

# BULLETIN DE LA S. M. F.

E. FOUVRY

M. NAIR

G. TENENBAUM

## **L'ensemble exceptionnel dans la conjecture de Szpiro**

*Bulletin de la S. M. F.*, tome 120, n° 4 (1992), p. 485-506.

[http://www.numdam.org/item?id=BSMF\\_1992\\_\\_120\\_4\\_485\\_0](http://www.numdam.org/item?id=BSMF_1992__120_4_485_0)

© Bulletin de la S. M. F., 1992, tous droits réservés.

L'accès aux archives de la revue « Bulletin de la S. M. F. » (<http://smf.emath.fr/Publications/Bulletin/Presentation.html>), implique l'accord avec les conditions générales d'utilisation (<http://www.numdam.org/legal.php>). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme  
Numérisation de documents anciens mathématiques  
<http://www.numdam.org/>

## L'ENSEMBLE EXCEPTIONNEL DANS LA CONJECTURE DE SZPIRO

PAR

E. FOUVRY, M. NAIR ET G. TENENBAUM (\*)

---

RÉSUMÉ. — Nous montrons que, pour les deux types naturels de mesures associés à ce problème, la conjecture de Szpiro sur les courbes elliptiques semi-stables est satisfaite presque partout, avec beaucoup de marge. Dans les deux cas, nous donnons une majoration effective de la taille de l'ensemble exceptionnel.

ABSTRACT. — We show that, for the two natural measures associated with this problem, Szpiro's conjecture on semi-stable elliptic curves is true, with a lot to spare, almost always. In both cases, we give effective upper bounds for the size of the exceptional set.

### 1. Introduction et énoncé des résultats

Soit  $E$  une courbe elliptique sur  $\mathbb{Q}$ , de discriminant minimal  $\Delta_E$  et de conducteur  $N_E$ . La *conjecture de Szpiro forte*, cf. par exemple l'exposé d'ESTERLÉ [E], consiste à supposer que, si  $E$  est semi-stable, il existe pour chaque nombre réel  $\varepsilon > 0$  une constante  $C(\varepsilon)$  telle que

$$(1.1) \quad |\Delta_E| \leq C(\varepsilon)N_E^{6+\varepsilon}.$$

ESTERLÉ [E] et MASSER [Ma] ont fourni des contre-exemples impliquant que cet énoncé est quasi-optimal, au sens où l'on ne peut y remplacer  $\varepsilon$  par 0, ni même  $C(\varepsilon)N_E^\varepsilon$  par une puissance de  $\log N_E$ .

---

(\*) Texte reçu le 8 février 1991, révisé le 30 janvier 1992.

E. FOUVRY, Mathématiques (Bât. 425), Université de Paris XI-Orsay, 91405 Orsay Cedex, France.

M. NAIR, Department of Mathematics, University Gardens, Glasgow G12 8QW, Scotland, Royaume Uni.

G. TENENBAUM, Département de Mathématiques, Université de Nancy 1, BP 239, 54506 Vandœuvre Cedex, France.

Classification AMS : 11G05, 11N45, 11N25.

Même sous sa *forme faible*, où l'on demande seulement que (1.1) soit satisfaite pour au moins un  $\varepsilon > 0$ , la conjecture de Szpiro possède des conséquences drastiques sur divers problèmes célèbres tels que la conjecture de Fermat, cf. FREY [Fr], la conjecture *abc*, le nombre des points entiers d'une courbe elliptique sur  $\mathbb{Q}$ , cf. HINDRY-SILVERMAN [H-S], etc. Le lecteur pourra trouver dans les survols d'ESTERLÉ [E] et LANG [La] de plus amples informations concernant les statuts relatifs de ces questions.

Pour chaque courbe  $E/\mathbb{Q}$ , on a  $N_E \geq 2$  et  $N_E \mid \Delta_E$ . En introduisant le *quotient de Szpiro*

$$(1.2) \quad \beta_E := \frac{\log |\Delta_E|}{\log N_E} \geq 1,$$

on voit donc que la conjecture de Szpiro faible équivaut à l'existence d'une constante absolue  $K$  telle que l'on ait

$$(1.3) \quad \beta_E \leq K$$

pour toute courbe semi-stable sur  $\mathbb{Q}$ . De plus, comme on peut rendre  $|\Delta_E|$  arbitrairement grand en excluant  $E$  d'un nombre fini de classes d'isomorphismes sur  $\mathbb{Q}$ , on peut énoncer la conjecture de Szpiro forte sous la forme équivalente : *pour  $K > 6$ , il n'y a qu'un nombre fini de classes d'isomorphismes de courbes elliptiques semi-stables sur  $\mathbb{Q}$  telles que*

$$(1.4) \quad \beta_E \geq K.$$

Nous nous proposons ici de montrer que la conjecture de Szpiro forte est vérifiée pour "presque toute" courbe elliptique, semi-stable ou non, et d'évaluer, en un sens que nous préciserons, la taille de l'ensemble des courbes exceptionnelles.

Ce programme nécessite un paramétrage de l'ensemble des classes d'isomorphismes de courbes elliptiques sur  $\mathbb{Q}$ , que nous décrivons maintenant.

Chaque classe contient une courbe, notée  $E(a, b)$ , dont l'équation de Weierstrass est de la forme

$$(1.5) \quad y^2 = x^3 + ax + b \quad (a, b \in \mathbb{Z})$$

et dont le discriminant, nécessairement non nul, vaut

$$(1.6) \quad \Delta(a, b) := -16(4a^3 + 27b^2).$$

Ce représentant est unique lorsqu'on impose, par application inductive d'isomorphismes du type  $x \mapsto x/u^2, y \mapsto y/u^3$  ( $u \in \mathbb{Z}$ ), la condition de minimalité

$$(1.7) \quad p^4 \mid a \implies p^6 \nmid b.$$

(Ici et dans la suite, la lettre  $p$  désigne génériquement un nombre premier.) On peut alors vérifier, classiquement, que les seuls isomorphismes susceptibles de faire décroître le discriminant en valeur absolue sont du type  $(x, y) \mapsto (X, Y)$  avec  $x = u^2X + r, y = u^3Y + u^2sX + t$  et  $u \in \{1, 2, 3, 6\}, r, s, t \in \mathbb{Q}$ , cf. [Si, p.49]. Comme un tel isomorphisme divise le discriminant par  $u^{12}$ , on en déduit que

$$(1.8) \quad \Delta_{E(a,b)} = u^{-12} \Delta(a, b) \quad (u = 1, 2, 3 \text{ ou } 6).$$

Soient  $K \geq 1, A \geq 1, B \geq 1, D \geq 1$ . Nous désignons par  $S_0(D; K)$  le nombre des couples  $(a, b)$  satisfaisant (1.7) et tels que

$$(1.9) \quad 0 < |\Delta(a, b)| \leq D, \quad \beta_{E(a,b)} \geq K.$$

Nous introduisons aussi le nombre  $S_0(A, B; K)$  des couples  $(a, b)$  satisfaisant (1.7) et

$$(1.10) \quad |a| \leq A, \quad |b| \leq B, \quad \beta_{E(a,b)} \geq K.$$

Parallèlement, nous définissons les quantités  $S_1(D; K), S_1(A, B; K)$  obtenues en imposant la condition supplémentaire que  $E(a, b)$  est semi-stable. Les rapports

$$(1.11) \quad \frac{S_j(D; K)}{S_j(D; 1)}, \quad \frac{S_j(A, B; K)}{S_j(A, B; 1)} \quad (j = 0, 1)$$

constituent alors, pour  $K > 1$ , une mesure asymptotique, lorsque  $D$  et  $\max(A, B)$  tendent vers  $+\infty$ , de l'ensemble exceptionnel pour la conjecture de Szpiro. Nous montrerons plus loin l'existence d'une constante absolue positive  $c_0$  telle que l'on ait pour  $A \geq 16, B \geq 16$ ,

$$(1.12) \quad \begin{cases} S_0(D; 1) \geq S_1(D; 1) \geq c_0 D^{5/6}, \\ S_0(A, B; 1) \geq S_1(A, B; 1) \geq c_0 AB. \end{cases}$$

Ces estimations permettent d'interpréter les énoncés suivants, qui constituent l'objet principal de ce travail.

THÉORÈME 1. — Soient  $\varepsilon > 0, K \geq 1$ . Il existe une constante  $c_1 = c_1(\varepsilon, K)$  telle que l'on ait pour  $D \geq 3$

$$(1.13) \quad S_0(D; K) \leq c_1 D^{1/K} \exp \left\{ \left( \frac{1 + \log(c_2 K)}{K} + \varepsilon \right) \frac{\log D}{\log_2 D} \right\}$$

avec  $c_2 = 23\,409$ .

THÉORÈME 2. — Soit  $K > 1$ . On a

$$(1.14) \quad \lim_{A, B \rightarrow +\infty} \frac{1}{AB} S_0(A, B; K) = 0.$$

Dans tout l'article nous notons  $\log_k$  la  $k$ -ième itérée de la fonction logarithme.

Les THÉORÈMES 1 et 2 signifient que les exceptions à la conjecture de Szpiro sont rares. On a ainsi

$$(1.15) \quad S_1(D; 6) \leq S_0(D; 6) \leq S_1(D; 1)^{1/5+o(1)} \quad (D \rightarrow +\infty)$$

bien que les contre-exemples de Masser et Esterlé mentionnés plus haut impliquent que  $S_1(D; 6) \rightarrow +\infty$  ( $D \rightarrow +\infty$ ). Semblablement, le THÉORÈME 2 établit que  $\beta_{E(a,b)}$  est "presque partout" voisin de 1.

L'estimation (1.13) n'est vraisemblablement non triviale que pour  $K > 6/5$ , car il est raisonnable de conjecturer que  $S_0(D; 1) = D^{5/6+o(1)}$ . Une telle évaluation est probablement très délicate et certainement hors d'atteinte des méthodes développées dans ce travail.

La preuve du THÉORÈME 1 repose sur un résultat profond de DAVENPORT-HEILBRONN [D-H] concernant la 3-partie du groupe des classes des corps quadratiques. Les techniques utilisées consécutivement font partie de l'arsenal standard de la théorie analytique des nombres.

La démonstration du THÉORÈME 2 nécessite des outils analytiques plus sophistiqués, comme le grand crible arithmétique et le grand crible de Gallagher. Nous étendons la méthode développée par HOOLEY, cf. [Ho, chap. 4], pour montrer qu'un polynôme cubique irréductible dans  $\mathbb{Z}[X]$  prend des valeurs sans facteur carré pour une proportion positive des entiers. La technique du présent article permettrait d'établir la relation

$$(1.16) \quad \lim_{A, B \rightarrow +\infty} \frac{1}{AB} \left| \left\{ (a, b) : |a| \leq A, |b| \leq B, \mu(|a^3 + b^2|)^2 = 1 \right\} \right| = c$$

pour une constante positive convenable  $c$ , où  $\mu$  désigne la fonction de Möbius. Le seul outil algébrique intervenant dans la preuve du THÉORÈME 2 est une majoration classique des sommes de Jacobi, cf. [I-R, p. 103].

Nous achevons cette introduction par la preuve des relations (1.12). Considérons, pour  $A \geq 16$ ,  $B \geq 16$ , l'ensemble  $\mathcal{H}(A, B)$  des couples  $(a, b)$  satisfaisant à

$$(1.17) \quad \begin{cases} 0 < a \leq A, & 0 < b \leq B, & (a, b) = 16, \\ 3 \nmid a, & a \text{ et } b \equiv 16 \pmod{64}. \end{cases}$$

On a clairement

$$(1.18) \quad (a, b) \in \mathcal{H}\left(\frac{1}{10}D^{1/3}, \frac{1}{10}D^{1/2}\right) \implies 0 < |\Delta(a, b)| \leq D.$$

De plus, la relation (1.7) est satisfaite pour tout couple  $(a, b)$  de  $\mathcal{H}(A, B)$  puisque  $(a, b) = 16$  et  $2^6 \nmid b$ . Nous allons montrer que  $E(a, b)$  est semi-stable pour tout couple  $(a, b)$  de  $\mathcal{H}(A, B)$  et que l'on a, pour une constante absolue positive convenable  $c_3$ ,

$$(1.19) \quad |\mathcal{H}(A, B)| \geq c_3 AB.$$

Cela implique pleinement la validité de (1.12).

En effectuant le changement de variables  $x = 4X$ ,  $y = 8Y + 4$  dans l'équation (1.15) pour  $E(a, b)$ , nous obtenons l'équation de Weierstrass

$$(1.20) \quad Y^2 + Y = X^3 + \frac{a}{16}X + \frac{b-16}{64}$$

dont les invariants  $c_4$  et  $\Delta$  associés sont (cf. [Si, p. 46])

$$(1.21) \quad c_4 = -8a, \quad \Delta = -\frac{4a^3 + 27b^2}{16^2}.$$

On a  $(c_4, \Delta) = 1$ . Cela implique que l'équation (1.20) est minimale et que  $E$  est semi-stable [Ta, p. 189].

Il reste à établir (1.19). Observons pour cela que  $\mathcal{H}(A, B)$  contient en particulier tous les couples  $(a, b)$  de la forme

$$a = 16(1 + 12\alpha), \quad b = 16(1 + 12\beta),$$

avec  $(1 + 12\alpha, 1 + 12\beta) = 1$ ,  $0 \leq \alpha \leq A_1 := [A/1000]$ ,  $0 \leq \beta \leq B_1 := [B/1000]$ . D'où, en posant  $M_1 = 1 + 12 \min(A_1, B_1)$ ,

$$(1.22) \quad \begin{aligned} |\mathcal{H}(A, B)| &\geq A_1 B_1 - \sum_{5 \leq p \leq M_1} \sum_{\substack{0 \leq \alpha \leq A \\ p \mid 1+12\alpha}} \sum_{\substack{0 \leq \beta \leq B \\ p \mid 1+12\beta}} 1 \\ &\geq A_1 B_1 - \sum_{5 \leq p \leq M_1} \left(\frac{A_1}{p} + 1\right) \left(\frac{B_1}{p} + 1\right) \\ &\geq A_1 B_1 \left(1 - \sum_{p \geq 5} p^{-2}\right) - (A_1 + B_1) \log M_1 - M_1 \\ &\geq c_5 AB \end{aligned}$$

dès que  $M_1$  est assez grand. Assortie à la minoration triviale

$$|\mathcal{H}(A, B)| \geq A_1 + B_1 + 1$$

obtenue en considérant les couples  $(a, b)$  de la forme  $(16, 16(1 + 12\beta))$  et  $(16(1 + 12\alpha), 16)$ , l'estimation (1.22) implique bien (1.19).

*Remerciements.* — Cet article doit beaucoup à de stimulantes discussions que les auteurs ont eues avec Marc HINDRY et Sinnou DAVID. Nous tenons à leur exprimer ici notre gratitude.

## 2. Démonstration du Théorème 1

Désignons par  $k(n)$  le noyau d'un entier relatif  $n$ , soit

$$(2.1) \quad k(n) := \prod_{p|n} p.$$

Nous posons pour  $n \in \mathbb{Z}$

$$(2.2) \quad \beta(n) := \begin{cases} \frac{\log |n|}{\log k(n)} & \text{si } |n| > 1, \\ 0 & \text{si } |n| \leq 1. \end{cases}$$

Nous n'utilisons, parmi les propriétés du conducteur  $N_E$  d'une courbe elliptique  $E/\mathbb{Q}$ , que la relation de divisibilité

$$(2.3) \quad k(\Delta_E) \mid N_E.$$

Ainsi, on a certainement, pour toute courbe  $E(a, b)$ ,

$$(2.4) \quad \beta_{E(a,b)} \leq \beta(\Delta_{E(a,b)}).$$

Maintenant, la relation (1.8) implique

$$(2.5) \quad k(\Delta(a, b)) \leq 6k(\Delta_{E(a,b)}),$$

de sorte que l'on peut écrire

$$(2.6) \quad S_0(D; K) \leq \sum_{\substack{0 < |n| \leq D \\ k(n) \leq 6 D^{1/K}}} R(n)$$

où  $R(n)$  désigne le nombre de représentations de l'entier  $n$  sous la forme  $n = \Delta(a, b)$ .

Posons  $\delta(a, b) = a^3 + b^2$ . On a

$$(2.7) \quad -27\Delta(a, b) = \delta(12a, 108b).$$

Si  $r(n)$  dénote le nombre de représentations de  $n$  sous la forme  $n = \delta(a, b)$ , on a donc  $R(n) \leq r(-27n)$  et il suit

$$(2.8) \quad S_0(D; K) \leq \sum_{\substack{0 < |n| \leq 27D \\ k(n) \leq 18 D^{1/K}}} r(n).$$

A ce stade, il faut disposer d'une majoration pour  $r(n)$ . En l'absence d'une technique produisant spécifiquement des évaluations en moyenne, nous avons recours à une estimation individuelle. Les résultats classiques concernant le nombre des points entiers d'une courbe elliptique fourniraient ici des bornes prohibitives, et nous employons un théorème de EVERTSE-SILVERMAN [E-S] relatif aux équations du type  $y^m = f(x)$ , voir aussi [Sp]. Nous énonçons le théorème 1 (a) de [E-S] dans un cas particulier.

LEMME 1 (EVERTSE-SILVERMAN). — Soient  $S$  un ensemble fini de nombres premiers,  $R_S$  l'anneau des  $S$ -entiers de  $\mathbb{Q}$ ,  $f(X)$  un polynôme de degré  $d \geq 2$  dont le discriminant est inversible dans  $R_S$ ,  $L$  une extension algébrique de  $\mathbb{Q}$  de degré  $\ell$  et contenant au moins deux zéros de  $f$ ,  $m$  un entier  $\geq 3$ , et  $\kappa_m(L)$  le  $m$ -rang du groupe des classes d'idéaux de  $L$ . On a

$$(2.9) \quad \left| \{ (x, y) \in R_S \times \mathbb{Q} : y^m = f(x) \} \right| \leq 17^{\ell(6+|S|)} m^{2\ell|S| + \kappa_m(L)}.$$

Nous voulons appliquer ce résultat avec  $m = 3$  et  $f(x) = x^2 - n$ , de discriminant  $4n$ . Cela impose de choisir  $S = \{p : p \mid 2n\}$ , d'où  $|S| \leq 1 + \omega(n)$ , avec la notation traditionnelle  $\omega(n) := \sum_{p \mid n} 1$ . On choisit ensuite  $L = \mathbb{Q}(\sqrt{n})$ , de sorte que  $\ell = 1$  ou  $2$ . La relation (2.9) fournit alors

$$(2.10) \quad r(n) \leq c_6 c_2^{\omega(n)} h_3(n)$$

avec  $c_6 = 17^{14} \times 3^4$ ,  $c_2 = 17^2 \times 3^4 = 23\,409$ , et

$$(2.11) \quad h_3(n) := 3^{\kappa_3(\mathbb{Q}(\sqrt{n}))}.$$

L'estimation classique de l'ordre maximal de la fonction  $\omega(n)$  implique que l'on a

$$(2.12) \quad \omega(n) \leq \left\{ \frac{1}{K} + o(1) \right\} \frac{\log D}{\log_2 D} \quad (D \rightarrow +\infty)$$

pour tout entier  $n$  apparaissant dans la sommation (2.8). Il suit, pour  $\varepsilon > 0$  et  $K > 1$  fixés,

$$(2.13) \quad S_0(D; K) \ll \exp \left\{ \left( \frac{\log c_2}{K} + \varepsilon \right) \frac{\log D}{\log_2 D} \right\} H_3(27D, 18D^{1/K}),$$

où l'on a posé

$$(2.14) \quad H_3(x, y) := \sum_{\substack{0 < |n| \leq x \\ k(n) \leq y}} h_3(n).$$

Nous allons estimer (2.14). Observons d'abord que chaque entier  $n$  de  $\mathbb{Z}$  peut se décomposer de manière unique sous la forme  $n = qm^2t^2$ , avec  $q \in \mathbb{Z}$ ,  $\mu(|q|)^2 = 1$ ,  $t \geq 1$ ,  $k(t) \mid q$ ,  $m \geq 1$ ,  $(m, q) = 1$ . On a alors

$$(2.15) \quad k(n) = |q|k(m) \quad \text{et} \quad h_3(n) = h_3(q).$$

En introduisant la quantité

$$(2.16) \quad N(\xi, \eta) := |\{n \leq \xi : k(n) \leq \eta\}|$$

et en reportant dans (2.14), il vient

$$(2.17) \quad H_3(x, y) = \sum_{0 < |q| \leq y} \mu(|q|)^2 h_3(q) \sum_{\substack{1 \leq t \leq \sqrt{x/|q|} \\ k(t) \mid q}} N\left(\frac{1}{t} \sqrt{\frac{x}{|q|}}, \frac{y}{|q|}\right).$$

A ce stade, nous faisons appel à deux résultats élémentaires prouvés dans [Te 2, th. II.1.13 et th. III.5.3, respectivement]. Le premier découle d'une utilisation simple de la "méthode de Rankin" pour les majorations de sommes arithmétiques, le second est établi par récurrence grâce à la formule d'Euler-Mac Laurin.

LEMME 2. — On a pour  $\xi \geq \eta \geq 2$

$$(2.18) \quad N(\xi, \eta) \ll \eta \log \eta \exp \{ \sqrt{8 \log \xi} \}.$$

LEMME 3. — Soient  $a_1, a_2, \dots, a_k$  des nombres réels positifs. Désignons par  $N_k(z)$  le nombre des  $k$ -uples d'entiers  $(\nu_1, \nu_2, \dots, \nu_k)$  tels que  $\nu_1 \geq 0, \dots, \nu_k \geq 0$  et  $\sum_{i=1}^k \nu_i a_i \leq z$ . On a

$$(2.19) \quad N_k(z) \leq \frac{(z + a_1 + \dots + a_k)^k}{k!} \prod_{i=1}^k \frac{1}{a_i}.$$

Appliquons d'abord (2.18) sous la forme

$$(2.20) \quad N\left(\frac{1}{t} \sqrt{\frac{x}{|q|}}, \frac{y}{|q|}\right) \ll \frac{y}{|q|} \exp \{ 3 \sqrt{\log x} \}$$

pour tout couple  $(t, q)$  apparaissant dans la sommation de (2.17). Nous pouvons ensuite faire appel à (2.19) pour estimer le nombre des entiers  $t$  admissibles : il suffit de choisir  $a_i = \log p_i$  où  $p_1, \dots, p_k$  sont les facteurs premiers distincts de  $q$ . On obtient

$$(2.21) \quad \sum_{\substack{1 \leq t \leq \sqrt{x/|q|} \\ k(t) | q}} 1 \leq \frac{(\log x)^k}{k!} \prod_{p | q} \frac{1}{\log p} \quad (k = \omega(|q|)).$$

On peut encore majorer le membre de droite en étendant le produit aux  $k$  plus petits nombres premiers. De plus, on a certainement

$$(2.22) \quad k \leq (1 + o(1)) \frac{\log y}{\log_2 y} \quad (y \rightarrow +\infty)$$

puisque  $|q| \leq y$ . En insérant cette inégalité dans (2.21) et en effectuant le calcul par la formule de Stirling et le théorème des nombres premiers, on obtient que l'on a, pour tout  $\varepsilon > 0$  et uniformément pour  $y \rightarrow +\infty, y \leq x$ ,

$$(2.23) \quad \sum_{\substack{1 \leq t \leq \sqrt{x/|q|} \\ k(t) | q}} 1 \leq \exp \left\{ (1 + o(1)) \frac{\log y}{\log_2 y} \log \left( \frac{e \log x}{\log y} \right) \right\}.$$

Évaluons (2.17) à l'aide de (2.20) et (2.23), puis reportons le résultat obtenu dans (2.13). Il vient

$$(2.24) \quad S_0(D; K) \ll \exp \left\{ \left( \frac{1 + \log(c_2 K)}{K} + \varepsilon \right) \frac{\log D}{\log_2 D} \right\} y \sum_{0 < |q| \leq y} \frac{\mu(|q|)^2 h_3(q)}{|q|}$$

où l'on a posé  $y := 18 D^{1/K}$ . La majoration du THÉORÈME 1 découle alors, par sommation d'Abel, de l'évaluation suivante de DAVENPORT-HEILBRONN [D-H, lemme 7] :

LEMME 4 (DAVENPORT-HEILBRONN). — Soit  $h_3^*(d)$  le nombre des classes d'idéaux d'ordre 3 dans le groupe des classes du corps quadratique de discriminant  $d$ . On a

$$(2.25) \quad \sum_{0 < |d| \leq X} h_3^*(d) \ll X \quad (X \rightarrow +\infty).$$

En effet, on a lorsque  $q$  est sans facteur carré

$$h_3(q) = \begin{cases} 1 & \text{si } q = 1, \\ h_3^*(4q) & \text{si } q \equiv 2 \text{ ou } 3 \pmod{4}, \\ h_3^*(q) & \text{si } q \neq 1 \text{ et } q \equiv 1 \pmod{4}. \end{cases}$$

On a donc

$$(2.26) \quad \sum_{0 < |q| \leq y} \frac{\mu(|q|)^2 h_3(q)}{|q|} \leq \sum_{0 < |d| \leq 4y} \frac{h_3^*(d)}{|d|} \ll \log y$$

grâce à (2.25). Cela complète la preuve du THÉORÈME 1.

Il est à souligner que DAVENPORT et HEILBRONN obtiennent en fait dans [D-H] un équivalent asymptotique de la somme (2.25). Ce résultat est notablement plus difficile que la majoration utilisée ici.

### 3. Démonstration du Théorème 2

Soit  $K > 1$ ,  $\varepsilon := \frac{1}{3}(K - 1) > 0$ . Les relations (2.4) et (2.5) impliquent l'existence d'une constante  $k_0 = k_0(\varepsilon)$  telle que l'on ait

$$(3.1) \quad \beta_{E(a,b)} \leq (1 + \varepsilon)\beta(\Delta(a, b))$$

dès que  $k(\Delta(a, b)) > k_0(\varepsilon)$ . En tenant compte de (2.7), nous pouvons donc écrire

$$(3.2) \quad S_0(A, B; K) \leq \sum_{\substack{n \in \mathbb{Z} \\ \beta(n) > 1 + \varepsilon}} r(n; A, B) + \sum_{\substack{n \in \mathbb{Z} \\ k(n) \leq k_0(\varepsilon)}} r(n; A, B)$$

où  $r(n; A, B)$  désigne le nombre de représentations de l'entier  $n$  sous la forme  $n = \delta(a, b)$  avec  $|a| \leq 12A$ ,  $|b| \leq 108B$ .

Nous aurons besoin de six résultats auxiliaires, que nous établissons maintenant. Les paramètres  $A, B$  sont toujours  $\geq 1$ , et nous posons systématiquement dans la suite

$$(3.3) \quad X := (12A)^3 + (108B)^2, \quad Y := A + B, \quad Z := \min(A, B).$$

LEMME 5. — Pour  $m \geq 1$ , posons

$$(3.4) \quad T(m; A, B) := \sum_{\substack{n \in \mathbb{Z} \\ n \equiv 0 \pmod{m}}} r(n; A, B).$$

On a pour toute puissance de nombre premier  $p^\nu$

$$(3.5) \quad T(p^\nu; A, B) \ll \frac{AB}{p^{\nu - \lfloor \nu/6 \rfloor}} + \frac{A}{p^{\lfloor (\nu+2)/3 \rfloor}} + \frac{B}{p^{\lfloor (\nu+1)/2 \rfloor}} + Z.$$

*Démonstration.* — Décomposons la somme (3.4) en trois sous-sommes  $S_1, S_2, S_3$ , correspondant respectivement aux conditions supplémentaires

$$(S_1) : p \nmid a; \quad (S_2) : p^\nu \mid a^3; \quad (S_3) : p^\mu \parallel a, \quad 0 < \mu < \frac{1}{3}\nu.$$

Si le couple  $(a, b)$  est compté dans  $S_1$ , alors  $p \nmid ab$ . Lorsque  $a$  est fixé, la congruence  $b^2 \equiv -a^3 \pmod{p^\nu}$  possède au plus quatre solutions — cette valeur correspondant au cas  $p = 2$ ,  $\nu \geq 3$ , et pouvant être remplacée par 2 si  $p > 2$ . On a donc

$$S_1 \ll A \left( \frac{B}{p^\nu} + 1 \right).$$

Similairement, lorsque  $b$  est fixé,  $p \nmid b$ , la congruence  $a^3 \equiv -b^2 \pmod{p^\nu}$  possède au plus trois solutions. On a donc aussi

$$S_1 \ll B \left( \frac{A}{p^\nu} + 1 \right)$$

et finalement

$$(3.6) \quad S_1 \ll \frac{AB}{p^\nu} + Z.$$

Pour tout couple  $(a, b)$  compté dans  $S_2$ , on a  $p^\nu \mid a^3$ ,  $p^\nu \mid b^2$ , donc  $p^{\lfloor (\nu+2)/3 \rfloor} \mid a$ ,  $p^{\lfloor (\nu+1)/2 \rfloor} \mid b$ , et donc

$$(3.7) \quad S_2 \ll \left( \frac{A}{p^{\lfloor (\nu+2)/3 \rfloor}} + 1 \right) \left( \frac{B}{p^{\lfloor (\nu+1)/2 \rfloor}} + 1 \right).$$

Cette estimation est de l'ordre de grandeur du membre de droite de (3.5) puisque l'on a pour  $\nu \geq 1$

$$\left\lceil \frac{\nu+2}{3} \right\rceil + \left\lceil \frac{\nu+1}{2} \right\rceil \geq \nu - \left\lfloor \frac{\nu}{6} \right\rfloor.$$

Considérons maintenant un couple  $(a, b)$  compté dans  $S_3$ . On a, pour un certain entier  $\mu$  tel que  $3\mu < \nu$ ,  $p^{3\mu} \parallel a^3$  et donc  $p^{3\mu} \parallel b^2$ . En particulier,  $\mu$  est pair, disons  $\mu = 2m$ , et l'on peut écrire  $b = b_1 p^{3m}$ ,  $a = a_1 p^{2m}$ , avec  $p \nmid a_1 b_1$  et

$$a_1^3 + b_1^2 \equiv 0 \pmod{p^{\nu-6m}}.$$

La borne (3.6) fournit alors la majoration suivante pour le nombre des couples  $(a_1, b_1)$

$$\begin{aligned} &\ll \frac{(Ap^{-2m})(Bp^{-3m})}{p^{\nu-6m}} + \min\left(\frac{A}{p^{2m}}, \frac{B}{p^{3m}}\right) \\ &\ll \frac{AB}{p^{\nu-m}} + \frac{Z}{p^{2m}}. \end{aligned}$$

En sommant cette estimation pour  $1 \leq m \leq \lfloor \frac{1}{6}(\nu - 1) \rfloor$ , on obtient

$$(3.8) \quad S_3 \ll \frac{AB}{p^{\nu - \lfloor \nu/6 \rfloor}} + Z,$$

une borne qui est encore compatible avec (3.5). Cela achève la démonstration du LEMME 5.

LEMME 6. — Pour  $t \geq 1$ ,  $n \in \mathbb{Z}$ , posons

$$(3.9) \quad n_t := \prod_{\substack{p \leq t \\ p^\nu \parallel n}} p^\nu.$$

On a uniformément pour  $A \geq 1$ ,  $B \geq 1$ ,  $t \geq 2$ ,  $T \geq 2$ ,

$$(3.10) \quad \sum_{\substack{n \in \mathbb{Z} \\ n_t \geq T}} r(n; A, B) \ll AB \frac{\log t}{\log T} + Z \frac{t \log^2 X}{\log^2 t \cdot \log T}.$$

Démonstration. — On a

$$\sum_{\substack{n \neq 0 \\ n_t \geq T}} r(n; A, B) \log n_t = \sum_{p \leq t} \sum_{\substack{\nu \geq 1 \\ p^\nu \leq X}} T(p^\nu; A, B) \log p^\nu.$$

Par (3.5), cette quantité est

$$\begin{aligned} &\ll AB \sum_{p \leq t} \sum_{\nu \geq 1} \frac{\nu \log p}{p^{\nu - \lfloor \nu/6 \rfloor}} + A \sum_{p \leq t} \sum_{\nu \geq 1} \frac{\nu \log p}{p^{[(\nu+2)/3]}} \\ &\quad + B \sum_{p \leq t} \sum_{\nu \geq 1} \frac{\nu \log p}{p^{[(\nu+1)/2]}} + Z \sum_{p \leq t} \frac{\log^2 X}{\log p} \\ &\ll AB \log t + Zt \left( \frac{\log X}{\log t} \right)^2. \end{aligned}$$

Cela implique bien (3.10).

LEMME 7 (Grand crible de Gallagher [Ho]). — Soit  $\mathcal{A} \subseteq \{n : 1 \leq n \leq x\}$ . Pour chaque puissance de nombre premier  $q$ , on suppose que  $\mathcal{A}$  est confiné modulo  $q$  à  $\nu(q)$  classes résiduelles. Alors on a

$$(3.11) \quad |\mathcal{A}| \leq \left( \sum_{q \in \mathcal{E}} \Lambda(q) - \log x \right) / \left( \sum_{q \in \mathcal{E}} \frac{\Lambda(q)}{\nu(q)} - \log x \right)$$

où  $\Lambda$  désigne la fonction de von Mangoldt et où  $\mathcal{E}$  est un ensemble arbitraire de modules  $q$  tels que le dénominateur soit positif.

LEMME 8 (Grand crible arithmétique [Bo]). — Soit

$$\mathcal{B} \subseteq \{n : M \leq n \leq M + N\}$$

un ensemble d'entiers confiné, pour chaque nombre premier  $p$ , à  $p - w(p)$  classes résiduelles modulo  $p$ . On pose

$$(3.12) \quad g(q) := \mu(q)^2 \prod_{p|q} \frac{w(p)}{p - w(p)} \quad (q \geq 1).$$

Alors on a pour tout  $Q \geq 1$

$$(3.13) \quad |\mathcal{B}| \leq \frac{N + Q^2}{L}$$

avec

$$(3.14) \quad L := \sum_{q \leq Q} g(q).$$

LEMME 9 (TENENBAUM [Te 1]). — Soient  $\lambda_1, \lambda_2$ , des constantes réelles telles que  $\lambda_1 > 0$ ,  $0 < \lambda_2 < 2$ . Pour toute fonction multiplicative  $f$  telle que

$$0 \leq f(p^\nu) \leq \lambda_1 \lambda_2^\nu \quad (p \geq 2, \nu \geq 1),$$

on a uniformément pour  $x \geq 2$ ,  $t \geq 2$ ,  $T \geq 2$ ,

$$(3.15) \quad \sum_{\substack{1 \leq n \leq x \\ n_t \geq T}} f(n) \ll x \exp \left\{ -\lambda_3 \frac{\log T}{\log t} + \sum_{p \leq x} \frac{f(p) - 1}{p} \right\}$$

où  $\lambda_3$  est une constante positive ne dépendant que de  $\lambda_2$ .

Le sixième et dernier lemme est une variante d'un résultat de HOOLEY [Ho, chap. 4].

LEMME 10. — Soit  $F(z)$  un polynôme à coefficients entiers, de degré 3. On note  $\rho(m)$  le nombre de solutions de la congruence  $F(\nu) \equiv 0 \pmod{m}$ . Alors on a pour  $x \geq m \geq 1$

$$(3.16) \quad \sum_{\substack{1 \leq n \leq x \\ F(n) = m\ell^2}} 1 \ll \sqrt{x} \frac{\rho(m)}{\sqrt{m}} \prod_{p|m} \left(1 + 2 \frac{\log p}{p}\right)$$

où la constante implicite ne dépend que du coefficient directeur de  $F(z)$ .

Démonstration. — Soient  $r_j$  ( $1 \leq j \leq \rho(m)$ ) les racines de  $F$  modulo  $m$ . Désignons par  $\gamma(m)$  le membre de gauche de (3.16). On a

$$(3.17) \quad \gamma(m) = \sum_{1 \leq j \leq \rho(m)} \gamma_j(m),$$

avec 
$$\gamma_j(m) := \sum_{\substack{1 \leq n \leq x \\ F(n) = m\ell^2 \\ n \equiv r_j \pmod{m}}} 1.$$

Soit  $c_7$  une constante positive que nous préciserons plus loin. Nous considérons l'ensemble  $\mathcal{P}$  des nombres premiers  $p$  satisfaisant à

$$(P) \quad c_7 < p \leq x, \quad p \nmid m.$$

Si l'entier  $n$  est compté dans  $\gamma_j(m)$ , alors  $F(n)/m$  est un carré, donc en particulier résidu quadratique modulo  $p$  pour tout  $p$  de  $\mathcal{P}$ . Il existe par conséquent un résidu quadratique  $a_p \pmod{p}$  tel que

$$(3.18) \quad F(n) \equiv ma_p \pmod{p}.$$

Cela implique  $n \equiv \nu \pmod{p}$  où  $\nu$  est solution d'une équation de congruence du type

$$(3.19) \quad F(\nu) \equiv m\ell^2 \pmod{p}.$$

Soit  $S(m, p)$  le nombre des couple  $(\nu, \ell)$  solutions de (3.19) dans  $\mathbf{F}_p^2$ . Si  $a_p \neq 0$ , alors  $a_p$  possède deux représentations sous la forme  $\ell^2$  modulo  $p$ . Si  $a_p = 0$  et si le coefficient directeur de  $F$  n'est pas divisible par  $p$  (ce qui est réalisé dès que  $c_7$  excède ce coefficient), il y a au plus trois valeurs de  $\nu$  qui satisfont (3.19). En tout état de cause,

on voit que, si  $n$  est compté dans  $\gamma_j(m)$ , alors  $n$  est confiné à au plus  $3 + \frac{1}{2}(S(m, p) - 3) = \frac{1}{2}(S(m, p) + 3)$  classes résiduelles modulo  $p$ .

Lorsque  $c_7$  excède le coefficient directeur de  $F$ , l'équation (3.19) est celle d'une cubique singulière ou d'une courbe elliptique sur  $\mathbf{F}_p$ . Dans le premier cas, on sait que que  $S(m, p) - p$  vaut 0, 1 ou  $-1$ , selon le type de réduction (cf. [Si, p. 240]). Dans le second cas, le théorème de Hasse (cf. par exemple [Si, th. V.1.1]) implique

$$(3.20) \quad |S(m, p) - p| \leq 2\sqrt{p} \quad (p \in \mathcal{P}).$$

Cette inégalité est donc en fait valable sans restriction.

Nous estimons alors chaque  $\gamma_j(m)$  par le LEMME 7. Pour chaque puissance de nombre premier  $q$ , nous choisissons

$$\nu(q) := \begin{cases} 1 & \text{si } q \mid m, \\ \frac{1}{2}(S(m, p) + 3) & \text{si } q = p \in \mathcal{P}, \\ q & \text{dans tout autre cas.} \end{cases}$$

Etant donné un paramètre  $P$ ,  $1 \leq P \leq x$ , à optimiser, nous prenons dans le LEMME 3

$$\mathcal{E} = (\mathcal{P} \cap [1, P]) \cup \{p^\nu : p^\nu \mid m\}.$$

Le dénominateur de (3.11) vaut alors

$$\begin{aligned} \sum_{q \in \mathcal{E}} \frac{\Lambda(q)}{\nu(q)} - \log x &= \sum_{q \mid m} \Lambda(q) + 2 \sum_{\substack{c_7 < p \leq P \\ p \nmid m}} \frac{\log p}{S(m, p) + 3} - \log x \\ &= \log m + 2 \sum_{\substack{c_7 < p \leq P \\ p \nmid m}} \frac{\log p}{p} (1 + O(1/\sqrt{p})) - \log x \\ &= \log(mP^2x^{-1}) + O(1) - 2 \sum_{p \mid m} \frac{\log p}{p} \geq 1 \end{aligned}$$

pour le choix

$$P := c_8 \sqrt{\frac{x}{m}} \exp\left\{ \sum_{p \mid m} \frac{\log p}{p} \right\}$$

où  $c_8$  ne dépend que de  $c_7$ . Avec cette valeur de  $P$ , le numérateur de (3.11) vaut

$$\sum_{q \mid m} \Lambda(q) + \sum_{\substack{c_7 < p \leq P \\ p \nmid m}} \log p - \log x \leq \sum_{p \leq P} \log p - \log\left(\frac{x}{m}\right) \ll P.$$

On obtient donc

$$(3.21) \quad \gamma_j(m) \ll \sqrt{\frac{x}{m}} \prod_{p|m} \left(1 + 2 \frac{\log p}{p}\right)$$

où la constante implicite ne dépend que de  $c_7$ . Compte tenu de (3.17), on en déduit (3.16).

*Remarque :* la conclusion du LEMME 10 persiste lorsque  $F$  est un polynôme à coefficients entiers de degré impair. Il suffit d'invoquer le théorème de Weil [We] à la place de celui de Hasse — cf. SCHMIDT [Sch, p. 10–13] pour un énoncé précis obtenu par voie élémentaire. En fait, nous n'utiliserons ici le LEMME 10 que pour le polynôme  $F(z) = z^3 + b^2$ . Dans ce cas, on peut remplacer l'emploi du théorème de Hasse par une majoration classique des sommes de Jacobi — voir par exemple [I-R, chap. 8, th. 5, p. 103].

*Démonstration du théorème 2.* — On a

$$(3.22) \quad S_0(A, B; K) \leq N_\varepsilon(A, B) + N'_\varepsilon(A, B)$$

où  $N_\varepsilon(A, B)$  et  $N'_\varepsilon(A, B)$  désignent respectivement les deux sommes apparaissant au membre de droite de (3.2).

L'estimation de  $N'_\varepsilon(A, B)$  est facile. On a

$$(3.23) \quad \begin{aligned} N'_\varepsilon(A, B) &\leq \sum_{|n| \leq X^{1/4}} r(n; A, B) + \sum_{n_{k_0(\varepsilon)} > X^{1/4}} r(n; A, B) \\ &\ll_\varepsilon X^{\frac{1}{4}} Z + \frac{AB}{\log X} + Z \log X = o(AB) \quad (Z \rightarrow +\infty) \end{aligned}$$

où nous avons utilisé la majoration triviale  $r(n; A, B) \ll Z$  et le LEMME 6 avec  $t = k_0(\varepsilon)$ ,  $T = X^{1/4}$ .

Soit  $\eta$  un paramètre positif que nous expliciterons plus loin. Nous répartissons les entiers  $n$  comptés dans  $N_\varepsilon(A, B)$  en trois classes, correspondant respectivement aux conditions supplémentaires

$$\begin{aligned} (C1) \quad &|n| \leq X^{1/4}; \\ (C2) \quad &n_t > T := X^\eta, \quad (t := X^{\eta^2}); \\ (C3) \quad &|n| > X^{1/4}, \quad n_t \leq X^\eta. \end{aligned}$$

Nous désignons alors par  $N_j$  la contribution à  $N_\varepsilon(A, B)$  des entiers  $n$  de la classe  $(C_j)$  ( $1 \leq j \leq 3$ ).

Comme précédemment, on a

$$(3.24) \quad N_1 \ll Z X^{1/4} \ll \frac{AB}{\sqrt{X}} = o(AB) \quad (Z \rightarrow +\infty).$$

Le LEMME 6 implique immédiatement

$$(3.25) \quad N_2 \ll \eta AB + \frac{tZ}{\eta^5 \log X} = o(AB) \quad (Z \rightarrow +\infty)$$

pourvu que l'on ait

$$(3.26) \quad \eta \rightarrow 0, \quad \eta^5 \log X \geq 1 \quad (Z \rightarrow \infty).$$

Nous supposons désormais cette condition réalisée.

Nous allons voir que chaque entier  $n$  compté dans  $N_3$  est de la forme

$$(3.27) \quad n = p^2 h, \quad p > t.$$

Supposons en effet que  $p > t \Rightarrow p^2 \nmid n$ . Alors

$$\frac{|n|}{|n|^{1/(1+\varepsilon)}} \leq \frac{|n|}{k(n)} = \frac{n_t}{k(n_t)} \leq X^\eta,$$

d'où  $|n| \leq X^{\eta(1+\varepsilon)/\varepsilon}$ , ce qui contredit  $|n| > X^{1/4}$  pour  $Z$  assez grand compte tenu de (3.26). Il suit

$$(3.28) \quad N_3 \leq \sum_{\substack{n \in \mathbb{Z} \setminus \{0\} \\ n = p^2 h, p > t}} r(n; A, B).$$

Soit  $T_1 := Y \log Y / \sqrt{\log Z}$ . Grâce au LEMME 6, on peut majorer la contribution à (3.28) des  $p$  tels que  $t < p \leq T_1$ . Elle n'excède pas

$$\begin{aligned} \sum_{t < p \leq T_1} T(p^2; A, B) &\ll \sum_{t < p \leq T_1} \left( \frac{AB}{p^2} + \frac{Y}{p} + Z \right) \\ &\ll \frac{AB}{t} + Y \log \left( \frac{\log T_1}{\log t} \right) + \frac{Z T_1}{\log T_1} = o(AB) \end{aligned}$$

pour le choix

$$(3.29) \quad \eta := \frac{1}{\log_2 Z},$$

qui satisfait (3.26).

Pour achever la démonstration du THÉORÈME 2, il reste donc à établir que l'on a

$$(3.30) \quad N'_3 := \sum_{\substack{n \in \mathbb{Z} \setminus \{0\} \\ n = p^2 h, p > T_1}} r(n; A, B) = o(AB) \quad (Z \rightarrow +\infty).$$

Posons  $F_b(a) = a^3 + b^2$ . Si  $n = F_b(a) \neq 0$  est de la forme  $p^2 h$  avec  $p > T_1$ , on a certainement  $n = \ell^2 m$  avec  $\ell > T_1$ ,  $\mu(|m|)^2 = 1$ ,  $|m| \leq XT_1^{-2}$ . De plus, l'équation  $F_b(a) = \ell^2 m$  n'est soluble, à  $m$  fixé, que si  $b^2$ , et donc  $b$ , appartient à la suite  $\mathcal{C}(m)$  des entiers relatifs qui sont résidus cubiques modulo  $m$ . On peut donc écrire

$$(3.31) \quad N'_3 \leq \sum_{0 < |m| \leq XT_1^{-2}} \mu(|m|)^2 \sum_{\substack{|b| \leq 108B \\ b \in \mathcal{C}(m)}} \sum_{\substack{|a| \leq 12A \\ F_b(a) = m\ell^2}} 1.$$

Le LEMME 10 permet de majorer la somme intérieure. On obtient l'estimation

$$(3.32) \quad \ll \sqrt{\frac{A}{m}} \rho_b(m) h(m)$$

où  $\rho_b(m)$  est le nombre de racines de  $F_b$  modulo  $m$  et où  $h$  désigne la fonction fortement multiplicative définie par  $h(p) = 1 + 2(\log p)/p$ . Comme le coefficient directeur de  $F_b$  est 1, la constante implicite dans (3.32) est absolue.

Lorsque  $b \in \mathcal{C}(m)$ , disons  $b^2 \equiv -\beta^3 \pmod{m}$ , alors  $F_b(a) \equiv 0 \pmod{m}$  équivaut à  $a \equiv \xi_p \beta \pmod{p}$ , pour chaque facteur premier  $p$  de  $m$ , avec

$$\beta \not\equiv 0 \pmod{p} \Rightarrow \xi_p^3 \equiv 1 \pmod{p}.$$

Cette dernière équation possède exactement trois solutions si  $p \equiv 1 \pmod{3}$ , et une seule dans les autres cas. On obtient donc

$$(3.33) \quad \rho_b(m) \leq 3^{\omega(m_1)} \quad (b \in \mathcal{C}(m), \mu(|m|)^2 = 1),$$

où l'on a posé

$$(3.34) \quad m_1 := \prod_{\substack{p|m \\ p \equiv 1 \pmod{3}}} p.$$

En reportant (3.33) dans (3.32) puis (3.31), il vient

$$(3.35) \quad N'_3 \ll \sqrt{A} \sum_{1 \leq m \leq XT_1^{-2}} \mu(m)^2 \frac{3^{\omega(m_1)} h(m)}{\sqrt{m}} \sum_{\substack{|b| \leq 108B \\ b \in \mathcal{C}(m)}} 1.$$

Le grand crible arithmétique nous permettra d'estimer la somme intérieure. Nous spécialisons, dans le LEMME 8,

$$(3.36) \quad \begin{cases} w(p) = 0 & (p \nmid m_1), & w(p) = \frac{2}{3}(p-1) & (p \mid m_1), \\ N = 216B + 1, & Q = \sqrt{B}. \end{cases}$$

Il suit

$$(3.37) \quad \sum_{\substack{|b| \leq 108B \\ b \in \mathcal{C}(m)}} 1 \ll BL(m_1, \sqrt{B})^{-1},$$

avec

$$L(m_1, z) := \sum_{\substack{d \mid m_1 \\ d \leq z}} g(d), \quad g(d) := \prod_{p \mid d} \frac{2(p-1)}{p+2}.$$

Reportons (3.37) dans (3.35). Il vient

$$(3.38) \quad N'_3 \ll \sqrt{AB} \sum_{1 \leq m \leq XT_1^{-2}} \frac{\mu(m)^2 h(m) 3^{\omega(m_1)}}{\sqrt{m} L(m_1, \sqrt{B})}.$$

Nous décomposons la somme en  $m$  sous la forme  $M_1 + M_2$  où  $M_1$  correspond à la condition de sommation supplémentaire

$$(3.39) \quad m_1^* := \prod_{\substack{p \mid m_1 \\ p \leq B_1}} p > \sqrt{B} \quad (B_1 := \exp\{(\log B)^{3/4}\}).$$

Lorsque  $m_1^* > \sqrt{B}$ , on a  $\left( \prod_{p \mid m, p \leq B_1} p \right) > \sqrt{B}$ . En minorant  $L(m_1, \sqrt{B})$

par 1 et en appliquant le LEMME 9 à la fonction multiplicative  $m \mapsto f(m) = \mu(m)^2 h(m) 3^{\omega(m_1)}$ , on obtient, uniformément pour  $M \geq 2$ ,

$$\begin{aligned} \sum_{\substack{1 \leq m \leq M \\ m_1^* > \sqrt{B}}} f(m) &\ll M \exp\left\{-\frac{1}{2} \lambda_3(\log B)^{1/4} + \sum_{\substack{p \leq M \\ p \equiv 1 \pmod{3}}} \frac{2}{p}\right\} \\ &\ll M \log M \exp\left\{-\frac{1}{2} \lambda_3(\log B)^{1/4}\right\}. \end{aligned}$$

On en déduit par sommation d'Abel

$$(3.40) \quad M_1 \ll \frac{\sqrt{X}}{T_1} \log Y \exp \left\{ -\frac{1}{2} \lambda_3 (\log B)^{1/4} \right\}.$$

Lorsque  $m$  est compté dans  $M_2$ , on a

$$L(m_1, \sqrt{B}) \geq \sum_{d|m_1^*} g(d) = \prod_{p|m_1^*} \frac{3p}{p+2} =: G(m_1^*).$$

La fonction  $\theta(m) := \mu(m)^2 h(m) 3^{\omega(m_1)} G(m_1^*)^{-1}$  est multiplicative. On a

$$\theta(m) \leq \sum_{d|m} \lambda(d) \quad (m \geq 1)$$

où  $\lambda$  est la fonction multiplicative définie par

$$\lambda(p) = \begin{cases} \frac{2 \log p}{p} & \text{si } p \not\equiv 1 \pmod{3}, \\ \frac{2}{p} \left\{ 1 + \left( 1 + \frac{2}{p} \right) \log p \right\} & \text{si } p \equiv 1 \pmod{3} \text{ et } p \leq B_1, \\ 2 + \frac{6 \log p}{p} & \text{si } p \equiv 1 \pmod{3} \text{ et } p > B_1, \end{cases}$$

et  $\lambda(p^\nu) = 0$  pour  $\nu \geq 2$ . On a donc pour  $M \geq 2$

$$\begin{aligned} \sum_{m \leq M} \theta(m) &\leq \sum_{1 \leq d \leq M} \left[ \frac{M}{d} \right] \lambda(d) \\ &\ll M \exp \left\{ \sum_{\substack{B_1 < p \leq M \\ p \equiv 1 \pmod{3}}} \frac{2}{p} \right\} \ll M \left( 1 + \frac{\log M}{\log B_1} \right). \end{aligned}$$

Par sommation d'Abel, il suit

$$(3.41) \quad M_2 \ll \frac{\sqrt{X} \log Y}{T_1 (\log B)^{3/4}}.$$

En remarquant que  $\sqrt{X} T_1^{-1} \log Y \ll \sqrt{A \log Z}$ , on déduit donc de (3.40) et (3.41), en reportant dans (3.38), que

$$(3.42) \quad N'_3 \ll AB \frac{\sqrt{\log Z}}{(\log B)^{3/4}} \ll \frac{AB}{(\log Z)^{1/4}} = o(AB).$$

Cela achève la démonstration du THÉORÈME 2.

## BIBLIOGRAPHIE

- [Bo] BOMBIERI (E.). — *Le grand crible dans la théorie analytique des nombres*, Astérisque, t. **18**, 1974.
- [D-H] DAVENPORT (H.) et HEILBRONN (H.). — *On the density of discriminants of cubic fields*, Proc. Roy. Soc. London Ser. A, t. **322**, 1971, p. 405–420.
- [E-S] EVERTSE (J.-H.) and SILVERMAN (J.). — *Uniform bounds for the number of solutions of  $Y^n = f(X)$* , Math. Proc. Cambridge Philos. Soc., t. **100**, 1986, p. 237–248.
- [H-S] HINDRY (M.) and SILVERMAN (J.). — *The canonical height and integral points on elliptic curves*, Invent. Math., t. **93**, 1988, p. 419–450.
- [Ho] HOOLEY (C.). — *Applications of sieve methods to the theory of numbers*, Cambridge Tracts in Math., t. **70**, 1976.
- [I-R] IRELAND (K.) and ROSEN (M.). — *A classical introduction to Modern Number Theory*, Graduate Texts in Math., t. **84**, 1990.
- [La] LANG (S.). — *Old and new conjectured diophantine inequalities*, Bull. Amer. Math. Soc. (NS), t. **23,1**, 1990, p. 37–75.
- [Ma] MASSER (D.). — *Note on a conjecture of Szpiro*, Astérisque, **183**, 1990, Séminaire sur les pincesaux de courbes elliptiques, [L. Szpiro éd.], p. 19–23, Soc. Math. de France.
- [E] ESTERLE (J.). — *Nouvelles approches du théorème de Fermat*, Séminaire Bourbaki 1987–88, exposé n° 694.
- [Sch] SCHMIDT (W.). — *Equations over finite fields : an elementary approach*, Lecture Notes in Math., t. **536**, 1976.
- [Si] SILVERMAN (J.H.). — *The arithmetic of Elliptic curves*, Graduate Texts in Math., t. **106**, 1986.
- [Sp] SPRINDZUK (V.G.). — *On the number of solutions of the diophantine equation  $x^3 = y^2 + A$* , Dokl. Akad. Nauk BSSR, t. **7**, 1963, p. 9–11.
- [Ta] TATE (J.). — *The arithmetic of elliptic curves*, Invent. Math., t. **23**, 1974, p. 179–206.
- [Te1] TENENBAUM (G.). — *Un problème de probabilité conditionnelle en arithmétique*, Acta Arith., t. **49**, 1987, p. 165–187.

- [Te2] TENENBAUM (G.). — *Introduction à la théorie analytique et probabiliste des nombres*, Publications de l'Institut Élie Cartan n° 13, Département de Mathématiques de l'Université de Nancy I, 1990.
- [We] WEIL (A.). — *Sur les courbes algébriques et les variétés qui s'en déduisent*, Actualités Sci. Indust., t. **1041**, 1948.