ACTA ARITHMETICA
LXXVIII.1 (1996)

Propriétés multiplicatives des valeurs de certains polynômes en deux variables

par

C. Dartyge (Nancy)

0. Introduction. Deshouillers et Iwaniec [D-I] ont démontré en 1982 que le plus grand facteur premier du produit $\prod_{x\le n\le 2x}(n^2+1)$ est supérieur à $x^{1.202}$ pour x assez grand, mais lorsque l'on remplace n par un nombre premier p, on n'est pas en mesure de trouver $\varepsilon>0$ tel que $P^+(\prod_{x\le p\le 2x}(p^2+1)) > x^{1+\varepsilon}$ quand $x\to\infty$, $P^+(m)$ étant le plus grand facteur premier de l'entier m, avec la convention $P^+(1)=0$. Hooley [H1] a montré en 1978 que sous l'hypothèse R^* de majoration de sommes courtes de Kloosterman, le plus grand facteur premier du produit $\prod_{n\le x}(n^3+2)$ est supérieur à $x^{31/30}$, pour x assez grand. Ce remarquable résultat est conditionnel, et sans l'hypothèse R^* on ne sait pas minorer le plus grand facteur premier du produit ci-dessus par $x^{1+\varepsilon}$.

L'objectif de ce travail est de montrer que ces inégalités sont vérifiées en moyenne et ainsi d'étudier les propriétés multiplicatives des valeurs de polynômes à coefficients entiers et en deux variables tels par exemple $f(p_1,p_2)=1+p_1^2+p_2^2$, ou $f(p_1,p_2)=1+p_1^3+p_2^3$, etc.

L'abord d'un tel problème passe par la mise en place d'estimations asymptotiques du cardinal d'ensembles de la forme

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

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 de Greaves [G3], 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 détectant les p_1p_2, et qui conduisent à des majorations de sommes d'exponentielles de la forme

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

avec la notation usuelle $e(x) = \exp(2i\pi x)$.

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 théorème suivant :

Théorème 1. *Soit f un polynôme irréductible, homogène, de degré $d \ge 2$, dont les coefficients sont premiers entre eux, et vérifiant l'hypothèse* (H1). *Pour tout $\lambda < 2 - 8/(d+7)$, on a l'inégalité*

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

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

$$C_p = \{(u,v) \in \mathbb{F}_p^2 : f(u,v) \equiv 0 \pmod p\}.$$

Plus précisement, pour $(g,h,t) \in \mathbb{Z}^3$, on définit les diviseurs de la courbe C_p suivants :

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

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

(H2) *Pour tout $t \in \mathbb{Z}$ et tous $(g,h) \in \mathbb{Z}^2$ tels que $(g,h,p) = 1$, on a $\deg D(g,h,t) = O(1)$, où 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 $f(x,y) = \sum_{k=0}^{d} c_k(ax+by+c)^k$.

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). *L'inégalité suivante est alors vérifiée* :

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

dès que

$$\lambda < \begin{cases} 36/35 & \text{si } d=2, \\ 20/19 & \text{si } d=3. \end{cases}$$

Ce résultat est une amélioration et une généralisation d'un résultat de Plaksin [P]. Celui-ci avait en effet obtenu pour le polynôme $f(p_1,p_2) = p_1^2+p_2^2+1$ un exposant $\lambda = 71/70$. Cette amélioration résulte du fait que les variables p_1p_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.

Dans l'esprit des travaux de Greaves ([G2], [G3]), et de Richert [H-R], nous nous sommes intéressé au problème de représentation de nombres presque premiers par des polynômes en deux variables. Pour $r \geq 1$, P_r désigne un entier ayant au plus r facteurs premiers. Nous montrons le

THÉORÈME 3. *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 [H-R]), que nous pouvons utiliser directement grâce aux lemmes intermédiaires qui ont servi à la preuve du théorème 2.

Nous regrettons que les théorèmes 2 et 3 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 s'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 crible pondéré de Richert qui est la clé de la preuve du théorème 3, et des estimations en moyenne des quantités $\mathcal{A}_m$ pour $m<x^{1-\varepsilon}$ 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 $m<x^{1-\varepsilon}$, à $m<x^{2-\varepsilon}$, lorsque f est un polynôme homogène, et à $m<x^{4/3-\varepsilon}$, 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 4. *Soit f un polynôme irréductible homogène en deux variables de degré d, dont les coefficients sont premiers entre eux. On a alors l'inégalité*

$$\left|\left\{(p_1,p_2)\sim x : \Omega(f(p_1,p_2))\le \frac{2d}{3}+8\right\}\right| \gg \frac{x^2}{\log^3 x},$$

où $\Omega(n)$ désigne le nombre de facteurs premiers de n.

Ce résultat est intéressant pour $2d/3+8<d+1$, c'est-à-dire pour $d\ge 22$. 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 termes 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 5. *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 :

$$\mathcal{E} = \{(p_1, p_2) : p_1, p_2 \sim x \text{ et vérifiant (i), (ii) et (iii)}\},$$

avec

(i) $p \mid f(p_1, p_2) \Rightarrow p > x^{1/4}$,
(ii) $p^2 \mid f(p_1, p_2) \Rightarrow p > x^{1-\varepsilon}$,
(iii) $\omega(f(p_1, p_2)) < k(d)$.

Lorsque $k(d) \geq 6d/7 + 6$, on a la minoration $|\mathcal{E}| \gg x^2/\log^3 x$.

Ce résultat apprend quelque-chose de nouveau pour $d > 30$, mais la remarque faite après le théorème 4 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 5 dit que $\omega(f(p_1, p_2)) \leq 862\ldots$

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.

Le premier chapitre de ce travail fournit des estimations de la fonction r, reprenant des travaux de Greaves sur ce sujet. Dans le deuxième, on donne des majorations de sommes d'exponentielles résultant des travaux de Weil qui seront reprises dans le chapitre trois où on établira des estimations asymptotiques des cardinaux d'ensembles du type

$$\{(n_1, n_2) : n_1, n_2 \sim x,\ n_1 n_2 \equiv 0 \pmod a,\ f(n_1, n_2) \equiv 0 \pmod m\},$$

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 $x^{1-\varepsilon}$. Les quantités $|\mathcal{A}_m|$ pour $m < x^{1-\varepsilon}$ sont estimées en moyenne dans le chapitre 4, à l'aide du théorème de Barban–Davenport–Halberstam.

Enfin, les derniers chapitres correspondent aux preuves des différents théorèmes annoncés.

Une telle démarche s'étend à des polynômes en trois variables et plus. Dans le cas des polynômes en 3 variables, les majorations de Hooley [H2] le long de surfaces de $\mathbb{F}_p$, obtenues à partir des travaux de Deligne, permettent d'avoir un résultat de caractère général, c'est-à-dire valable pour des

polynômes de $\mathbb{Z}[x_1, x_2, x_3]$ vérifiant des conditions du type les hypothèses (H1) et (H2). Le rajout d'une troisième variable rallonge cependant les différentes étapes des démonstrations. Cette méthode permet alors de montrer que pour de tels polynômes f de degré 3, il existe une proportion positive de triplets (p_1, p_2, n_3) compris entre x et $2x$, tels qu'on ait $P^+(f(p_1, p_2, n_3)) > x^{7/6}$. Dans le cas des polynômes en 4 variables et plus les travaux de Deligne ne sont pas tout à fait suffisants. Katz et Laumon [K-L] ont montré, pour presque tout k-uplet d'entiers $(h_1, \dots, h_k)$, la majoration suivante :

$$\sum_{\substack{u_1,\dots,u_k \bmod p \\ f(u_1,\dots,u_k)\equiv 0 \,(\mathrm{mod}\, p)}} e\left(\frac{h_1u_1 + \dots + h_ku_k}{p}\right) = O(p^{(k-1)/2}).$$

Ce résultat n'est pas applicable dans ce contexte, car les h_i exclus peuvent être très petits. Laumon [L] a cependant obtenu des majorations de sommes d'exponentielles le long d'hypersurfaces diagonales que l'on peut appliquer dans certains cas. On pourra trouver dans [D] un exposé détaillé de tout ceci.

Ce travail a été réalisé sous la direction du Professeur Etienne Fouvry. Je le remercie vivement pour les nombreuses suggestions qu'il a proposées.

1. Résultats préliminaires sur les fonctions r. La fonction r est jumelée avec la fonction ϱ définie par

$$\varrho(m) = |\{(u, v) : 0 \le u, v < m,\ f(u, v) \equiv 0 \pmod m\}|.$$

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.

1.1. *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 suivant :

LEMME 1.1. (i) *On a l'inégalité $\varrho(p) = O(p)$, où la constante du O ne dépend que du polynôme f.*

(ii) *Pour $Q > 2$, on a l'égalité*

$$\sum_{p<Q} \frac{\varrho(p)\log p}{p^2} = \log Q + O(1).$$

(iii) *Pour $\alpha \ge 3$, on a $\varrho(p^\alpha) = O(p^{\alpha+[\alpha(1-2/d)]})$, et pour $\alpha = 2$, on a*

$$\varrho(p^2) = O(p^2).$$

(iv) *La fonctions r associée vérifie des propriétés similaires.*

1.2. *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 $\mathbb{F}_p$, Weil a prouvé que $\varrho(p) = p+O(\sqrt{p})$. 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 $\mathbb{Q}$. Dans ce cas, il existe une extension algébrique K de $\mathbb{Q}$ dans laquelle f se factorise en produit de facteurs absolument irréductibles $f = g_1 \dots g_m$. Les coefficients de g_1 engendrent une extension $\mathbb{Q}(\theta_1)$ de $\mathbb{Q}$. Soit O_{θ_1} l'anneau des entiers de $\mathbb{Q}(\theta_1)$. On a le résultat ([G3]) suivant :

Lemme 1.2.1. *Pour tout p, sauf un nombre fini, on a*

$$\varrho(p) = ps_p + O(\sqrt{p}),$$

où s_p est le nombre d'idéaux premiers P de O_{θ_1} tels que $\mathrm{Norm}(P) = p$.

Ensuite, en utilisant le corollaire de Nagell [N1] du théorème des idéaux premiers, on a l'égalité

$$\sum_{p\le Q} \frac{s_p \log p}{p} = \log Q + O(1),$$

et ainsi,

$$\sum_{p\le Q} \frac{\varrho(p) \log p}{p^2} = \log Q + O(1). \tag{1.1}$$

Cette dernière égalité est une condition d'application des cribles de Selberg et de Rosser–Iwaniec.

Il reste encore à évaluer $\varrho(p^\alpha)$ pour $\alpha \ge 2$. On montre le lemme suivant :

Lemme 1.2.2. *Pour tout $\alpha \ge 2$, on a la majoration*

$$\varrho(p^\alpha) = O(\alpha p^{4\alpha/3}).$$

Les constantes implicites ne dépendent que de f.

Preuve du lemme 1.2.2. 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 $g(v) \equiv 0 \pmod{p^\alpha}$ 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 1.2.3. *Soit g un polynôme primitif de degré d et de discriminant D. La fonction $\sigma_g(n) = |\{0 \le u < n : g(u) \equiv 0 \pmod{n}\}|$ est multiplicative, et vérifie les propriétés suivantes* :

(i) *pour tout p premier, on a $\sigma_g(p) \leq d$,*
(ii) *si $p \nmid D$, alors pour tout $\alpha \geq 1$, on a l'égalité*

$$\sigma_g(p^\alpha) = \sigma_g(p),$$

(iii) *si $p \mid D$, et plus précisément si $p^\mu \parallel D$, 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 $a, b \bmod p^\alpha$ donnés, on définit les polynômes g_a et h_b par $g_a(t) = f(a,t)$, et $h_b(t) = f(t,a)$. On note $D(g_a)$, $D(h_b)$ leur discriminant respectif.

On part de l'égalité

$$\varrho(p^\alpha) = \sum_{0 \leq \beta \leq \alpha} \Psi(\beta),$$

avec

$$\Psi(\beta) = \sum_{\substack{0 \leq u,v < p^\alpha \\ f(u,v) \equiv 0 \,(\mathrm{mod}\, p^\alpha) \\ p^\beta = (D(g_u), D(h_v), p^\alpha)}} 1.$$

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

$$\Psi(\beta) \leq \sum_{\substack{0 \leq u < p^\alpha \\ D(g_u) \equiv 0 \,(\mathrm{mod}\, p^\beta)}} \sum_{\substack{0 \leq v < p^\alpha \\ D(h_v) \equiv 0 \,(\mathrm{mod}\, p^\beta)}} 1.$$

Les sommes sur u et sur v sont alors des $O(p^{\alpha-\beta})$, d'après le point (iv) du lemme 1.2.3 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

$$\Psi(\beta) \leq \sum_{\substack{0 \leq u < p^\alpha \\ p^\beta \parallel (D(g_u), p^\alpha)}} \sigma_{g_u}(p^\alpha) + \sum_{\substack{0 \leq v < p^\alpha \\ p^\beta \parallel (D(h_v), p^\alpha)}} \sigma_{h_v}(p^\alpha).$$

D'après les points (iii) et (iv) du lemme 1.2.3, 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 la preuve du lemme 1.2.2.

A partir des lemmes 1.2.1 et 1.2.2 et de l'égalité (1.1), nous avons facilement le résultat suivant :

COROLLAIRE 1.2.4. *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 $r(p^\alpha) = O(\alpha p^{4\alpha/3})$.*

2. Quelques résultats sur les sommes d'exponentielles. Dans ce paragraphe, on donne des estimations des sommes d'exponentielles que l'on rencontre lorsque l'on développe les conditions de congruences définissant les quantités $|\mathcal{A}_d|$ en série de Fourier.

Soit f un polynôme irréductible en deux variables. Soient $m \ge 1$ un entier sans facteur carré, et g, h deux autres entiers. Il s'agit alors d'étudier la somme

$$S_f(m, g, h) = \sum_{\substack{0 \le x, y < m \\ f(x,y) \equiv 0 \,(\mathrm{mod}\, m)}} e\left(\frac{gx + hy}{m}\right).$$

On commence par observer le

LEMME 2.1. *Soient m et n deux entiers premiers entre eux. On a l'égalité*

$$S_f(mn, g, h) = S_f(m, g\overline{n}, h\overline{n}) S_f(n, g\overline{m}, h\overline{m}),$$

où $\overline{m}$ désigne un inverse de m modulo n, et $\overline{n}$ un inverse de n modulo m.

Preuve du lemme 2.1. 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

$$S_f(mn, g, h) = \sum_{\substack{0 \le x_1, y_1 < n \\ 0 \le x_2, y_2 < m \\ f(x_1 m + y_1 n, x_2 m + y_2 n) \equiv 0 \,(\mathrm{mod}\, mn)}} e\left(\frac{gx_1 + hy_1}{n}\right) e\left(\frac{gx_2 + hy_2}{m}\right).$$

La condition $f(x_1 m + y_1 n, x_2 m + y_2 n) \equiv 0 \pmod{mn}$ se scinde en

$$f(x_1 m, y_1 m) \equiv 0 \pmod{n}, \qquad f(x_2 n, y_2 n) \equiv 0 \pmod{m},$$

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 de la forme $S_f(p,g,h)$, 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

$$S_f(p,g,h) = \sum_{0\le k<p} e\left(\frac{k}{p}\right) w(k),$$

avec $w(k) = |\{(u,v) : 0 \le u,v < p,\ f(u,v) \equiv 0 \pmod p,\ gu+hv \equiv k \pmod p\}|$. 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 2.2. *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 provenant de la géométrie algébrique. On montre ici le lemme suivant :

LEMME 2.3. *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 dans le symbole O ne dépend que de f.

Preuve du lemme 2.3. Lorsque $p \,|\, (g,h)$, ce résultat est contenu dans le lemme 1.2.1. Dans la suite on suppose donc que $(p,g,h)=1$.

On estime alors cette somme à l'aide d'un résultat de Bombieri [B], qui, en reprenant les travaux de Weil, a obtenu un résultat général sur les sommes d'exponentielles le long d'une courbe.

C'est la proposition suivante :

PROPOSITION 2.4. *Soit X une courbe projective de degré d_1 définie sur $\mathbb{F}_p$, incluse dans $\mathbb{P}^2$, le plan projectif sur $\mathbb{F}_p$. Soit $R(x_1,x_2,x_3)$ une fraction rationnelle homogène de $\mathbb{P}^2$ à valeurs dans $\mathbb{F}_p$, 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 $\Gamma_1, \ldots, \Gamma_s$, 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 $\overline{\mathbb{F}}_p$ de $\mathbb{F}_p$, 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 [B]. Ce dernier théorème est bien plus général que la version présentée ici, mais celle-ci est suffisante pour la preuve du lemme 2.3.

Soit $F(x, y, z)$, le polynôme homogène associé à f. La courbe X est alors celle définie par

$$X = \{(x_1, x_2, x_3) \in \mathbb{P}^2,\ F(x_1, x_2, x_3) \equiv 0 \pmod{p}\},$$

et en prenant comme application rationnelle R, celle qui à $x \in \mathbb{P}^2$, $x = (x_1, x_2, x_3)$, 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 2.3 est donc vérifiée, d'après la proposition 2.4.

Grâce à ce lemme nous sommes en mesure de donner une majoration de la somme suivante (qui sert à la preuve du théorème 2) :

$$\widetilde{S}_f(p, g, h) = \sum_{\substack{0<x_1,x_2<p \\ f(x_1,x_2)\equiv 0 \,(\mathrm{mod}\, p)}} e\left(\frac{gx_1 + hx_2}{p}\right).$$

A partir du lemme 2.3, on montre le :

Corollaire 2.5. *Soit f un polynôme irréductible, vérifiant l'hypothèse* (H2). *On a la majoration*

$$\widetilde{S}_f(p, g, h) = O(p^{1/2}(p, g, h)^{1/2}).$$

La constante du O ne dépend que de f.

Preuve du corollaire. On part de l'égalité :

$$\widetilde{S}_f(p,g,h) = S_f(p,g,h) - \sum_{\substack{0\le x_2<p\\ f(0,x_2)\equiv 0 \,(\mathrm{mod}\, p)}} e\left(\frac{hx_2}{p}\right) - \sum_{\substack{0\le x_1<p\\ f(x_1,0)\equiv 0 \,(\mathrm{mod}\, p)}} e\left(\frac{gx_1}{p}\right) + l(0,0),$$

avec

$$l(0,0) = \begin{cases} 1 & \text{si } f(0,0) \equiv 0 \pmod p,\\ 0 & \text{sinon.}\end{cases}$$

Lorsque p est assez grand, les polynômes $f(0,x_2)$, et $f(x_1,0)$ ne sont pas identiquement nuls sur $\mathbb{F}_p$, la deuxième et la troisième somme sont donc des $O(1)$. Le lemme 2.3 permet de conclure.

Lorsque le polynôme f est homogène, de la même manière, mais plus facilement, on montre que $\widetilde{S}_f(p,g,h) = O(p, f(-h,g))$.

3. Préparations aux cribles. Dans cette partie, on obtient des estimations asymptotiques des quantités

$$|\mathcal{C}_m| = |\{(n_1,n_2) : x \le n_1, n_2 \le 2x,\ f(n_1,n_2) \equiv 0 \pmod m\}|, \tag{3.1}$$

pour $x \ge 1$ 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 3. Nous étudierons encore les ensembles

$$\mathcal{C}_m(a) = \{(n_1,n_2) \in C(a,m) : x \le n_1, n_2 \le 2x\}, \tag{3.2}$$

où $C(a,m)$ est l'ensemble des conditions

$$(n_1n_2, m) = 1, \quad n_1n_2 \equiv 0 \pmod a, \quad f(n_1,n_2) \equiv 0 \pmod m.$$

Les démonstrations des théorèmes 4 et 5 passent par l'étude des ensembles

$$\mathcal{B}_m(a) = \{(n_1,n_2) : n_1, n_2 \sim x,\ n_1n_2 \equiv 0 \pmod a,\ f(n_1,n_2) \equiv 0 \pmod m\}, \tag{3.3}$$

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.

On obtient ainsi les résultats suivants :

Lemme 3.1. *Soit f un polynôme irréductible en deux variables dont les coefficients sont premiers entre eux, et vérifiant l'hypothèse* (H2).

(i) *Pour m sans facteur carré, on a pour tout $\varepsilon > 0$ l'égalité*

$$|\mathcal{C}_m| = \frac{x^2\varrho(m)}{m^2} + O\left(\frac{x^{1+\varepsilon}}{\sqrt{m}} + x^\varepsilon\sqrt{m}\right).$$

(ii) *Soient a et m deux entiers sans facteur carré et premiers entre eux. Pour tout $\varepsilon > 0$, on a l'égalité*

$$|\mathcal{C}_m(a)| = \frac{x^2 r(m)\lambda(a)}{a^2 m^2} + O\Big(\frac{x^{1+\varepsilon}}{\sqrt{m}} + x^\varepsilon \sqrt{m}\Big),$$

où λ est la fonction multiplicative définie par $\lambda(p) = 2p - 1$.

(iii) *Soient a et m deux entiers sans facteur carré. Soit ϱ_0 la fonction suivante* :

$$\varrho_0(d) = |\{(u,v) : 0 \le u, v < d,\ uv \equiv 0 \pmod d,\ f(u,v) \equiv 0 \pmod d\}|.$$

(*Cette fonction est multiplicative, et vérifie $\varrho_0(p) = \varrho(p) - r(p)$.*) *Soit $\delta = (a,m)$. On écrit alors $a = a_1\delta$, $m = m_1\delta$. Pour tout $\varepsilon > 0$, on a l'égalité*

$$|\mathcal{B}_m(a)| = \frac{x^2 \varrho(m_1)\lambda(a_1)\varrho_0(\delta)}{a_1^2\delta^2 m_1^2} + O\Big(\frac{x^{1+\varepsilon}}{\delta\sqrt{m_1}} + x^\varepsilon\sqrt{m_1}\Big).$$

Les preuves des trois différents points (i)–(iii) sont semblables à quelques détails près. Nous ne donnons donc ici que la preuve du point (iii). En reprenant la définition (3.3), on a l'égalité

$$|\mathcal{B}_m(a)| = \sum_{\substack{u,v \pmod{am} \\ uv \equiv 0 \pmod a \\ f(u,v)\equiv 0 \pmod m}} \ \sum_{\substack{n_1,n_2 \sim x \\ n_1 \equiv u \pmod{am} \\ n_2 \equiv v \pmod{am}}} 1.$$

On développe ensuite les sommes sur n_1 et n_2 en sommes d'exponentielles :

$$|\mathcal{B}_m(a)| = \frac{1}{a^2m^2} \sum_{0 \le g,h < am} \ \sum_{n_1,n_2 \sim x} e\Big(\frac{-gn_1 - hn_2}{am}\Big) \sum_{\substack{u,v \pmod{am} \\ uv \equiv 0 \pmod a \\ f(u,v)\equiv 0 \pmod m}} e\Big(\frac{gu+hv}{am}\Big).$$

On note $\Sigma(a,m,\delta,g,h)$ la somme portant sur u et v. Le terme en $g = h = 0$ fournira la contribution principale. On sépare les différentes conditions de congruence *via* l'identité de Bezout :

$$\Sigma(a,m,\delta,g,h) = \lambda(a_1,g,h) S_f(m_1, \overline{a_1\delta^2}g, \overline{a_1\delta^2}h) T_f(\delta, \overline{a_1m_1}g, \overline{a_1m_1}h),$$

où $S_f(m_1,g,h)$ a été définie puis étudiée au précédent paragraphe,

$$\lambda(a_1,g,h) = \sum_{\substack{u,v \bmod a_1 \\ uv \equiv 0 \pmod{a_1}}} e\Big(\frac{gu+hv}{a_1}\Big),$$

et

$$T_f(\delta, \overline{a_1m_1}g, \overline{a_1m_1}h) = \sum_{\substack{0 \le u,v < \delta^2 \\ uv \equiv 0 \pmod\delta \\ f(u,v)\equiv 0 \pmod\delta}} e\Big(\frac{\overline{a_1m_1}(gu+hv)}{\delta^2}\Big).$$

La fonction λ s'évalue facilement avec des méthodes élémentaires. Lorsque a est sans facteur carré, on montre le

LEMME 3.2. *La fonction $\lambda(a,k,l)$ est multiplicative par rapport à a, et vérifie, pour $a=p$ premier*

$$\lambda(p,k,l)=\begin{cases}-1 & \text{si } (p,kl)=1,\\ \varphi(p) & \text{si } p\,|\,kl, \text{ mais } (p,k,l)=1,\\ 2p-1 & \text{si } p\,|\,(k,l).\end{cases}$$

Preuve du lemme 3.2. La multiplicativité se vérifie avec le théorème chinois. Pour $a=p$ premier, on a l'égalité

$$\lambda(p,k,l)=\sum_{0\le u<p} e\Big(\frac{ku}{p}\Big)+\sum_{0\le v<p} e\Big(\frac{lv}{p}\Big)-1,$$

ce qui correspond au résultat annoncé.

Dans toute la suite nous écrirons $\lambda(a)$ pour $\lambda(a,0,0)$.

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

$$T_f(\delta,\overline{a_1m_1}g,\overline{a_1m_1}h)=\prod_{p|\delta}T_f(p,\overline{a_1m_1\widehat{p}^2}g,\overline{a_1m_1\widehat{p}^2}h),$$

avec la notation $\widehat{p}=\delta/p$.

Il suffit donc d'étudier des sommes du type

$$T_f(p,g,h)=\sum_{\substack{0\le u,v<p^2\\ uv\equiv 0\,(\mathrm{mod}\,p)\\ f(u,v)\equiv 0\,(\mathrm{mod}\,p)}} e\Big(\frac{gu+hv}{p^2}\Big).$$

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

$$\begin{aligned}T_f(p,g,h)&=\sum_{\substack{0\le u_0,v_0<p\\ u_0v_0\equiv 0\,(\mathrm{mod}\,p)\\ f(u_0,v_0)\equiv 0\,(\mathrm{mod}\,p)}} e\Big(\frac{gu_0+hv_0}{p^2}\Big)\sum_{0\le\lambda,\mu<p} e\Big(\frac{g\lambda+h\mu}{p}\Big)\\ &=\begin{cases}p^2\varrho_0(p) & \text{si } g\equiv h\equiv 0 \pmod{p^2},\\ O(p^2) & \text{si } g\equiv h\equiv 0 \pmod{p},\\ 0 & \text{sinon.}\end{cases}\end{aligned}$$

En utilisant ceci et en appliquant les lemmes 2.3 et 3.2, on a l'inégalité

$$\Sigma(a,m,\delta,g,h)=O((a_1,gh)m_1^{1/2+\varepsilon}(m_1,g,h)^{1/2}(\delta,g,h)^2),$$

puis en sommant sur les différentes variables on obtient le résultat annoncé.

Cas des polynômes homogènes. Lorsque f est un polynôme homogène, on majore les sommes $S_f(m,k,l)$ avec le lemme 2.2, ce qui donne

$S_f(m,k,l) = O(x^\varepsilon(m, f(-l,k)))$. Ainsi la somme $\Sigma(a,m,\delta,g,h)$ est un $O((a_1,gh)(m_1,f(-h,g))(\delta,g,h)^2)$, et on a

$$|\mathcal{B}_m(a)| = \frac{x^2\lambda(a_1)\varrho_0(\delta)\varrho(m)}{a_1^2m_1^2\delta^2} + O\Big(\frac{x^{1+\varepsilon}}{a^2m^2}\sum_{0<g<am/2}\frac{am}{g}((m_1,f(-g,0))+(m_1,f(0,-g)))\Big) + O\Big(x^\varepsilon\sum_{0<g,h<am/2}\frac{(a_1,gh)}{gh}(m_1,f(-g,h))(\delta,g,h)^2\Big).$$

On note R_1 et R_2 les deux termes d'erreur de la ligne précédente. Ces deux termes s'évaluent plus facilement en moyenne sur a et sur m. On admet provisoirement que l'équation $f(u,v)=0$ a $(0,0)$ comme seul couple solution sur $\mathbb{Z}^2$. On a alors la suite d'inégalités

$$\sum_{\substack{0<m<M\\0<a<A}} R_2(a,m) \ll x^\varepsilon \sum_{0<k,l<AM}\sum_{\delta<AM}\sum_{\substack{0<m_1<M/\delta\\0<a_1<A\delta\\\max(k,l)<am}}\frac{(a_1,kl)(f(-l,k),m_1)(\delta,k,l)^2}{kl}$$

$$\ll x^\varepsilon\sum_{0<k,l<AM} AM\frac{\tau(kl)\tau(f(-l,k))}{kl} \ll AMx^\varepsilon,$$

où 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 $f(-l,k)=0$ avec $(k,l)\neq(0,0)$. Si par exemple $l\neq 0$, alors $f(-l,k) = (-l)^d f(1,-k/l)$, et le polynôme $g(t)=f(1,t)$ a une racine rationnelle. Il admet alors une factorisation sur $\mathbb{Q}[t]$ 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 $f_i(x,y)=x^{d_i}g(y/x)$, ce qui contredit le fait que f soit irréductible. Donc $f(-k,l)$ a comme seule solution $(0,0)$ sur $\mathbb{Z}^2$.

On a ainsi le lemme suivant :

LEMME 3.3. *Soit f un polynôme irréductible homogène dont les coefficients sont premiers entre eux. Soient a et m deux entiers sans facteur carré. Les deux assertions suivantes sont vérifiées* :

(i) *Pour* $(a,m)=1$, *on a*

$$|\mathcal{C}_m(a)| = x^2\frac{r(m)\lambda(a)}{a^2m^2} + R(a,m).$$

(ii) *Pour* $\delta=(a,m)$, *avec* $a=a_1\delta$ *et* $m=m_1\delta$, *on a*

$$|\mathcal{B}_m(a)| = x^2\frac{\varrho(m_1)\lambda(a_1)\varrho_0(\delta)}{a_1^2m_1^2\delta^2} + R'(a,m),$$

où les termes d'erreurs vérifient, pour tout $\varepsilon>0$,

$$\sum_{\substack{0<a<A\\0<m<M}} |R(a,m)| \ll x^{1+\varepsilon}A + x^{\varepsilon}AM.$$

Les termes $R'(a,m)$ *vérifient une inégalité similaire.*

4. Un résultat en moyenne de Greaves. 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 $\mathcal{E}_m$ l'ensemble $\mathcal{E}_m=\{a\in\mathcal{E} : a\equiv 0 \pmod m\}$.

A partir du théorème de Barban–Davenport–Halberstam, Greaves [G3] a montré le lemme :

Lemme 4. *Pour* $x\geq 2$, *et pour tout* $\varepsilon>0$, *on a l'inégalité*

$$\sum_{\substack{m<x^{1-\varepsilon}\\ \mu^2(m)=1}} \left||\mathcal{E}_m| - \frac{r(m)}{\varphi(m)^2}|\mathcal{E}|\right| \ll_{\varepsilon} \frac{x^2}{\log^{10}x}.$$

La condition $m<x^{1-\varepsilon}$ peut être remplacée par $m<x\log^{-A}x$ pour un $A>0$ assez grand.

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 aux preuves des théorèmes 1 et 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 1 reprend la méthode de Tchebychev–Hooley. 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 suivante : $\log f(p_1,p_2) = d\log x + O(1)$. En appliquant le théorème des nombres premiers on obtient alors la première estimation suivante :

$$\log V(x) = \frac{dx^2}{\log x} + O\bigg(\frac{x^2}{\log^2 x}\bigg). \tag{5.1}$$

Par ailleurs, on a encore

$$\log V(x) = \sum_{\substack{p,\alpha\\ p^\alpha \ll x^d}} |\mathcal{E}_{p^\alpha}| \log p,$$

avec

$$\mathcal{E}_{p^\alpha} = \{(p_1,p_2) : p_1,p_2 \sim x,\ f(p_1,p_2) \equiv 0 \pmod{p^\alpha}\}.$$

Pour $\varepsilon > 0$, on procède alors au découpage suivant :

$$\begin{aligned}\log V(x) &= \sum_{p^\alpha < x^{1-\varepsilon}} |\mathcal{E}_{p^\alpha}| \log p + \sum_{\substack{\alpha\ge 2\\ p^\alpha \ge x^{1-\varepsilon}}} |\mathcal{E}_{p^\alpha}| \log p + \sum_{x^{1-\varepsilon}\le p<P} |\mathcal{E}_p| \log p\\ &= S_1 + S_2 + S_3,\end{aligned}$$

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

$$S_1 = \sum_{p<x^{1-\varepsilon}} |\mathcal{E}_p| \log p + \sum_{p^\alpha<x^{1-\varepsilon},\,\alpha\ge 2} |\mathcal{E}_{p^\alpha}| \log p = S_1' + S_1'',$$

par définition. La somme S_1' fournit le terme principal. Elle est estimée avec le lemme 4.

Grâce à ce lemme, on a l'égalité

$$S_1' = \frac{x^2}{\log^2 x} \sum_{p<x^{1-\varepsilon}} \frac{r(p)}{\varphi(p)^2} \log p + O\bigg(\frac{x^2}{\log^2 x}\bigg).$$

D'après le point (ii) du corollaire 1.2.4, on a l'estimation

$$S_1' = (1-\varepsilon)\frac{x^2}{\log x} + O\bigg(\frac{x^2}{\log^2 x}\bigg).$$

La somme S_1'' est, par contre, négligeable. En effet, d'après le théorème de Brun–Titchmarsh, pour $p^\alpha < x^{1-\varepsilon}$, on a l'inégalité

$$|\mathcal{E}_{p^\alpha}| \ll \bigg(\frac{x}{\varphi(p^\alpha)\log x}\bigg)^2 r(p^\alpha).$$

De plus, d'après le corollaire 1.2.4, on a $r(p^\alpha) = O(\alpha p^{4\alpha/3})$, ce qui permet d'écrire l'inégalité

$$S_1'' \ll \frac{x^2}{\log^2 x} \sum_{\substack{p^\alpha < x^{1-\varepsilon} \\ \alpha \geq 2}} \frac{\alpha \log p}{p^{2\alpha/3}} \ll \frac{x^2}{\log^2 x}.$$

Ainsi, on vient d'établir le lemme suivant :

Lemme 5.1. *On a l'égalité*

$$S_1 = (1-\varepsilon)\frac{x^2}{\log x} + O\bigg(\frac{x^2}{\log^2 x}\bigg).$$

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

$$S_2 \ll \sum_{\substack{\alpha \geq 2 \\ p^\alpha \geq x^{1-\varepsilon}}} \sum_{\substack{m \sim x^2 \\ m \equiv 0 \,(\mathrm{mod}\, p^\alpha)}} v_f(m),$$

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, ne dépendant que de f, 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 $a,b,c,d,e,A,B,C,M \in \mathbb{Z}$, 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

$$|\{(x,y) \in \mathbb{Z}^2 : n = Ax^2 + By^2\}| = O(n^\varepsilon).$$

Or ce cardinal est inférieur à $|\{0 \leq v < n : v^2 + AB \equiv 0 \pmod n\}|$ (cf. par exemple [Sm], Art. 86, p. 172), on a donc bien l'inégalité annoncée.

Ceci donne la majoration

$$S_2 \ll x^{2+\eta} \sum_{\substack{\alpha \geq 2 \\ p^\alpha > x^{1-\varepsilon}}} \frac{1}{p^\alpha} \ll x^{1.9}. \tag{5.2}$$

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 important facteur carré ou un important facteur cubique.

Pour $\eta > 0$, minuscule, on découpe la somme S_2 de la manière suivante :

$$S_2 = \sum_{\substack{p<x^{1-\eta},\alpha\geq 2\\ p^\alpha>x^{1-\varepsilon}}} |\mathcal{E}_{p^\alpha}|\log p + \sum_{p>x^{1-\eta}} |\mathcal{E}_{p^2}|\log p + \sum_{p>x^{1-\eta}} |\mathcal{E}_{p^3}|\log p \tag{5.3}$$
$$= R_1 + R_2 + R_3,$$

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 la majoration suivante :

Lemme 5.2. *On a la majoration $R_1 \ll x^2/\log^{10} x$.*

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

$$R(\alpha) = \sum_{x^{(1-\varepsilon)/\alpha}<p<x^{1-\eta}} |\mathcal{E}_{p^\alpha}|.$$

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 $\gcd(\Delta_{p_1},\Delta_{p_2},p^\alpha)$.

On écrit donc l'égalité

$$R(\alpha) = \sum_{x^{(1-\varepsilon)/\alpha}<p<x^{1-\eta}} \sum_{\substack{p_1,p_2\sim x\\ f(p_1,p_2)\equiv 0\,(\mathrm{mod}\,p^\alpha)\\ (p^\alpha,\Delta_{p_1},\Delta_{p_2})<\log^{100}x}} 1$$
$$+ \sum_{x^{(1-\varepsilon)/\alpha}<p<x^{1-\eta}} \sum_{\substack{p_1,p_2\sim x\\ f(p_1,p_2)\equiv 0\,(\mathrm{mod}\,p^\alpha)\\ (p^\alpha,\Delta_{p_1},\Delta_{p_2})\geq\log^{100}x}} 1$$
$$= R_1(\alpha) + R_2(\alpha),$$

par définition.

• *Majoration de $R_1(\alpha)$.* La condition $(p^\alpha,\Delta_{p_1},\Delta_{p_2})<\log^{100}x$ entraîne que $(p^\alpha,\Delta_{p_1})<\log^{100}x$, ou $(p^\alpha,\Delta_{p_2})<\log^{100}x$. Les sommes sur p_1 et sur

p_2 se majorent alors par

$$\sum_{\substack{p_1\sim x\\ (p^\alpha,\Delta_{p_1})<\log^{100}x}}\ \sum_{\substack{0\le v<p^\alpha\\ f(p_1,v)\equiv 0\,(\mathrm{mod}\,p^\alpha)}}\ \sum_{\substack{p_2\sim x\\ p_2\equiv v\,(\mathrm{mod}\,p^\alpha)}} 1 + \sum_{\substack{p_2\sim x\\ (p^\alpha,\Delta_{p_2})<\log^{100}x}}\ \sum_{\substack{0\le v<p^\alpha\\ f(v,p_2)\equiv 0\,(\mathrm{mod}\,p^\alpha)}}\ \sum_{\substack{p_1\sim x\\ p_1\equiv v\,(\mathrm{mod}\,p^\alpha)}} 1.$$

Ces deux sommes se traitent de la même façon.

Pour la première, comme $(\Delta_{p_1},p^\alpha)<\log^{100}x$, d'après le point (iii) du lemme 1.2.3, on a

$$|\{0\le v<p^\alpha : f(u,v)\equiv 0 \pmod{p^\alpha}\}| = O((\Delta_{p_1},p^\alpha)^2) = O(\log^{200}x).$$

Les deux sommes ci-dessus sont donc majorées par

$$O\bigg(x(\log^{200}x)\bigg(\frac{x}{p^\alpha}+1\bigg)\bigg).$$

En reportant ce résultat dans $R_1(\alpha)$, cela donne la majoration

$$\begin{aligned} R_1(\alpha) &\ll x(\log^{200}x)\sum_{x^{(1-\varepsilon)/\alpha}<p<x^{1-\eta}}\bigg(\frac{x}{p^\alpha}+1\bigg)\\ &\ll x^{5/3+\varepsilon/3}(\log^{200}x)\sum_{x^{(1-\varepsilon)/\alpha}<p<x^{1-\eta}}\frac{x}{p^{2\alpha/3}}+x^{2-\eta}\log^{200}x\\ &\ll x^{2-h}, \end{aligned}$$

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

$$\{p_1,p_2\sim x,\ (p^\alpha,\Delta_{p_1},\Delta_{p_2})\ge\log^{100}x\} \subset \bigcup_{\substack{\beta>0\\ p^\beta\ge\log^{100}x}}\{p_1,p_2\sim x,\ \Delta_{p_1}\equiv\Delta_{p_2}\equiv 0 \pmod{p^\beta}\}.$$

A partir de ceci on a la majoration

$$\begin{aligned} R_2(\alpha) &\ll \sum_{\log^{100}x\le p^\beta,\,p<x^{1-\eta}}\ \sum_{\substack{p_1\sim x\\ \Delta_{p_1}\equiv 0\,(\mathrm{mod}\,p^\beta)}}\ \sum_{\substack{p_2\sim x\\ \Delta_{p_2}\equiv 0\,(\mathrm{mod}\,p^\beta)}} 1\\ &\ll \sum_{\log^{100}x\le p^\beta,\ p<x^{1-\eta}}\bigg(\frac{x^2}{p^{2\beta}}+1\bigg), \end{aligned}$$

et ainsi, $R_2(\alpha)\ll x^2/\log^{20}x$.

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 suivant :

LEMME 5.3. *Pour tout $\varepsilon > 0$, il existe $\eta > 0$ assez petit tel qu'on ait la majoration $R_2 \ll x^{1.9+\varepsilon}$.*

Pour détecter les grands facteurs carrés de l'ensemble contenant d'éventuelles répétitions :

$$\{f(p_1, p_2) : p_1, p_2 \sim x\},$$

on a recours à un crible approprié, le crible à carrés de Heath-Brown [HB], que l'on énonce sous la forme suivante :

LEMME 5.4. *Soit $\mathbb{A} = (\omega(n))_n$ une suite de réels, avec $\omega(n) \geq 0$ pour tout n, et tel que $\sum \omega(n) < \infty$. On définit $S(\mathbb{A}) = \sum_{n=1}^{\infty} \omega(n^2)$. Soit $\mathbb{P}$ 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*

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

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 $|\mathcal{C}_d|$ définie au troisième chapitre (cf. (3.1)), on écrit la majoration

$$R_2 \leq \sum_{p > x^{1-\varepsilon}} |\mathcal{C}_{p^2}| \log p \ll \log x \sum_{m > x^{1-\varepsilon}} |\mathcal{C}_{m^2}|.$$

Si n_1 et n_2 vérifient $f(n_1, n_2) = m^2 d$ avec $m > x^{1-\varepsilon}$, on a encore l'écriture $f(n_1, n_2) = m'^2 d'$, avec toujours $m' > x^{1-\varepsilon}$, 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

$$R_2 \ll x^{\varepsilon'} \sum_{d < x^{1+\varepsilon}} \mu^2(d) R_2(d),$$

avec

$$R_2(d) = \sum_{m^2 > x^{2-2\varepsilon}} \omega_d(m^2),$$

et

$$\omega_d(m) = \left| \left\{ (n_1, n_2) : n_1, n_2 \sim x, \ \frac{f(n_1, n_2)}{d} = m \right\} \right|.$$

On applique alors le lemme 5.4 sur chaque quantité $R_2(d)$, en choisissant

$$\mathbb{P}_d = \{p < x^{\theta} : (p, d) = 1\},$$

où θ est un réel positif que l'on précisera plus tard. Ainsi P, le cardinal $|\mathbb{P}_d|$, est de l'ordre de $x^\theta/\log x$.

On a donc la majoration

$$R_2(d) \ll x^{\varepsilon'} P^{-1} \sum_{\substack{n_1,n_2\sim x\\ f(n_1,n_2)\equiv 0 \,(\mathrm{mod}\, d)}} 1 + x^{\varepsilon'} P^{-2} \sum_{p\neq q\in\mathbb{P}} \left| \sum_{\substack{n_1,n_2\sim x\\ f(n_1,n_2)\equiv 0 \,(\mathrm{mod}\, d)}} \left(\frac{f(n_1,n_2)/d}{pq}\right)\right|.$$

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 ainsi 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

$$\Sigma_2 = \sum_{p\neq q\in\mathbb{P}_d} |T(p,q,d)|,$$

avec évidemment

$$T(p,q,d) = \sum_{\substack{n_1,n_2\sim x\\ f(n_1,n_2)\equiv 0 \,(\mathrm{mod}\, d)}} \left(\frac{f(n_1,n_2)/d}{pq}\right).$$

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

$$T(p,q,d) = \frac{1}{p^2q^2d^2} \sum_{g,h \bmod pqd} \sum_{\substack{0\le u,v<pqd\\ f(u,v)\equiv 0 \,(\mathrm{mod}\, d)}} \left(\frac{d}{pq}\right)\left(\frac{f(u,v)}{pq}\right) \times \sum_{n_1,n_2\sim x} e\left(\frac{g(u-n_1)+h(v-n_2)}{pqd}\right). \tag{5.4}$$

Ensuite on sépare ces différentes sommes, ce qui est permis d'après le théorème chinois car $(pq,d)=1$:

$$T(p,q,d) = \frac{1}{p^2q^2d^2}\left(\frac{d}{pq}\right)\sum_{0\le g,h<pqd}\sum_{n_1\sim x} e\left(\frac{-gn_1}{pqd}\right)\sum_{n_2\sim x} e\left(\frac{-hn_2}{pqd}\right) \times H_f(p,g,h)H_f(q,g,h)S_f(d,g,h), \tag{5.5}$$

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 :

$$H_f(p,g,h) = \sum_{0\le u,v<p}\left(\frac{f(u,v)}{p}\right)e\left(\frac{gu+hv}{p}\right).$$

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 résultat de Hooley [H2] concernant les majorations de sommes d'exponentielles le long de surfaces), tandis que d'après le lemme 2.3, 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

$$Q_2 = \frac{x^2\varrho(d)}{d^2p^2q^2}\sum_{0\le u,v<p}\left(\frac{f(u,v)}{p}\right)\sum_{0\le u,v<q}\left(\frac{f(u,v)}{q}\right). \tag{5.6}$$

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*

$$\sum_{0\le u,v<p}\left(\frac{f(u,v)}{p}\right) = O(p^{3/2}).$$

La constante implicite ne dépend 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 $g(x) \in \mathbb{F}_p[x]$ un polynôme de degré 3, non constant. On a alors l'inégalité*

$$\left| \sum_{x \in \mathbb{F}_p} \left(\frac{g(x)}{p} \right) \right| \ll \sqrt{p}.$$

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 $\mathbb{F}_p$ 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 $\mathbb{F}_p$. 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 lemme 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) :

$$Q_2 \ll \frac{x^2 \varrho(d)}{d^2 \sqrt{pq}}.$$

Au chapitre 1, on a vu que $\varrho(d) = O(d)$, et on a donc finalement

$$T(p,q,d) \ll \frac{x^{1+\varepsilon_1} pq}{\sqrt{d}} + p^2 q^2 \sqrt{d} x^{\varepsilon_1} + \frac{x^2}{d\sqrt{pq}}.$$

On reporte ceci dans Σ_2 :

$$\Sigma_2 \ll \frac{P^4 x^{1+\varepsilon_1}}{\sqrt{d}} + P^6 x^{\varepsilon_1} \sqrt{d} + \frac{P x^{2+\varepsilon_1}}{d}. \tag{5.7}$$

Ainsi pour tout d sans facteur carré on a l'inégalité

$$R_2(d) \ll x^{\varepsilon'} \left(P^{-1} \frac{x^2}{d} + dP^{-1} + \frac{P^2 x^{1+\varepsilon_2}}{\sqrt{d}} + P^4 \sqrt{d} x^{\varepsilon_2} + \frac{P^{-1} x^2}{d} \right),$$

c'est-à-dire,

$$R_2 \ll \sum_{d<x^{1+\varepsilon}} R_2(d) \ll x^2 P^{-1} x^{\varepsilon_3} + P^4 x^{3/2+\varepsilon_3}.$$

En choisissant $P = x^\theta = x^{1/10}$, on a l'inégalité $R_2 \ll x^{1.9+\varepsilon}$.

5.5. *Estimations de S_3.* D'après les lignes (5.1) et (5.2), les lemmes 5.1–5.3, nous avons les égalités :

• lorsque f est un polynôme du second degré :

$$S_3 = \log V(x) - S_1 - S_2 = \frac{(1+\varepsilon)x^2}{\log x} + O\Big(\frac{x^2}{\log^2 x}\Big), \tag{5.8}$$

• lorsque le degré de f est trois :

$$S_3 = \frac{(2+\varepsilon)x^2}{\log x} + O\Big(\frac{x^2}{\log^2 x}\Big). \tag{5.9}$$

Le principe de la méthode de Tchebychev–Hooley 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 :

$$S_3 = \sum_{p>x^{1-\varepsilon}} |\mathcal{E}_p| \log p.$$

On écarte les (p_1, p_2) de $\mathcal{E}_p$ tels que $p \,|\, p_1 p_2$:

$$S_3 = \sum_{p>x^{1-\varepsilon}} |\mathcal{F}_p| \log p + O(x^{1+\varepsilon}),$$

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*

$$|\mathcal{F}_p| \leq \frac{2x^2}{\log^2 z} \cdot \frac{r(p)}{p^2} + O\Big(\frac{z^2 x^{1+\varepsilon}}{\sqrt{p}} + \sqrt{p} z^2 x^\varepsilon\Big).$$

P r e u v e d u l e m m e 5.7. On détecte les nombres premiers p_1, p_2 en recourant au crible, pour $z \geq 1$, on écrit la majoration

$$|\mathcal{F}_p| \leq \sum_{\substack{n_1, n_2 \sim x \\ q \mid n_1 n_2 \Rightarrow q > z \\ (n_1 n_2, p) = 1 \\ f(n_1, n_2) \equiv 0 \,(\mathrm{mod}\, p)}} 1.$$

Les familles d'entiers correspondant à ce problème de crible sont exactement les ensembles $\mathcal{C}_p(a)$ étudiés au chapitre 3, définis par (3.2); d'après le point (ii) du lemme 3.1, pour a sans facteur carré, et premier à p, on a l'égalité

$$|\mathcal{C}_p(a)| = x^2\frac{r(p)\lambda(a)}{p^2a^2} + O\Big(\frac{x^{1+\varepsilon}}{\sqrt{p}} + x^{\varepsilon}\sqrt{p}\Big),$$

avec $\lambda(q) = 2q-1$ lorsque q est un nombre premier.

Les conditions d'application du crible de Selberg de dimension 2 (cf. [H-R], théorème 6.3, p. 202) sont remplies, et on a ainsi la majoration

$$|\mathcal{F}_p| \le \frac{x^2r(p)}{p^2}2e^{2\gamma}\prod_{q<z}\Big(1-\frac{\lambda(q)}{q^2}\Big)\Big(1+O\Big(\frac{1}{\log z}\Big)\Big) + \sum_{a<z^2}3^{\nu(a)}\mu^2(a)\Big(\frac{x^{1+\varepsilon}}{\sqrt{p}} + x^{\varepsilon}\sqrt{p}\Big). \tag{5.10}$$

Le produit eulérien vaut exactement $\prod_{q<z}(1-1/p)^2$; 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 :

$$S_3 \le 2x^2\sum_{x^{1-\varepsilon}<p<P}\log p\frac{r(p)}{p^2\log^2 z_p}\Big(1+O\Big(\frac{1}{\log z_p}\Big)\Big) + O\Big(\sum_{x^{1-\varepsilon}<p<P}\log p\Big(\frac{z_p^2x^{1+\varepsilon}}{\sqrt{p}} + \sqrt{p}z_p^2x^{\varepsilon}\Big)\Big). \tag{5.11}$$

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

$$S_3 \le 2x^2\sum_{x^{1-\varepsilon}<p<P}\frac{\log p}{\log^2(x^{1-2\varepsilon}p^{-3/4})}\cdot\frac{r(p)}{p^2} + O\Big(x^{2-\varepsilon} + \frac{x^2}{\log^2 x}\Big).$$

On applique le point (ii) du corollaire 1.2.4, ce qui donne l'inégalité

$$S_3 \le 2x^2\int_{x^{1-\varepsilon}}^{P}\frac{dt}{t\log^2(x^{1-2\varepsilon}t^{-3/4})} + O\Big(\frac{x^2}{\log^2 x} + x^{2-\varepsilon}\Big).$$

En écrivant alors $P = x^{\Lambda}$ (avec $\Lambda < 4/3 - 10\varepsilon$), puis en calculant l'intégrale ci-dessus on aboutit à la majoration

$$S_3 \le \frac{x^2}{\log x}\Big(\frac{8}{3(1-3\Lambda/4)} - \frac{32}{3} + \varepsilon\Big) + O\Big(\frac{x^2}{\log^2 x}\Big). \tag{5.12}$$

5.6. *Conclusion dans le cas où f est un polynôme du second degré.* En comparant (5.8) avec (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

$$\log V(x) = \frac{dx^2}{\log x} + O\left(\frac{x^2}{\log^2 x}\right) = S_1 + S_2 + S_3.$$

D'après le lemme 4, et les estimations de $r(p^\alpha)$ données au paragraphe 1, on a l'égalité

$$S_1 = \sum_{p^\alpha < x^{1-\varepsilon}} |\mathcal{E}_{p^\alpha}| \log p = (1-\varepsilon)\frac{x^2}{\log x} + O\left(\frac{x^2}{\log x}\right).$$

Pour S_2, on a la majoration

$$S_2 \leq R_1 + d \sum_{p > x^{1-\eta}} |\mathcal{E}_{p^2}| \log p,$$

où R_1 est la quantité définie au paragraphe 5.3. Dans ce paragraphe on a obtenu la majoration $R_1 \ll x^2/\log^{10} x$, et ceci est toujours valable pour des polynômes homogènes.

Sinon, Greaves a établi dans [G4], l'inégalité suivante (valable seulement pour des polynômes homogènes) :

$$\sum_{x^{1-\eta} < p} |\mathcal{E}_{p^2}| \log p \ll \frac{x^2}{\log^2 x},$$

et ainsi, on a : $S_2 \ll x^2 \log^{-2} x$.

Pour S_3, l'homogénéité de f permet d'avoir une majoration plus fine que celle du paragraphe 5.5, en utilisant le lemme 3.3 à la place du lemme 3.1. Le z_p correspondant vaut alors $z_p = x^{1-\varepsilon}p^{-1/2}$, pour $p < x^{2-\varepsilon}$, et on obtient

la majoration

$$S_3 \le \int_{x^{1-\varepsilon}}^{P} \frac{2x^2}{t\log^2(x^{1-\varepsilon}t^{-1/2})}\,dt + O\Big(\frac{x^2}{\log^2 x}\Big).$$

En écrivant $P = x^H$, puis en calculant cette intégrale, on a la majoration

$$S_3 \le \frac{x^2}{\log x}\Big(4\Big(\frac{1}{1-H/2}\Big) - 8 + \varepsilon\Big) + O\Big(\frac{x^2}{\log^2 x}\Big).$$

Ainsi, $P = x^H$ doit vérifier $d - 1 < 8/(2-H) - 8$, c'est-à-dire, $H > 2 - 8/(d+7)$.

6. Nombres presque premiers représentés par des polynômes. Le théorème 3 est une conséquence facile du lemme 3.1. En effet, d'après le lemme 3.1, pour tout entier d dans facteur carré, on a

$$\begin{aligned}|\mathcal{C}_d| &= |\{(x_1,x_2) : x_1, x_2 \sim x,\ f(x_1,x_2) \equiv 0 \pmod d\}| \\ &= x^2\frac{\varrho(d)}{d^2} + O\Big(\frac{x^{1+\varepsilon}}{\sqrt{d}} + x\varepsilon\sqrt{d}\Big).\end{aligned}$$

On applique le crible pondéré de Richert, plus précisément le théorème 9.3, p. 253 du livre de [H-R] donne alors le résultat.

7. 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.

7.1. *Les poids de Richert.* Le principe de la preuve du théorème 5 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 $\mathcal{C} = \{f(p_1,p_2) : p_1, p_2 \sim x\}$, avec d'éventuelles répétitions. On a alors l'égalité

$$X = |\mathcal{C}| = \frac{x^2}{\log^2 x} + O\Big(\frac{x^2}{\log^3 x}\Big).$$

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) :

$$w_p(n) = \begin{cases} \lambda\Big(1 - u\dfrac{\log p}{\log X}\Big) & \text{si } X^{1/v} \le p < X^{1/u},\ p \,|\, n, \\ 0 & \text{sinon,}\end{cases}$$

où $u < v$, λ sont des paramètres à optimiser. On étudie alors

$$W(\mathcal{C},u,v,\lambda) = \sum_{\substack{a\in\mathcal{C}\\ p\mid a\Rightarrow p>X^{1/v}}} \Big(1 - \sum_{X^{1/v}<p<X^{1/u}} w_p(a)\Big) \tag{7.1}$$

$$= S(\mathcal{C},X^{1/v}) - \lambda \sum_{X^{1/v}<p<X^{1/u}} \Big(1 - u\frac{\log p}{\log X}\Big) S(\mathcal{C}_p, X^{1/v}),$$

où, selon les notations standard,

$$S(\mathcal{C},X^{1/v}) = |\{a\in\mathcal{C} : p\,|\,a\Rightarrow p > X^{1/v}\}|.$$

Soit $a\in\mathcal{C}$ ayant une contribution positive dans (7.1). Cet entier a vérifie alors clairement le point (i) du théorème 5, et sa contribution à (7.1) est inférieure à

$$1-\lambda\Big(\omega(a) - u\frac{\log|a|}{\log X}\Big) \le 1-\lambda\Big(\omega(a)-\frac{ud}{2}\Big).$$

Ainsi tout $a\in\mathcal{C}$ ayant une contribution positive dans (7.1) vérifie

$$\omega(a) < \lambda^{-1} + ud/2. \tag{7.2}$$

Parmis ceux-ci, Greaves a montré dans [G3], p. 5, que le nombre de ceux qui ne vérifiaient pas le point (ii) du théorème 5 est un $O(X\log^{-2}X)$.

Les quantités $S(\mathcal{C},X^{1/v})$ et $S(\mathcal{C}_p,X^{1/v})$ intervenant dans (7.1), sont estimées, lorsque p est petit, avec le lemme 4, comme l'avait fait Greaves dans [G3].

Quand p est grand on utilise des méthodes de crible pour détecter à la fois les p_1p_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 6.1. On passe du niveau $\alpha = 1/2$ de Greaves à $\alpha = 2/3$. Cependant, nous ne sommes pas en mesure de majorer les $\mathcal{C}_{p^2}$ de façon satisfaisante lorsque $p > x$ et $d > 3$; c'est pourquoi le théorème 5 n'apprend rien de nouveau sur $\Omega(n)$, et nous devons nous contenter de l'assertion (ii).

7.2. *Minoration de* $S(\mathcal{C},X^{1/v})$. D'après le lemme 4, on a l'égalité

$$|\mathcal{C}_d| = X\frac{r(d)}{\varphi(d)^2} + R_d,$$

avec

$$\sum_{d<X^{1/2-\varepsilon}} 3^{\omega(d)}\mu^2(d)R_d \ll \frac{X}{\log^2 X}.$$

D'après le lemme 1.2.4, les conditions d'application du crible linéaire de Rosser–Iwaniec [I] sont vérifiées, et on a ainsi le

Lemme 7.1. *On a la minoration*

$$S(\mathcal{C}, X^{1/v}) \geq \frac{CX}{\log X}\left(ve^{-\gamma} f\left(\frac{\log X^{1/2-\varepsilon}}{\log X^{1/v}}\right) + O\left(\frac{1}{\log X}\right)\right),$$

où C est le produit convergent

$$C = \prod_{q} \left(1 - \frac{r(q)}{\varphi(q)^2}\right)\left(1 - \frac{1}{q}\right)^{-1}.$$

7.3. *Première majoration de $S(\mathcal{C}_p, X^{1/v})$.* On procède comme au paragraphe 7.2, mais en utilisant bien sûr le crible majorant au lieu du crible minorant.

On obtient ainsi le

Lemme 7.2. *En écrivant $p = X^{\mu}$, on a la majoration pour tout $\varepsilon > 0$ et pour $p < X^{1/2-2\varepsilon}$:*

$$S(\mathcal{C}_p, X^{1/v}) \leq \frac{CX}{\log X} \cdot \frac{r(p)}{\varphi(p)^2}\left(\frac{2}{1/2 - \mu - \varepsilon} + O\left(\frac{1}{\log X}\right)\right) + O\left(\frac{X^{1-\varepsilon}}{p^2}\right).$$

7.4. *Deuxième majoration de $S(\mathcal{C}_p, X^{1/v})$.* Pour être en mesure d'utiliser du crible, on part de l'inégalité

$$S(\mathcal{C}_p, X^{1/v}) \leq \sum_{\substack{n_1, n_2 \sim x \\ f(n_1,n_2) \equiv 0 \,(\mathrm{mod}\, p) \\ q \mid n_1 n_2 \Rightarrow q > z \\ q \mid f(n_1,n_2) \Rightarrow q > X^{1/v}}} 1.$$

On a vu au chapitre 3 que les ensembles $\mathcal{B}_m(a)$ définis dans (3.3) vérifiaient, d'après le point (iii) du lemme 3.1, 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 $(a_1, m_1) = 1$

$$|\mathcal{B}_m(a)| = x^2 \frac{\varrho(m_1)\lambda(a_1)\varrho_0(\delta)}{a_1^2 m_1^2 \delta^2} + R(a, m),$$

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

$$\frac{\omega(a, m)}{am} = \frac{\varrho(m_1)\lambda(a_1)\varrho_0(\delta)}{a_1^2 m_1^2 \delta^2}.$$

En criblant faiblement ces deux variables ensemble à l'aide d'un lemme fondamental correspondant à un crible de dimension 3, on a alors le

Lemme 7.3. *Pour $U \geq u \geq 2$, on pose $s = \log U / \log u$. 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

$$S_p(a_1,a_2,u)=\sum_{\substack{n_1,n_2\sim x\\ n_1n_2\equiv 0\,(\mathrm{mod}\,a_2)\\ f(n_1,n_2)\equiv 0\,(\mathrm{mod}\,a_1p)\\ q\mid n_1n_2f(n_1,n_2)\Rightarrow q>u}}1.$$

On a alors l'égalité

$$S_p(a_1,a_2,u)=x^2V(u)\frac{\omega(a_1,a_2)}{a_1a_2}\cdot\frac{\varrho(p)}{p^2}\Big\{1+O\Big(\frac{e^{-s}}{\log^{1/3}U}\Big)\Big\}+O\Big(\sum_{\substack{m\mid P(u)\\ m<U}}\mu^2(m)\sum_{m_1m_2=m}R(a_1m_1,a_2m_2)\Big),$$

avec

$$V(u)=\prod_{q<u}\Big(1-\frac{\Omega(q)}{q}\Big),$$

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 $\omega(q,1)=\varrho(q)/q$, $\omega(1,q)=\lambda(q)/q$, $\omega(q,q)=\varrho_0(q)$.

Au paragraphe 3, on a observé l'égalité $\varrho_0(p)=\varrho(p)-r(p)$. On a donc, d'après les valeurs de Ω données au lemme 7.3, les égalités

$$V(u)=\prod_{q<u}\Big(1-\frac{\Omega(q)}{q}\Big)=\prod_{q<u}\Big(1-\frac{r(q)}{q^2}-\frac{\lambda(q)}{q^2}\Big)=\prod_{q<u}\Big(1-\frac{r(q)}{\varphi(q)^2}\Big)\Big(1-\frac{1}{q}\Big)^2,$$

ce qui nous permettra de comparer facilement le résultat que l'on obtiendra avec le lemme 7.2.

On utilise les poids de Rosser–Iwaniec (cf. [I]), correspondant à des cribles linéaires pour détecter les facteurs premiers de $f(n_1,n_2)$ supérieurs à u.

Plus précisement, ces poids sont définis par $\lambda_1=1$, $\lambda_m=0$, si $m>M_1$, ou si m a un facteur carré, et pour $m=p_1\dots p_r$, avec $p_1>\dots>p_r$ on impose

$$\lambda_m=\begin{cases}(-1)^r & \text{si } p_1\dots p_{2l}p_{2l+1}^3<M_1 \text{ pour tout } 0\le l\le (r-1)/2,\\ 0 & \text{sinon.}\end{cases}$$

Par contre pour cribler n_1n_2, on utilise les poids μ de Selberg propres au crible de dimension deux dont la fonction de crible correspondante est $\omega(q,1)=\lambda(q)/q=2-1/q$. 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 $\prod_{z_1\le p<z_2} p$, on a l'inégalité

$$\begin{aligned} S(\mathcal{C}_p,X^{1/v}) &\le \sum_{\substack{n_1,n_2\sim x\\ f(n_1,n_2)\equiv 0\,(\mathrm{mod}\,p)\\ q\mid n_1n_2f(n_1,n_2)\Rightarrow q>u}} \Big(\sum_{\substack{m_1\mid P(u,X^{1/v})\\ m_1\mid f(n_1,n_2)}}\lambda_{m_1}\Big)\Big(\sum_{\substack{m_2\mid P(u,z)\\ m_2\mid n_1n_2}}\mu_{m_2}\Big)^2\\ &\le \sum_{\substack{m_1\mid P(u,X^{1/v})\\ m_2,m_2'\mid P(u,z)}} \lambda_{m_1}\mu_{m_2}\mu_{m_2'}S_p(m_1,[m_2,m_2'],u). \end{aligned}$$

On applique alors le lemme 7.3 :

$$\begin{aligned} &S(\mathcal{C}_p,X^{1/v})\\ &\quad\le x^2\frac{\varrho(p)}{p^2}V(u)\Big\{1+O\Big(\frac{e^{-s}}{\log U}\Big)\Big\}\\ &\qquad\times\sum_{\substack{m_1\mid P(u,X^{1/v})\\ m_2,m_2'\mid P(u,z)}}\lambda_{m_1}\mu_{m_2}\mu_{m_2'}\frac{\omega(m_1,[m_2,m_2'])}{m_1[m_2,m_2']}\\ &\qquad+O\Big(\sum_{\substack{l\mid P(u)\\ l<U}}\sum_{l_1l_2=l}\sum_{\substack{m_1\mid P(u,X^{1/v})\\ m_1<M_1\\ m_2,m_2'\mid P(u,z)\\ m_2,m_2'<M_2}}|\lambda_{m_1}\mu_{m_2}\mu_{m_2'}|R(pm_1l_1,[m_2,m_2']l_2)\Big). \end{aligned}$$

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 invoqués dans un contexte plus difficile par Brüdern et Fouvry [B-F] pour rendre les variables m_1 et m_2 indépendantes sont applicables ici, et en choisissant $u=X^{\varepsilon^2}$, $U=X^{\varepsilon}$, on a l'égalité

$$\begin{aligned} &S(\mathcal{C}_p,X^{1/v})\\ &\quad\le x^2\frac{\varrho(p)}{p^2}V(u)\Big\{1+O\Big(\frac{e^{-s}}{\log U}\Big)\Big\}\\ &\qquad\times\sum_{\substack{m_1\mid P(u,X^{1/v})\\ m_1<M_1}}\frac{\lambda_{m_1}\omega(m_1,1)}{m_1}\sum_{\substack{m_2,m_2'\mid P(u,z)\\ m_2,m_2'<M_2}}\frac{\mu_{m_2}\mu_{m_2'}\omega(1,[m_2,m_2'])}{[m_2,m_2']}\\ &\qquad+O(X^{1-\varepsilon^2/2}); \end{aligned}$$

le reste $O(X^{1-\varepsilon^2/2})$ provient des erreurs *de nettoyage de pgcd* occasionnées par le processus de séparation des variables.

On utilise ensuite les majorations données par le crible linéaire de Rosser–Iwaniec pour majorer la somme sur m_1, et celles données par le crible de Selberg de dimension 2 pour les sommes sur m_2, m_2', et on obtient

$$\begin{aligned} S(\mathcal{C}_p, X^{1/v}) \le x^2 \frac{\varrho(p)}{p^2} V(u) \prod_{u<q<X^{1/v}} \Big(1 - \frac{r(q)}{\varphi(q)^2}\Big) \prod_{u<p<z} \Big(1 - \frac{1}{p^2}\Big) \\ \times \bigg(F\Big(\frac{\log M_1}{\log X^{1/v}}\Big) F_2\Big(\frac{\log M_2}{\log z}\Big) + O_\varepsilon\Big(\frac{1}{\log X}\Big)\bigg) \\ + O\Big(\frac{X^{1-\varepsilon}}{p} + M_1^{3/2} M_2 \sqrt{p} X^\varepsilon\Big). \end{aligned}$$

Comme le produit

$$C = \prod_p \Big(1 - \frac{r(p)}{\varphi(p)^2}\Big)\Big(1 - \frac{1}{p}\Big)^{-1}$$

est convergent, on a la majoration

$$\begin{aligned} S(\mathcal{C}_p, X^{1/v}) \le x^2 \frac{\varrho(p)}{p^2} \cdot \frac{e^{-3\gamma} C}{\log M_1 \log^2 M_2} \\ \times \bigg(F\Big(\frac{\log M_1}{\log X^{1/v}}\Big) \frac{1}{\sigma_2(\log M_2/\log z)} + O_\varepsilon\Big(\frac{1}{\log X}\Big)\bigg) \\ + O\Big(\frac{X^{1-\varepsilon}}{p} + M_1^{3/2} M_2 \sqrt{p} X^\varepsilon\Big). \end{aligned}$$

Lorsque

$$\frac{\log M_1}{\log X^{1/v}} \le 3 \quad \text{et} \quad \frac{\log M_2}{\log z} \le \alpha_2 = 5.3577\ldots$$

le terme principal vaut

$$x^2 \frac{r(p)}{\varphi(p)^2} \cdot \frac{4C}{\log M_1 \log^2 M_2}.$$

Pour faciliter les calculs on choisit M_1 en fonction de p, et 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 $M \ll X^{2/3 - 2\alpha/3 - \mu - \varepsilon}$, et le terme principal devient

$$\frac{x^2}{\log^3 X} \cdot \frac{r(p)}{\varphi(p)^2} \cdot \frac{4C}{\alpha^2(2/3 - 2\alpha/3 - \mu)}.$$

En optimisant par rapport à α cette dernière formule, on obtient le

Lemme 7.4. *On a la majoration*

$$S(\mathcal{C}_p, X^{1/v}) \le \frac{x^2 C}{\log^3 X} \cdot \frac{\varrho(p)}{p^2} \Big(\frac{12}{(2/3 - \mu)^3} + O\Big(\frac{1}{\log X}\Big)\Big) + O\Big(\frac{X^{1-\varepsilon}}{p}\Big),$$

où on a posé $p = X^\mu$ *et* μ *vérifie alors* $0 < \mu < 2/3$.

7.5. *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 7.3 devient plus fine que celle du lemme 7.2 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 $\mu_0 = 0.496728234\ldots$

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, avait choisit pour som crible pondéré (le théorème 9.3, p. 259 de [HR]) $u = u_r = (1+3^{-r})/\alpha$ (ici $\alpha = 1/2$). Lorsque $r < 4$, $\mu_0 > 1/u$, et le lemme 7.4 est toujours moins bon. Ce lemme devient vraiment intéressant quand r est grand, c'est-à-dire lorsque le degré de f est grand.

7.6. *Conclusion.* En tenant compte des calculs du paragraphe 7.5, on écrit

$$\sum_{X^{1/v}<p<X^{1/u}} \left(1 - \frac{u\log p}{\log X}\right) S(\mathcal{C}_p, X^{1/v}) = S_1 + S_2,$$

avec

$$S_1 = \sum_{X^{1/v}<p\le X^{\mu_0}} \left(1 - \frac{u\log p}{\log X}\right) S(\mathcal{C}_p, X^{1/v})$$

et

$$S_2 = \sum_{X^{\mu_0}<p<X^{1/u}} \left(1 - \frac{u\log p}{\log X}\right) S(\mathcal{C}_p, X^{1/v}).$$

On majore alors S_1 avec le lemme 7.2, et S_2 avec le lemme 7.4. En utilisant le corollaire 1.2.4 pour les fonctions r, on obtient alors

$$S_1 + S_2 \le \frac{XC}{\log X} \int_{1/v}^{\mu_0} \frac{2(1-u\mu)}{(1/2-\mu)\mu}\, d\mu + \frac{XC}{\log X} \int_{\mu_0}^{1/u} \frac{3(1-u\mu)}{\mu(2/3-\mu)^3}\, d\mu + O\left(\frac{X}{\log^2 X} + X^{1-\varepsilon}\right).$$

Toutes ces intégrales se calculent et nous avons

$$S_1 + S_2 \le (H_1(u,v) + H_2(u))\frac{CX}{\log X} + O\left(X^{1-\varepsilon} + \frac{X}{\log^2 X}\right),$$

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 7.1 l'inégalité

$$S(\mathcal{C}, X^{1/v}) \le \frac{X}{\log X} Ce^{-\gamma} 8f(4) + O\left(\frac{X}{\log^2 X}\right) = \frac{CX}{\log X}\left(4\log 3 + O\left(\frac{1}{\log X}\right)\right),$$

ce qui fournit la minoration

$$W(\mathcal{C}, u, v, \lambda) \ge \frac{CX}{\log X}(4\log 3 - \lambda(H_1(u, 8) + H_2(u)))(1 + O(\log^{-1} X)).$$

En prenant $u = 12/7$, on a $\lambda^{-1} > 5.2779\ldots$, et en reportant ceci dans (7.2), on obtient le théorème 5.

7.7. *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 4. Grâce à leur homogénéité, ces polynômes vérifient la condition (Ω_3) du théorème 9.3 de [HR]. Greaves a en effet montré dans [G4] en raisonnant en terme de réseaux l'inégalité

$$\sum_{X^{1/v} < p < X^{1-\varepsilon}} |\mathcal{C}_{p^2}| = O\left(\frac{X}{\log^2 X}\right).$$

C'est pourquoi le théorème 4 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 lemmes 7.1 et 7.2 était le lemme 4, résultant du théorème de Barban–Davenport–Halberstam, et ces deux résultats restent valables lorsque le polynôme est homogène.

On a ainsi les deux inégalités en reprenant les notations des précédents paragraphes :

$$S(\mathcal{C}, X^{1/v}) \ge \frac{CX}{\log X}\left(ve^{-\gamma} f\left(\frac{\log X^{1/2-\varepsilon}}{\log X^{1/v}}\right) + O\left(\frac{1}{\log X}\right)\right),$$

et en écrivant $p = X^{\mu}$

$$S(\mathcal{C}_p, X^{1/v}) \le \frac{CX}{\log X} \cdot \frac{r(p)}{\varphi(p)^2}\left(\frac{2}{1/2 - \mu - \varepsilon} + O\left(\frac{1}{\log X}\right)\right).$$

En faisant ensuite les mêmes opérations que celles du paragraphe 7.4, mais en utilisant le lemme 3.3 à la place du lemme 3.1, on a la majoration

$$S(\mathcal{C}_p, X^{1/v}) \le \frac{CX}{\log X} \cdot \frac{\varrho(p)}{p^2}\left(\frac{27}{4(1-\varepsilon-\mu)^3} + O\left(\frac{1}{\log X}\right)\right).$$

Cette dernière majoration est plus précise que la précédente, lorsque

$$\frac{27}{4(1-\mu)^3} \le \frac{2}{1/2-\mu},$$

c'est-à-dire, pour $\mu \ge 7/4 - 3\sqrt{3}/4 = \mu_0$. ($\mu_0$ est solution de l'équation $16(1-t)^3 - 27(1-2t) = 0$, $\mu_0 = 0.4509\ldots$)

En faisant alors des calculs analogues à ceux effectués au paragraphe 7.6, on a

$$\begin{aligned}\sum_{X^{1/v}<p<X^{1/u}} &\left(1 - u\frac{\log p}{\log X}\right) S(\mathcal{C}_p, X^{1/v}) \\ &\le \frac{XC}{\log X}\left\{ \int_{1/v}^{\mu_0} \frac{2(1-u\mu)}{(1/2-\mu)\mu}\, d\mu + \int_{\mu_0}^{1/u} \frac{27(1-u\mu)}{(1-\mu)^3}\, d\mu \right\} \\ &\quad + O\left(\frac{X}{\log^2 X} + X^{1-\varepsilon}\right) \\ &\le \frac{XC}{\log X}\left(H_3(u,v) + H_4(u) + O\left(\frac{1}{\log X}\right)\right),\end{aligned}$$

par définition.

Un calcul direct donne (on rappelle que $\mu_0 = 7/4 - 3\sqrt{3}/4$)

$$H_3(u,v) = 4\log(\mu_0 v) + 2(2-u)(\log(1/2-1/v) - \log(1/2-\mu_0))$$

et

$$\begin{aligned}H_4(u) = \frac{27}{4}\Bigg\{ &\log(1/u) - \log\mu_0 + \log(1-\mu_0) \\ &+ \frac{1}{1-1/u} - \frac{1}{1-\mu_0} + \frac{1-u}{2}\left(\frac{1}{(1-1/u)^2} - \frac{1}{(1-\mu_0)^2}\right)\Bigg\}.\end{aligned}$$

En prenant $v = 8$, on a la minoration

$$W(\mathcal{C}, u, v, \lambda) \ge \frac{CX}{\log X}\left(4\log 3 - \lambda(H_3(u,8) + H_4(u)) + O\left(\frac{1}{\log X}\right)\right).$$

Pour $u = 4/3$, on obtient $\lambda^{-1} = 8.238\ldots$, et ainsi

$$\Omega(f(p_1,p_2)) < 2d/3 + 8.24.$$

7.8. Remarque. Il est certainement possible d'obtenir des améliorations des théorèmes 4 et 5, 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.

Bibliographie

[B] E. Bombieri, *On exponential sums in finite fields*, Amer. J. Math. 88 (1966), 71–105.

[B-F] J. Brüdern et E. Fouvry, *Le crible à vecteurs*, Compositio Math. 102 (1996), 337–355.

[D] C. Dartyge, *Propriétés multiplicatives des valeurs de certains polynômes*, Thèse de doctorat ès sciences, Université de Paris XI, Orsay, 1994.

[D-I] J.-M. Deshouillers and H. Iwaniec, *On the greatest prime factor of* $n^2 + 1$, Ann. Inst. Fourier (Grenoble) 32 (4) (1982), 1–11.

[G1] G. Greaves, *On the divisor-sum problem for binary cubic forms*, Acta Arith. 17 (1970), 1–28.

[G2] —, *Large prime factors of binary forms*, J. Number Theory 3 (1971), 35–59, and Corrigendum, ibid. 9 (1977), 561–562.

[G3] —, *An application of a theorem of Barban, Davenport and Halberstam*, Bull. London Math. Soc. 6 (1974), 1–9.

[G4] —, *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.

[HB] D.-R. Heath-Brown, *The square sieve and consecutive square-free numbers*, Math. Ann. 266 (1984), 251–259.

[H1] C. Hooley, *On the greatest prime factor of a cubic polynomial*, J. Reine Angew. Math. 303/304 (1978), 21–50.

[H2] —, *On exponential sums and certain of their applications*, in: Journées Arithmétiques, London Math. Soc. Lecture Note Ser. 56, Cambridge Univ. Press, 1980, 92–122.

[I] H. Iwaniec, *A new form of the error term in the linear sieve*, Acta Arith. 37 (1980), 307–320.

[K-L] N. M. Katz et G. Laumon, *Transformation de Fourier et majoration de sommes d'exponentielles*, Publ. Math. I.H.E.S. 62 (1985), 361–418.

[L] G. Laumon, *Majoration de sommes d'exponentielles attachées aux hypersurfaces diagonales*, Ann. Sci. École Norm. Sup. (4) 16 (1983), 1–58.

[N1] T. Nagell, *Généralisation d'un théorème de Tchebycheff*, J. Math. Pures Appl. 4 (1921), 343–356.

[N2] —, *Introduction to the Number Theory*, New York, 1951.

[P] V. A. Plaksin, *An asymptotic formula for the number of solutions of a nonlinear equation for prime numbers*, Math. USSR-Izv. 18 (1982), 275–348.

[Si] J. H. Silverman, *The Arithmetic of Elliptic Curves*, Grad. Texts in Math. 106, Springer, New York, 1986.
[Sm] H. J. S. Smith, *Report on the Theory of Numbers*, Chelsea, New York, 1965.

Département de Mathématiques
Université de Nancy I
B.P. 239
54 506 Vandœuvre-lès-Nancy Cedex, France
E-mail: dartyge@iecn.u-nancy.fr

Reçu le 24.1.1996 (2917)