudier le produit

$$W(x) = \prod_{p_1,p_2,n_3 \sim x} f(p_1,p_2,n_3).$$

On commence par évaluer $\log W(x)$ à l'aide du théorème des nombres premiers :

$$\begin{aligned} \log W(x) &= \sum_{p_1,p_2,n_3 \sim x} \log f(p_1,p_2,n_3) \\ &= \frac{3x^3}{\log x} + O\left(\frac{x^3}{(\log x)^2}\right). \end{aligned} \tag{6.1}$$

Par ailleurs, pour tous $\varepsilon, \eta > 0$, on a l'égalité :

$$\begin{aligned} \log W(x) = &\sum_{\substack{p,\alpha \\ p^\alpha < x^{1-\varepsilon}}} \log p |\mathcal{G}_{p^\alpha}| + \sum_{\substack{p^\alpha > x^{1-\varepsilon} \\ p < x^{1-\eta},\ \alpha \geq 2}} \log p |\mathcal{G}_{p^\alpha}| \\ &+ \sum_{\substack{p^\alpha > x^{1-\varepsilon} \\ p > x^{1-\eta},\ \alpha \geq 2}} \log p |\mathcal{G}_{p^\alpha}| + \sum_{x^{1-\varepsilon} < p < P} \log p |\mathcal{G}_p|, \end{aligned}$$

avec,

$$\mathcal{G}_{p^\alpha} = \{(p_1,p_2,n_3),\ ,p_1,p_2,n_3 \sim x,\ f(p_1,p_2,n_3) \equiv 0 \pmod{p^\alpha}\}.$$

On a ainsi le découpage $\log W(x) = T_1 + T_2 + T_3 + T_4$, et ces quantités sont évaluées dans l'ensemble de la même manière que les sommes S_1, S_2, S_3, étudiées au chapitre 4, mais en utilisant les résultats des chapitres 1, 2, 3, 4 propres aux polynômes en trois variables.

6.1. Évaluation de T_1.

Comme au paragraphe 5.1, on met de côté les $|\mathcal{G}_{p^\alpha}|$, avec $\alpha \geq 2$:

$$\begin{aligned} T_1 &= \sum_{p < x^{1-\varepsilon}} \log p |\mathcal{G}_p| + \sum_{p^\alpha < x^{1-\varepsilon},\ \alpha \geq 2} \log p |\mathcal{G}_{p^\alpha}| \\ &= T_1' + T_1'', \end{aligned}$$

par définition.

D'après le lemme 4.2, on a l'égalité :

$$T_1' = \frac{x^3}{\log^2 x} \sum_{p<x^{1-\epsilon}} \log p \frac{r(p)}{\varphi(p)^3} + O\left(\frac{x^3}{\log^2 x}\right).$$

Le terme principal a déja été estimé au paragraphe 1.4, et d'après le point (ii) du corollaire 1.4.4, on a l'égalité :

$$T_1' = (1-\varepsilon)\frac{x^3}{\log x} + O\left(\frac{x^3}{\log^2 x}\right). \tag{6.2}$$

De la même manière qu'au paragraphe 5.1, on montre que T_1'' est un $O\left(\frac{x^3}{\log^2 x}\right)$.
En utilisant le théorème de Brun-Titchmarsh on établit l'inégalité :

$$|\mathcal{G}_{p^\alpha}| \ll \frac{x^3}{\log^2 x} \frac{\rho(p^\alpha)}{p^{3\alpha}},$$

pour $p^\alpha < x^{1-\epsilon}$.
D'après la proposition 1.4.3, $\rho(p^2) = O(p^4)$, $\rho(p^\alpha) = O(\alpha^3 p^{18\alpha/7})$, et ainsi :

$$\sum_{p,\alpha\geq 2} \frac{\log p \rho(p)}{p^{3\alpha}} = O(1),$$

et on a donc (6.3) $T_1'' = O\left(\frac{x^3}{\log^2 x}\right)$.
Les deux inégalités (6.2) et (6.3) donnent alors :

$$T_1 = (1-\varepsilon)\frac{x^3}{\log x} + O\left(\frac{x^3}{(\log x)^2}\right). \tag{6.4}$$

6.2. Majoration de T_2.

Cette majoration est assez laborieuse, car il faut travailler avec trois variables, mais est sans difficulté particulière, car on reprend des idées utilisées aux paragraphes 5.3 et 1.4. On montre le lemme

LEMME 6.1. *On a l'inégalité :* $T_2 \ll \frac{x^3}{(\log x)^2}$.

preuve du lemme 6.1.
On part encore de l'écriture :

$$T_2 \ll \log x \sum_{2\leq\alpha\ll\log x} T(\alpha),$$

avec

$$T(\alpha) = \sum_{x^{\frac{1-\epsilon}{\alpha}}<p<x^{1-\eta}} |\mathcal{G}_{p^\alpha}|.$$

On note $\Delta_{p_1p_2}$ le discriminant du polynôme $t \mapsto f(p_1,p_2,t)$, $\Delta_{p_1n_3}$, celui de $t \mapsto f(p_1,t,n_3)$, $\Delta_{p_2n_3}$, celui de $t \mapsto f(t,p_2,n_3)$.
On découpe T_2 suivant la taille du pgcd $(p^\alpha, \Delta_{p_1p_2}, \Delta_{p_2n_3}, \Delta_{p_1n_3})$ et on écrit l'inégalité :

$$\begin{aligned} T(\alpha) &\ll \sum_{x^{\frac{1-\epsilon}{\alpha}}<p<x^{1-\eta}} \sum_{\substack{p_1,p_2,n_3\sim x \\ (\Delta_{p_1p_2},\Delta_{p_1n_3},\Delta_{p_2n_3},p^\alpha)<(\log x)^{100} \\ f(p_1,p_2,n_3)\equiv 0 \pmod{p^\alpha}}} 1 \\ &+ \sum_{x^{\frac{1-\epsilon}{\alpha}}<p<x^{1-\eta}} \sum_{\substack{p_1,p_2,n_3\sim x \\ (\Delta_{p_1p_2},\Delta_{p_1n_3},\Delta_{p_2n_3},p^\alpha)\geq(\log x)^{100} \\ f(p_1,p_2,n_3)\equiv 0 \pmod{p^\alpha}}} 1 \\ &\ll T_1(\alpha) + T_2(\alpha), \end{aligned} \tag{6.5}$$

par définition.
Parmi les trois discriminants Δ intervenant dans la somme $T_1(\alpha)$, il en existe au moins tel que $(\Delta_{..}, p^\alpha) < (\log x)^{100}$. Dans la première somme $T_1(\alpha)$, les conditions sur p_1, p_2 et n_3 se scindent donc en trois sommes du type :

$$\sum_{\substack{p_1,p_2\sim x \\ (\Delta_{p_1p_2},p^\alpha)<(\log x)^{100}}} \sum_{\substack{0\leq w<p^\alpha \\ f(p_1,p_2,w)\equiv 0 \pmod{p^\alpha}}} \sum_{\substack{n_3\sim x \\ n_3\equiv w \pmod{p^\alpha}}} 1.$$

Le nombre de solutions w est un $O((\Delta_{p_1p_2}, p^\alpha)^2)$, d'après le point (iii) du lemme 1.3.3, et ainsi on a la majoration :

$$\begin{aligned} T_1(\alpha) &\ll \sum_{x^{\frac{1-\epsilon}{\alpha}}<p<x^{1-\eta}} (\log x)^{200}\left(\frac{x^3}{p^\alpha} + x^2\right) \\ &\ll x^{8/3+h} + x^{3-\eta}(\log x)^{200}, \end{aligned} \tag{6.6}$$

avec $0 < h < 1/3$.

Pour majorer $T_2(\alpha)$, on oublie la condition $f(p_1,p_2,n_3) \equiv 0 \pmod{p^\alpha}$ et on fixe une deuxième variable. On fait alors le découpage :

$$\begin{aligned} T_2(\alpha) &\ll \sum_{\substack{x^{\frac{1-\epsilon}{\alpha}}<p<x^{1-\eta} \\ p^\beta>(\log x)^{100}}} \sum_{\substack{p_1,p_2,n_3\sim x \\ p^\beta|(\Delta_{p_1,p_2},\Delta_{p_1,n_3},\Delta_{p_2,n_3})}} 1 \\ &\ll \sum_{p<x^{1-\eta},\ p^\beta>(\log x)^{100}} T_2(\alpha,\beta). \end{aligned} \tag{6.7}$$

On considère chacun des discriminants Δ_{p_1,p_2}, Δ_{p_1,n_3}, Δ_{p_2,n_3} comme des polynômes en deux variables et on est quasiment dans la situation du paragraphe 5.2. On bloque une deuxième variable, mais là encore on se heurte à des problèmes de divisibilité par p des discriminants des discriminants ... On définit alors les polynômes suivants :
on note $D_{p_1}^{(1)}$ le discriminant de $p_2 \to \Delta_{p_1p_2}$, $D_{p_1}^{(2)}$ celui de $n_3 \to \Delta_{p_1n_3}$, $D_{p_2}^{(1)}$ le discriminant de $p_1 \to \Delta_{p_1p_2}$, $D_{p_2}^{(2)}$ le discriminant de $n_3 \to \Delta_{p_2n_3}$, $D_{n_3}^{(1)}$ le discriminant de $p_1 \to \Delta_{p_1n_3}$, $D_{n_3}^{(2)}$ le discriminant de $p_2 \to \Delta_{p_2n_3}$.
On écrit ensuite l'inégalité :

$$\begin{aligned} T_2(\alpha,\beta) &\ll \sum_{\substack{p^\beta>(\log x)^{100} \\ x^{\frac{1-\epsilon}{\alpha}}<p<x^{1-\eta}}} \sum_{\substack{p_1,p_2,n_3\sim x \\ D_1(p_1,p_2,n_3)\equiv 0 \pmod{p^\beta} \\ (p^\beta,D_2(p_1,p_2,n_3))<(\log x)^{10}}} 1 \\ &+ \sum_{\substack{p^\beta>(\log x)^{100} \\ x^{\frac{1-\epsilon}{\alpha}}<p<x^{1-\eta}}} \sum_{\substack{p_1,p_2,n_3\sim x \\ D_1(p_1,p_2,n_3)\equiv 0 \pmod{p^\beta} \\ (p^\beta,D_2(p_1,p_2,n_3))\geq(\log x)^{10}}} 1 \\ &\ll R_1(\alpha,\beta)+R_2(\alpha,\beta), \end{aligned}$$

par définition, et où pour alléger l'écriture, on a posé :

$$D_1(p_1,p_2,n_3)=(\Delta_{p_1p_2},\Delta_{p_1n_3},\Delta_{p_2n_3}),$$

et

$$D_2(p_1,p_2,n_3)=(D_{p_1}^{(1)},D_{p_1}^{(2)},D_{p_2}^{(1)},D_{p_2}^{(2)},D_{n_3}^{(1)},D_{n_3}^{(2)}).$$

Dans $R_1(\alpha,\beta)$, au moins un des discriminants intervenant dans D_2 a une valuation p-adique inférieure à $(\log x)^{10}$, la somme $R_1(\alpha,\beta)$ est alors majorée par 6 sommes du type :

$$S(\alpha,\beta)=\sum_{p^\beta>(\log x)^{100},\ p<x^{1-\eta}} \sum_{\substack{p_1,n_3\sim x \\ (p^\beta,D_{p_1}^{(1)})<(\log x)^{10}}} \sum_{\substack{p_2\sim x \\ \Delta_{p_1p_2}\equiv 0 \pmod{p^\beta}}} 1.$$

D'après le point (iii) du lemme 1.3.3, la somme sur p_2 est un $O\left((\frac{x}{p^\beta}+1)(D_{p_1}^{(1)},p^\beta)^2\right)$, on majore ensuite trivialement les sommes sur p_1 et sur p_2, et ainsi on a l'inégalité:

$$\begin{aligned} S(\alpha,\beta) &\ll \sum_{\substack{p^\beta>(\log x)^{100} \\ x^{\frac{1-\epsilon}{\alpha}}<p<x^{1-\eta}}} \left(\frac{x^3(\log x)^{20}}{p^\beta}+x^2(\log x)^{20}\right) \\ &\ll \frac{x^3}{(\log x)^{10}}. \end{aligned}$$

On a ainsi

$$R_1(\alpha,\beta) \ll \frac{x^3}{(\log x)^9}. \tag{6.8}$$

La somme $R_2(\alpha,\beta)$ est plus facile à estimer. On oublie la condition portant sur D_1, et on considère chaque discriminant de D_2 comme un polynôme en une variable, on réorganise la somme en :

$$R_2(\alpha,\beta) \ll \sum_{p^\gamma \geq (\log x)^{10},\ p<x^{1-\eta}} \sum_{\substack{p_1,p_2,n_3\sim x \\ D^{(1)}_{p_1}\equiv D^{(1)}_{p_2}\equiv D^{(1)}_{n_3}\equiv 0 \pmod{p^\gamma}}} 1$$
$$\ll \sum_{p^\gamma \geq (\log x)^{10},\ p<x^{1-\eta}} \left(1+\frac{x^3}{p^{3\gamma}}\right),$$

d'après le point (iv) du lemme 1.3.3.
On obtient donc :

$$R_2(\alpha,\beta) \ll \frac{x^2}{(\log x)^{10}}. \tag{6.9}$$

Les inégalités (6.6), (6.8), (6.9) prouvent alors le lemme 6.1.

6.3. Majoration de T_3.

Ce paragraphe est consacré à la preuve du lemme

LEMME 6.2. *Pour x assez grand, on a la majoration : $T_3 \ll x^{2,9}$.*

En faisant les mêmes raisonnements qu'au paragraphe 5.3, on remarque que :

$$T_3 \ll \sum_{p>x^{1-\eta}} \log p|\mathcal{G}_{p^3}| + \sum_{p>x^{1-\eta}} \log p|\mathcal{G}_{p^2}|$$
$$\ll x^{\varepsilon_1} \sum_{d\ll x^{1+2\eta}} \mu(d)^2 |\{(n_1,n_2,n_3,m),\ n_1,n_2,n_3\sim x,\ f(n_1,n_2,n_3)=dm^2\}|$$
$$\ll x^{\varepsilon_1} \sum_{d\ll x^{1+2\eta}} \mu^2(d) T_3(d),$$

par définition.
On a commencé par observer que la deuxième somme était comprise dans la première, puis dans l'écriture de $f(p_1,p_2,n_3)$, on a mis de coté tous les facteurs carrés, et supprimé les conditions de primalité.
On majore ensuite les quantités $T_3(d)$ individuellement avec le crible à carrés, c'est à dire en appliquant le lemme 5.4. En reprenant les notations de ce lemme, et en choisissant $\mathbf{P_d} = \{p<P,\ (p,d)=1\}$, pour tout $\varepsilon'>0$, on a l'inégalité :

$$T_3(d) \ll x^{\varepsilon'} P^{-1} \mu^2(d) \sum_{\substack{n_1,n_2,n_3\sim x \\ f(n_1,n_2,n_3)\equiv 0 \pmod d}} 1$$
$$+ x^{\varepsilon'} P^{-2} \sum_{p\neq q\in \mathbf{P_d}} \left| \sum_{\substack{n_1,n_2,n_3\sim x \\ f(n_1,n_2,n_3)\equiv 0 \pmod d}} \left(\frac{\frac{f(n_1,n_2,n_3)}{d}}{pq}\right)\right|$$
$$\ll x^{\varepsilon'}(P^{-1}\Sigma_1 + P^{-2}\Sigma_2), \tag{6.10}$$

par définition.

Comme d est sans facteur carré, la première somme du membre de droite de (6.10), s'évalue facilement, on a $\rho(d) = O(d^2)$ d'après le lemme 1.4.2, et ainsi l'inégalité :

$$\Sigma_1 \ll d^2 \left(\frac{x}{d}+1\right)^3 \ll \frac{x^3}{d} + d^2. \tag{6.11}$$

La deuxième somme de (6.10) s'évalue comme la somme Σ_2 estimée au paragraphe 5.3. Il s'agit d'étudier les quantités :

$$T_3(p,q,d) = \sum_{\substack{n_1,n_2,n_3 \sim x \\ f(n_1,n_2,n_3)\equiv 0 \pmod d}} \left(\frac{\frac{f(n_1,n_2,n_3)}{d}}{pq}\right),$$

lorsque d est sans facteur carré, et premier avec p et q.
On développe alors les quantités $T_3(p,q,d)$ en sommes d'exponentielles comme on l'avait fait à la ligne (5.4), puis on sépare ces sommes suivant (5.5), on rencontre alors deux types de sommes :
• les sommes $S_f(d,h_1,h_2,h_3)$ étudiées au chapitre 2, d'après le lemme 2.3.1 , on a la majoration pour d sans facteur carré : $S_f(d,h_1,h_2,h_3) = O(d(d,h_1,h_2,h_3))$.

• les sommes $H_f(p,h_1,h_2,h_3)$ définies par :

$$H_f(p,h_1,h_2,h_3) = \sum_{0\le u,v,w<p} \left(\frac{f(u,v,w)}{p}\right) e\left(\frac{h_1u+h_2v+h_3w}{p}\right),$$

Lorsque $(h_1,h_2,h_3) \neq (0,0,0)$, on majore les sommes H_f trivialement par des $O(p^3)$.

On utilise le lemme 5.6 pour majorer $H_f(p,0,0,0)$. On part de l'égalité :

$$H_f(p,0,0,0) = \sum_{0\le u,v<p}{}^{*} \sum_{0\le w<p} \left(\frac{f(u,v,w)}{p}\right) + O(p|Z_p|), \tag{6.12}$$

où $*$ indique que la somme porte sur les $(u,v) \in \mathbf{F}_p^2$ tels que le polynôme $w \to f(u,v,w) = g(w)$ ne soit pas constant sur $\mathbf{F}_p$, tandis que Z_p est l'ensemble des couples (u,v) dégénérés, c'est à dire :

$$Z_p = \{(u,v) \in F_p^2 / \ \exists a \in \mathbf{F_p},\ \forall\, w \in \mathbf{F_p},\ f(u,v,w) \equiv a \pmod p\}.$$

En écrivant g sous la forme $g(w) = \sum_{0\le i\le d} h_i(u,v)w^i$, le polynôme f vérifiant l'hypothèse (H4), il ne peut pas se ramener à un polynôme en deux variables, il existe $0 < i \le d$ tel que $h_i(u,v)$ ne soit pas le polynôme nul. On a alors la majoration $|Z_p| \ll \rho_{h_i}(p) = O(p)$.
D'après le lemme 5.6, la somme sur les w de la ligne (6.12) est un $O(p^{1/2})$, et ainsi, on a l'inégalité :

$$H_f(p,0,0,0) = O(p^{5/2}).$$

Comme au chapitre 5, on n' a pas cherché à donner un exposant optimal.

On termine ensuite les calculs comme au paragraphe 5.3, et en tenant compte de (6.11), on arrive à la majoration :

$$T_3(d) \ll P^{-1}\frac{x^3}{d} + P^{-1}d^2 + P^2\frac{x^{2+\varepsilon_2}}{d} + P^4x^{1+\varepsilon_2} + P^6d^{1+\varepsilon_2}.$$

En sommant ensuite sur d on obtient alors :

$$T_3 \ll P^{-1}x^{3+6\eta+\varepsilon'} + x^{2+2\eta+\varepsilon'}P^6.$$

On choisit alors $P = x^{2/15}$, η et ε' étant arbitrairement petits, on a : $T_3 \ll x^{2,9}$.

6.4. Estimations de T_4.

On a tout d'abord d'après les lignes (6.1) et (6.2), et les lemmes 6.1 et 6.2, la minoration :

$$\begin{aligned} T_4 &= \log W(x) - T_1 - T_2 - T_3 \\ &= (2+\varepsilon)\frac{x^3}{\log x} + O\left(\frac{x^3}{(\log x)^2}\right). \end{aligned} \tag{6.13}$$

Par ailleurs, en reprenant la définition de T_4, on a l'égalité pour tout $h > 0$:

$$T_4 = \sum_{p>x^{1-\epsilon}} \log p|\mathcal{H}_p| + O(x^{2+h}), \tag{6.14}$$

avec

$$\mathcal{H}_p = \{(p_1,p_2,n_3),\ p_1,p_2,n_3 \sim x,\ (p_1p_2n_3,p) = 1,\ f(p_1,p_2,n_3) \equiv 0 \pmod p\}.$$

Le terme d'erreur de (6.14) correspond aux $f(p_1,p_2,n_3) \equiv 0 \pmod p$, tels que $p|p_1p_2n_3$.
Avec une telle définition de $\mathcal{H}_p$, il est malaisé d'appliquer un crible de dimension 2 pour détecter les p_1p_2, et on préfère l'écriture :

$$\mathcal{H}_p = \sum_n w_p(n),$$

où $w_p(n)$ est le nombre de solutions du sytème d'équations aux inconnues p_1, p_2, n_3 :

$$p_1,p_2,n_3 \sim x,\ n = p_1p_2,\ (p_1p_2n_3,p) = 1,\ f(p_1,p_2,n_3) \equiv 0 \pmod p.$$

Comme au paragraphe 5.5, on obtient avec des méthodes de cribles la majoration

LEMME 6.3. *Pour $z \geq 1$, on a l'inégalité :*

$$|\mathcal{H}_p| \leq \frac{2x^3}{\log^2 z}\frac{r(p)}{p^3}\left(1 + O\left(\frac{1}{\log z}\right)\right) + O\left(\frac{z^2x^{2+\varepsilon}}{p} + z^2x^{1+\varepsilon} + z^2x^{\varepsilon}p\right).$$

Preuve du lemme 6.3. Pour $z \geq 1$, on part de l'inégalité :

$$\mathcal{H}_p \leq \sum_{q|n \Rightarrow q>z} w_p(n).$$

Soient $(\lambda_d)_{d\geq 1}$ les coefficients du crible de Selberg ([H-R] chapitre 3).
A partir de ces poids on a la majoration

$$|\mathcal{H}_p| \leq \sum_n w_p(n) \left(\sum_{d|n} \lambda_d \right)^2 .$$

En développant ce carré, et en reprenant la notation (3.3) du chapitre 3 on a :

$$|\mathcal{H}_p| \leq \sum_{d_1,d_2|P(z)} \lambda_{d_1}\lambda_{d_2} |\mathcal{B}_p([d_1,d_2])|,$$

$P(z)$ étant le produit de tous les nombres premiers inférieurs à z.
Dans ce chapitre, et plus précisément au lemme 3.4, on a montré pour tout $\varepsilon > 0$, et pour tout entier a sans facteur carré et premier à p l'égalité :

$$|\mathcal{B}_p(a)| = \frac{x^3 \lambda(a) r(p)}{a^2 p^3} + O(x^{2+\varepsilon} p^{-1} + x^{1+\varepsilon} + x^{\varepsilon} p),$$

où λ est une fonction multiplicative vérifiant pour tout q premier ;

$$\lambda(q) = 2q - 1.$$

Les conditions d'application du théorème A2 sont vérifiées pour $\kappa = 2$, et ce théorème fournit la majoration :

$$|\mathcal{H}_p| \leq 2e^{2\gamma} \frac{x^3 r(p)}{p^3} \prod_{q<z} \left(1 - \frac{\lambda(q)}{q^2}\right) \left(1 + O\left(\frac{1}{\log z}\right)\right)$$
$$+ \sum_{a<z^2} 3^{\nu(a)} \mu^2(a) \left(\frac{x^{2+\varepsilon}}{p} + x^{1+\varepsilon} + x^{\varepsilon} p \right),$$

ce qui après un petit calcul, correspond au résultat annoncé.

En reportant ce résultat dans (6.14), et en choisissant $z = z_p = x^{3/2-\varepsilon} p^{-1}$, de telle sorte que les erreurs soient petites en moyenne, puis en appliquant le lemme 1.3.2 pour estimer le terme principal, on a la majoration :

$$T_4 \leq 2x^3 \int_{x^{1-\varepsilon}}^{P} \frac{dt}{t \log^2(x^{3/2-\varepsilon} t^{-1})} + O\left(\frac{x^3}{\log^2 x}\right).$$

Un calcul direct de cette intégrale donne après avoir posé $P = x^{\tau}$:

$$T_4 \leq 2\frac{x^3}{\log x} \left(\frac{1}{(3/2-\tau)} - 2 \right) + O\left(\frac{\varepsilon x^3}{\log x}\right).$$

En comparant avec (6.12), cela impose pour τ:

$$\left(\frac{2}{(3/2-\tau)} - 4 \right) \geq 2 - \varepsilon,$$

ε pouvant être pris aussi petit que l'on veut, on obtient donc

$$\tau \geq 7/6.$$

6.5. Un résultat en quatre variables.

On montre ici le théorème 3 bis concernant le polynôme $f(t_1,t_2,t_3,t_4) = 1+t_1^4+t_2^4+t_3^5+t_4^6$, en suivant une démarche analogue à celle des précédents paragraphes.
La somme d'exponentielles cruciale liée à ce problème, est la suivante :

$$S(p,h_1,h_2,h_3,h_4) = \sum_{\substack{0\le u_1,u_2,u_3,u_4<p \\ 1+u_1^4+u_2^4+u_3^5+u_4^6\equiv 0 \pmod p}} e\left(\frac{h_1u_1+h_2u_2+h_3u_3+h_4u_4}{p}\right).$$

En profitant des travaux de Laumon [Lau] sur les sommes d'exponentielles le long d'hypersurfaces diagonales, on montre le :

LEMME 6.4. *Les 4 assertions suivantes sont vérifiées :*

i) $S(p,0,0,0,0) = \rho(p) = p^3 + O(p^{5/2})$,

ii) si $h_1h_2 \equiv 0 \pmod p$, *et si* $(p,h_1,h_2,h_3,h_4) = 1$, *on a alors l'inégalité :* $S(p,h_1,h_2,h_3,h_4) = O(p^{3/2})$,

iii) si $(h_1^4+h_2^4,p) = 1$, *alors* $S(p,h_1,h_2,h_3,h_4) = O(p^{3/2})$,

iv) Si $h_1 \not\equiv 0 \pmod p$, *et si* $h_1^4+h_2^4 \equiv 0 \pmod p$, *alors* $S(p,h_1,h_2,h_3,h_4) = O(p^2)$.

Preuve du lemme 6.4.
Le polynôme f peut s'écrire sous la forme $f(t_1,t_2,t_3,t_4) = t_3^5 - g(t_1,t_2,t_4)$, où 5 est premier au degré de g. Ce polynôme est donc d'après Schmidt [Schm] absolument irréductible sur $\mathbf{Z}$ et ainsi, d'après le lemme B1, il est irréductible sur $\bar{\mathbf{F}}_p$ pour presque tout p.
On a donc d'après [L-W], $\rho(p) = p^3 + O(p^{5/2})$, ce qui finit la preuve du point (i).

Les points (ii) et (iii) se vérifient directement à partir du corollaire 4.3 de [Lau].

Preuve de (iv).
Le cas $h_1 \not\equiv 0$, et $h_1^4+h_2^4 \equiv 0 \pmod p$ est le cas critique pour lequel le résultat de Laumon n'est pas applicable.
On part de l'inégalité :

$$S(p,h_1,h_2,h_3,h_4) \le \sum_{0\le u_2<p} \left| \sum_{\substack{0\le u_1,u_3,u_4<p \\ 1+u_2^4+u_1^4+u_3^5+u_4^6\equiv 0 \pmod p}} e\left(\frac{h_1u_1+h_2u_2+h_3u_3+h_4u_4}{p}\right)\right|.$$

Pour tout $u_2 \bmod p$ les conditions d'application du lemme 2.3.2 (résultat de Hooley sur les sommes d'exponentielles le long de surfaces) sont vérifiées, et les constantes issues de ce lemme sont absolues, c'est à dire qu'elles ne dépendent ni de p ni de u_2. On a donc $S(p, h_1, h_2, h_3, h_4) = O(p^2)$.

Dans la démonstration du théorème 3 bis, interviendra la fonction définie pour tout couple (n_3, n_4) fixé, par :

$$r_{n_3,n_4}(p^\alpha) = |\{(u,v),\ 0 \le u, v < p^\alpha,\ (uv,p) = 1,\ 1+u_1^4+u_2^4+n_3^5+n_4^6 \equiv 0 \,(\mathrm{mod}\, p^\alpha)\}|.$$

On utilise alors le

LEMME 6.5. *Les deux assertions suivantes sont vérifiées :*

i) pour $\alpha \ge 2$, et $p > 3$, on a $r_{n_3,n_4}(p^\alpha) = p^{\alpha-1} r_{n_3,n_4}(p)$ et ainsi l'inégalité $r_{n_3,n_4}(p^\alpha) = O(p^\alpha)$.

ii) pour tout $\varepsilon > 0$, on a l'égalité :

$$\sum_{\substack{n_3 \sim x^{4/5} \\ n_4 \sim x^{2/3}}} r_{n_3,n_4}(p) = x^{22/15} p + O(x^\varepsilon p^{3/2} + \sqrt{p} x^{4/5+\varepsilon}).$$

preuve du lemme 6.5. Pour $p > 3$, on montre de la même manière avec un argument de descente, que l'on a $r_{n_3,n_4}(p^\alpha) = p r_{n_3,n_4}(p^{\alpha-1})$.
Pour montrer (ii), on développe tout en sommes d'exponentielles :

$$\sum_{\substack{n_3 \sim x^{4/5} \\ n_4 \sim x^{2/3}}} r_{n_3,n_4}(p) = \frac{1}{p^2} \sum_{0 \le g,h < p} \sum_{\substack{n_3 \sim x^{4/5} \\ n_4 \sim x^{2/3}}} e\left(\frac{-gn_3 - hn_4}{p}\right) S(p,0,0,g,h).$$

Le terme $g = h = 0$ fournit le terme principal : $\dfrac{r(p)}{p^2} x^{4/5+2/3} = x^{22/15} p + O(x^{22/15}\sqrt{p})$. Sinon pour $(g,h) \ne (0,0)$, on a d'après le lemme 6.5, l'inégalité $S(p,0,0,g,h) = O(p^{3/2})$, et on termine comme dans les preuves des différents lemmes du chapitre 3.

Preuve du théorème 3 bis.
Il s'agit d'évaluer $\log(W_4(x))$, avec

$$\log(W_4(x)) = \sum_{\substack{p_1,p_2 \sim x \\ n_3 \sim x^{4/5} \\ n_4 \sim x^{2/3}}} \log(1 + p_1^4 + p_2^4 + n_3^5 + n_4^6).$$

Un calcul direct utilisant le théorème des nombres premiers donne :

$$\log(W_4(x)) = \frac{4x^{52/15}}{\log x} + O\left(\frac{x^{26/15}}{(\log x)^2}\right). \tag{6.15}$$

On effectue ensuite le découpage :

$$\log(W_4(x)) = \sum_{p^\alpha < x^{1-\epsilon}} \log p |\mathcal{K}_{p^\alpha}| + \sum_{\substack{p^\alpha > x^{1-\epsilon}, \alpha \geq 2 \\ p < x \log^{-3} x}} \log p |\mathcal{K}_{p^\alpha}|$$

$$= \sum_{\frac{x}{\log^2 x} < p < P_1} \log p |\mathcal{K}_p| + W_4, \tag{6.16}$$

par définition, et avec

$$\mathcal{K}_{p^\alpha} = \{(p_1, p_2, n_3, n_4),\ p_1, p_2 \sim x,\ n_3 \sim x^{4/5}, n_4 \sim x^{2/3},$$
$$1 + p_1^4 + p_2^4 + n_3^5 + n_4^6 \equiv 0 \pmod{p^\alpha}\}.$$

On cherche $P_1 = x^\lambda$ le plus grand possible tel que

$$\log(W_4(x)) - W_1 - W_2 - W_3 \gg \frac{x^{52/15}}{\log x}.$$

La quantité W_1 s'évalue à l'aide de l'assertion (ii) du lemme 4.1. On part de l'égalité :

$$W_1 = \sum_{n_3, n_4 \sim x} \sum_{p^\alpha < x^{1-\epsilon}} \log p |\mathcal{K}_{p^\alpha}(n_3, n_4),|$$

avec

$$\mathcal{K}_{p^\alpha}(n_3, n_4) = \{p_1, p_2 \sim x,\ 1 + p_1^4 + p_2^4 + n_3^5 + n_4^6 \equiv 0 \pmod{p^\alpha}\}.$$

D'après le lemme 4.1, pour n_3 et n_4 fixés, on a :

$$\sum_{p^\alpha < x^{1-\epsilon}} |\mathcal{K}_{p^\alpha}(n_3, n_4)| \log p = \frac{x}{\log^2(x)} \sum_{p^\alpha < x^{1-\epsilon}} \frac{r_{n_3, n_4}(p^\alpha) \log p}{\varphi(p^\alpha)^2} + O\left(\frac{x^2}{\log^2 x}\right). \tag{6.17}$$

La constante du $O\left(\dfrac{x^3}{\log^2 x}\right)$ devrait *a priori* dépendre de n_3 et de n_4, mais ce n'est pas le cas. En effet, dans la preuve du lemme 4.1, le seul moment où intervient le polynôme est quand il faut majorer la somme $\displaystyle\sum_{\substack{0<u<m \\ (u,m)=1}} \left(\frac{\sigma_{f_u}(m)}{\varphi(m)}\right)^2$, où dans notre situation

$$\sigma_{f_u}(m) = |\{0 \leq v < m,\ 1 + n_3^5 + n_4^6 + u^4 + v^4 \equiv 0 \pmod{m}\}|,$$

et ainsi $\sigma_{f_u}(m) \leq 4^{\omega(m)}$.

D'après le point (i) du lemme 6.5, la contribution à (6.17) des termes en $\alpha \geq 2$ est négligeable. Pour $\alpha = 1$, on somme (6.17) sur n_3, n_4, puis on applique le point (ii) du lemme 6.5, et on obtient pour W_1 :

$$W_1 = \frac{x^{52/15}}{\log x}(1 - \varepsilon) + O\left(\frac{x^{52/15}}{\log^2 x}\right). \tag{6.18}$$

Pour estimer W_2, on reprend l'écriture ci-dessus :

$$|\mathcal{K}_{p^\alpha}| \ll \sum_{p_2\sim x, n_3\sim x^{4/5}, n_4\sim x^{2/3}} \sum_{\substack{0\le u<p^\alpha \\ 1+p_2^4+n_3^5+n_4^6+u^4\equiv 0 \pmod{p^\alpha}}} \sum_{\substack{p_1\sim x \\ p_1\equiv u \pmod{p^\alpha}}} 1.$$

Le nombre de solutions u est au plus 4 quand $p > 3$, et on a ainsi la majoration :

$$|\mathcal{K}_{p^\alpha}| \ll x^{1+4/5+2/3}\left(\frac{x}{p^\alpha}+1\right).$$

Pour tous ε et $\eta > 0$, il existe $h(\eta,\varepsilon) > 0$, tel qu'on ait la majoration $W_2 \ll x^{52/15-h(\eta,\varepsilon)}$.

Pour estimer W_3, on a recours au crible, ce qui nécessite une connaissance précise de :

$$|\mathcal{K}_p(a)| = |\{(n_1,n_2,n_3,n_4),\ n_1,n_2 \sim x^{3/2},\ n_3,n_4\sim x,\ (n_1n_2n_3n_4,p)=1,$$
$$n_1n_2 \equiv 0 \pmod a,\ 1+n_1^4+n_2^4+n_3^5+n_4^6 \equiv 0 \pmod p\}|.$$

En faisant les mêmes opérations que celles du paragraphe 6.3, on rencontre les sommes $S(p,h_1,h_2,h_3,h_4)$ présentées au début de ce paragraphe. En injectant le lemme 6.4 dans la méthode suivie pour établir les résultats du chapitre 3, on a :

$$|\mathcal{K}_p(a)| = \frac{x^{52/15}\rho(p)\lambda(u)}{a^2p^4} + R(a,p),$$

où le terme d'erreur $R(a,p)$ est évalué en moyenne (à cause du cas particulier $h_1^4+h_2^4 \equiv 0 \pmod p$), de la même façon que le terme d'erreur du lemme 3.2.3 (concernant les polynômes homogènes). On obtient l'inégalité :

$$\sum_{\substack{a<A\\p<P}} R(a,p) \ll x^\varepsilon AP^{5/2} + Ax^{1+\varepsilon}P^{3/2} + Ax^{2+\varepsilon}P^{1/2} + Ax^{14/5+\varepsilon}P^{-1/2}.$$

Grâce à ceci, nous sommes en mesure d'obtenir une majoration de $|\mathcal{K}_p|$, et ainsi de W_3. En posant alors $P_1 = x^\Lambda$ on arrive à :

$$W_3 \le \frac{x^{52/15}}{\log x}\frac{8}{5}\left\{\frac{1}{(26/15-5\Lambda/4)} - \frac{60}{29} + \varepsilon\right\}.$$

A partir de cette majoration on en déduit que $\log(W_4(x)) - W_1 - W_2 - W_3 > 0$ lorsque $\lambda < \dfrac{16248}{13725}$, ce qui finit la preuve du théorème 3 bis.

Remarques.
Le résultat de Laumon qui est la clé du lemme 6.5 concerne en fait les majorations de sommes d'exponentielles de la forme :

$$\sum_{1+c_1x^{d_1}+\ldots+c_mx^{d_m}} e\left(\frac{a_1x_1+\ldots+xa_mx_m}{p}\right),$$

et il donne la majoration espérée $O(p^{\frac{m-1}{2}})$ pour quasiment tous les a_i.

Cependant, il n'est pas toujours aisé de traiter à part d'une manière satisfaisante les sommes sur les $(a_1, ..., a_m)$ exclus.
Le polynôme f a été choisi pour éviter les situations critiques suivantes :

- sommes de plus de 3 termes de même puissance $1 + x_1^d + x_2^d + x_3^d + x_4^{d'}$.

- certaines sommes de 2 termes de puissance impaire comme par exemple $1 + x_1^3 + x_2^3 + x_3^4 + x_4^5$, les a_i exclus sont alors ceux vérifiant $a_1^3 - a_2^3 \equiv 0 \pmod p$ et la contribution des $a_1 = a_2$ est importante. Cependant, il faut remarquer que le polynôme $1 + x_1^3 + 2x_2^3 + x_3^4 + x_4^5$ marche, car les a_i exclus sont alors ceux vérifiant $a_1^3 - 2a_2^3 \equiv 0 \pmod p$, et comme l'équation $x^3 - 2y^3 = 0$ n'a pas de solution entière, le nombre de p tels que $a_1^3 - 2a_2^3 \equiv 0 \pmod p$ est inférieur à $\tau(a_1^3 - 2a_2^3)$, ce qui est assez petit.

On n'a pas tenu non plus à étudier les sommes de carrés comme par exemple $1 + x_1^2 + x_2^2 + x_3^3 + x_4^4$, car cette somme peut être traitée différement : en utilisant le procédé de Plaksin développé au paragraphe 2.2 pour le polynôme $1 + x_1^2 + x_2^2$, on peut transformer cette somme en somme d'exponentielles d'une fraction rationnelle sur trois variables, et si cette méthode aboutit, elle pourra s'appliquer au polynôme $1 + n_1^2 + n_2^2 + n_3^3 + n_4^3$.

Les résultats de Laumon s'appliquent facilement lorsque tous les x_i ont un exposant différent $1 + x_1^{d_1} + x_2^{d_2} + x_3^{d_3} + x_4^{d_4}$, avec $d_1 < d_2 < d_3 < d_4$. Mais on a préféré donner un même poids aux variables p_1, p_2, afin d'appliquer les théorèmes de répartition en moyenne des nombres premiers dans les progressions arithmétiques, sur une zone de $\mathcal{K}_p$ la plus grande possible.

Chapitre 7
Preuve du théorème 4

Ce chapitre est consacré à la preuve du théorème 4 concernant le polynôme $f(x,y) = x^2+y^2+1$. On reprend le système de poids de Friedlander [Fr2] présenté dans la première partie de la thèse c'est à dire les poids :

$$g(p_1,p_2) = \sharp\{(m,n),\ p_1^2+p_2^2+1 = mn,\ P^+(mn) < y,\ N_1 < n < N_2,\ et\ p|n \Rightarrow p > z\}$$

avec $N_1 = x^{1+\delta}$, $N_2 = x^{1+2\delta}$, $\delta > 0$ et $z \geq 1$.

Si on écrit $z = x^\beta$, le nombre $p_1^2+p_2^2+1$ a alors au plus $\frac{2}{\beta}$ facteurs premiers supérieurs à z, et ainsi $g(p_1,p_2) \leq 2^{\frac{2}{\beta}}$. À partir de ceci, on a la minoration :

$$\Psi(x,y) \geq \sum_{\substack{p_1,p_2\sim x \\ g(p_1,p_2)>0}} 1 \gg_\beta \sum_{p_1,p_2\sim x} g(p_1,p_2).$$

Il suffit d'établir une minoration de $\sum_{p_1,p_2\sim x} g(p_1,p_2)$, et on part alors de l'égalité :

$$\begin{aligned}
\sum_{p_1,p_2\sim x} g(p_1,p_2) &= \sum_{\substack{P^+(mn)<y \\ N_1<n<N_2 \\ p|n\Rightarrow p>z}} |\{(p_1,p_2),\ p_1,p_2\sim x,\ p_1^2+p_2^2+1 = mn\}| \\
&\geq \sum_{\substack{P^+(m)<y \\ N_1<n<N_2 \\ p|n\Rightarrow p>z}} |\{(p_1,p_2),\ p_1,p_2\sim x,\ p_1^2+p_2^2+1 = mn\}| \\
&\quad - \sum_{\substack{P^+(n)\geq y \\ N_1<n<N_2 \\ p|n\Rightarrow p>z}} |\{(p_1,p_2),\ p_1,p_2\sim x,\ p_1^2+p_2^2+1 = mn\}| \\
&\geq S_1 - S_2, \qquad (7.1)
\end{aligned}$$

par définition.

Pour estimer S_1, on crible les $\dfrac{p_1^2+p_2^2+1}{m}$. Comme $m \leq x^{1-\delta}$, et que z est très petit, on pourra utiliser le point (ii) du lemme 4.1, et ainsi obtenir une minoration très précise.

La quantité S_2 sera majorée par des méthodes de cribles pour détecter les p_1p_2, et on utilisera alors le lemme 3.2.2.

Certains points de la démonstration sont quasiment identiques à ceux qui ont servi à la preuve du théorème 2 de la première partie de la thèse, et ne seront donc pas détaillés dans ce chapitre.

7.1. Évaluation de S_1.

Dans cette partie, on montre le lemme suivant :

LEMME 7.1. *Pour $x^{\delta/2} \geq D > z \geq 2$, et pour tout $\varepsilon > 0$, on a la minoration :*

$$\begin{aligned} S_1 \geq{}& \frac{x^2}{(\log x)^2}\left(1-\log\left(\frac{\log x}{\log y}\right)\right)\log\left(\frac{N_2}{N_1}\right) \\ &\times \frac{e^{-\gamma}}{\log z} f\left(\frac{\log D}{\log z}\right)\left(1+O(\delta)+O_\delta\left(\frac{1}{\log z}\right)\right) \\ &+ O\left(\frac{\varepsilon x^2}{(\log x)^2}+\frac{x^2}{(\log x)^3}\right), \end{aligned}$$

où f est la fonction de minoration de crible linéaire.

Preuve du lemme 7.1.
En reprenant la définition de S_1 donnée dans (7.1), on a l'égalité :

$$S_1 = \sum_{\substack{\frac{8x^2}{N_2}<m<\frac{2x^2}{N_1} \\ P^+(m)<y}} |\{(p_1,p_2),\ p_1,p_2 \sim x,\ p_1^2+p_2^2+1 \equiv 0 \bmod m \text{ et } p|\frac{p_1^2+p_2^2+1}{m} \Rightarrow r > z\}|.$$

Comme dans la première partie de la thèse, on utilise les poids $(\lambda)^-$ de Rosser-Iwaniec correspondant à un crible de niveau D. On pose $P(z) = \prod_{p<z} p$. À partir des poids $(\lambda)^-$, et en reprenant les notations des chapitres 4 et 5, on a la minoration :

$$\begin{aligned} S_1 &\geq \sum_{\substack{\frac{8x}{N_2}\leq m\leq\frac{2x}{N_1} \\ P^+(m)<y}} \sum_{\substack{d<D \\ d|P(z)}} \lambda_d^- |\{(p_1,p_2),\ p_1,p_2 \sim x,\ p_1^2+p_2^2+1 \equiv 0 \bmod md\}| \\ &\geq \sum_{\substack{\frac{8x^2}{N_2}\leq m\leq\frac{2x^2}{N_1} \\ P^+(m)<y}} \sum_{\substack{d<D \\ d|P(z)}} \lambda_d^- \frac{r(md)}{\varphi(md)^2}|\mathcal{E}| + O\left(\sum_{\frac{8x^2}{N_2}\leq m\leq\frac{2x^2}{N_1}} \sum_{\substack{d<D \\ d|P(z)}} \left||\mathcal{E}_{md}| - \frac{r(md)}{\varphi(md)^2}|\mathcal{E}|\right|\right) \\ &(7.2) \geq TP + E, \end{aligned}$$

par définition.

• *Majoration du terme d'erreur.*
On commence par regrouper les variables m et d :

$$\begin{aligned} E &= \sum_{\frac{8x^2}{N_2}\leq m\leq\frac{2x^2}{N_1}} \sum_{\substack{d<D \\ d|P(z)}} \left||\mathcal{E}_{md}| - \frac{r(md)}{\varphi(md)^2}|\mathcal{E}|\right| \\ &\leq \sum_{m\leq\frac{2x^2D}{N_1}} \tau(m)\left||\mathcal{E}_m| - \frac{\rho(m)}{\varphi(m)^2}|\mathcal{E}|\right|. \end{aligned}$$

On ne peut pas majorer $\tau(m)$ par x^{ϵ}, puis appliquer le point (ii) du lemme 4.1, car on obtiendrait alors un $O(x^{2+\epsilon}(\log x)^{-100})$, ce qui n'est pas suffisant. On commence donc par appliquer l'inégalité de Cauchy-Schwarz :

$$E \leq \left(\sum_{m \leq \frac{2x^2 D}{N_1}} \tau(m)^2 \left| |\mathcal{E}_m| - \frac{r(m)}{\varphi(m)^2} |\mathcal{E}| \right| \right)^{1/2} \left(\sum_{m \leq \frac{2x^2 D}{N_1}} \left| |\mathcal{E}_m| - \frac{r(m)}{\varphi(m)^2} |\mathcal{E}| \right| \right)^{1/2}.$$

En choisissant $D \leq x^{\delta/2}$, ce qui donne $\dfrac{Dx^2}{N_1} = x^{1-\delta/2}$ et on peut alors appliquer le lemme 4.1 pour majorer le deuxième terme du produit du membre de droite par un $O\left(\dfrac{x}{(\log x)^{10}}\right)$.
Sinon, on majore directement le premier terme. En effet, on a les inégalités :

$$\begin{aligned} |\mathcal{E}_m| &= \sum_{\substack{0<u,v<m \\ (uv,m)=1 \\ u^2+v^2+1 \equiv 0 \bmod m}} \left(\sum_{\substack{p_1 \sim x \\ p_1 \equiv u \bmod m}} 1 \right) \left(\sum_{\substack{p_2 \sim x \\ p_2 \equiv v \bmod m}} 1 \right) \\ &\ll \frac{x^2 \tau(m)}{m}, \end{aligned}$$

et ainsi le premier terme est $\ll x \left(\sum_{m \leq \frac{2x^2 D}{N_1}} \dfrac{\tau^3(m)}{m} \right)^{1/2} \ll x \log^6 x.$

En tenant compte de toutes ces majorations, on obtient :

$$E \ll \frac{x^2}{(\log x)^3}. \tag{7.3}$$

• *Évaluation du terme principal.*
D'après (7.2), on a :

$$TP = |\mathcal{E}| \sum_{\substack{\frac{8x^2}{N_2} \leq m \leq \frac{2x^2}{N_1} \\ P^+(m) < y}} \sum_{\substack{d<D \\ d \mid P(z)}} \lambda_d^- \frac{r(dm)}{\varphi(md)^2}$$

où, d'après le théorème des nombres premiers, on a : $|\mathcal{E}| = \dfrac{x^2}{(\log x)^2} + O\left(\dfrac{x^2}{(\log x)^3}\right)$.

Pour m fixé, la fonction multiplicative ω_m définie par :

$$\omega_m(p) = \begin{cases} 1 & \text{si } p|m, \\ \dfrac{r(p)}{\varphi(p)^2} & \text{si } p \not| m, \end{cases}$$

est une fonction de crible vérifiant les conditions d'applications du théorème A1, et en appliquant ce résultat, on a l'inégalité :

$$TP \geq \frac{x^2}{(\log x)^2} \sum_{\substack{\frac{8\pi^2}{N_2}<m<\frac{2\pi^2}{N_1} \\ P^+(m)<y}} \frac{r(m)}{\varphi(m)^2} \prod_{\substack{p<z \\ (p,m)=1}} \left(1-\frac{r(p)}{\varphi(p)^2}\right) \prod_{\substack{p<z \\ p|m}} \left(1-\frac{1}{p}\right) \left(f\left(\frac{\log D}{\log z}\right)-\varepsilon\right)$$

$$\geq \frac{x^2}{(\log x)^2} \left(f\left(\frac{\log D}{\log z}\right)-\varepsilon\right) \prod_{p<z} \left(1-\frac{r(p)}{\varphi(p)^2}\right)$$

$$(7.4) \quad \times \sum_{\substack{\frac{8\pi^2}{N_2}<m<\frac{2\pi^2}{N_1} \\ P^+(m)<y}} \frac{r(m)}{\varphi(m)^2} \prod_{\substack{p<z \\ p|m}} \left(1-\frac{1}{p}\right) \left(1-\frac{r(p)}{\varphi(p)^2}\right)^{-1}.$$

Il s'agit alors d'évaluer la somme

$$\sum_{\frac{8\pi^2}{N_2}<m<\frac{2\pi^2}{N_1}} h_z(m),$$

avec

$$h_z(m) = \frac{r(m)}{\varphi(m)^2} \prod_{\substack{p|m \\ p<z}} \left(1-\frac{1}{p}\right) \left(1-\frac{r(p)}{\varphi(p)^2}\right)^{-1}.$$

Pour évaluer ceci, on reprend les arguments qui ont servi à l'estimation de $\sum \frac{\omega_z(m)}{m}$ lors de la preuve du théorème 2 de la première partie de la thèse. On écrit la série génératrice $\sum \dfrac{h_z(m)m}{m^s}$ sous la forme $\zeta(s)G(s)$, où G est holomorphe et bornée sur $\Re s > \sigma_0$, avec $\sigma_0 > 0$. En appliquant ensuite le procédé d'intégration complexe utilisant des propriétés classiques de la fonction ζ effectué lors de la preuve du lemme 2.1.1 (de la première partie de la thèse), on a l'égalité :

$$\sum_{\substack{\frac{8\pi^2}{N_2}\leq m\leq\frac{2\pi^2}{N_1} \\ P^+(m)<y}} h_z(m) = \tilde{G}(1)\log\frac{N_2}{N_1}\left(1-\log\frac{\log x}{\log y}\right)+O(\delta)+O_\delta\left(\frac{1}{\log x}\right),$$

avec

$$\tilde{G}(1) = \frac{1}{2}\prod_{2<p<z}\frac{\varphi(p)^3}{p(\varphi(p)^2-r(p))}.$$

n reportant ceci dans (7.4), puis en profitant de la simplification :

$$\tilde{G}(1)\prod_{p<z}\left(1-\frac{r(p)}{\varphi(p)^2}\right)=\prod_{p<z}\left(1-\frac{1}{p}\right),$$

et en appliquant la formule de Mertens, le terme principal TP vaut :

$$TP\geq\frac{x^2e^{-\gamma}}{\log(x)^2\log z}f\left(\frac{\log D}{\log z}\right)\log\frac{N_2}{N_1}\left(1-\log\frac{\log x}{\log y}\right)\left(1-\varepsilon+O(\delta)+O_\delta\left(\frac{1}{\log z}\right)\right)+E.$$

ce qui avec (7.4), finit la preuve du lemme 7.1.

7.2. Majoration de S_2.

On va montrer le résultat suivant :

LEMME 7.2. *Pour $z=x^{\frac{1}{\beta}}$, $0<\theta<\frac{1}{8}$, et pour tout $\varepsilon>0$, on a la majoration :*

$$S_2\leq\frac{2}{\theta^2}\frac{x^2}{(\log x)^2}\log\left(\frac{N_2}{N_1}\right)\frac{e^{-\gamma}}{\log z}\log\frac{\log x}{\log y}\left(1+O(\delta)+O_\delta\left(\frac{1}{\log z}\right)\right)+E,$$

où le terme d'erreur E vérifie :

$$E\ll\frac{x^2}{(\log x)^3}+O(x^{3/2+2\theta+2\delta+\varepsilon}).$$

Preuve du lemme 7.2.
On revient à la définition de S_2 donnée dans l'introduction de ce chapitre :

$$\begin{aligned}S_2&=\sum_{\substack{P^+(n)>y\\ p|n\Rightarrow p>z\\ N_1<n<N_2}}\ \sum_{\substack{p_1,p_2\sim x\\ p_1^2+p_2^2+1\equiv 0\ (\mathrm{mod}\ n)}}1\\&=\sum_{\substack{y<p<N_2\\ N_1<pd<N_2\\ (d,P(z))=1}}|\mathcal{F}_{pd}|+O(x^{2-\varepsilon}),\end{aligned}$$

avec les notations du paragraphe 5.5. Dans ce paragraphe, on a établi une majoration de $|\mathcal{F}_p|$ qui reposait sur le lemme 3.2.

En utilisant le lemme 3.2.3, à la place, et en faisant les mêmes démarches que celles effectuées au paragraphe 5.6, on obtient une majoration du même genre que celle donnée au lemme 5.7, mais valable pour des entiers m non nécessairement premiers. Grâce à ceci, on a l'inégalité :

$$\begin{aligned} S_2 &\leq \frac{2}{\theta^2}\frac{x^2}{(\log x)^2}\sum_{y<p<N_2}\frac{r(p)}{p^2}\sum_{\substack{N_1<pd<N_2\\(d,P(z))=1}}\frac{r(d)}{d^2}\prod_{\substack{q|d\\q<x^\theta}}\left(\frac{q}{\varphi(q)}\right)^2 \\ &\quad + O\left(\sum_{\substack{y<p<N_2\\N_1<pd<N_2\\(d,P(z))=1}}\left(\frac{x^{1+2\theta+\varepsilon}}{\sqrt{pd}}+x^{2\theta+\varepsilon}\sqrt{pd}\right)\right) \\ &\leq T+E_1+E_2, \end{aligned}$$

par définition.
La condition $(d,P(z))=1$ n'apporte qu'un facteur log, il est donc inutile d'en tenir compte pour le calcul du terme d'erreur. On commence par majorer l'erreur E_1 :

$$\begin{aligned} E_1 &= x^{1+2\theta+\varepsilon}\sum_{y<p<N_2}\frac{1}{\sqrt{p}}\sum_{\frac{N_1}{p}<n<\frac{N_2}{p}}\frac{1}{\sqrt{n}} \\ &\ll x^{1+2\theta+\varepsilon}\sqrt{N_2}\sum_{y<p<N_2}\frac{1}{p} \\ &\ll x^{\frac{3}{2}+2\theta+\delta+\varepsilon}. \end{aligned}$$

De même pour E_2, on a :

$$\begin{aligned} E_2 &= x^{2\theta+\varepsilon}\sum_{y<p<N_2}\sqrt{p}\sum_{\frac{N_1}{p}<n<\frac{N_2}{p}}\sqrt{n} \\ &\ll x^{\frac{3}{2}+2\theta+3\delta+\varepsilon}. \end{aligned}$$

Donc $E_1+E_2 \ll x^{2-\varepsilon}$ pour $\theta<1/8$, car δ est choisi arbitrairement petit.

Il reste à évaluer T :

$$\begin{aligned} T &= \frac{2}{\theta^2}\frac{x^2}{(\log x)^2}\sum_{\substack{y<p<N_2\\N_1<pd<N_2\\(d,P(z))=1}}\frac{r(p)}{p^2}\frac{r(d)}{d^2}\prod_{\substack{q|d\\q<x^\theta}}\left(\frac{q}{\varphi(q)}\right)^2 \\ &\leq \frac{2}{\theta^2}\frac{x^2}{(\log x)^2}\sum_{\substack{y<p<N_2\\N_1<pd<N_2\\(d,P(z))=1}}\frac{r(p)}{\varphi(p)^2}\frac{r(d)}{\varphi(d)^2}. \end{aligned}$$

Pour estimer les sommes ci-dessus, on a recours aux travaux de Friedlander [Fr1] sur les entiers sur les entiers sans petit et sans grand facteur premier. Plus précisement, on utilise le :

LEMME 7.2.1. *Pour $\varepsilon > 0$, $N = y^u = z^v$, avec $1 + \varepsilon < u < v < \varepsilon^{-1}$, on a:*

$$\sum_{\substack{n \leq N \\ p|n \Rightarrow z \leq p \leq y}} 1 = \frac{N}{\log z}\sigma(u,v) + O_\varepsilon\left(\frac{N}{(\log z)^2}\right),$$

avec $\sigma(u,v) = e^{-\gamma}\eta(u) + O(v^{-1}\log v)$, où η est la fonction continue définie par $\eta(u) = 1$ pour $0 < u \leq 1$, et $u\eta'(u) = -\eta(u-1)$.

Ce lemme résulte des théorèmes 1 et 5 de [Fr1], il s'applique très bien à la présente situation, le paramètre v correspond à $1/\beta$, β étant extrêmement petit. À partir de ceci, on établit le :

LEMME 7.2.2. *Pour $z = x^\beta$, avec $\beta = \delta^2$, et $y = x^\alpha$ avec $1/4 \leq \alpha \leq 2$ les égalités suivantes sont vérifiées :*

$$\sum_{\substack{N_1 < n < N_2 \\ (n,P(z))=1}} \frac{r(n)}{\varphi(n)^2} = \frac{e^{-\gamma}}{\log z}\log\left(\frac{N_2}{N_1}\right)\left\{1 + O(\delta) + O_\delta\left(\frac{1}{\log x}\right)\right\},$$

$$\sum_{\substack{N_1 < n < N_2 \\ p|n \Rightarrow z < p < y}} \frac{r(n)}{\varphi(n)^2} = \frac{e^{-\gamma}}{\log z}\log\left(\frac{N_2}{N_1}\right)\left\{1 - \log\left(\frac{\log x}{\log y}\right) + O(\delta) + O_\delta\left(\frac{1}{\log x}\right)\right\}.$$

preuve du lemme 7.2.2.
On commence par montrer que si d ne possède pas de petit facteur premier, la quantité $\dfrac{dr(d)}{\varphi(d)^2}$ vaut quasiment 1.
D'après le lemme 1.1.2, on a $r(p^k) = p^{k-1}r(p)$, pour $k \geq 1$, et pour $p > 2$, la fonction r vaut : $r(p) = \varphi(p) - 1 - 3\chi_4(p)$, ainsi on peut écrire la suite d'égalités :

$$\begin{aligned}\frac{dr(d)}{\varphi(d)^2} &= \prod_{p|d}\frac{pr(p)}{\varphi(p)^2} \\ &= \prod_{p|d}\left(1 + \frac{A(p)}{p}\right),\end{aligned}$$

avec $|A(p)| \leq 10$.

Pour x assez grand, et pour tout d tel que $(P(z), d) = 1$, on a l'encadrement :

$$\left(1 - \frac{10}{z}\right)^{1/\beta} \leq \frac{dr(d)}{\varphi(d)^2} \leq \left(1 + \frac{10}{z}\right)^{1/\beta},$$

et ainsi l'égalité : $\dfrac{dr(d)}{\varphi(d)^2} = 1 + O\left(\dfrac{1}{\beta z}\right)$, quand z tend vers $+\infty$.
On en déduit que :

$$\begin{aligned}\sum_{\substack{n<N \\ p|n \Rightarrow z<p<y}} \frac{nr(n)}{\varphi(n)^2} &= \sum_{\substack{n<N \\ p|n \Rightarrow z<p<y}} 1 + O\left(\frac{N}{\beta z}\right) \\ &= \frac{N}{\log z}\sigma\left(\frac{\log N}{\log y}, \frac{\log N}{\log z}\right) + O\left(\frac{N}{\beta(\log N)^2}\right),\end{aligned}$$

d'après le lemme 7.2.1.
Ensuite, en faisant une intégration par parties, on a l'égalité :

$$\begin{aligned}\sum_{\substack{n<N \\ p|n \Rightarrow z<p<y}} \frac{nr(n)}{\varphi(n)^2} &= \int_{N_1}^{N_2} \sigma\left(\frac{\log t}{\log y}, \frac{\log t}{\log z}\right) \frac{dt}{t \log z} + O_\delta\left(\frac{1}{\log x}\right) \\ &= \frac{e^{-\gamma}}{\log z} \log \frac{N_2}{N_1} \left[1 - \log\left(\frac{\log x}{\log y}\right) + O(\delta) + O_\delta\left(\frac{1}{\log x}\right)\right]\end{aligned}$$

ceci, car $1 \leq \dfrac{\log t}{\log y} \leq 2$, et pour $1 \leq u \leq 2$, on $\eta(u) = 1 - \log u$.
On a ainsi prouvé le deuxième résultat du lemme 7.2.2.
Le premier résultat s'obtient de la même manière.

Retour à la majoration de S_2.
Pour injecter le lemme 7.2.2 dans l'expression de T, on écrit :

$$\begin{aligned}T &= \frac{2}{\theta^2} \frac{x^2}{(\log x)^2} \sum_{\substack{y<p<N_2 \\ N_1<pd<N_2 \\ (d,P(z))=1}} \frac{r(pd)}{\varphi(pd)^2} \\ &= \frac{2}{\theta^2} \frac{x^2}{(\log x)^2} \left[\sum_{\substack{y<p<N_2 \\ (d,P(z))=1}} \frac{r(n)}{\varphi(n)^2} - \sum_{\substack{y<p<N_2 \\ p|n \Rightarrow z<p<y}} \frac{r(n)}{\varphi(n)^2}\right].\end{aligned}$$

Avec le lemme 7.2.2, et en tenant compte des différentes majorations des termes d'erreur obtenues précédement, on a la majoration :

$$\begin{aligned}S_2 \leq \frac{2}{\theta^2} \frac{x^2}{(\log x)^2} \log\left(\frac{N_2}{N_1}\right) \frac{e^{-\gamma}}{\log z} \log\left(\frac{\log x}{\log y}\right) \left(1 + O(\delta) + O_\delta\left(\frac{1}{\log z}\right)\right) \\ + O(x^{3/2+2\theta+3\delta+\varepsilon}),\end{aligned}$$

ce qui finit la preuve du lemme 7.2.

7.3. Conclusion.

En choisissant $\beta = \delta^2$, $D = x^{\delta/2}$, $f\left(\frac{\log D}{\log z}\right) = f\left(\frac{1}{2\delta}\right) \geq 1 - 10^{-8}$ dès que $\delta < 1/20$

D'après les lemmes 7.1 et 7.2, pour $\theta < 1/8$, et en posant $y = x^\alpha$, on a :

$$S_1 - S_2 \geq \frac{x^2}{(\log x)^2} \log \frac{N_2}{N_1} \frac{e^{-\gamma}}{\log z}(1 - 10^{-8}) \left[\left(1 - \log \frac{1}{\alpha}\right) - \frac{2}{\theta^2} \log(1/\alpha)\right]$$
$$\times \left\{1 + O_\delta\left(\frac{1}{\log x}\right) + O(\delta)\right\}$$
$$+ O\left(\frac{\varepsilon x^2 \log x + x^2}{(\log x)^3}\right).$$

Cette minoration est valable dès que

$$(1 - \log(1/\alpha)) - \frac{2}{\theta^2} \log(1/\alpha) > 0$$

c'est à dire, pour $\theta < 1/4$, $\alpha > \dfrac{1}{\exp \frac{1}{33}} = 0,97...$

Chapitre 8
Nombres presque premiers représentés par des polynômes

Ce chapitre est consacré à la preuve du théorème 5. Le polynôme f est un polynôme irréductible, en deux variables de degré 3, dont les coefficients sont premiers entre eux, et vérifiant l'hypothèse (H2).
La démonstration repose sur le travail de Richert suivant (cf [H-R] th 9.3 p. 253) :

LEMME 8.1. *Soit $\mathcal{A}$ une collection d'entiers pouvant contenir des répétitions, de cardinal X. Soit $\mathcal{P}$ un ensemble de nombres premiers. On adopte les notations standards suivantes :*

$$\mathcal{A}_d = \{a \in \mathcal{A},\ a \equiv 0 \pmod d\}.$$

On suppose que l'on a les égalités :

$$|\mathcal{A}_d| = \frac{X\omega(d)}{d} + R_d,$$

où ω est une fonction multiplicative .

On suppose que les conditions sont vérifiées :

(Ω_1) *Il existe $A_1 \geq 1$, tel que* $0 \leq \dfrac{\omega(p)}{p} \leq 1 - \dfrac{1}{A_1}$.

($\Omega_2^*(1)$) *Il existe A_2 tel que pour $2 \leq v \leq w$, on ait :*

$$-A_2 \log\log(3X) \leq \sum_{v \leq p < w} \frac{\omega(p)}{p} \log p - \log\frac{w}{v} \leq A_2.$$

(Ω_3) *Pour tous $X^{1/v} \leq y$, avec $v > 0$, il existe A_3 tel que*

$$\sum_{\substack{X^{1/v} \leq p < y \\ p \in \mathcal{P}}} |\mathcal{A}_{p^2}| \leq A_3(v) \left(\frac{X}{\log^2 X}\right).$$

($R(1,\alpha)$) *On suppose qu'il existe A_4, A_5 tels que*

$$\sum_{\substack{d < \frac{X^\alpha}{(\log X)^{A_4}} \\ p|d \Rightarrow p \in \mathcal{P}}} \mu^2(d) 3^{\nu(d)} |R_d| \leq A_5 \frac{X}{\log^2 X}.$$

Pour tout entier r, on définit la suite Λ_r par :

$$\Lambda_r = r + 1 - \frac{\log 4}{(1 + 3^{-r}) \log r}.$$

On suppose que pour tout $a \in \mathcal{A}$, on ait $p|a \Rightarrow p \in \mathcal{P}$.

Soit δ vérifiant $0 < \delta \leq 2/3$, et soit $r \geq 2$ assez grand pour que $|a| \leq X^{\alpha(\Lambda_r - \delta)}$ pour tout $a \in \mathcal{A}$.

On a alors pour $X \geq X_0 = X_0(r, \delta)$:

$$|\{P_r,\ P_r \in \mathcal{A}\}| \geq \frac{\delta}{\alpha} \prod_p \frac{\left(1 - \frac{\omega(p)}{p}\right)}{\left(1 - \frac{1}{p}\right)} \frac{X}{\log X}.$$

De plus, si $q = q(P_r)$ est le plus petit facteur premier de P_r, alors pour tout P_r compté ci dessus, on a $q(P_r) \geq X^{\alpha/4}$.

On a préféré prendre comme condition (Ω_3) celle donnée par Greaves dans [G3], qui correspond mieux à notre situation, les autres conditions (Ω_1), $(\Omega_2^*(1))$, $R(1, \alpha)$ se rencontrent dans tous les problèmes de crible.
Pour la preuve du théorème 5, on choisit

$$\mathcal{A} = \{f(x_1, x_2),\ x_1, x_2 \sim x\},$$

les $f(x_1, x_2)$ étant comptés avec d'éventuelles répétitions, on a ainsi $X = x^2$.
D'après le lemme 3.1, pour tout entier d sans facteur carré, on a l'égalité :

$$\mathcal{A}_d = X \frac{\rho(d)}{d^2} + R_d,$$

avec $R_d = O\left(\frac{x^{1+\varepsilon}}{\sqrt{d}} + x^{\varepsilon}\sqrt{d}\right)$.
Les conditions (Ω_1) et (Ω_2^*) sont vérifiées d'après le lemme 1.3.1, et la ligne (1.1).
Au vu de la majoration de R_d donnée ci-dessus, la condition $R(1, \alpha)$ est vérifiée pour $\alpha < 2/3 - \varepsilon$.
Greaves a montré dans [G3] que (Ω_3) était vérifiée pour $y < x$. Il reste donc à prouver que pour $y < x^2$, on ait :

$$\sum_{x^{1-\varepsilon} < p < y} |\mathcal{A}_{p^2}| \ll \frac{X}{\log^2 X}.$$

Ceci a déja été fait dans le paragraphe 5.3 lors de la majoration de R_3. Enfin pour $r = 3$, Λ_3 convient et on a le résultat annoncé avec $\delta = 0.533...$

Chapitre 9
Entiers ayant peu de facteurs premiers distincts représentés par des polynômes en deux variables pris en des valeurs premières

Maintenant, f est un polynôme irréductible de degré d supérieur à 3, en deux variables, dont les coefficients sont premiers entre eux et vérifiant l'hypothèse (H2). Pour tout entier n, on note $\omega(n)$, le nombre de facteurs premiers distincts de n.

9.1. Les poids de Richert.

Le principe de la preuve du théorème 7 consiste à combiner un crible pour détecter les p_1p_2, au système de poids de Richert et d'utiliser les résultats des précédents chapitres pour mener à bien cette démarche.
La collection d'entiers liée à ce problème, est $\mathcal{A} = \{f(p_1,p_2),\ p_1,p_2 \sim x\}$, avec d'éventuelles répétitions. On a alors l'égalité :

$$X = |\mathcal{A}| = \frac{x^2}{\log^2 x} + O\left(\frac{x^2}{\log^3 x}\right).$$

On prend pour $\mathcal{P}$, l'ensemble de tous les nombres premiers. Les poids de Richert sont alors les suivants (cf [H-R] p. 242) :

$$w_p(n) = \begin{cases} \lambda\left(1 - u\frac{\log p}{\log X}\right) & \text{si } X^{1/v} \le p < X^{1/u},\ p|n \\ 0 & \text{sinon ,} \end{cases}$$

où $u < v$, λ sont des paramètres à optimiser. On étudie alors :

$$(9.1) W(\mathcal{A},u,v,\lambda) = \sum_{\substack{a\in\mathcal{A} \\ p|a\Rightarrow p>X^{1/v}}} \left(1 - \sum_{X^{1/v}<p<X^{1/u}} w_p(a)\right)$$

$$= S(\mathcal{A},X^{1/v}) - \lambda \sum_{X^{1/v}<p<X^{1/u}} \left(1 - u\frac{\log p}{\log X}\right) S(\mathcal{A}_p,X^{1/v}),$$

où, selon les notations standards,

$$S(\mathcal{A},X^{1/v}) = |\{a\in\mathcal{A},\ p|a \Rightarrow p > X^{1/v}\}|.$$

Soit $a \in \mathcal{A}$ ayant une contribution positive dans (9.1). Cet entier a vérifie alors clairement le point (i) du théorème 7, et sa contribution à (9.1) est inférieure à :

$$1 - \lambda\left(\omega(a) - u\frac{\log|a|}{\log X}\right) \le 1 - \lambda(\omega(a) - \frac{ud}{2}).$$

Ainsi tout $a \in \mathcal{A}$ ayant une contribution positive dans (9.1) vérifie

$$(9.2) \qquad \omega(a) < \lambda^{-1} + \frac{ud}{2}.$$

Parmi ceux-ci, Greaves a montré dans [G3] p. 5 que le nombre de ceux qui ne vérifiaient pas (ii) est un $O(X(\log X)^{-2})$.

Les quantités $S(\mathcal{A}, X^{1/v})$ et $S(\mathcal{A}_p, X^{1/v})$ intervenant dans (9.1), sont estimées, lorsque p est petit, avec le lemme 4.1, comme l'avait fait Greaves dans [G3].

Quand p est grand on utilise des méthodes de crible pour détecter à la fois les $p_1 p_2$, et les diviseurs de $f(p_1, p_2)$ afin d'augmenter la taille du α vérifiant la condition $R(1, \alpha)$ énoncée au lemme 8.1. On passe du niveau $\alpha = 1/2$ de Greaves à $\alpha = 2/3$. Cependant nous ne sommes pas en mesure de vérifier une hypothèse (Ω_3) correspondante c'est pourquoi le théorème 5 n'apprend rien de nouveau sur $\Omega(n)$, et nous devons nous contenter de l'assertion (ii).

9.2. Minoration de $S(\mathcal{A}, X^{1/v})$.

D'après le point (i) du lemme 4.1, on a l'égalité :

$$|\mathcal{A}_d| = X \frac{r(d)}{\varphi(d)^2} + R_d,$$

avec

$$\sum_{d < X^{1/2-\varepsilon}} 3^{\omega(d)} \mu^2(d) R_d \ll \frac{X}{(\log X)^2}.$$

D'après le lemme 1.3.4, les conditions (1) et (2) du théorème A1 sont vérifiées, et en appliquant ce résultat, on a

LEMME 9.1. *On a la minoration*

$$S(\mathcal{A}, X^{1/v}) \geq \frac{CX}{\log X} \left(v e^{-\gamma} f\left(\frac{\log X^{1/2-\varepsilon}}{\log X^{1/v}} \right) + O\left(\frac{1}{\log X} \right) \right).$$

où C est le produit convergent

$$C = \prod_q \left(1 - \frac{r(q)}{\varphi(q)^2}\right) \left(1 - \frac{1}{q}\right)^{-1}.$$

9.3. Première majoration de $S(\mathcal{A}_p, X^{1/v})$.

On procède comme au paragraphe 9.2, mais en utilisant bien sûr le crible majorant au lieu du crible minorant.
On obtient ainsi le

LEMME 9.2. *En écrivant $p = X^{\mu}$, on a la majoration pour tout $\varepsilon > 0$ et pour $p < X^{1/2-2\varepsilon}$:*

$$S(\mathcal{A}_p, X^{1/v}) \leq \frac{CX}{\log X} \frac{r(p)}{\varphi(p)^2} \left(\frac{2}{(1/2 - \mu - \varepsilon)} + O\left(\frac{1}{\log X} \right) \right) + O\left(\frac{X^{1-\varepsilon}}{p^2} \right).$$

9.4. Deuxième majorations de $S(\mathcal{A}_p, X^{1/v})$.

Pour être en mesure d'utiliser du crible, on part de l'inégalité :

$$S(\mathcal{A}_p, X^{1/v}) \leq \sum_{\substack{n_1,n_2\sim x \\ f(n_1,n_2)\equiv 0 \pmod p \\ q|n_1n_2 \Rightarrow q>z \\ q|f(n_1,n_2)\Rightarrow q>X^{1/v}}} 1.$$

On a vu au chapitre 3 que les ensembles $\mathcal{C}_m(a)$ définis dans (3.4), vérifiaient, d'après le lemme 3.3, l'égalité, pour a et m des entiers sans facteur carré et liés par l'écriture $a = a_1\delta$, $m = m_1\delta$, avec $(a_1, m_1) = 1$:

$$|\mathcal{C}_m(a)| = x^2 \frac{\rho(m_1)\lambda(a_1)\rho_0(\delta)}{a_1^2 m_1^2 \delta^2} + R(a,m),$$

le terme d'erreur vérifiant la majoration :

$$R(a,m) = O\left(\frac{x^{1+\varepsilon}}{\delta\sqrt{m_1}} + x^{\varepsilon}\sqrt{m_1}\right).$$

Les variables a et m ne sont pas indépendantes. Elles *sont liées* par la fonction de crible ω définie par :

$$\frac{\omega(a,m)}{am} = \frac{\rho(m_1)\lambda(a_1)\rho_0(\delta)}{a_1^2 m_1^2 \delta^2}.$$

On commence comme dans la preuve du théorème 2 de la partie I de la thèse concernant le polynôme n^2+1, par les cribler faiblement ensemble, en utilisant un lemme fondamental correspondant à un crible de dimension 3, on a alors le

LEMME 9.3. *Pour $U \geq u \geq 2$, on pose $s = \dfrac{\log U}{\log u}$. Soient a_1 et a_2 deux entiers sans facteur carré, premiers à p, et ayant tous leurs facteurs supérieurs à u. On définit les quantités*

$$S_p(a_1,a_2,u) = \sum_{\substack{n_1,n_2\sim x \\ n_1n_2\equiv 0 \pmod{a_2} \\ f(n_1,n_2)\equiv 0 \pmod{a_1p} \\ q|n_1n_2f(n_1,n_2)\Rightarrow q>u}} 1.$$

On a alors l'égalité :

$$S_p(a_1,a_2,u) = x^2 V(u)\frac{\omega(a_1,a_2)}{a_1a_2}\frac{\rho(p)}{p^2}\left\{1 + O\left(\frac{e^{-s}}{(\log U)^{1/3}}\right)\right\}$$
$$+ O\left(\sum_{\substack{m|P(u) \\ m<U}} \mu^2(m) \sum_{m_1m_2=m} R(a_1m_1, a_2m_2)\right),$$

avec

$$V(u) = \prod_{q<u} \left(1 - \frac{\Omega(q)}{q}\right),$$

et d'après le principe d'inclusion-exclusion la fonction Ω *vérifie :*

$$\frac{\Omega(q)}{q} = \frac{\omega(1,q)}{q} + \frac{\omega(q,1)}{q} - \frac{\omega(q,q)}{q^2},$$

avec $\omega(q,1) = \dfrac{\rho(q)}{q}$, $\omega(1,q) = \dfrac{\lambda(q)}{q}$, $\omega(q,q) = \rho_0(q)$.

Au paragraphe 3.3, on a observé l'égalité : $\rho_0(p) = \rho(p) - r(p)$. On a donc d'après les valeurs de Ω données au lemme 9.3, les égalités :

$$V(u) = \prod_{q<u}\left(1 - \frac{\Omega(q)}{q}\right) = \prod_{q<u}\left(1 - \frac{r(q)}{q^2} - \frac{\lambda(q)}{q^2}\right) = \prod_{q<u}\left(1 - \frac{r(q)}{\varphi(q)^2}\right)\left(1 - \frac{1}{q}\right)^2,$$

ce qui nous permettra de comparer facilement le résultat que l'on obtiendra avec le lemme 9.2.
On utilise les poids de Rosser-Iwaniec cf [I1] correspondant à des cribles linéaires pour détecter les facteurs premiers de $f(n_1,n_2)$ supérieurs à u.
Plus précisemment ces poids sont définis par $\lambda_1 = 1$, $\lambda_m = 0$, si $m > M_1$, ou si m a un facteur carré et pour $m = p_1 \ldots p_r$, avec $p_1 > \ldots > p_r$ on impose :

$$\lambda_m = \begin{cases} (-1)^r & \text{si } p_1 \ldots p_{2\ell} p_{2\ell+1}^3 < M_1 \text{ pour tout } 0 \le \ell \le (r-1)/2, \\ 0 & \text{sinon.} \end{cases}$$

Par contre pour cribler $n_1 n_2$, on utilise les poids μ de Selberg propres au crible de dimension deux dont la fonction de crible correspondante est
$\omega(q,1) = \frac{\lambda(q)}{q} = 2 - 1/q$. Ils vérifient entre autre les propriétés suivantes : $\mu_1 = 1$, $\mu_m = 0$ si m a un facteur carré, ou si $m > M_2$. (Pour une définition plus précise, on peut consulter le livre d'Halberstam et Richert [H-R] lignes (1.3), (1.4) p. 98)

En notant $P(z_1,z_2)$ le produit $\displaystyle\prod_{z_1 \le p < z_2} p$, on a l'inégalité :

$$S(\mathcal{A}_p, X^{1/v}) \le \sum_{\substack{n_1,n_2 \sim x \\ f(n_1,n_2) \equiv 0 \pmod p \\ q \mid n_1 n_2 f(n_1,n_2) \Rightarrow q > u}} \left(\sum_{\substack{m_1 \mid P(u, X^{1/v}) \\ m_1 \mid f(n_1,n_2)}} \lambda_{m_1}\right)\left(\sum_{\substack{m_2 \mid P(u,z) \\ m_2 \mid n_1 n_2}} \mu_{m_2}\right)^2$$

$$\le \sum_{\substack{m_1 \mid P(u,X^{1/v}) \\ m_2, m_2' \mid P(u,z)}} \lambda_{m_1} \mu_{m_2} \mu_{m_2'} S_p(m_1, [m_2, m_2'], u).$$

On applique alors le lemme 9.3 :

$$S(\mathcal{A}_p, X^{1/v}) \leq x^2 \frac{\rho(p)}{p^2} V(u) \left\{ 1 + O\left(\frac{e^{-s}}{\log U} \right) \right\}$$
$$\times \sum_{\substack{m_1 | P(u, X^{1/v}) \\ m_2, m_2' | P(u,z)}} \lambda_{m_1} \mu_{m_2} \mu_{m_2'} \frac{\omega(m_1, [m_2, m_2'])}{m_1 [m_2, m_2']}$$
$$+ O\Bigg(\sum_{\substack{\ell | P(u) \\ \ell < U}} \sum_{\ell_1 \ell_2 = \ell} \sum_{\substack{m_1 | P(u, X^{1/v}) \\ m_1 < M_1 \\ m_2, m_2' | P(u,z) \\ m_2, m_2' < M_2}} |\lambda_{m_1} \mu_{m_2} \mu_{m_2'}| R(p m_1 \ell_1, [m_2, m_2'] \ell_2) \Bigg).$$

Le terme d'erreur est alors un $O(\sqrt{p} M_1^{3/2} M_2^{1+\varepsilon})$.
Le pgcd des quantités m_1 et $[m_2, m_2'']$ a tous ses facteurs premiers supérieurs à u ; les raisonnements qui ont servi à rendre les variables m_1 et m_2 indépendantes dans la fin du paragraphe 2.7 de la preuve du théorème 2 de la première partie de la thèse, sont applicables ici, et en choisissant $u = X^{\varepsilon^2}$, $U = X^{\varepsilon}$, on a l'égalité :

$$S(\mathcal{A}_p, X^{1/v}) \leq x^2 \frac{\rho(p)}{p^2} V(u) \left\{ 1 + O\left(\frac{e^{-s}}{\log U} \right) \right\}$$
$$\times \sum_{\substack{m_1 | P(u, X^{1/v}) \\ m_1 < M_1}} \frac{\lambda_{m_1} \omega(m_1, 1)}{m_1} \sum_{\substack{m_2, m_2' | P(u,z) \\ m_2, m_2' < M_2}} \frac{\mu_{m_2} \mu_{m_2'} \omega(1, [m_2, m_2'])}{[m_2, m_2']}$$
$$+ O(X^{1-\varepsilon^2/2}),$$

le reste $O(X^{1-\varepsilon^2/2})$ provient des erreurs *de nettoyage de pgcd* occasionnées par le processus de séparation des variables.
On applique ensuite les résultats d'Iwaniec pour la somme sur m_1, c'est à dire le théorème A1, ceux de Selberg, énoncés au théorème A2, pour les sommes sur m_2, m_2' pour obtenir :

$$S(\mathcal{A}_p, X^{1/v}) \leq x^2 \frac{\rho(p)}{p^2} V(u) \prod_{u < q < X^{1/v}} \left(1 - \frac{r(q)}{\varphi(q)^2} \right) \prod_{u < p < z} \left(1 - \frac{1}{p^2} \right)$$
$$\times \left(F\left(\frac{\log M_1}{\log X^{1/v}} \right) \sigma_2 \left(\frac{\log M_2}{\log z} \right)^{-1} + O_\varepsilon \left(\frac{1}{\log X} \right) \right)$$
$$+ O\left(\frac{X^{1-\varepsilon}}{p} + M_1^{3/2} M_2 \sqrt{p} X^{\varepsilon} \right).$$

Comme le produit $C = \prod_p \left(1 - \frac{r(p)}{\varphi(p)^2} \right) \left(1 - \frac{1}{p} \right)^{-1}$ est convergent, on a la

majoration :

$$S(\mathcal{A}_p, X^{1/v}) \leq x^2 \frac{\rho(p)}{p^2} \frac{e^{-3\gamma} C}{\log M_1 \log^2 M_2} \times \left(F\left(\frac{\log M_1}{\log X^{1/v}}\right) \frac{1}{\sigma_2\left(\frac{\log M_2}{\log z}\right)} + O_\varepsilon\left(\frac{1}{\log X}\right)\right) + O\left(\frac{X^{1-\varepsilon}}{p} + M_1^{3/2} M_2 \sqrt{p} X^\varepsilon\right).$$

Lorsque $\dfrac{\log M_1}{\log X^{1/v}} \leq 3$, et $\dfrac{\log M_2}{\log z} \leq \alpha_2 = 5.3577..$, le terme principal vaut :

$$x^2 \frac{r(p)}{\varphi(p)^2} \frac{4C}{\log M_1 \log^2 M_2}.$$

Pour faciliter les calculs on choisit M_1 en fonction de p, on écrit $M_1 = M/p$, avec M vérifiant $M^{3/2} M_2 \ll X^{1-\varepsilon}$.
Si on écrit $M_2 = X^\alpha$, $p = X^\mu$, alors $M_2 \ll X^{2/3-2\alpha/3-\mu-\varepsilon}$, et le terme principal devient :

$$\frac{x^2}{(\log X)^3} \frac{r(p)}{\varphi(p)^2} \frac{4C}{\alpha^2(2/3 - 2\alpha/3 - \mu)}.$$

En optimisant par rapport à α cette dernière formule, on obtient le

LEMME 9.4. *On a la majoration :*

$$S(\mathcal{A}_p, X^{1/v}) \leq \frac{x^2 C}{(\log X)^3} \frac{\rho(p)}{p^2} \left(\frac{12}{(2/3-\mu)^3} + O\left(\frac{1}{\log X}\right)\right) + O\left(\frac{X^{1-\varepsilon}}{p}\right),$$

où on a posé $p = X^\mu$ *et* μ *vérifie alors* $0 < \mu < 2/3$.

9.5. Comparaison des deux méthodes.

On commence par remarquer que pour tout $\varepsilon > 0$, on a les inégalités :

$$(2-\varepsilon)\log x < \log X < (2+\varepsilon)\log x...$$

Un calcul direct tenant compte de ceci, montre que la majoration du lemme 9.3 devient plus fine que celle du lemme 9.2 pour $p > X^{\mu_0}$, où μ_0 est solution de l'équation

$$54\mu^3 - 108\mu^2 - 9\mu + 49/2 = 0,$$

c'est à dire $\mu_0 = 0.496728234..$
Cette valeur de μ_0 est très proche de $1/2$ qui est la limite de la première méthode. Richert, pour détecter les P_r du lemme 8.1, avait choisi $u = u_r = \dfrac{1+3^{-r}}{\alpha}$, (ici $\alpha = 1/2$). Lorsque $r < 4$, $\mu_0 > 1/u$, et le lemme 9.2 est toujours moins bon. Ce lemme devient vraiment intéressant quand r est grand, c'est à dire lorsque le degré de f est grand.

9.6. Conclusion

En tenant compte des calculs du paragraphe 9.5, on écrit :

$$\sum_{X^{1/v}<p<X^{1/u}} \left(1-\frac{u\log p}{\log X}\right) S(\mathcal{A}_p, X^{1/v}) = S_1 + S_2,$$

avec

$$S_1 = \sum_{X^{1/v}<p<X^{\mu_0}} \left(1-\frac{u\log p}{\log X}\right) S(\mathcal{A}_p, X^{1/v}),$$

et

$$S_2 = \sum_{X^{\mu_0}<p<X^{1/u}} \left(1-\frac{u\log p}{\log X}\right) S(\mathcal{A}_p, X^{1/v}).$$

On majore alors S_1 avec le lemme 9.2, et S_2 avec le lemme 9.4. En utilisant le corollaire 1.3.4 pour les fonctions r, on obtient alors

$$S_1 + S_2 \leq \frac{XC}{\log X}\int_{1/v}^{\mu_0} \frac{2(1-u\mu)}{(1/2-\mu)\mu}d\mu + \frac{XC}{\log X}\int_{\mu_0}^{1/u} \frac{3(1-u\mu)}{\mu(2/3-\mu)^3}d\mu + O\left(\frac{X}{\log^2 X} + X^{1-\varepsilon}\right).$$

Toutes ces intégrales se calculent et nous avoı

$$S_1 + S_2 \leq (H_1(u,v) + H_2(u))\frac{CX}{\log X} + O\left(X^{1-\varepsilon} + \frac{X}{\log^2 X}\right),$$

avec

$$H_1(u,v) = 4\log(\mu_0 v) + 2(2-u)[\log(1/2-1/v) - \log(1/2-\mu_0)],$$

et

$$H_2(u) = \frac{81}{8}\log(1/u) - \frac{81}{8}\log\mu_0 - \frac{81}{8}\log(2/3-1/u) + \frac{81}{8}\log(2/3-\mu_0) + \frac{27}{(8/3-4/u)} - \frac{27}{(8/3-4\mu_0)} + \frac{3}{2}(3/2-u)\left[\frac{1}{(2/3-1/u)^2} - \frac{1}{(2/3-\mu_0)^2}\right].$$

Pour des facilités de calculs nous choisissons $v = 8$, et on a d'après le lemme 9.1 l'inégalité :

$$S(\mathcal{A}, X^{1/v}) \leq \frac{X}{\log X} Ce^{-\gamma} 8f(4) + O(\frac{X}{\log^2 X}) = \frac{CX}{\log X}\left(4\log 3 + O\left(\frac{1}{\log X}\right)\right),$$

ce qui fournit la minoration :

$$W(\mathcal{A}, u, v, \lambda) \geq \frac{CX}{\log X}(4\log 3 - \lambda(H_1(u,8) + H_2(u))(1 + O((\log X)^{-1}).$$

En prenant $u = 12/7$, on a $\lambda^{-1} > 5.2779..$, et en reportant ceci dans (9.2), on obtient le théorème 7.

9.7. Cas des polynômes homogènes.

Dans ce paragraphe, on suppose que f est un polynôme homogène, et on reprend les arguments des précédents paragraphes pour montrer le théorème 6.
Grâce à leur homogénéité, ces polynômes vérifient la condition (Ω_3) du lemme 8.1, Greaves a en effet montré dans [G4] en raisonnant en terme de réseaux l'inégalité

$$\sum_{X^{1/v}<p<X^{1-\epsilon}} |\mathcal{A}_{p^2}| = O\left(\frac{X}{(\log X)^2}\right).$$

C'est pourquoi, le théorème 6 donne un résultat sur le nombre de facteurs premiers de $f(p_1, p_2)$ et non seulement sur $\omega(f(p_1, p_2))$.

L'ingrédient principal des lemme 9.1, et 9.2 était le lemme 4.1, résultant du théorème de Barban-Halberstam-Richert, et ces deux résultats restent valables lorsque le polynôme est homogène.

On a ainsi les deux inégalités en reprenant les notations des précédents paragraphes :

$$S(\mathcal{A}, X^{1/v}) \geq \frac{CX}{\log X}\left(ve^{-\gamma} f\left(\frac{\log X^{1/2-\epsilon}}{\log X^{1/v}}\right) + O\left(\frac{1}{\log X}\right)\right),$$

et en écrivant $p = X^{\mu}$:

$$S(\mathcal{A}_p, X^{1/v}) \leq \frac{CX}{\log X}\frac{r(p)}{\varphi(p)^2}\left(\frac{2}{(1/2-\mu-\epsilon)} + O\left(\frac{1}{\log X}\right)\right).$$

En faisant ensuite les mêmes opérations que celles du paragraphe 9.4, mais en utilisant le lemme 3.3.1 à la place du lemme 3.3, on a la majoration :

$$S(\mathcal{A}_p, X^{1/v}) \leq \frac{CX}{\log X}\frac{\rho(p)}{p^2}\left(\frac{27}{4(1-\epsilon-\mu)^3} + O\left(\frac{1}{\log X}\right)\right).$$

Cette dernière majoration est plus précise que la précédente, lorsque :

$$\frac{27}{4(1-\mu)^3} \leq \frac{2}{1/2-\mu},$$

c'est à dire pour $\mu \geq 7/4 - \frac{3\sqrt{3}}{4} = \mu_0$. ($\mu_0$ est solution de l'équation : $16(1-t)^3 - 27(1-2t) = 0$ $\mu_0 = 0.4509..$).
En faisant alors des calculs analogues à ceux effectués au paragraphe 9.6, on a :

$$\begin{aligned}\sum_{X^{1/v}<p<X^{1/u}} \left(1 - u\frac{\log p}{\log X}\right) S(\mathcal{A}_p, X^{1/v}) &\leq \frac{XC}{\log X} \\ &\times \left\{\int_{1/v}^{\mu_0} \frac{2(1-u\mu)}{(1/2-\mu)\mu} d\mu + \int_{\mu_0}^{1/u} \frac{27(1-u\mu)}{(1-\mu)^3} d\mu\right\} \\ &+ O\left(\frac{X}{\log^2 X} + X^{1-\epsilon}\right) \\ &\leq \frac{XC}{\log X}\left(H_3(u,v) + H_4(u) + O\left(\frac{1}{\log X}\right)\right),\end{aligned}$$

par définition.

Un calcul direct donne (on rappelle que $\mu_0 = 7/4 - \frac{3\sqrt{3}}{4}$) :

$$H_3(u,v) = 4\log(\mu_0 v) + 2(2-u)\left(\log(1/2 - 1/v) - \log(1/2 - \mu_0)\right),$$

et

$$\begin{aligned} H_4(u) = 27/4\Big\{ &\log(1/u) - \log\mu_0 + \log(1-\mu_0) \\ &+ \frac{1}{(1-1/u)} - \frac{1}{1-\mu_0} \\ &+ \frac{1-u}{2}\left(\frac{1}{(1-1/u)^2} - \frac{1}{(1-\mu_0)^2}\right)\Big\}. \end{aligned}$$

En prenant $v = 8$, on a la minoration :

$$W(\mathcal{A}, u, v, \lambda) \geq \frac{CX}{\log X}\left(4\log 3 - \lambda(H_3(u,8) + H_4(u)) + O\left(\frac{1}{\log X}\right)\right).$$

Pour $u = 4/3$, on obtient $\lambda^{-1} = 8.238...$, et ainsi :

$$\Omega(f(p_1, p_2)) < 2d/3 + 8.24.$$

9.8. Remarque.

Il est certainement possible d'obtenir des améliorations des théorèmes 6 et 7, en utilisant des systèmes de poids plus récents et donc plus performants que ceux de Richert, tels par exemple les poids de Laborde, ou de Greaves, etc. Mais ces systèmes de poids se combinent bien plus difficilement avec le crible de Selberg que ceux de Richert que nous avons utilisés, et leur application aurait considérablement compliqué l'élaboration, puis la présentation de ce chapitre.

ANNEXE A

LES CRIBLES DE SELBERG ET DE ROSSER-IWANIEC

Soit $\mathcal{A}$ une collection finie d'entiers strictement positifs pouvant contenir des répétitions, soit $\mathcal{P}$ un ensemble de nombres premiers.

On définit les ensembles $\mathcal{A}_d = \{a \in \mathcal{A},\ a \equiv 0 \pmod d\}$,
et pour $z \geq 1$, $S(\mathcal{A}, \mathcal{P}, z) = |\{a \in \mathcal{A},\ p \in \mathcal{P},\ p|a \Rightarrow p \geq z\}|$.
On note encore $P(z) = \prod_{p<z,\ p\in\mathcal{P}} p$.

On suppose que les $\mathcal{A}_d$ peuvent s'écrire sous la forme :

$$|\mathcal{A}_d| = \frac{\omega(d)}{d} X + R_d,$$

où ω est multiplicative, et $0 \leq \omega(p) < p$, pour $p \in \mathcal{P}$.

On suppose qu'il existe $\kappa \geq 1$, et K et L tels que les deux inégalités suivantes soient vérifiées :

$$(1) \qquad \prod_{\substack{w<p<z \\ p\in\mathcal{P}}} \left(1 - \frac{\omega(p)}{p}\right)^{-1} \leq \left(\frac{\log z}{\log w}\right)^{\kappa} \left(1 + \frac{K}{\log w}\right),$$

$$(2) \qquad \sum_{\substack{w\leq p<z \\ p\in\mathcal{P}}} \sum_{\alpha\geq 2} \frac{\omega(p^\alpha)}{p^\alpha} \leq \frac{L}{\log 3w},$$

La constante κ est appelée la dimension du crible.
On définit encore $V(z) = \prod_{p<z,\ p\in\mathcal{P}} \left(1 - \frac{\omega(p)}{p}\right)$.

Pour $\kappa = 1$, le crible est alors un crible linéaire, et on a le résultat d'Iwaniec suivant ([I1] théorème 1) :

THÉORÈME A1. *Soient $0 < \varepsilon < 1/3$, $M > 1$, $N > 1$, $D = MN$. Si les hypothèses (1) et (2) sont vérifiées, alors pour tout $2 \leq z \leq D^{1/2}$, on a :*

$$S(\mathcal{A}, \mathcal{P}, z) \leq V(z)X\{F(s) + E(\varepsilon, D, K, L)\} + R^+(\mathcal{A}, M, N),$$

$$S(\mathcal{A}, \mathcal{P}, z) \geq V(z)X\{f(s) - E(\varepsilon, D, K, L)\} + R^-(\mathcal{A}, M, N),$$

avec $s = \dfrac{\log D}{\log z}$, $E(\varepsilon, D, K, L) \ll \varepsilon + \varepsilon^{-8} e^{K+L} (\log D)^{-1/3}$, *et pour* $\nu = \pm$,

$$R^\nu(\mathcal{A}, M, N) = \sum_{\ell < exp(8\varepsilon^{-3})} \sum_{\substack{m < M \\ m | P(z)}} \sum_{\substack{n < N \\ n | P(z)}} a^\nu_{m,\ell}(M, N, \varepsilon) b^\nu_{n,\ell}(M, N, \varepsilon) R_{mn}.$$

Les coefficients $a^\nu_{m,\ell}, b^\nu_{n,\ell}$ dépendent au plus de M et N et sont majorés par 1 en valeur absolue.

Les fonctions f et F sont déterminées par :

$uF(u) = 2e^\gamma$, $uf(u) = 0$ pour $0 < u \leq 2$,

$(uF(u))' = f(u-1)$, $(uf(u))' = F(u-1)$ pour $u \geq 2$.

Dans la thèse, on profite en fait à un seul moment (au paragraphe 1.3 de la première partie) de la présentation sous forme bilinéaire du terme d'erreur $R^\nu(\mathcal{A}, M, N)$. Dans les autres situations le théorème A2 que nous allons énoncer aurait suffi. Pour $\kappa > 1$, en fait, on sera toujours dans le cas $\kappa = 2$, le crible de Selberg fournit de bonnes majorations. On utilisera abondemment la majoration énoncée dans le théorème 6.3 p. 202 du livre de [H-R], que l'on rappelle donc ici :

THÉORÈME A2. *On suppose que pour $\kappa \geq 1$, les conditions (1) et (2) sont vérifiées. Alors pour $D \geq z \geq 2$, on a :*

$$S(\mathcal{A}, \mathcal{P}, z) \leq XV(z) \left\{ \frac{1}{\sigma_\kappa(s)} + O\left(\frac{K}{\log z} s^{2\kappa+1} \right) \right\} + \sum_{\substack{d < D \\ d | P(z)}} 3^{\nu(d)} |R_d|.$$

Les fonctions σ_κ sont définies de la manière suivante :

$\sigma_\kappa(u) = \dfrac{2^{-\kappa} e^{-\gamma\kappa}}{\Gamma(\kappa+1)} u^\kappa$ si $0 \leq u \leq 2$,

$(u^{-\kappa}\sigma_\kappa(u))' = -\kappa u^{-\kappa-1}\sigma_\kappa(u-2)$, pour $u > 2$,

et σ_κ est continue en $u = 2$.

ANNEXE B

QUELQUES RÉSULTATS DE GÉOMÉTRIE ALGÉBRIQUE.

Dans cette annexe, on donne quelques résultats de géométrie algébrique qui servent au chapitre 1 de la deuxième partie de la thèse. Les énoncés qui vont suivre sont loin d'être les plus généraux possibles, mais ils répondent aux besoins de cette thèse.

Sauf mention du contraire, tous les polynômes considérés sont à coefficients entiers.

Le problème rencontré dans de nombreuses étapes de cette thèse est de vérifier si certaines propriétés réalisées par des variétés ou des polynômes sur $\mathbf{Q}$ ou sur $\mathbf{Z}$ se conservent lorqu'on les réduit modulo p.
Le premier résultat concerne l'irréductibilité des polynômes, c'est le :

LEMME B1. *Soit f un polynôme en deux ou trois variables, irréductible sur $\mathbf{C}$, et à coefficients dans K, une extension algébrique de $\mathbf{Q}$. Soit O_K l'anneau des entiers de K, $\wp$ un idéal premier de O_K contenant p. Soit $\mathbf{F}_\wp$ le corps résiduel correspondant. On note encore $\bar{f}$ la réduction de f sur $\mathbf{F}_\wp$. Alors pour tout p sauf un nombre fini, $\bar{f}$ est irréductible sur $\bar{\mathbf{F}}_p$.*

Ce lemme résulte du théorème 2A et du corollaire 2B p. 190-193 de [Schm].

Les lemmes suivants sont plus géométriques et pour les énoncer on a besoin des notations suivantes
Soit f un polynôme n variables, soit F le polynôme homogène associé. Pour tout corps k, on note $\mathbf{P}_k^n$ l'espace projectif de dimension n sur k. On associe alors à F et f les variétés :

$$Y = \{(x_1, x_2, ..., x_n, t) \in \mathbf{P}_{\mathbf{Q}}^n,\ F(x_1, x_2, ..., x_n, t) = 0\},$$

et pour tout nombre premier p :

$$Y_p = \{(x_1, x_2, ..., x_n, t) \in \mathbf{P}_{\mathbf{F}_p}^n,\ F(x_1, x_2, ..., x_n, t) \equiv 0 \ (\mathrm{mod}\, p)\},$$

et

$$X_p = \{(x_1, x_2, ..., x_n) \in \mathbf{F}_p^n,\ f(x_1, x_2, ..., x_n) \equiv 0 \ (\mathrm{mod}\, p)\}.$$

On a alors le

LEMME B2. *Si Y est lisse sur $\mathbf{P}_{\mathbf{Q}}^n$, alors pour tout p sauf un nombre fini, Y_p la variété réduite de Y est lisse sur $\mathbf{P}_{\mathbf{F}_p}^n$, et X_p est lisse sur $\mathbf{F}_p$.*

On n'a besoin de ce résultat que dans les cas où f est un polynôme en au plus quatre variables, et on pourrait alors démontrer un résultat analogue sans passer par les polynômes homogènes, mais en raisonnant à partir des résultants de f et des dérivées partielles de f, mais les démonstrations sont alors assez longues, surtout dans le cas où f est un polynôme en trois variables et plus, alors que la géométrie algébrique fournit une démonstration directe.
On considère le morphisme :

$$\Psi : \tilde{Y} = Proj\,(\mathbf{Z}[X_1, ..., X_n, T]/(F)) \to Spec\mathbf{Z}.$$

Comme Y est lisse sur $\mathbf{Q}$, d'après la proposition 3.24 p. 31 de [M], il existe un ouvert V de $Spec\mathbf{Z}$, tel que $\Psi : \Psi^{-1}(V) \to V$ soit lisse. Comme tout ouvert de $SpecZ$ contient tous les nombres premiers sauf un nombre fini, il existe $P > 0$ tel que pour $p > P$, les courbes Y_p soient lisses sur $\mathbf{P}^n_{\mathbf{F}_p}$. Pour montrer que les courbes X_p sont alors lisses sur $\mathbf{F}^n_p$, on utilise la formule d'Euler. Pour $M = (x_1, ..., x_n, t) \in \mathbf{P}^n_{\mathbf{F}_p}$, on a l'égalité :

$$degF.F(M) = x_1 \frac{\partial F}{\partial x_1}(M) + ... + x_n \frac{\partial F}{\partial x_n}(M) + t\frac{\partial F}{\partial t}(M).$$

Si X_p n'était pas lisse sur $\mathbf{F}_p$, alors il existerait $(x_1, x_2, ..., x_n, 1) \in Y_p$ tel que :

$$\frac{\partial F}{\partial x_1}(x_1, ..., x_n, 1) = ... = \frac{\partial F}{\partial x_n}(x_1, ..., x_n, 1) = 0,$$

et $\frac{\partial F}{\partial t}(x_1, ..., x_n, 1) \neq 0$. Mais en reportant ceci dans la formule d'Euler, on obtient $F(x_1, ..., x_n, 1) \neq 0$, ce qui est absurde. Ceci finit la preuve du lemme B2.

Pour déterminer les valeurs des fonctions ρ étudiées dans la deuxième partie de la thèse, on utilise le :

LEMME B3. *Soient f et g deux polynômes en trois variables premiers entre eux. On a alors :*

$$|\{(x, y, z) \in \mathbf{F}^3_p,\ f(x, y, z) \equiv g(x, y, z) \equiv 0 \pmod p\}| = O(p),$$

la constante du O ne dépend que des degrés de f et g.

Ce résultat correspond à l'exercice 1.10 p. 368 de [Ha].

Le dernier résultat que l'on utilise est le

LEMME B4. *Soit f un polynôme en trois variables irréductible sur $\mathbf{F_p}$. Pour p assez grand, l'ensemble des points singuliers de la variété X_p associée à f est un $O(p)$, la constante du O, ne dépendant que du degré de f.*

On a l'inclusion :

$$S_p \subset \{(x,y,z) \in \mathbf{F_p^3},\ f(x,y,z) \equiv \frac{\partial f}{\partial x}(x,y,z) \equiv 0 \pmod{p}\}.$$

Le polynôme f étant irréductible, lorsque p est assez grand (pour que $\frac{\partial f}{\partial x}(x,y,z)$ ne soit pas identiquement nul), les polynômes f et $\frac{\partial f}{\partial x}(x,y,z)$ sont premiers entre eux. On applique alors le lemme B3 à ces deux polynômes.

BIBLIOGRAPHIE

[A] E. ARTIN : Theory of algebraic numbers, Göttingen (1959).

[Ba] A. BALOG : $p + a$ without large prime factors, Séminaire de Théorie des Nombres de Bordeaux 1983-1984 exposé 31.

[Bo] E. BOMBIERI : On exponential sums in finite fields, Amer. J. Math. 88 (1966), 71-105.

[B-F] J. BRÜDERN and E. FOUVRY : Lagrange Four Squares Theorem with almost Prime Variables, J. f. d. reine u. angew. Mathematik 454 (1994), 59-96.

[D] P. DELIGNE : Application de la formule des traces aux sommes trigonométriques, Séminaire de géométrie algébrique du Bois Marie-SGA 4 1/2, 168-232.

[D-I1] J-M. DESHOUILLERS and H. IWANIEC : On the greatest prime factor of $n^2 + 1$, Ann. Inst. Fourier. Grenoble 32, 4 (1982) 1-11.

[D-I2] J-M. DESHOUILLERS and H. IWANIEC : Kloosterman sums and Fourier coefficients of cusp forms, Inv. Math. 70 (1982), 219-288.

[E] P. ERDÖS : On the greatest prime factor of $\prod_{k=1}^{\infty} f(k)$, J. Lond. Math. Soc. 27 (1952) p. 379-384.

[Fo1] E. FOUVRY : Répartition des suites dans les progressions arithmétiques-Résultats du type Bombieri-Vinogradov avec exposant supérieur à 1/2, Thèse de Doctorat ès Sciences, Université de Bordeaux I (1981).

[Fo2] E. FOUVRY : Le problème des diviseurs de Titchmarsh, J. f. d. reine u. angew. Mathematik 356 (1985), 51-76.

[Fr1] J. B. FRIEDLANDER : Integers free from large and small primes, Proc. Math. Soc (3) 33 (1976), 565-576.

[Fr2] J. B. FRIEDLANDER : Shifted primes without large prime factors, Number Theory and applications (Banff, AB, 1988), 393-401.

[G1] G. GREAVES : The divisor-sum problem for binary cubic forms, Acta Arith. 27 (1970) 1-28.

[G2] G. GREAVES : Large prime factors of binary forms, J. Number Theory 3 (1971), 35-59, and corrigendum, ibid. 9 (1977), 561-562.

[G3] G. GREAVES : An application of a theorem of Barban, Davenport and Halberstam, Bull. London Math. Soc. 6 (1974), 1-9.

[G4] G. GREAVES : Power-free values of binary forms, Quart. J. Math. Oxford (2), 43 (1992), 45-65.

[H-R] H. HALBERSTAM and H.-E. RICHERT : Sieve methods, Academic Press, London 1974.

[Ha] R. HARTSHORNE : Algebraic Geometry, GTM 52, Springer Verlag.

[HB] D.-R. HEATH-BROWN : The square sieve and consecutive square-free numbers, Math. Ann. 266 (1984) No 3, 251-259.

[H1] C. HOOLEY : Applications of sieve methods to the theory of numbers, Cambridge University Press, London 1976.

[H2] C. HOOLEY : On the greatest prime factor of a cubic polynomial, J. f. d. reine u. angew. Mathematik. 304/304 (1978), 21-50.

[H3] C.HOOLEY : On exponential sums and certain of their applications, In : Journées Arithmétiques, London : Math. Soc. 1980 (Lecture Notes Series 56), 92-122.

[H] HUA LOO KENG : Introduction to number theory, Springer Verlag 1982.

[I1] H. IWANIEC : A new form of the error term in the linear sieve, Acta Arith. 37. (1980), 307-320.

[I2] H. IWANIEC : On the Brun-Titchmarsh theorem, J. Math. Soc. Japan vol 34 No 1 (1982), 95-123.

[K-L] N. M. KATZ et G. LAUMON : Transformation de Fourier et majoration de sommes exponentielles, Pub. Math. I.H.E.S No 62 (1985), 361-418.

[Lan] E. LANDAU : Elementary Number Theory, Chelsea, New-York (1958).

[L-W] S. LANG and A. Weil : Number of points on varieties in finite fields, Amer. J. Math. 76 (1954), 819-827.

[Lau] G. LAUMON : Majoration de sommes d'exponentielles attachées aux hypersurfaces diagonales, Ann. Scient. de l'école normale supérieure, 4ème série, t. 16, (1983), 1-58.

[M] MILNE : Etale Cohomology, Princeton (1980).

[N1] T. NAGELL : Généralisation d'un théorème de Tchebychev, J. de Mathématiques, 4 (1921) 343-356.

[N2] T. NAGELL : Introduction to number theory, New York 1951.

[Pl] V. A. PLAKSIN : An asymptotic formula for the number of solutions of a nonlinear equation for prime numbers, Math. USSR Izvestija 18 (1982), 275-348.

[Po] J. POMYKALA : On the greatest prime divisor of quadratic sequences, Séminaire de Théorie des Nombres, Bordeaux 3 (1991), 361-375.

[Schin] A. SCHINZEL : Two theorems of Gelfond and some of their applications, Acta Arith. 13 (1967), 177-236.

[Schm] W. M. SCHMIDT : Equations over finite fields, Lecture Notes in Mathematics 536, Springer Verlag, (Berlin-Heidelberg-New York, 1976).

[Si] J. H. SILVERMAN : Arithmetic of elliptic curves GTM 106.

[Sm] H. J. S. SMITH : Report on the theory of numbers, Chelsea, New-York, 1965.

[T1] G. TENENBAUM : Sur une question d'Erdös et Schinzel, II, Inv. Math. 99 (1990), 215-224.

[T2] G. TENENBAUM : Introduction à la théorie analytique et probabiliste des nombres, Revue de l'institut Elie Cartan 13, Département de Mathématiques de l'université de Nancy I (1990).

[W] D. WOLKE : Über die mittlere Verteilung der Werte zahlentheoretischer Funktionen auf Restklassen . 2, Math. Ann. 204 (1973), 145-153.