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

Yann Bugeaud (Strasbourg)

1. Introduction

Mahler [6] 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 $X := \max\{|x|, |y|\} \to \infty$ 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 [5] gave an explicit version of the above theorem of Mahler, and generalized it to the number field case. Namely, he proved that there exist effectively computable positive constants $c_1 = c_1(a,b,m,n)$ and $c_2 = c_2(a,b,m,n)$ such that

$$P[ax^m + by^n] \geq c_1 \left((\log\log X)\,(\log\log\log X) \right)^{1/2}, \tag{1}$$

whenever $X \geq c_2$, where $x, y \in \mathbf{Z}$, $\gcd(x,y) = 1$.

In this work, we considerably improve the lower bound (1) and make explicit the constant corresponding to c_1. In our proof we follow a more direct approach by using our recent explicit bounds (cf. [1]) for the solutions of the generalized superelliptic equations.

2. Statement of the results

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. *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 $c_3 > 0$ and an effective constant c_4, depending on m, n, A and $\mathbf{K}$, such that*

$$P[\alpha x^m + \beta y^n] \geq c_3\, \frac{\log\log \max\{|\mathrm{N}(x)|, |\mathrm{N}(y)|\}}{d\, m^3\, n^3\, h_{\mathbf{K}}},$$

provided that $\max\{|\mathrm{N}(x)|, |\mathrm{N}(y)|\} \geq c_4$.

This theorem is a direct consequence of the next proposition, which requires some more notation.

Let S be a finite set of places on $\mathbf{K}$, including the set of infinite places S_∞. Denote by $\mathfrak{p}_1, \ldots, \mathfrak{p}_t$ the t prime ideals corresponding to the finite places of S and by O_S the ring of

S-integers in $\mathbf{K}$. Further, let P be the largest of the rational primes lying below the finite places of S, with the convention that $P=1$ if $S=S_\infty$. We consider a monic polynomial

$$f(X) := \prod_{i=1}^{r} (X-\alpha_i)^{e_i} \in O_{\mathbf{K}}[X]$$

of degree $n \geq 2$ and distinct roots $\alpha_1, \ldots, \alpha_r$. Put $m_i := m/\gcd(e_i, m)$ for $i = 1, \ldots, r$.

Let $m \geq 2$ be an integer and $a \in O_{\mathbf{K}} \setminus \{0\}$. Consider the equation

$$f(x) = a\, y^m \ \text{ in } \ (x, y) \in O_S \times \mathbf{K}. \tag{2}$$

Put $\Delta_f := \prod_{i \neq j} (\alpha_i - \alpha_j)$ and denote by H the height (for definition, see Section 3) of the polynomial f. Further, suppose that $|\mathrm{N}(a)|$ is at most $A\,(\geq e)$.

The proposition below is a more explicit version of Theorem 2 of [1].

Proposition. *Suppose that there exist $1 \leq i \neq j \leq r$ such that $gcd(m_i, m_j) \geq 3$. If $gcd(m_i, m_j)$ is not a power of 2, let m' be the smallest odd prime number dividing it, otherwise put $m' = 4$. Then all the solutions of (2) satisfy*

$$\mathrm{h}(x) \leq H^{m'+1} \exp\bigl\{\bigl(c_5\, n\, m(d+t)\bigr)^{c_6\, n^2 m(d+t)}\, P^{dn^2 m'^3}\, (\log^* P)^{tn^2 m'}$$
$$|D_{\mathbf{K}}|^{5n^2 m'/2}\, |\mathrm{N}(\Delta_f)|^{5nm'}\, A^{n^2 m'} \bigl(\log |A\, D_{\mathbf{K}}\, \mathrm{N}(\Delta_f)|\bigr)^{2dn^2 m'}\bigr\},$$

where c_5 and c_6 are effectively computable positive absolute constants.

Remark 1 : It is worth noting that the improvement of Kotov's result is mainly due to the new approach of Bugeaud and Győry in giving improved explicit upper bounds for the solutions of the S-unit equation and the Thue-Mahler equation. Indeed, in [2] and [3], the authors use fundamental systems of S-units and S-regulators in order to improve the dependence on S in the parameters of the ground field $\mathbf{K}$. Thanks to this new method, they manage to remove the dependence on the number of finite places in S in the exponent of the regulator of $\mathbf{K}$. Consequently, as explained in [1], the exponents of H, $|D_{\mathbf{K}}|$ and $|\mathrm{N}(\Delta_f)|$ occurring in the above proposition are all independent of t. And they would be linear in t if we would use earlier results about S-unit equations : see Trelina [9] and Theorem 1.2 of Chapter *VII* in the book of Sprindžuk [8]. That is the reason why we are able to replace $\bigl((\log\log X)(\log\log\log X)\bigr)^{1/2}$ by $\log\log X$ in (1).

Remark 2 : With a slight modification, the conclusion of the Theorem remains true in the case $m = n \geq 3$. Indeed, Győry [4, Corollary 3] proved that

$$P[\alpha x^m + \beta y^m] > \bigl((13n!+1)d\bigr)^{-1} \log\log \max\bigl\{|\mathrm{N}(x)|, |\mathrm{N}(y)|\bigr\}$$

for all coprime algebraic integers x, y in $\mathbf{K}$, provided that $\max\bigl\{|\mathrm{N}(x)|, |\mathrm{N}(y)|\bigr\}$ is sufficiently large. Notice however that the constant $\bigl((13n!+1)d\bigr)^{-1}$ can be considerably reduced by using the new results of Bugeaud & Győry [2, 3].

3. Auxiliary results

Let $\mathbf{K}$ be a number field with the same parameters as in Section 2. 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 $\mathbf{K}$. We recall that $\mathrm{h}(\alpha^{-1}) = \mathrm{h}(\alpha)$ for $\alpha \in \mathbf{K} \setminus \{0\}$, and

$$\mathrm{h}(\alpha_1 \dots \alpha_m) \le \mathrm{h}(\alpha_1) \dots \mathrm{h}(\alpha_m),$$
$$\mathrm{h}(\alpha_1 + \dots + \alpha_m) \le m\mathrm{h}(\alpha_1) \dots \mathrm{h}(\alpha_m)$$

for $\alpha_1, \dots, \alpha_m \in \mathbf{K}$.

For a polynomial $F(X) = X^l + b_{l-1}X^{l-1} + \dots + b_0 \in \mathbf{K}[X]$, we define its height $\mathrm{h}(F)$ by

$$\mathrm{h}(F) = \Big(\prod_{v \in \Omega_{\mathbf{K}}} \max\{1, |b_0|_v, \dots, |b_{l-1}|_v\} \Big)^{1/d}.$$

Lemma 1 ensures that every non-zero algebraic integer in $\mathbf{K}$ has an associate with relatively small height.

Lemma 1. *For every $\alpha \in O_{\mathbf{K}} \setminus \{0\}$ and every integer $n \ge 1$, there exists a unit $\varepsilon \in O_{\mathbf{K}}$ such that*

$$\mathrm{h}(\varepsilon^n \alpha) \le |\mathrm{N}(\alpha)|^{1/d} \exp\{n\, d^{3d}\, R_{\mathbf{K}}\}.$$

Proof : This is a weaker version of Lemma 2 of [3]. We use inequality (5.5) of [3] (due to Voutier, see [10]) in order to obtain the upper bound (notation of [3]) :

$$c_{10}(d, r) \le c_{10}(d, d-1) \le (d-1)^d \left(\log(3d)\right)^{3d-6} \le d^{3d},$$

and the lemma follows. □

We also need some well-known results about the order of magnitude of the n-th prime number.

Lemma 2. *Let $2 =: p_1 < p_2 < \dots < p_t < \dots$ be the sequence of prime numbers in increasing order. Then we have for every integer $t \ge 2$:*

(i)
$$t \log t \le p_t \le 3t \log t$$

(ii)
$$t^t \le \prod_{i=1}^{t} p_i \le t^{4t}.$$

Proof : These inequalities follow from inequalities (3.12), (3.13), (3.33) and (3.32) of [7]. □

4. Proofs

Proof of the Proposition.

We only outline the proof and point out the most crucial steps, where the final dependence on d, m, n and t appears. In the sequel, $\kappa_1, \ldots, \kappa_{12}$ denote computable numerical positive constants and $c_{51}, \ldots, c_{69}$ are the constants occurring in [1].

It is not difficult to see that the constants c_{51} to c_{55} are bounded from above by $\kappa_1\, t\,(nmd)^{\kappa_2\, nd}$. Further, since the cardinality of $S_{\mathbf{M}}$ is not greater than $tn^2m + dn^2m$, it follows from [3, Theorem 2] that we can take $c_{56} \le \kappa_3 \bigl((d+t)nm\bigr)^{\kappa_4\,(d+t)n^2m}$. Finally, noticing that $c_{60} \le \kappa_5\, m^{\kappa_6\, n^2 d}$, we clearly obtain that $c_{62} \le \kappa_7 \bigl((d+t)nm\bigr)^{\kappa_8\,(d+t)n^2m}$.

We now deal with Case (ii). We see easily that $\mathbf{M}_1$ contains at most dmn^2 (resp. tn^2m) infinite (resp. finite) places. Hence, using [2, Theorem], we infer that $c_{65} \le \kappa_9 \bigl((d+t)nm\bigr)^{\kappa_{10}\,(d+t)n^2m}$, a similar bound being valid for c_{69}.

Since the same arguments are used for Cases (iii) to (v), they clearly yield the same bounds. Hence, the constant $c_3(d,n,m,t)$ occurring in Theorem 2 of [1] is bounded above by $\kappa_{11} \bigl((d+t)nm\bigr)^{\kappa_{12}\,(d+t)n^2m}$, as claimed. $\square$

Proof of the Theorem.

Denote by $2 =: p_1 < p_2 < \ldots < p_t < \ldots$ the sequence of primes ranged in increasing order, and by $\mathfrak{p}_{i,1}, \ldots, \mathfrak{p}_{i,l_i}$ the prime ideals in $\mathbf{K}$ lying above the prime number p_i. Since α, β, x and y are all algebraic integers, there exist non-negative integers $u_{i,j}$ such that

$$(\alpha^m\, x^m + \alpha^{m-1}\,\beta\, y^n) O_{\mathbf{K}} = \mathfrak{p}_{1,1}^{u_{1,1}} \ldots \mathfrak{p}_{t,l_t}^{u_{t,l_t}}. \tag{3}$$

Suppose first that $\alpha^m\, x^m + \alpha^{m-1}\,\beta y^n$ is not a unit. Then at least one of the $u_{i,j}$'s is non-zero and there is no restriction in assuming that $u_{t,1}$ is positive. Observe that $p_t = P[\alpha^m\, x^m + \alpha^{m-1}\,\beta\, y^n]$ and set $P := p_t$.

By Lemma 1, there exists a generator $\pi_{i,j}$ of the principal ideal $\mathfrak{p}_{i,j}^{h_{\mathbf{K}}}$ satisfying

$$\mathrm{h}(\pi_{i,j}) \le \mathrm{N}\bigl(\mathfrak{p}_{i,j}\bigr)^{h_{\mathbf{K}}/d}\, \exp\bigl\{d^{3d}\, R_{\mathbf{K}}\bigr\}. \tag{4}$$

Denoting by $w_{i,j}$ the quotient in the Euclidean division of $u_{i,j}$ by $mnh_{\mathbf{K}}$, we deduce from (3) that

$$\alpha^m\, x^m + \alpha^{m-1}\,\beta\, y^n = \delta\, \pi_{1,1}^{mnw_{1,1}} \ldots \pi_{t,l_t}^{mnw_{t,l_t}}, \tag{5}$$

where $\delta \in O_{\mathbf{K}}$ and $\mathfrak{p}_{i,j}^{mnh_{\mathbf{K}}}$ does not divide δ for all i, j with $1 \le i \le t$ and $1 \le j \le l_i$. Further, we have

$$\bigl|\mathrm{N}(\delta)\bigr| \le \prod_i \Bigl(\prod_j \mathrm{N}\bigl(\mathfrak{p}_{i,j}\bigr)^{mnh_{\mathbf{K}}}\Bigr) \le \prod_i p_i^{dmnh_{\mathbf{K}}},$$

and, since $t \ge 1$, we infer from (ii) of Lemma 2 that

$$\bigl|\mathrm{N}(\delta)\bigr| \le \max\bigl\{2^{dmnh_{\mathbf{K}}}, t^{4tdmnh_{\mathbf{K}}}\bigr\} \le (2t)^{4tdmnh_{\mathbf{K}}}. \tag{6}$$

Further, we infer from Lemma 1 that there exist a unit $\eta \in O_{\mathbf{K}}$ and $\varepsilon \in O_{\mathbf{K}}$ such that

$$(7) \qquad \delta = \eta^{mn}\,\varepsilon \text{ and } \mathrm{h}(\varepsilon) \leq (2t)^{4tmnh_{\mathbf{K}}} \exp\{mnd^{3d}\,R_{\mathbf{K}}\}.$$

Put $\rho := \prod_{i,j} \pi_{i,j}^{w_{i,j}}$. From (5) we obtain

$$(8) \qquad \left(\frac{\alpha x}{(\eta\rho)^n}\right)^m - \varepsilon = -\alpha^{m-1}\,\beta\left(\frac{y}{(\eta\rho)^m}\right)^n.$$

In order to apply our proposition to equation (8), we need to define the set of places S and to give a precise estimate for the discriminant Δ_f and the height $h(f)$ of the polynomial $f(X) := X^m - \varepsilon$. To this end, we use (6) and (7) and we easily deduce that

$$(9) \qquad \left|\mathrm{N}(\Delta_f)\right| \leq m^{md}\left|\mathrm{N}(\varepsilon)\right|^{m-1} \leq (2t)^{5tdm^2nh_{\mathbf{K}}}$$

and

$$(10) \qquad H(f) = h(\varepsilon) \leq (2t)^{4tmnh_{\mathbf{K}}} \exp\{mnd^{3d}\,R_{\mathbf{K}}\}.$$

Further, let S be the set composed by the infinite places of $\mathbf{K}$ and the finite places corresponding to the prime ideals $\mathfrak{p}_{1,1}, \ldots, \mathfrak{p}_{t,l_t}$. Together with (9), (10), $\left|\mathrm{N}(\alpha^{m-1}\,\beta)\right| \leq A^{md}$, (i) of Lemma 2 and the estimate $R_{\mathbf{K}} \leq |D_{\mathbf{K}}|^{1/2}\left(\log|D_{\mathbf{K}}|\right)^{d-1}$ (see [3], inequality (6.27)), our proposition yields after a few calculations the upper bound

$$(11) \qquad \log^*\log^*\mathrm{h}\left(\frac{\alpha x}{(\eta\rho)^n}\right) \leq c_7\left(P\,d\,m^3\,n^3\,h_{\mathbf{K}} + d\,m^2\,n\,\log|dD_{\mathbf{K}}| + d\,m^3\,n\,\log A\right),$$

where c_7, and also c_8, c_9, c_{10} below, are effectively computable numerical positive constants.

Put $w := \max_{i,j} w_{i,j}$ and choose i and j such that $w = w_{i,j}$. Notice that $v_{\mathfrak{p}_{i,j}}(\alpha^{m-1}\,\beta) \leq (\log 2)^{-1}\,m\,d\,\log A$. Thus, assuming that $w > (\log 2)^{-1}\,m\,d\,\log A$, we infer from (5) and from $\gcd(x,y) = 1$ that

$$v_{\mathfrak{p}_{i,j}}\left(x/(\eta\rho)^n\right) \leq (\log 2)^{-1}\,m\,d\,\log A - n\,h_{\mathbf{K}}\,w,$$

and

$$\mathrm{h}\left(\frac{\alpha x}{(\eta\rho)^n}\right)A^{md+1} \geq 2^{nh_{\mathbf{K}}w/d} \geq 8^{w/d}.$$

Hence, in any case, we obtain the bound

$$(12) \qquad w \leq d\left(\log^*\mathrm{h}\left(\alpha x/(\rho\eta^n)\right) + (md+1)\log A\right).$$

Using $|\mathrm{N}(\alpha)| \geq 1$ and $|\mathrm{N}(\gamma)| \leq \mathrm{h}(\gamma)^d$ for $\gamma \in \mathbf{K}$, we have

$$(13) \qquad |\mathrm{N}(x)| \leq \mathrm{h}\left(\frac{\alpha x}{(\eta\rho)^n}\right)^d\,|\mathrm{N}(\rho)|^n$$

and, by (8),

$$
\begin{aligned}
|\mathrm{N}(y)| \le |\mathrm{N}(y^n)| &\le \Big|\mathrm{N}\Big(\big(y/(\rho\eta)^m\big)^n\,\alpha^{m-1}\,\beta\Big)\Big|\cdot|\mathrm{N}(\rho)|^{mn}\\
&\le \mathrm{h}\left(\left(\frac{\alpha x}{(\eta\rho)^n}\right)^m-\varepsilon\right)^d|\mathrm{N}(\rho)|^{mn}\\
&\le 2^d\,\mathrm{h}\left(\frac{\alpha x}{(\eta\rho)^n}\right)^{md}\mathrm{h}(\varepsilon)^d\,|\mathrm{N}(\rho)|^{mn}.
\end{aligned}
\tag{14}
$$

Recall that $\rho := \prod_{i,j}\pi_{i,j}^{w_{i,j}}$. Hence, by (4), (ii) of Lemma 2 and (12), we get $|\mathrm{N}(\rho)| \le (2t)^{4tdwh_{\mathbf{K}}}$ and

$$
\begin{aligned}
\log^*\log^*|\mathrm{N}(\rho)| &\le \log(dh_{\mathbf{K}})+2\log(2t)+\log w\\
&\le 2\log(2tdh_{\mathbf{K}})+2\log(2md\log A)+\log^*\log^*\mathrm{h}\left(\frac{\alpha x}{(\eta\rho)^n}\right).
\end{aligned}
\tag{15}
$$

Finally, combining (11), (13), (14) and (15), we obtain the upper bound

$$
\log^*\log^*\max\big\{|\mathrm{N}(x)|,|\mathrm{N}(y)|\big\} \le c_8\,\big(P\,d\,m^3\,n^3\,h_{\mathbf{K}}+d\,m^2\,n\,\log|dD_{\mathbf{K}}|+d\,m^3\,n\,\log A\big),
$$

whence

$$
P \ge c_9\left(\frac{\log^*\log^*\max\big\{|\mathrm{N}(x)|,|\mathrm{N}(y)|\big\}}{d\,m^3\,n^3\,h_{\mathbf{K}}}-\frac{\log|dD_{\mathbf{K}}|}{m\,n^2\,h_{\mathbf{K}}}-\frac{\log A}{n^2h_{\mathbf{K}}}\right).
\tag{16}
$$

If $\alpha^m\,x^m+\alpha^{m-1}\,\beta\,y^n$ is a unit, we use the same argument as above. In this case, δ and ε are units and we apply the Proposition with $S=S_\infty$. After a few calculations, we get

$$
\log^*\log^*\max\big\{|\mathrm{N}(x)|,|\mathrm{N}(y)|\big\} \le c_{10}\,d\,m^2\,n\,\big(\log|d\,n\,D_{\mathbf{K}}|+m\,\log A\big).
\tag{17}
$$

Since $P=\max\big\{P[\alpha],P[\alpha\,x^m+\beta\,y^n]\big\}$, the theorem follows from (16) and (17). $\square$

References

[1] Y. Bugeaud, Bounds for the solutions of superelliptic equations, Compositio Math., to appear.

[2] Y. Bugeaud and K. Győry, Bounds for the solutions of unit equations, Acta Arith. 74 (1996), 67–80.

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

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

[5] 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.

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

[7] J. B. Rosser and L. Schönfeld, Approximate formulas for some functions of prime numbers, Illinois J. Math. 6 (1962), 64–94.

[8] V. G. Sprindžuk, Classical diophantine equations, Lecture Notes in Math. 1559, Springer-Verlag, 1993.

[9] L. A. Trelina, S-integral solutions of diophantine equations of hyperelliptic type (Russian), Dokl. Akad. Nauk. BSSR 22 (1978), 881-884, 955.

[10] P. M. Voutier, An effective lower bound for the height of algebraic numbers, Acta Arith. 74 (1995), 81–95.

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

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