Théorie des nombres / *Number Theory*

# SUR LE PLUS GRAND FACTEUR PREMIER DE $ax^m + by^n$

Yann Bugeaud

**Résumé** – Soient $a \neq 0$, $b \neq 0$ et $n \geq 2$ des entiers tels que $(a, b) = 1$. On montre que le plus grand facteur premier de $ax^m + by^n$, où $x$, $y$ et $m$ sont des entiers non nuls vérifiant $(ax, by) = 1$, $|x| > 1$ et $m \geq 2$, est minoré par $\log m$, modulo une constante multiplicative effective dépendant seulement de $a$, $b$ et $n$.

**On the greatest prime factor of $ax^m + by^n$**

**Abstract** – Let $a$, $b$ and $n$ be non-zero integers with $(a, b) = 1$ and $n \geq 2$. We show that the greatest prime factor of $ax^m + by^n$, where $x$, $y$ and $m$ are non-zero integers satisfying $(ax, by) = 1$, $|x| > 1$ and $m \geq 2$, is not less than $\log m$ times an effectively computable positive constant depending only on $a$, $b$ and $n$.

---

*Abridged English Version*

We denote by $P[n]$ the greatest prime factor of the rational integer $n$, with the convention that $P[n] = 1$ if $n \in \{0, \pm 1\}$. Shorey [3] proved that if the rational integers $a$, $b$, $x$, $y$ and $n$ satisfy

$$ab \neq 0, \quad |x| > 1, \quad y \neq 0, \quad (ax, by) = 1 \text{ and } n \geq 2, \tag{1}$$

then there exists an effectively computable positive constant $c_1 = c_1(a, b, n)$ such that for any integer $m \geq 2$ we have

$$P[ax^m + by^n] > c_1 (\log m)^{1/2} (\log\log m)^{1/2}. \tag{2}$$

In this Note, we substantially improve the above estimate.

**Theorem.** *Let $a$, $b$, $x$, $y$ and $n$ be rational integers satisfying (1). There exists an effectively computable positive constant $c_2 = c_2(a, b, n)$ such that for any integer $m \geq 2$ we have*

$$P[ax^m + by^n] > c_2 \log m.$$

For the proof of the Theorem, we carefully follow the same arguments as Shorey [3] (see also [4, Theorem 10.3]), excepted that we use a fundamental system of $S$-units with small height, which is the main source of our improvement.

Let us briefly sketch the proof. Assume for simplicity that $a = 1$ and $b = -1$. Denote by $2 =: p_1 < p_2 < \ldots$ the increasing sequence of prime numbers. Let $x$, $y$ and $n$ be integers satisfying (1), and let $m \geq 2$. Then, taking for $s$ the smallest integer such that $p_s \geq \max\{n, P[x^m - y^n]\}$, we can write $y^n - Az^n = x^m$, where $z$ is composed by the $p_i$'s and $A = \pm p_1^{t_1} \ldots p_s^{t_s}$, with $0 \leq t_i < n$. Letting $\mathbf{K} = \mathbf{Q}(\alpha)$, where $\alpha$ is a $n^{\text{th}}$ root of $A$, there exist two integer ideals $\mathfrak{a}$ and $\mathfrak{b}$ in $\mathbf{K}$ such that

$$(y - \alpha z)\, O_{\mathbf{K}} = \mathfrak{a}\, \mathfrak{b}^m \quad \text{and} \quad \mathfrak{a} \,\Big|\, \left( \prod_{i=1}^{s} p_i \right)^{m-1} O_{\mathbf{K}}.$$

Denote by $h$ the class number of $\mathbf{K}$ and by $r$ its unit rank. We infer from Lemme 1 and Lemme 2 (which directly follow from Lemmas 1, 2 and 3 and inequality (6.27) of [2]), that there exist a root of unity $\zeta \in \mathbf{K}$, a fundamental system $\varepsilon_1, \ldots, \varepsilon_r$ of units in $\mathbf{K}$, rational integers $m_i$, a generator $a_0$ of the principal ideal $\mathfrak{a}^h$ and $b_0 \in O_{\mathbf{K}}$ such that (6) is satisfied.

Then, taking for $S$ the set of places on $\mathbf{K}$ composed by the infinite places and the places induced by the $p_i$'s, we apply Lemme 1 to get a fundamental system $\xi_1, \ldots, \xi_{t-1}$ of $S$-units in $\mathbf{K}$ with small height, and, writing $a_0$ and $\varepsilon_1, \ldots, \varepsilon_r$ in terms of the $\xi_i$'s, we deduce (7) from (4), (5) and (6). Now, it suffices to use the same arguments as in [3] and [4, Chapter 10]. The upper bound for $m$ mainly depend on the quantity $E := \prod_{i=1}^{t-1} \log \mathrm{h}(\xi_i)$, and thus on the discriminant $D$ of the field $\mathbf{K}$, whose absolute value is not greater than $n^n \, (p_1^{t_1} \ldots p_s^{t_s})^{n-1}$. More precisely, we have the estimate (8), whence we get the desired result.

**Remark.** The same method allows us to recover a lower bound for $|x^m - y^n|$ of similar quality than Theorem 1 of [1].

---

## 1. Introduction et résultat

On note $P[n]$ le plus grand facteur premier de l'entier $n$, en convenant que $P[n] = 1$ si $n \in \{0, \pm 1\}$. Shorey [3] a montré que si les entiers $a$, $b$, $x$, $y$ et $n$ vérifient

$$ab \neq 0, \quad |x| > 1, \quad y \neq 0, \quad (x, y) = 1 \text{ et } n \geq 2, \tag{1}$$

alors il existe une constante effective $c_1 = c_1(a, b, n) > 0$, ne dépendant que de $a$, $b$ et $n$, telle que, pour tout entier $m \geq 2$, on ait

$$P[ax^m + by^n] > c_1 \, (\log m)^{1/2} \, (\log \log m)^{1/2}. \tag{2}$$

Dans cette Note, nous améliorons substantiellement cette estimation.

**Théorème.** *Soient $a$, $b$, $x$, $y$ et $n$ des entiers vérifiant (1). Il existe une constante effective $c_2 = c_2(a, b, n) > 0$ telle que, pour tout entier $m \geq 2$, on ait*

$$P[ax^m + by^n] > c_2 \log m.$$

Ce théorème constitue un cas particulier du résultat général suivant (*cf.* [4, Chapter 10]) dont nous présenterons une version explicite dans un travail ultérieur.

**Théorème ST.** *Soient $\mathbf{K}$ un corps de nombres, $O_{\mathbf{K}}$ son anneau d'entiers et $U_{\mathbf{K}}$ l'ensemble des unités de $\mathbf{K}$. Soit $f(X, Z) \in O_{\mathbf{K}}[X, Z]$ un polynôme homogène tel que $f(X, 1)$ est unitaire et possède au moins deux racines simples. Soient $\pi_1, \ldots, \pi_s$ des éléments de $O_{\mathbf{K}} \setminus U_{\mathbf{K}}$ et posons $\mathcal{S} := \{\pi_1^{a_1} \ldots \pi_s^{a_s} \mid a_i \geq 0\}$. Soit $\tau$ un réel strictement positif. Si $x \in O_{\mathbf{K}}$, $z \in \mathcal{S}$, $y \in O_{\mathbf{K}} \setminus U_{\mathbf{K}}$, $\gamma \in \mathcal{S}$, $\varepsilon \in U_{\mathbf{K}}$ et $m \geq 2$ vérifient $y \neq 0$ et $\min\{\mathrm{ord}_{\mathfrak{p}}(x), \mathrm{ord}_{\mathfrak{p}}(z)\} \leq \tau$ pour tout idéal premier $\mathfrak{p}$ de $O_{\mathbf{K}}$, et s'ils satisfont la relation*

$$f(x, z) = \varepsilon \, \gamma \, y^m,$$

*alors $m$ est majoré par une constante effective dépendant uniquement de $\mathbf{K}$, $f$, $\mathcal{S}$ et $\tau$.*

La démonstration du Théorème suit pas à pas celle de Shorey [3] (*cf.* également [4, Theorem 10.3]), à ceci près que l'on utilise un système fondamental de $S$-unités de petite hauteur, source principale de l'amélioration qualitative de (2).

## 2. Systèmes fondamentaux de $S$-unités

Soit $\mathbf{K}$ un corps de nombres de degré $d$ et de discriminant $D$. Soit $S$ un ensemble fini de places de $\mathbf{K}$ contenant l'ensemble $S_\infty$ des places infinies. On désigne par $s$ le cardinal de $S$ et par $P$ le plus grand nombre premier situé au-dessous d'une place finie de $S$, en convenant que $P = 1$ si $S$ est réduit à $S_\infty$.

A toute place $v$ sur $\mathbf{K}$, on associe une valeur absolue $|\,.\,|$ de la manière suivante. Si $v$ est infinie et correspond au plongement complexe $\sigma : \mathbf{K} \to \mathbf{C}$, on pose, pour tout $\alpha \in \mathbf{K}$,

$$|\alpha|_v = |\sigma(\alpha)|^{d_v},$$

avec $d_v = 1$ ou 2, selon que $\sigma(\mathbf{K})$ est contenu dans $\mathbf{R}$ ou non. Si $v$ est finie et correspond à l'idéal premier $\mathfrak{p}$ de $\mathbf{K}$, on pose $|0|_v = 0$ et, pour tout $\alpha \in \mathbf{K} \setminus \{0\}$,

$$|\alpha|_v = \mathrm{N}(\mathfrak{p})^{-\mathrm{ord}_{\mathfrak{p}}(\alpha)}.$$

La hauteur de Weil $\mathrm{h}(\alpha)$ d'un nombre algébrique $\alpha \in \mathbf{K}$ est définie par

$$\mathrm{h}(\alpha) = \Bigg( \prod_{v \text{ place sur } \mathbf{K}} \max\{1, |\alpha|_v\} \Bigg)^{1/d}.$$

En outre, on désigne par $\log^* u$ la quantité $\max\{\log u, 1\}$. Les lemmes ci-dessous se déduisent facilement des Lemmas 1, 2 et 3 et de l'inégalité (6.27) de [2].

**Lemme 1.** *Il existe un système fondamental $\xi_1, \ldots, \xi_{s-1}$ de $S$-unités de $\mathbf{K}$ possédant les propriétés suivantes*

$$\prod_{i=1}^{s-1} \log \mathrm{h}(\xi_i) \le s^{2s}\, |D|^{1/2} (\log^* |D|)^{d-1} (\log^* P)^s; \tag{3}$$

$$\log \mathrm{h}(\xi_i) \le s^{4s}\, |D|^{1/2} (\log^* |D|)^{d-1} (\log^* P)^s, \qquad i = 1, \ldots, s-1; \tag{4}$$

$$\begin{gathered} \textit{les coefficients de la matrice inverse de } (\log |\xi_i|_{v_j})_{i,j=1,\ldots,s-1} \\ \textit{sont majorés en valeur absolue par } s^{4s}. \end{gathered} \tag{5}$$

**Lemme 2.** *Pour tout entier algébrique $\alpha \in \mathbf{K} \setminus \{0\}$, il existe une unité $\varepsilon \in \mathbf{K}$ telle que*

$$\mathrm{h}(\varepsilon\, \alpha) \le |\mathrm{N}_{\mathbf{K}/\mathbf{Q}}(\alpha)|^{1/d} \exp\{d^{3d}\, |D|^{1/2} (\log^* |D|)^{d-1}\}.$$

### 3. Démonstration du Théorème

Afin de simplifier la rédaction, on se contente de traiter le cas particulier $a = 1$ et $b = -1$. On note $2 =: p_1 < p_2 < \ldots$ la suite ordonnée des nombres premiers et on utilisera, sans le préciser explicitement, que $l \log l \le p_l \le 3 l \log l$, pour tout entier $l > 1$. Soient $x$, $y$ et $n$ des entiers satisfaisant aux hypothèses du Théorème, et soit $m \ge 2$. Soit $s$ le plus petit entier vérifiant $p_s \ge \max\{n, P[x^m - y^n]\}$, il existe des entiers $u_1, \ldots, u_s$, positifs ou nuls, tels que $y^n \pm p_1^{u_1} \ldots p_s^{u_s} = x^m$. Après division euclidienne des $u_i$ par $n$, on aboutit à l'équation $y^n - A z^n = x^m$, avec $A = \pm p_1^{t_1} \ldots p_s^{t_s}$ et $0 \le t_i < n$, pour $1 \le i \le s$. Soit $\alpha$ une racine $n^{\text{ème}}$ de $A$ et soit $\mathbf{K}$ le corps $\mathbf{Q}(\alpha)$. On note $O_{\mathbf{K}}$ l'anneau des entiers de $\mathbf{K}$ et $D$ son discriminant.

Comme $p_s \ge n$, le discriminant du polynôme $X^n - A$ est produit de nombres premiers inférieurs ou égaux à $p_s$, donc, $y$ et $z$ étant premiers entre eux, il existe des idéaux entiers $\mathfrak{a}$ et $\mathfrak{b}$ appartenant à $\mathbf{K}$ tels que

$$(y - \alpha z)\, O_{\mathbf{K}} = \mathfrak{a}\, \mathfrak{b}^m \quad \text{et} \quad \mathfrak{a} \,\Bigg|\, \Bigg( \prod_{i=1}^{s} p_i \Bigg)^{m-1} O_{\mathbf{K}}.$$

Soient $h$ le nombre de classes de $\mathbf{K}$ et $r$ le rang du groupe des unités de $\mathbf{K}$. Les lemmes 1 et 2 appliqués avec $S$ réduit à l'ensemble des places infinies assurent l'existence d'un générateur $a_0$ de l'idéal principal $\mathfrak{a}^h$, d'un système fondamental $\varepsilon_1, \ldots, \varepsilon_r$ d'unités de $\mathbf{K}$, d'une racine de l'unité $\zeta \in \mathbf{K}$, d'entiers $m_i$, $1 \le i \le r$, et de $b_0 \in O_{\mathbf{K}}$ tels que

$$\begin{gathered} (y - \alpha z)^h = \zeta\, \varepsilon_1^{m_1} \ldots \varepsilon_r^{m_r}\, a_0\, b_0^m, \\ \log \mathrm{h}(a_0) \le n^{3n}\, |D|^{1/2} (\log^* |D|)^{n-1} + 5hms \log s, \\ \log \mathrm{h}(\varepsilon_i) \le n^{4n}\, |D|^{1/2} (\log^* |D|)^{n-1} \text{ et } 0 \le m_i < m, \; 1 \le i \le r. \end{gathered} \tag{6}$$

Soit $S$ l'ensemble des places de $\mathbf{K}$ formé des places infinies et des places induites par les idéaux de $\mathbf{K}$ situés au-dessus des $p_i$, $1 \le i \le s$. Soit $t$ le cardinal de $S$ et soit $\xi_1, \ldots, \xi_{t-1}$ un système fondamental de $S$-unités de $\mathbf{K}$ donné par le Lemme 1. Comme $a_0$ et les $\varepsilon_i$ sont des $S$-unités, ils s'écrivent comme produit des $\xi_i$ et d'une racine de l'unité. Ainsi, il découle de (4), (5), (6) et de la majoration $h \le |D|^{1/2} (\log^* |D|)^{n-1}$ qu'il existe une racine de l'unité $\zeta_0$ et des entiers $v_i$, $1 \le i \le t-1$, tels que

$$\begin{aligned} (y - \alpha z)^h &= \zeta_0 \, \xi_1^{v_1} \ldots \xi_{t-1}^{v_{t-1}} \, b_0^m \\ \text{avec} \qquad |v_i| &\le m \, t^{10t} \, |D|^{1/2} (\log^* |D|)^{n-1} (\log^* P)^t =: V. \end{aligned} \tag{7}$$

Il suffit maintenant de reprendre les arguments développés dans [3] et [4, Chapter 10]. Soit $\eta$ une racine primitive $n^{\text{ème}}$ de l'unité. On travaille dans le corps de nombres $\mathbf{K}(\eta) = \mathbf{Q}(\alpha, \eta)$ et l'équation $y^n - Az^n = x^m$ devient $\prod_{i=1}^{n} (y - \alpha \, \eta^i \, z) = x^m$. Pour toute valeur absolue $| \cdot |_v$ définie sur $\mathbf{K}(\eta)$, on minore les quantités $\left| \left( \frac{y - \alpha z}{y - \alpha \, \eta z} \right)^h - 1 \right|_v$ à l'aide des résultats de Waldschmidt [5] et de Kunrui Yu [6] concernant les formes linéaires de logarithmes archimédiens et ultramétriques. L'estimation finale dépend essentiellement de la quantité $E := \prod_{i=1}^{t-1} \log \mathrm{h}(\xi_i)$. Plus précisément, on obtient

$$\log \left( \frac{m}{\log^2 V} \right) \le c_3 \, n^2 \, p_s + c_4 \, \log E, \tag{8}$$

où $c_3$ et $c_4$ sont des constantes numériques effectives. Il découle de (3) et des majorations $t \le n(s+1)$ et $|D| \le n^n \, (p_1^{t_1} \ldots p_s^{t_s})^{n-1}$ que $\log E$ est borné par $c_5(n) \, p_s$, tandis que, dans les travaux antérieurs, la quantité jouant le même rôle est de l'ordre de $c_6(n) \, s \, p_s$ : le progrès résulte du Lemme 1 et plus particulièrement de (3). Les constantes $c_5(n), \ldots, c_9(n) > 0$ sont effectives et ne dépendent que de $n$. On déduit alors des inégalités (7) et (8) l'estimation $\log m \le c_7(n) \, p_s$. En outre, par définition de $s$, si $P[x^m - y^n]$ diffère de $p_s$, le postulat de Bertrand entraîne $p_s \le 2n$ et donc $m \le c_8(n)$. Ainsi, la minoration

$$P[x^m - y^n] \ge c_9(n) \, \log m$$

est valable dans tous les cas, comme annoncé.

**Remarque 1.** Si l'on avait utilisé directement la généralisation aux $S$-entiers du Lemme 2 (*cf.* [2, Lemma 2]) afin d'écrire $(y - \alpha z)^h = \zeta_1 \, \xi_1^{w_1} \ldots \xi_{t-1}^{w_{t-1}} \, b_1^m$, on n'aurait pas été en mesure d'affirmer que le nombre algébrique $b_1$ ainsi obtenu est entier. Or ce fait est déterminant dans la suite de la démonstration.

**Remarque 2.** En écrivant $x^m - y^n = \pm \, p_{i_1}^{w_1} \ldots p_{i_s}^{w_s}$, où les $p_{i_j}$ sont des nombres premiers distincts et les $w_j$ des entiers strictement positifs, puis en suivant la démonstration précédente, on obtient une minoration de $|x^m - y^n|$ indépendante de $x$ et de $y$, d'une qualité comparable au résultat principal de [1]. Il est intéressant de noter que le Théorème 1 de [1] repose uniquement sur des estimations de formes linéaires de logarithmes archimédiens et ne fait pas appel à la théorie ultramétrique.

**Références bibliographiques**

[1] **Bugeaud Y., 1996**. Sur la distance entre deux puissances pures, *C. R. Acad. Sci. Paris*, 322, Série I, p. 1119–1121.

[2] **Bugeaud Y. et Győry K., 1996**. Bounds for the solutions of Thue-Mahler equations and norm form equations, *Acta Arith.*, 74, p. 273–292.

[3] **Shorey T. N., 1980**. On the greatest prime factor of $ax^m + by^n$, *Acta Arith.*, 36, p. 21–25.

[4] **Shorey T. N. et Tijdeman R., 1986**. *Exponential Diophantine Equations*, Cambridge University Press, Cambridge.

[5] **Waldschmidt M., 1993**. Minorations de combinaisons linéaires de logarithmes de nombres algébriques, *Canadian J. Math.*, 45, p. 176–224.

[6] **Yu K., 1994**. Linear forms in $p$-adic logarithms *III*, *Compositio Math.*, 91, p. 241–276.

Yann Bugeaud
Université Louis Pasteur
U. F. R. de mathématiques
7, rue René Descartes
67084 STRASBOURG

e-mail : bugeaud@math.u-strasbg.fr
tel : 03 88 41 66 05 fax : 03 88 61 90 69