ON THE GREATEST PRIME FACTOR OF $ax^m + by^n$, *II*

YANN BUGEAUD (Strasbourg)

Abstract. In the present work, we provide a new lower bound for the greatest prime factor of the norm of algebraic numbers of the form $ax^m + by^n$. The improvement concerns the dependence on the number field containing a, b, x and y.

1. Introduction

Mahler [9] proved that the greatest prime factor of $ax^m + by^n$, where $m \geq 2$, $n \geq 3$, a and b are rational integers, tends to infinity as $\max\{|x|, |y|\} \to \infty$ with x, $y \in \mathbf{Z}$, $\gcd(x, y) = 1$. His proof was based on the method of Thue and Siegel and hence was ineffective. Using explicit upper bounds for the solutions of the Thue-Mahler equation, obtained by means of the theory of linear forms in logarithms, Kotov [8] gave an explicit version of the above theorem of Mahler, and generalized it to the number field case. Very recently, by means of our recent explicit bounds (see [3]) for the solutions of the generalized superelliptic equations, we have (see [4]) improved Kotov's result as follows. Let $\mathbf{K}$ be a number field of degree d with ring of integers $O_{\mathbf{K}}$. Denote by $h_{\mathbf{K}}$, $R_{\mathbf{K}}$ and $D_{\mathbf{K}}$ its class number, regulator and discriminant, respectively. For convenience, we write simply N instead of $\mathrm{N}_{\mathbf{K}/\mathbf{Q}}$ for the norm from $\mathbf{K}$ to $\mathbf{Q}$. If δ is a non-zero algebraic integer in $\mathbf{K}$, we denote by $P[\delta]$ the greatest prime number lying below a prime ideal dividing $\delta\, O_{\mathbf{K}}$. Further, we stand the notation $\log^* x$ for $\max\{\log x, 1\}$. Let α and β be algebraic integers in $\mathbf{K}$, with height (for definition, see Section 3) at most $A\,(A \geq 3)$.

Theorem 1. *Let $m \geq 2$ and $n \geq 3$ be distinct integers. Suppose that x and y are coprime algebraic integers in $\mathbf{K}$. Then there exist an effective absolute constant $c_1 > 0$ and an effective constant c_2, depending on m, n, A and $\mathbf{K}$, such that*

$$P[\alpha x^m + \beta y^n] \geq c_1 \, \frac{\log\log\max\{|\mathrm{N}(x)|, |\mathrm{N}(y)|\}}{d\, m^3\, n^3\, h_{\mathbf{K}}}, \tag{1}$$

provided that $\max\{|\mathrm{N}(x)|, |\mathrm{N}(y)|\} \geq c_2$.

We emphasize that Kotov's result involves the function $(\log\log)^{1/2} \times (\log\log\log)^{1/2}$ instead of an iterated logarithm. Further, Kotov did not make explicit the dependence of the constant in terms of m, n and $\mathbf{K}$.

1991 Mathematics Subject Classification : 11D61.

However, it turns out that Theorem 1 is not entirely satisfactory since the right-hand side of (1) heavily depends on the ground field $\mathbf{K}$. The aim of this note is to prove that we can suppress the factor $h_{\mathbf{K}}$ in (1), and thus relax the dependence on $\mathbf{K}$ to the dependence on the degree of $\mathbf{K}$, only. The result we obtain is best possible for the method and it is likely that it cannot be improved upon without a substantially new idea. We stress that, modulo standard results in algebraic number theory and Baker's theory, our text is self-contained.

2. Statement of the result

Theorem 1 can be sharpened as follows.

Theorem 2. *Let $m \geq 2$ and $n \geq 2$ be rational integers with $mn \geq 6$. Suppose that x and y are coprime algebraic integers in $\mathbf{K}$. Let $\varepsilon > 0$ be a real number. Then there exists an effectively computable constant c_3, depending on ε, m, n, A and $\mathbf{K}$, such that*

$$P[\alpha x^m + \beta y^n] \geq \frac{\log\log \max\{|\mathrm{N}(x)|, |\mathrm{N}(y)|\}}{(7+\varepsilon)\, d\, m\, n\, \min\{m, n\}},$$

provided that $\max\{|\mathrm{N}(x)|, |\mathrm{N}(y)|\} \geq c_3$.

Remark 1 : We point out that, unlike in Theorem 1, the integers m and n are not assumed to be distinct in the statement of Theorem 2. Hence, when $m = n \geq 3$, we obtain a slight sharpening of a previous result of Győry [7, Corollary 3].

Remark 2 : As already mentioned (see [4, Remark 1]), the improvement of Kotov's result regarding the dependence on $\max\{|\mathrm{N}(x)|, |\mathrm{N}(y)|\}$ is mainly due to the new approach of Bugeaud & Győry [5, 6] in giving improved explicit upper bounds for the solutions of the S-unit equation and the Thue-Mahler equation. The sharpening occurring in the present note is essentially a consequence of a very precise estimate of the different of an extension of number fields (*i.e.* the Dedekind-Hensel bound for relative discriminants).

Remark 3 : The usual way to prove a result like Theorem 1 is to deduce it from a general statement on superelliptic equations. This has been done in [4], using the bounds obtained in [3]. We notice that Theorem 2 may also be proved with this method. To this end, we first have to improve upon Theorem 2 of [3] by the use of the Dedekind-Hensel lemma : the factor $|\mathrm{N}_{\mathbf{K}/\mathbf{Q}}(\Delta_g)|$ arising in the estimate can be replaced by the product of the distinct prime factors dividing it, raised to the power $[\mathbf{K} : \mathbf{Q}]$. It suffices then to follow the proof of [4].

Acknowledgement : The author is very grateful to Yuri Bilu for kindly supplying him a self-contained proof of Theorem 2, which advantageously replaces his original proof.

3. Proof

Without loss of generality, we assume that $n \geq m$, hence that $n \geq 3$. In the sequel, $C_1, \ldots, C_7$ and all constants implied by $\ll$ and $\gg$ are effectively computable constants, which may depend on ε, $\mathbf{K}$, α, β, m and n, but are independent of x and y.

Denote by $\Omega_{\mathbf{K}}$ the set of places on $\mathbf{K}$. We choose a valuation $|\cdot|_v$ for every $v \in \Omega_{\mathbf{K}}$ in the following way : if v is infinite and corresponds to $\sigma : \mathbf{K} \to \mathbf{C}$ then we put, for $\alpha \in \mathbf{K}$, $|\alpha|_v = |\sigma(\alpha)|^{k_v}$, where $k_v = 1$ or 2 according as $\sigma(\mathbf{K})$ is contained in $\mathbf{R}$ or not; if v is finite and corresponds to the prime ideal $\mathfrak{p}$ in $\mathbf{K}$ then we put $|\alpha|_v = \mathrm{N}(\mathfrak{p})^{-\mathrm{ord}_{\mathfrak{p}}(\alpha)}$ for $\alpha \in \mathbf{K} \setminus \{0\}$ and $|0|_v = 0$.

The (absolute) height of $\alpha \in \mathbf{K}$ is defined by

$$\mathrm{h}(\alpha) = \prod_{v \in \Omega_{\mathbf{K}}} \max\{1, |\alpha|_v\}^{1/d}.$$

It depends only on α, and not on the choice of the number field containing α. In the sequel, we use the notation $\mathrm{h}^*(\cdot)$ for $\max\{\mathrm{h}(\cdot), 1\}$.

For a place v of $\mathbf{K}$ we denote by $\mathrm{N}v$ (respectively, p_v) the absolute norm of the corresponding prime ideal (respectively, the underlying rational prime), with the conventions $\mathrm{N}v = e$ and $p_v = 1$ for an infinite place v.

Let S_0 be the finite set of places of $\mathbf{K}$ consisting of the infinite places and the places v with $|\alpha x^m + \beta y^n|_v < 1$, and let

$$S = S_0 \cup \big\{v \mid p_v \leq \max\{m, n\}\big\} \cup \big\{v \mid |\alpha|_v < 1 \text{ or } |\beta|_v < 1\big\}.$$

Put $s = |S|$ and $\Delta = \prod_{v \in S} \mathrm{N}v$. Also, denote by $P = P[S]$ the maximal prime number below S. We may assume that $P[S] = P[S_0]$, since otherwise $P[S_0] \ll 1$, and there is nothing to prove.

To establish our result, it suffices to prove an estimate of the form

$$\mathrm{h}(x^m/y^n) \leq e^{7dm^2nP}\, C_1^{P \log\log P/\log P}. \tag{2}$$

Indeed, when x and y are coprime, $\mathrm{h}(x^m/y^n) \gg \log\max\{|\mathrm{N}x|, |\mathrm{N}y|\}$, and the theorem follows.

Put $\xi = x^m + \frac{b}{a}y^n$. Then $\mathrm{h}(x^m/y^n) \leq \mathrm{h}(x^m/\xi) + C_2$. Therefore it is sufficient to establish (2) with $\mathrm{h}(x^m/\xi)$ in the left-hand side.

To this end, we let ζ_m and ζ_n be primitive m-th and n-th roots of unity, respectively, and we put

$$\mu = \big((x\xi^{-1/m} - 1)^{1/n} - \zeta_n(x\xi^{-1/m} - \zeta_m)^{1/n}\big)^n.$$

Here, we use the branch of the function $z \mapsto z^{1/n}$ defined by $-\pi/n < \arg z^{1/n} \leq \pi/n$. It immediately follows that

$$\mathrm{h}^*(\mu) \ll \mathrm{h}^*(x^m/\xi) \ll \mathrm{h}^*(\mu). \tag{3}$$

We summarize useful results on μ and on the field $\mathbf{M} = \mathbf{K}(\mu)$ in the following assertion.

Proposition 1. *We have* $[\mathbf{M}:\mathbf{K}] \le m^2 n$ *and the discriminant* $D_{\mathbf{M}}$ *of* $\mathbf{M}$ *satisfies* $|D_{\mathbf{M}}| \ll \Delta^{m^2 n}$. *Further,* μ *is a* T*-unit, where* T *denotes the set of places of* $\mathbf{M}$ *lying above* S.

Proof : The field $\mathbf{L} := \mathbf{K}\bigl(\xi^{1/m}, \zeta_m\bigr)$ is of degree at most m^2 over $\mathbf{K}$, and $[\mathbf{M}:\mathbf{L}] \le n$ since

$$\mu = \bigl(x\xi^{-1/m} - \zeta_m\bigr)\left(\zeta_n^{-1}\left(\frac{x\xi^{-1/m}-1}{x\xi^{-1/m}-\zeta_m}\right)^{1/n} - 1\right)^n.$$

Hence we have $[\mathbf{M}:\mathbf{K}] \le m^2 n$.

To estimate the discriminant of $\mathbf{M}$, observe first of all that only places from S may be ramified in $\mathbf{L}$. Further, let w be a place of $\mathbf{L}$. The equality $-\frac{b}{a}y^n = \prod_{k=0}^{m-1}\bigl(x - \zeta_m^k \xi^{1/m}\bigr)$ implies that $n \mid \mathrm{ord}_w\bigl(x - \xi^{1/m}\bigr)$ unless w lies above S. Hence only places from S may be ramified in $\mathbf{L}\bigl(\zeta_n, (x-\xi^{1/m})^{1/n}\bigr)$, as well as in $\mathbf{L}\bigl(\zeta_n, (x-\zeta_m\xi^{1/m})^{1/n}\bigr)$. It follows that only places from S may be ramified in $\mathbf{M}$. The Dedekind-Hensel inequality (see e.g. Proposition 4.2.1 of [2]) yields $\mathrm{N}_{\mathbf{M}/\mathbf{Q}}\bigl(\mathrm{diff}_{\mathbf{M}/\mathbf{K}}\bigr) \ll \Delta^{[\mathbf{M}:\mathbf{K}]} \ll \Delta^{m^2 n}$, where $\mathrm{diff}_{\mathbf{M}/\mathbf{K}}$ denotes the different of $\mathbf{M}$ over $\mathbf{K}$. Hence we get $|D_{\mathbf{M}}| \ll \Delta^{m^2 n}$, as asserted.

Finally, μ is, obviously, a T-integer, and the equality

$$\prod_{k=1}^{n}\left(\bigl(x\xi^{-1/m}-1\bigr)^{1/n} - \zeta_n^k\bigl(x\xi^{-1/m}-\zeta_m\bigr)^{1/n}\right) = \zeta_m - 1$$

shows that μ is a T-unit. Proposition 1 is proved. □

The following assertion summarizes standard facts about T-units, which we apply to μ. We denote by R_T the T-regulator of $\mathbf{M}$ (for definition, see [5]).

Proposition 2. *There exists in* $\mathbf{M}$ *an independent system* $\eta_1, \dots, \eta_t$ *of the group of* T*-units modulo torsion with satisfies*

$$\mathrm{h}^*(\eta_1)\cdots\mathrm{h}^*(\eta_t) \ll t^t R_T.$$

If $\mu = \eta_0\eta_1^{b_1}\cdots\eta_t^{b_t}$, *where* η_0 *is a root of unity and the* b_i*'s are integers, then*

$$B := \max\{1, |b_1|\dots|b_t|\} \ll t^t \mathrm{h}^*(\mu).$$

Further, we have

$$R_T \ll |D_{\mathbf{M}}|^{1/2}\left(\log|D_{\mathbf{M}}|\right)^{dm^2 n}\left(dm^2 n\log P\right)^t.$$

Proof : A similar result (with t^t replaced by t^{2t}) concerning a *fundamental* system follows easily from Lemmas 1 and 3 of [5], inequality (5) of [5] and a lower bound for the height of algebraic numbers due to Voutier [10]. We just observe that the proof of Lemma 1 of [5] covers as well the case of *independent* systems and allows us to gain slightly on the dependence on t. □

In addition to μ, we also consider

$$\tilde\mu = \left((x\xi^{-1/m} - 1)^{1/n} - \zeta_n^2 (x\xi^{-1/m} - \zeta_m)^{1/n}\right)^n.$$

With obvious notation, we have $\tilde\mu = \tilde\eta_0 \tilde\eta_1^{\tilde b_1} \cdots \tilde\eta_{\tilde t}^{\tilde b_{\tilde t}}$, where $\tilde\eta_0$ is a root of unity, and analogous results as in Proposition 2 are true for $\tilde\mu$. Hence, with $\tilde B := \max\{1, |\tilde b_1| \dots |\tilde b_{\tilde t}|\}$, and noticing that t ant $\tilde t$ are bounded by sm^2n, we have:

$$\begin{aligned}
&\mathrm{h}^*(\eta_1)\cdots \mathrm{h}^*(\eta_t) \ll (sm^2n)^{sm^2n}\, \Delta^{m^2n/2} \,(\log\Delta)^{dm^2n}\,(dm^2n\log P)^{sm^2n},\\
&\mathrm{h}^*(\tilde\eta_1)\cdots \mathrm{h}^*(\tilde\eta_t) \ll (sm^2n)^{sm^2n}\, \Delta^{m^2n/2} \,(\log\Delta)^{dm^2n}\,(dm^2n\log P)^{sm^2n}
\end{aligned} \tag{4}$$

and

$$B \ll (sm^2n)^{sm^2n}\, \mathrm{h}^*(\mu), \quad \tilde B \ll (sm^2n)^{sm^2n}\, \mathrm{h}^*(\mu). \tag{5}$$

Since x^m/ξ is an S-integer, there exists $v \in S$ with $\log|x^m/\xi|_v \geq s^{-1}\mathrm{h}^*(x^m/\xi)$. We extend $|\cdot|_v$ to a metric of the algebraic closure of $\mathbf{K}$. For shorten the formulas, we set

$$\lambda := x\xi^{-1/m} - 1 \quad \text{and} \quad \lambda_1 := x\xi^{-1/m} - \zeta_m,$$

and we write Siegel's identity (at this point, we use that $n \geq 3$)

$$(1-\zeta_n)(\lambda - \zeta_n^2\,\lambda_1) + (\zeta_n - \zeta_n^2)(\lambda - \lambda_1) + (\zeta_n^2 - 1)(\lambda - \zeta_n\lambda_1) = 0. \tag{6}$$

We deduce from (6) that

$$\left|\frac{(1-\zeta_n^2)(\lambda - \zeta_n\lambda_1)}{(1-\zeta_n)(\lambda - \zeta_n^2\,\lambda_1)} - 1\right|_v = \left|\frac{(\zeta_n - \zeta_n^2)(\lambda - \lambda_1)}{(1-\zeta_n)(\lambda - \zeta_n^2\,\lambda_1)}\right|_v \ll \left|\frac{x^m}{\xi}\right|_v^{-1/m},$$

whence we get

$$\Lambda := \left|\left(\frac{1-\zeta_n^2}{1-\zeta_n}\right)^n \frac{\mu}{\tilde\mu} - 1\right|_v \ll \left|\frac{x^m}{\xi}\right|_v^{-1/m} \leq \exp\left(-\frac{\mathrm{h}^*(x^m/\xi)}{ms}\right). \tag{7}$$

We may assume that $\Lambda \neq 0$ since otherwise one immediately obtains a very sharp upper estimate for $\mathrm{h}(x^m/\xi)$. Putting $\theta = \eta_0\tilde\eta_0\left(\frac{1-\zeta_n^2}{1-\zeta_n}\right)^n$, we reproduce (7) as

$$-\log\Lambda = -\log\left|\theta\eta_1^{b_1}\cdots\eta_t^{b_t}\tilde\eta_1^{\tilde b_1}\cdots\tilde\eta_{\tilde t}^{\tilde b_{\tilde t}} - 1\right|_v \gg \frac{\mathrm{h}^*(x^m/\xi)}{s}. \tag{8}$$

Thanks to Baker's theory of linear forms in the logarithms of algebraic numbers, we can bound Λ from below. Applying the Theorem of Baker & Wüstholz [1] if v is archimedean, and the result stated in the Introduction of the paper by Kunrui Yu [11] if v is non–archimedean, we deduce from (4) that

$$\begin{aligned}
\log\Lambda &\geq -(t+\tilde t)^{2(t+\tilde t)}\, C_3^{t+\tilde t}\, P^{dm^2n^2}\, \mathrm{h}^*(\eta_1)\cdots\mathrm{h}^*(\eta_t)\,\mathrm{h}^*(\tilde\eta_1)\cdots\mathrm{h}^*(\tilde\eta_{\tilde t})\,\log(B+\tilde B)\\
&\geq -s^{6sm^2n}\, C_4^s\,\Delta^{m^2n}\,(\log\Delta)^{2dm^2n}\,P^{dm^2n^2}\,(\log P)^{2sm^2n}\,\log(B+\tilde B)
\end{aligned}$$

We infer from the Prime Number Theorem that $s^s \ll e^{dP}$ and $\Delta \leq e^{dP} \, C_5^{P \log\log P / \log P}$, hence we get

$$\log \Lambda \geq -e^{7dm^2nP} \, C_6^{P \log\log P / \log P} \, \log(B + \tilde{B}),$$

which, by (3), (5) and (8), yields $\mathrm{h}(x^m/\xi) \leq e^{7dm^2nP} \, C_7^{P \log\log P / \log P}$, as required.

Further, we may notice that it is possible to slightly refine the numerical constant 7 occurring in Theorem 2 by a suitable choice of the algebraic numbers μ and $\tilde{\mu}$. □

References

1. A. Baker and G. Wüstholz, 'Logarithmic forms and group varieties', *J. reine angew Math.* 442 (1993), 19–62.

2. Y. Bilu, 'Quantitative Siegel's theorem for Galois coverings', *Compositio Math.* 106 (1997), 125–158.

3. Y. Bugeaud, 'Bounds for the solutions of superelliptic equations', *Compositio Math.* 107 (1997), 187–219.

4. Y. Bugeaud, 'On the greatest prime factor of $ax^m + by^n$', Proceedings of the Number Theory Conference, Eger 1996, Eds. Győry, Pethő, Sós. de Gruyter, p. 115–122, 1998.

5. Y. Bugeaud and K. Győry, 'Bounds for the solutions of unit equations', *Acta Arith.* 74 (1996), 67–80.

6. Y. Bugeaud and K. Győry, 'Bounds for the solutions of Thue-Mahler equations and norm form equations', *Acta Arith.* 74 (1996), 273–292.

7. K. Győry, 'On the greatest prime factors of decomposable forms at integer points', *Ann. Acad. Sci. Fenn. Ser. A1* 4 (1979), 341–355.

8. S. V. Kotov, 'Ueber die maximale Norm der Idealteiler des Polynoms $\alpha x^m + \beta y^n$ mit den algebraischen Koeffizienten', *Acta Arith.* 31 (1976), 219–230.

9. K. Mahler, 'On the greatest prime factor of $ax^m + by^n$', *Nieuw Archief voor Wisk.* 3 (1953), 113–132.

10. P. M. Voutier, 'An effective lower bound for the height of algebraic numbers', *Acta Arith.* 74 (1996), 81–95.

11. Kunrui Yu, 'P–adic logarithmic forms and group varieties I', *J. reine angew. Math.* 502 (1998), 29–92.

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

e-mail : bugeaud@math.u-strasbg.fr