FUNDAMENTAL SYSTEMS OF S-UNITS WITH SMALL HEIGHT AND THEIR APPLICATIONS TO DIOPHANTINE EQUATIONS

Yann Bugeaud (Strasbourg)

À Kálmán Győry pour son soixantième anniversaire

1. Introduction

Since works of Thue, Siegel and Mahler, it is known that S-unit equations and Thue-Mahler equations have only finitely many solutions. However, one had to wait until Baker's theory of linear forms in the logarithms of algebraic numbers to be able to compute effectively upper bounds for the size of these solutions. Many authors, including Baker, Coates, Győry, Kotov, Papp and Sprindžuk, provided such estimates, and the current best bounds are due to Bugeaud & Győry (see [10, 11, 25, 26] for references). As already noticed by Siegel, the proofs involve fundamental (or independent) systems of S-units of a suitable number field, with small height. The most significantly improvements obtained in [10, 11] for effective upper estimates for the size of the solutions of S-unit equations and Thue–Mahler equations concern the dependence on the set of places S and are achieved thanks to the use of systems of S-units, whose heights depend only slightly on S.

This survey paper is organized as follows. The key lemmas are recalled in Section 2, and we display some of the new estimates for the size of the solutions of classical Diophantine equations in Section 3, including S-unit equations, Thue–Mahler equations and superelliptic equations. It appears that this approach also leads to considerable sharpenings of previous lower bounds for the greatest prime factor of $ax^m + by^n$ obtained by Kotov [20] and Shorey [23]. We outline the proofs of our new results in Sections 4 and 5, and we try to point out where is the source of the improvement. By the same method, we also provide new lower estimates for the greatest square–free divisor of $ax^m + by^n$.

In Sections 3 to 5, for sake of simplicity, we do not state our results in full generality, and we choose to restrict ourselves to the case where the ground field is the field $\mathbf{Q}$.

2. Notations and the key lemmas

The following notation will be used throughout this work.

For an algebraic number field $\mathbf{K}$ of degree d, we denote by $O_{\mathbf{K}}$ the ring of integers in $\mathbf{K}$ and 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 $\alpha \in \mathbf{K}$, $|\alpha|_v = |\sigma(\alpha)|^{d_v}$, where $d_v = 1$ or 2 according as $\sigma(\mathbf{K})$ is contained in $\mathbf{R}$ or not; if v is finite and is associated 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 $\mathbf{K}$.

Further, there exists a $\lambda(d) > 0$, depending only on d, such that $\log \mathrm{h}(\alpha) \geq \lambda(d)$ for any non-zero algebraic number α of degree d which is not a root of unity. For $d \geq 2$, Voutier [28] has shown that one can take

$$\lambda(d) = \frac{2}{d(\log(3d))^3},$$

while $\lambda(1) = \log 2$ is suitable.

Let S be a finite subset of $\Omega_{\mathbf{K}}$ containing the set of infinite places S_∞. Denote by O_S the ring of S-integers, and by O_S^* the group of S-units in $\mathbf{K}$. For $\alpha \in \mathbf{K} \setminus \{0\}$, the ideal (α) generated by α can be uniquely written in the form $\mathfrak{a}_1 \mathfrak{a}_2$ where the ideal $\mathfrak{a}_1$ (resp. $\mathfrak{a}_2$) is composed of prime ideals outside (resp. inside) S. The S-norm of α, denoted by $\mathrm{N}_S(\alpha)$, is defined as $\mathrm{N}(\mathfrak{a}_1)$. The S-norm is multiplicative, and, for $S = S_\infty$, we have $\mathrm{N}_S(\alpha) = |\mathrm{N}_{\mathbf{K}/\mathbf{Q}}(\alpha)|$. For any $\alpha \in \mathbf{K} \setminus \{0\}$, we see that $\mathrm{N}_S(\alpha) = \prod_{v \in S} |\alpha|_v$. Further, if $\alpha \in O_S \setminus \{0\}$, then $\mathrm{N}_S(\alpha)$ is a positive integer and $\mathrm{N}_S(\alpha) \leq \big(\mathrm{h}(\alpha)\big)^d$.

Denote by s the cardinality of S. Let $v_1, \ldots, v_{s-1}$ be a subset of S, and let $\{\varepsilon_1, \ldots, \varepsilon_{s-1}\}$ be a fundamental system of S-units in $\mathbf{K}$. Denote by R_S the absolute value of the determinant of the matrix $(\log |\varepsilon_i|_{v_j})_{i,j=1,\ldots,s-1}$. It is easy to verify that R_S is a positive number which is independent of the choice of $v_1, \ldots, v_{s-1}$ and of the fundamental system of S-units $\{\varepsilon_1, \ldots, \varepsilon_{s-1}\}$. We call R_S the S-regulator of $\mathbf{K}$. If in particular $S = S_\infty$, then R_S is just the regulator, $R_{\mathbf{K}}$, of $\mathbf{K}$.

Throughout this paper, we stand the notation $\log^* a$ for $\max\{\log a, 1\}$.

As mentioned in the Introduction, upper estimates for the size of the solutions of S-unit equations depend on the product of the logarithmic heights of an independent (or a fundamental) system of S-units. That is the reason why we need independent (or fundamental) systems of S-units with small height. A result similar to Lemma 1 below has been proved by Hajdu [19], and we shall also mention works of Brindza [3] and Pethő [21]. In order to compare the estimates provided by Lemma 1 with previous ones, we have to bound the new quantity introduced there, namely the S-regulator. This is the purpose of Lemma 2, which has been independently obtained by Bilu [1]. Further, Lemma 3 asserts that every principal integer ideal in $\mathbf{K}$ has a generator with small height. This is very useful since most of the proofs depend on the factorization of ideals in number fields, see *e.g.* [5].

For the proofs of Lemmas 1 to 3 below we refer the reader to [10]. A variant of Lemma 3 is also proved in [6].

Put

$$c_1 = c_1(d,s) = \big((s-1)!\big)^2/(2^{s-2}d^{s-1}), \;\; c_1' = c_1'(d,s) = (s-1)!/d^{s-1},$$

$$c_2 = c_2(d,s) = c_1\big(\lambda(d)\big)^{2-s}, \;\; c_2' = c_2'(d,s) = c_1'\big(\lambda(d)\big)^{2-s},$$

and

$$c_3 = c_3(d,s) = c_1\, d^{s-2}/\lambda(d), \;\; c_3' = c_3'(d,s) = c_1'\, d^{s-2}/\lambda(d).$$

Lemma 1. *There exists in* $\mathbf{K}$ *a fundamental (resp. independent) system* $\{\varepsilon_1, \ldots, \varepsilon_{s-1}\}$ *of* S*-units with the following properties :*

(i)
$$\prod_{i=1}^{s-1} \log \mathrm{h}(\varepsilon_i) \leq c_1\, R_S \qquad (\mathit{resp.}\;\; c_1'\, R_S);$$

(ii)
$$\log \mathrm{h}(\varepsilon_i) \leq c_2 R_S, \qquad (\mathit{resp.}\;\; c_2'\, R_S) \quad i = 1, \ldots, s-1;$$

(iii) *the absolute values of the entries of the inverse matrix of* $(\log |\varepsilon_i|_{v_j})_{i,j=1,\ldots,s-1}$ *do not exceed* c_3 *(resp.* c_3'*).*

Denote by $h_{\mathbf{K}}$ and $r = r_{\mathbf{K}}$ the class number and unit rank of $\mathbf{K}$, respectively. Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_t$ be the prime ideals corresponding to the finite places in S, and denote by P the largest of the rational primes lying below $\mathfrak{p}_1, \ldots, \mathfrak{p}_t$. Put $c_4 = c_4(d,r) = \frac{1}{2}\, r^{r+1} \big(d\lambda(d)\big)^{-(r-1)}$.

Lemma 2. *If $t > 0$, then we have*

$$R_S \le R_{\mathbf{K}} h_{\mathbf{K}} \prod_{i=1}^{t} \log \mathrm{N}(\mathfrak{p}_i) \le R_{\mathbf{K}} h_{\mathbf{K}} (d \log^* P)^t$$

and

$$R_S \ge R_{\mathbf{K}} \prod_{i=1}^{t} \log \mathrm{N}(\mathfrak{p}_i) \ge 0.2\,(\log 2)^d\,(\log^* P).$$

Lemma 3. *For every $\alpha \in O_S \setminus \{0\}$ and every integer $n \ge 1$ there exists an S-unit ε such that*

$$\mathrm{h}(\varepsilon^n \alpha) \le \mathrm{N}_S(\alpha)^{1/d} \exp\bigl\{n(c_4 R_{\mathbf{K}} + t h_{\mathbf{K}} \log^* P)\bigr\}.$$

In the next Sections, we will point out numerous consequences of these three lemmas.

3. Applications to S-unit equations and some other classical Diophantine equations

Let $\mathbf{K}$ be as in Section 2 and let α, β be non-zero elements of $\mathbf{K}$ with

$$\max\{\mathrm{h}(\alpha), \mathrm{h}(\beta)\} \le H \quad (H \ge e).$$

Consider the S-unit equation

$$\alpha x + \beta y = 1 \quad \text{in } x, y \in O_S^*. \tag{1}$$

When $S = S_\infty$ (i.e. $t = 0$) then (1) is an (ordinary) unit equation. Two new totally explicit bounds for the size of the solutions of (1) have recently been given in [10] and by Bombieri [2]. The beginnings of their proofs are the same and differ slightly from the earlier approach. Namely, assuming that $\mathrm{h}(x)$ is not less than $\mathrm{h}(y)$ and using a fundamental system $\varepsilon_1, \ldots, \varepsilon_{s-1}$ of S-units of $\mathbf{K}$ provided by Lemma 1, we can write

$$\alpha\, x = 1 - \zeta\, \beta\, \varepsilon_1^{b_1} \ldots \varepsilon_{s-1}^{b_{s-1}},$$

where ζ is a root of unity and the b_i's are rational integers. Thus, we have explained how a fundamental system of S-units occurs. In [10], we then apply the theory of linear forms in logarithms in order to have a lower bound for $|\alpha\, x|_v$, where v is a place on $\mathbf{K}$ such that $|\alpha\, x|_v \le |\alpha\, x|_w$, for all places w. And, as is well known, we encounter the quantity $\prod \log \mathrm{h}(\varepsilon_i)$, which also naturally appears in Bombieri's method [2]. The latter does not depend on Baker's theory and is slightly more difficult to explain, hence we refer the reader respectively to [10, 2, 6], where all the details can be found. Here, we quote the main result of [10].

Theorem 1. *With the notation of Section 2, all solutions x, y of (1) satisfy*

$$\max\{\mathrm{h}(x), \mathrm{h}(y)\} < \exp\bigl\{c_5 P^d R_S (\log^* R_S)(\log^*(P R_S)/\log^* P) \log H\bigr\}, \tag{2}$$

where

$$c_5 = c_5(d, s, \mathbf{K}) = 3^{25}\,\bigl(9d/\lambda(d)\bigr)^{s+1}\, s^{5s+10}.$$

Further, if in particular $S = S_\infty$ (i.e. $t = 0$), then the bound in (2) can be replaced by

$$\exp\bigl\{c_6 R_K (\log^* R_K) \log H\bigr\}$$

where

$$c_6 = c_6(d, r, \mathbf{K}) = 3^{r+27}\,(r+1)^{5r+17}\, d^{2-r}\, \lambda(d)^{-(r+1)}.$$

Compare now Theorem 1 with the earlier bounds (see [13, 14, 15, 25, 26]). The numerical constants have been significantly improved, and this is essentially a consequence of the recent sharpenings for lower bounds for linear forms in logarithms, due, in the archimedean case, to Waldschmidt [29] and, in the non–archimedean case, to Yu [30]. Here, we are mostly interested in the dependence on S and, thanks to Lemma 2, we see that we have managed to replace a factor $R_{\mathbf{K}}^s$ by a factor $R_{\mathbf{K}}$, hence to remove the dependence on s in the exponent of the regulator. This improvement also occurs in Theorem 2 (compare with [18, 25, 26]) and in Theorem 3 below (compare with [25, 26]). It is ultimately the cause of the significant sharpening stated in Theorem 5.

We now quote a corollary of the main theorem of [11]. For sake of simplicity, we do not state our result in their full generality.

Theorem 2. *Let α be an algebraic number of degree $d \geq 3$ and height less than A $(\geq e)$, and put $\mathbf{K} = \mathbf{Q}(\alpha)$. Let $p_1 < \ldots < p_t$ be distinct prime numbers, and put $T = \{p_1, \ldots, p_t, \infty\}$. Denote by O_T the set of T-integers in $\mathbf{Q}$ and let S stand for the set of all extensions to $\mathbf{K}$ of the places in T. We use the same notation as in Section 2. Let $0 \neq b \in \mathbf{Q}$ with (absolute) height at most B and with T-norm not exceeding B^* $(\geq e)$. Then all solutions $x, y \in O_T$ of*

$$\mathrm{N}_{\mathbf{K}/\mathbf{Q}}(x + \alpha\, y) = b$$

satisfy

$$\max\{\mathrm{h}(x), \mathrm{h}(y)\} < B^{1/d} \exp\bigl\{c_7\, p_t^N\, R_S (\log^* R_S)\bigl(\log^*(p_t\, R_S)/\log^* p_t\bigr)\bigl(R_{\mathbf{K}} + t h_{\mathbf{K}} + \log(AB^*)\bigr)\bigr\} \qquad (3)$$

where $N = d(d-1)(d-2)$ and

$$c_7 = c_7(d, t, N) = 3^{t+25}\, t^{5t+12}\, N^{3t+4d}.$$

Further, if $t = 0$, then the bound in (3) can be replaced by

$$B^{1/d} \exp\bigl\{c_8\, R_{\mathbf{K}} (\log^* R_{\mathbf{K}})\, (R_{\mathbf{K}} + \log(AB^*))\bigr\} \qquad (4)$$

where

$$c_8 = c_8(d, r) = 3^{r+26}\, (r+1)^{7r+19}\, d^{4r+2}\, d^{2(d+r+6)}.$$

Remarks : In [11], we prove Theorem 2 without using bounds for S-unit equations. However, as shown by Győry [16], a slighlty less sharp estimate can be obtained as a corollary of a more general result on decomposable form equations (see below), the proof of which rests on Theorem 1.

Although the constant c_8 is huge, the estimate (4) appears to be sharp enough in some particular applications. Indeed, in [12], we have delt, among others, with the equation

$$5\, X^{71} - 4\, Y^{71} = 1. \qquad (5)$$

Our goal was to prove that (5) has no solution (X, Y) with X or Y a perfect power. We did not completely solve (5), but the bound (4) was good enough to show that, for an integer solution (X, Y) of (5), neither X nor Y can be an n-th power, for any $n \geq 10^{700}$. This was sufficient for our purpose, since we managed to treat the case $n \leq 10^{700}$ by means of congruence arguments. To be more precise, we had to rework the proof of Theorem 2 and to use the precise shape of (5) in order to get the above bound; notice that a direct application of (4) leads to around 10^{1300}, which is far too large.

As is well–known, superelliptic equations

$$f(x) = y^m, \qquad (6)$$

where $m \geq 2$ and $f(X) \in \mathbf{K}[X]$ is an irreducible monic polynomial of degree $n \geq 2$ with $mn \geq 6$, reduce to unit equations and Thue equations. Following this classical method, we apply Theorems 1 and 2 to compute in [5] new upper bounds for the size of the S-integer solutions of (6), in a more general setting. To illustrate our new results, we quote the following corollary of the Proposition of [8], which appears to be crucial for the proof of Theorem 5 in the next Section.

For any polynomial $g(X)$ with integer coefficients, we denote by $\mathrm{H}(g)$ its height, defined as the maximum of the absolute values of its coefficients.

Theorem 3. *Let $p_1 < \ldots < p_t$ be distinct prime numbers and set $T = \{p_1, \ldots, p_t, \infty\}$. Let $m \geq 3$ be an integer. Let $f \in \mathbf{Z}[X]$ be a monic irreducible polynomial of degree $n \geq 2$, with height $\mathrm{H}(f)$ and discriminant Δ_f. Then all the solutions $(x, y) \in \mathbf{Q}^2$ of (6) with x a T-integer satisfy*

$$\begin{aligned}\mathrm{h}(x) \leq \mathrm{H}(f)^{m+1} \exp\bigl\{\bigl(c_9\, n\, m(t+1)\bigr)^{c_{10}\, n^2 m(t+1)}\, p_t^{n^2 m^3}\, (\log^* p_t)^{tn^2 m} \\ |\Delta_f|^{5nm}\, \bigl(\log |\Delta_f|\bigr)^{2n^2 m}\bigr\},\end{aligned} \qquad (7)$$

where c_9 and c_{10} are effectively computable positive absolute constants.

We point out that in the previous bounds (see [25, 26]) the exponent of $|\Delta_f|$ depends linearly on t, the number of prime numbers in T. This improvement is a direct consequence of the improvements concerning the dependence on the set of places S obtained in Theorems 1 and 2. Indeed, to prove (7), we work in a number field $\mathbf{K}$ generated by two roots of f, and we bound the product $R_{\mathbf{K}}\, h_{\mathbf{K}}$ (which occurs by applications of Theorem 1, Theorem 2 and Lemma 2) in terms of $D_{\mathbf{K}}$, the discriminant of $\mathbf{K}$, hence, ultimately, in terms of Δ_f.

Remark : It is possible to slightly improve upon Theorem 3. Indeed, in (7), one can replace Δ_f by the product of its distinct prime factors. This allows us to sharpen the generalization to arbitrary number fields of Theorem 5 below, proved in [8].

We recall that, by definition, decomposable form equations over the rationals are equations of the form

$$F(x_1, \dots, x_m) = b \qquad \text{in } (x_1, \dots, x_m) \in \mathbf{Z}^m,$$

where $b \in \mathbf{Z} \setminus \{0\}$ and $F \in \mathbf{Z}[X_1, \dots, X_m]$ is an homogeneous polynomial which factorizes into linear forms with algebraic coefficients. For instance, they include Thue equations. It is known that a large class $\mathcal{C}$ of decomposable form equations ultimately reduce to unit equations. Hence, applying Theorem 1, Győry [16] proves a new upper bound for the size of the solutions of the equations belonging to $\mathcal{C}$. His results cover the more general case of S-integer solutions over an arbitrary number field. They include new upper bounds for the size of the solutions of discriminant form equations and index form equations, and also the following statement about polynomials with given discriminant.

Theorem 4. *Let $f(X) \in \mathbf{Z}[X]$ be a monic polynomial with degree n and non–zero discriminant Δ_f. Let $\mathbf{K}$ be the splitting field of f. Then, there exists an integer $a \in \mathbf{Z}$ such that the polynomial $f^*(X) := f(X+a)$ satisfies*

$$\mathrm{H}(f^*) < \exp\Big\{ \big(c_{11}\, n^{c_{12}\, n}\, |\Delta_f|\big)^{(n+1)!} \Big\},$$

where c_{11} and c_{12} are effectively computable positive absolute constants.

Proof : This is Corollary 4 of [17], combined with the Lemma of [9] and inequality (5) of [10]. □

The above polynomials f and f^* have clearly the same discriminant. Hence, one can deduce from Theorems 3 and 4 an upper bound for $|y|$, when x and y are integers satisfying (6), depending only on the discriminant of f and not on its height.

Corollary 1. *Let $f \in \mathbf{Z}[X]$ be a monic irreducible polynomial of degree $n \geq 3$ and discriminant Δ_f. Let $(x, y) \in \mathbf{Z}^2$ be a solution of (6). Then there exist effectively computable positive absolute constants c_{13} and c_{14} such that*

$$|y| \leq \exp\Big\{ \big((c_{13}\, m\, n)^{c_{14}\, n}\, |\Delta_f|\big)^{m\,(n+1)!} \Big\}.$$

Further, one should mention that Poulakis [22] applied Theorem 1 to establish explicit upper bounds for the size of solutions of a wide class of Diophantine equations, including elliptic equations and Thue equations. Namely, let $F(X,Y) \in \mathbf{K}[X,Y]$ be an absolutely irreducible polynomial and denote by C the algebraic curve defined by the equation $F(x,y) = 0$ and by $\mathbf{K}[C]$ the ring of regular functions on C over $\mathbf{K}$. Assuming that there is a unit ϕ in $\mathbf{K}[C] \setminus \mathbf{K}$ such that $1 - \phi$ is also a unit, Poulakis obtained explicit upper bounds for the size of the algebraic integers $x, y \in O_{\mathbf{K}}$ satisfying $F(x,y) = 0$.

4. The greatest prime factor of $ax^m + by^n$ when m and n are fixed

Unless the contrary is explicitly stated, the constants $c_{15}, \dots, c_{39}$ occurring below are effective absolute positive constants.

In this Section and in the next one, we denote by $P[z]$ (*resp.* by $Q[z]$) the greatest prime factor (*resp.* the greatest square-free part) of a rational integer z, with the convention that $P[-1] = P[1] = P[0] = Q[1] =$

$Q[-1] = Q[0] = 1$. We observe that we always have $Q[z] \le \exp\{P[z]\}$. Further, we will often use the fact that there exist two numerical constants c_{15} and c_{16} such that the t-th prime number belongs to the interval $[c_{15}\, t\, \log t, c_{16}\, t\, \log t]$.

The following lower bound for $P[ax^m + by^n]$ has been proved in [9] in the case of an arbitrary number field (see also [8]). It considerably improves previous work by Kotov [20]. Notice that the estimate for $Q[ax^m + by^n]$ given in Theorem 5 has not been stated explicitly previously.

Theorem 5. *Let $m \ge 2$ and $n \ge 2$ be integers such that $mn \ge 6$. Let a and b be non-zero integers. Then there exist effective absolute constants $c_{17} > 0$ and $c_{18} > 0$ and an effective constant c_{19}, depending on m, n, a and b, such that*

$$Q[ax^m + by^n] \ge \big(\log^* \max\{|x|, |y|\}\big)^{1/(c_{17}\, m\, n\, \min\{m,n\})}$$

and

$$P[ax^m + by^n] \ge c_{18}\, \frac{\log^* \log^* \max\{|x|, |y|\}}{m\, n\, \min\{m, n\}},$$

provided that x and y are two coprime integers satisfying $\max\{|x|, |y|\} \ge c_{19}$.

Proof : For simplicity, we sketch the proof in the case $a = 1$ and $b = -1$. If $m = n$, the theorem follows from the main result of [11] and also from Corollary 1 of [16]. We may then assume that $n > m$. If $|x^m - y^n| = 1$, then Tijdeman [27] proved that $|x|$ and $|y|$ are bounded by an absolute constant. Hence, we may suppose that $|x^m - y^n| > 1$ and write $x^m - y^n = \pm p_1^{u_1} \ldots p_t^{u_t}$, where the u_i's are positive rational integers, hence $Q[x^m - y^n] = p_1 \ldots p_t$. Using Euclidean divisions, we obtain a T-integer solution (x', y'), with $x' = (x/p_1^{v_1} \ldots p_t^{v_t})$ and $y' = (y/p_1^{w_1} \ldots p_t^{w_t})$, of the Diophantine equation $X^m \pm p_1^{r_1} \ldots p_t^{r_t} = Y^n$, where $0 \le r_i < nm$ and $T = \{p_1, \ldots, p_t, \infty\}$. Notice that, by the Lemma of [9], the discriminant Δ of the polynomial $X^m \pm p_1^{r_1} \ldots p_t^{r_t}$ satisfies $|\Delta| \le m^{m^2} (p_1 \ldots p_t)^m$. Since $n \ge 3$, we can apply Theorem 3 and we get for $|x'|$ and $|y'|$ the bound $\exp\{e^{c_{20}\, m^2\, n\, t\, \log t}\, e^{c_{21}\, m^4\, n^3\, t}\}$. However, we observe that $c_{22}\, t\, \log t \le \log Q$ and that $e^t \le c_{23} Q^{1/\log^* \log^* Q}$ (to see this, distinguish the cases $t \ge \log^* Q / \log^* \log^* Q$ and $t \le \log^* Q / \log^* \log^* Q$), whence we get

$$\max\{|x'|, |y'|\} \le \exp\{Q^{c_{24}\, m^2\, n}\, Q^{c_{25}\, m^4\, n^3 / \log^* \log^* Q}\}.$$

This yields $\log \max\{|x'|, |y'|\} \le Q^{c_{26}\, m^2\, n}$, provided that $\max\{|x'|, |y'|\}$ is large enough in terms of m and n. The theorem follows since x and y are coprime. If we use the previous estimates for the size of the solutions of superelliptic equations, we have to replace the $|\Delta_f|$ occurring in Theorem 4 by $|\Delta_f|^t$, and arguing as above, we get $\log \max\{|x'|, |y'|\} \le Q^{c_{27}\, m^2\, n\, t}$, hence $\log \max\{|x'|, |y'|\} \le Q^{c_{28}\, m^2\, n\, \log^* Q / \log^* \log^* Q}$. This yields a lower bound for $\log^* Q$ of the shape $(\log^* \log^* \max\{|x|, |y|\})^{1/2} (\log^* \log^* \log^* \max\{|x|, |y|\})^{1/2}$ and implies the result of Kotov [20] on the greatest prime factor of $x^m - y^n$. □

In order to improve upon Theorem 5, it seems necessary to develop new arguments, because even a dramatic sharpening for linear forms in logarithms would presumably not be sufficient.

5. The greatest prime factor of $ax^m + by^n$ when n is fixed

Since the work of Shorey *et al.* [24], it is known that if a, b and $n \ge 2$ are fixed non-zero rational integers, then $P[ax^m + by^n]$ tends effectively to infinity as the integer m grows to infinity, independently of the coprime non–zero rational integers x and y with $|x| > 1$. An explicit form of this result is due to Shorey [23], and Shorey & Tijdeman [25, Chapter 10] generalized it to the number field case. Thanks to Lemmata 1 to 3, we are now able to considerably sharpen Shorey's estimate, as shown in [7]. Notice that the lower bound for $Q[ax^m + by^n]$ given in Theorem 6 has not been stated explicitly previously.

Theorem 6. *Let a, b, x, y and n be rational integers satisfying*

$$ab \ne 0, \;\; |x| > 1, \;\; y \ne 0, \;\; (ax, by) = 1 \;\text{ and }\; n \ge 2.$$

There exist effective absolute constants c_{29} and c_{30} and an effective constant c_{31}, depending on a, b and n, such that

$$Q[ax^m + by^n] > m^{c_{29}/n}$$

and

$$P[ax^m + by^n] > c_{30}\,\frac{\log m}{n}$$

for any integer $m \geq c_{31}$.

Proof : Let us briefly sketch the proof. Assume for simplicity that $a = 1$ and $b = -1$. Let x, y and n be integers satisfying the hypothesis of the theorem, and let $m \geq 2$. Write $x^m - y^n = \pm\, p_1^{u_1} \dots p_t^{u_t}$, where the u_i's are positive rational integers, hence $Q[x^m - y^n] = p_1 \dots p_t$. Then, we observe that we have $y^n - Az^n = x^m$, where z is composed by the p_i's and $A = \pm\, p_1^{t_1} \dots p_s^{t_s}$, with $0 \leq t_i < n$. We work in the number field $\mathbf{K}$ generated by a n-th root of A, and, 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 Lemma 1 to get a fundamental system $\xi_1, \dots, \xi_{v-1}$ of S-units in $\mathbf{K}$ with small height.

The upper bound for m mainly depends on the quantity $\prod_{i=1}^{v-1} \log \mathrm{h}(\xi_i)$, and thus on the discriminant D of the field $\mathbf{K}$, whose absolute value is not greater than $n^{n^2}\,(p_1 \dots p_t)^{n-1}$. More precisely, we have then the estimate

$$m \leq Q^{c_{32}\, n}\, Q^{c_{33}\, n^2 / \log^* \log^* Q}, \tag{8}$$

yielding $Q \geq m^{1/c_{34}\, n}$ provided that m is large enough.

In his work, Shorey [23] did not use a fundamental system of S-units and he obtained the upper bound $m \leq Q^{c_{35}\, n^2 t}$ to get finally a lower estimate for $\log Q$ of the shape $(\log m)^{1/2}\,(\log\log m)^{1/2}$. Our improvement rests once again on Lemmata 1 to 3. $\square$

We observe that the proof of Theorem 6 shows also that there exists an effective absolute constant c_{36} and an effective constant c_{37}, depending on a and b such that $P[ax^m + by^n] > c_{36}\,(\log m)/n^2$ for any integer $m \geq c_{37}$. Putting this together with Theorem 5, we get

Corollary 2. *Let a, b, x and y be non-zero integers with $(x, y) = 1$, $|x| \geq 2$ and $(ax, by) = 1$. Fix an integer $n \geq 2$. There exists an effective positive constant c_{38} depending on a and b such that*

$$P[ax^m + by^n] \geq \frac{c_{38}}{n^2}\left(\log m + \frac{\log^* \log^* \max\{|x|, |y|\}}{m}\right).$$

for every integer $m \geq 2$ with $mn \geq 6$.

Further, we recover a result of a similar strength as Theorem 1 of [4]. Namely, we infer from (8) that there exists a positive constant c_{39} such that for any integers $x \geq 1$, $y \geq 2$, $n \geq 2$, $m \geq 2$ with $x^n \neq y^m$, we have

$$|x^n - y^m| \geq Q[x^n - y^m] \geq m^{c_{39}/n^2}.$$

This is slightly weaker than Theorem 1 of [4], which yields the estimate

$$|x^n - y^m| \geq m^{2/5n}\, n^{-5}\, 2^{-6-42/n}.$$

We remark that the proof of the latter lower bound is more direct and does not involve estimates for linear forms in non–archimedean logarithms, unlike the proof of Theorem 6.

References

[1] Y. Bilu, Effective analysis of integral points on algebraic curves, thesis, Beer Sheva, 1993.

[2] E. Bombieri, Effective Diophantine approximation on $\mathbf{G}_m$, Ann. Scuola Norm. Sup. Pisa (IV) 20 (1993), 61-89.

[3] B. Brindza, On the generators of S-unit groups in algebraic number fields, Bull. Austral. Math. Soc. 43 (1991), 325-329.

[4] Y. Bugeaud, Sur la distance entre deux puissances pures, C. R. Acad. Sci. Paris 322 (1996), 1119–1121.

[5] Y. Bugeaud, Bounds for the solutions of superelliptic equations, Compositio Math. 107 (1997), 187–219.

[6] Y. Bugeaud, Bornes effectives pour les solutions des équations en S-unités et des équations de Thue-Mahler, J. Number Th. 71 (1998), 227–244.

[7] Y. Bugeaud, Sur le plus grand facteur premier de $ax^m + by^n$, C. R. Acad. Sci. Paris 326 (1998), 661–665.

[8] 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.

[9] Y. Bugeaud, On the greatest prime factor of $ax^m + by^n$, *II*, submitted.

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

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

[12] Y. Bugeaud, M. Mignotte, Y. Roy and T. N. Shorey, The Diophantine equation $\frac{x^n-1}{x-1} = y^q$ has no solution with x square, Math. Proc. Camb. Phil. Soc. 127 (1999), 353–372.

[13] K. Győry, On the number of solutions of linear equations in units of an algebraic number field, Comment. Math. Helv. 54 (1979), 583-600.

[14] K. Győry, On the solutions of linear Diophantine equations in algebraic integers of bounded norm, Ann. Univ. Sci. Budapest. Eötvös, Sect. Math. 22/23 (1980), 225-233.

[15] K. Győry, *Résultats effectifs sur la représentation des entiers par des formes décomposables*, Queen's papers in pure and applied mathematics, No. 56, Kingston, Canada, 1980.

[16] K. Győry, Bounds for the solutions of decomposable form equations, Publ. Math. Debrecen 52 (1998), 1–31.

[17] K. Győry, Recent bounds for the solutions of decomposable form equations, Proceedings of the Number Theory Conference, Eger 1996, Eds. Győry, Pethő, Sós. de Gruyter, p. 255–270, 1998.

[18] K. Győry and Z. Z. Papp, Norm form equations and explicit lower bounds for linear forms with algebraic coefficients, in "Studies in Pure Mathematics to the Memory of Paul Turán", Akadémiai Kiadó, Budapest, and Birkhäuser Verlag, Basel, 1983, pp. 245-257.

[19] L. Hajdu, A quantitative version of Dirichlet's S-unit theorem in algebraic number fields, Publ. Math. Debrecen 42 (1993), 239-246.

[20] 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.

[21] A. Pethő, *Beiträge zur Theorie der S-Ordnungen*, Acta. Math. Acad. Sci. Hungar. 37 (1981), 51-57.

[22] D. Poulakis, Integer points on algebraic curves with exceptional units, J. Austral. Math. Soc. (Series A) 63 (1997), 145–164.

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

[24] T. N. Shorey, A. J. van der Poorten, R. Tijdeman and A. Schinzel, Applications of the Gelfond-Baker method to Diophantine equations, Advances in transcendence theory, Academic Press, London and New-York 1977.

[25] T. N. Shorey and R. Tijdeman, Exponential Diophantine Equations, Cambridge University Press, Cambridge, 1986.

[26] V. G. Sprindžuk, Classical Diophantine Equations, Lecture Notes in Math. 1559, Springer Verlag, 1993.

[27] R. Tijdeman, On the equation of Catalan, Acta Arith. 29 (1976), 197–209.

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

[29] M. Waldschmidt, Minorations de combinaisons linéaires de logarithmes de nombres algébriques, Canadian J. Math. 45 (1993), 176-224.

[30] Kunrui Yu, Linear forms in p-adic logarithms III, Compositio Math. 91 (1994), 241-276.

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

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