LOWER BOUNDS FOR THE DIFFERENCE $ax^n - by^m$

Y. Bugeaud and L. Hajdu*

Abstract. In this work we give totally explicit lower bounds for $|ax^n - by^m|$ depending only on a, b, n, m and a, b, n, x, respectively.

1. Introduction

Let a, b, x, y, n and m be non-zero integers such that

$$n \geq 2, m \geq 2, |y| \geq 2 \text{ and } ax^n \neq by^m. \tag{1}$$

The first explicit lower bound independent of x and y for $|ax^n - by^m|$ was proved by Turk [10] when $a = b = 1$. A result of similar strength valid for arbitrary a and b, however not completely explicit, can also be deduced from the work of Shorey [9]. Recently, using a new approach of Brindza, Evertse and Győry [3] for bounding solutions of exponential diophantine equations, Bugeaud [4] was able to considerably sharpen Turk's estimate in the case $a = b = 1$. The purpose of the present work is to extend Bugeaud's result to arbitrary a and b, and thanks to some refined arguments, also to improve his lower bound.

2. The main results

Throughout the paper, for every positive real number s we put $\log_* s = \max\{1, \log s\}$.

Theorem 1. *If a, b, x, y, n and m are integers satisfying* (1)*, then we have*

$$|ax^n - by^m| \geq m^{2/5n}(20n)^{-2-11/n}\left(|a| \log_*^{\frac{1}{n}} |b|\right)^{-1}. \tag{2}$$

Remark. Our Theorem 1 extends Théorème 1 of [4] and sharpens it in the particular case when $a = b = 1$. The improvement occurs essentially in the factor n^{-2}, which replaces n^{-5}. This is the consequence of three refinements. First, we use the fact that the unit rank of the field in which we work is at most equal to half of its degree. Secondly, we work with an independent system of units, rather than a fundamental one: there are almost no changes in the proof, but a slight gain. Finally, to bound our linear forms in logarithms we use the estimate of Baker

*Research supported in part by the Hungarian Academy of Sciences, by Grants 023800 and T 016 975 from the Hungarian National Foundation for Scientific Research, by the Universitas Foundation of the Kereskedelmi Bank Rt and by the Pro Regione Foundation of the Hajdúsági Agráripari Rt.

and Wüstholz [1], which is more convenient for our purposes, instead of the one of Waldschmidt [11].

As in [10] and [4], by combining Theorem 1 with an estimate for the size of the solutions of superelliptic equations, we derive a lower bound for $|ax^n - by^m|$ in terms of ax^n.

Theorem 2. *If a, b, x, y, n and m are integers satisfying $m \geq 3$ and (1), then we have*

$$|ax^n - by^m| > c_1 n^{-2} \, |a|^{-1} \, \log_*^{-\frac{10}{9n}} |b| (\log_* \log_* |a\, x^n|)^{\frac{1}{3n}},$$

where c_1 denotes an absolute, effectively computable constant.

Remark. Let $F(X) \in \mathbb{Z}[X]$ be a polynomial of degree $n \geq 2$, and let b, x, y and m be integers with $m \geq 2$ and $|y| \geq 2$. Suppose that $F(x) - by^m \neq 0$, and if F is of the special form $t_1(X - t_2)^n + t_3$ with $t_1, t_2, t_3 \in \mathbb{Z}$ then also assume that $F(x) - by^m \neq t_3$. In the terms of n, m, b and the height of F (or in the terms of n, x, b and the height of F, respectively) one can give lower bounds for $|F(x) - by^m|$ of similar types as our Theorems 1 and 2. We do not work out the details here.

3. Auxiliary results

For a non-zero algebraic number α, we denote by $h(\alpha)$ the logarithmic height of α. Let $\mathbb{K}$ be a number field with degree $d_{\mathbb{K}}$, unit rank $r_{\mathbb{K}}$ and regulator $R_{\mathbb{K}}$. In the course of our proof, we use an independent system of units in $\mathbb{K}$ with small height, provided by the following lemma.

Lemma. *There exists an independent system $\{\varepsilon_1, \ldots, \varepsilon_{r_{\mathbb{K}}}\}$ of units in $\mathbb{K}$ satisfying*

$$\prod_{i=1}^{r_{\mathbb{K}}} h(\varepsilon_i) \leq d_{\mathbb{K}}^{-r_{\mathbb{K}}} \, r_{\mathbb{K}}! \, R_{\mathbb{K}} \tag{3}$$

and

$$h(\varepsilon_i) \leq r_{\mathbb{K}}! \, d_{\mathbb{K}}^{-1} \, \left(9 \, (\log 3d_{\mathbb{K}})^3/8\right)^{r_{\mathbb{K}}-1} \, R_{\mathbb{K}}, \quad i = 1, \ldots, r_{\mathbb{K}}. \tag{4}$$

Moreover, for all non-zero algebraic integer $\alpha \in \mathbb{K}$, there exists a unit ε in the multiplicative subgroup generated by $\varepsilon_1, \ldots, \varepsilon_{r_{\mathbb{K}}}$ such that

$$h(\varepsilon \, \alpha) \leq (\log N_{\mathbb{K}/\mathbb{Q}}(\alpha))/(2d_{\mathbb{K}}) + (r_{\mathbb{K}} + 1)^{r_{\mathbb{K}}+1} \, \log^{3r_{\mathbb{K}}+3}(3d_{\mathbb{K}}) \, R_{\mathbb{K}}. \tag{5}$$

Proof. This is implied by Lemme 1 and Lemme 2 of [5]. □

Our proof ultimately depends on Baker's theory of linear forms in logarithms, and for our purpose the sharpest estimate is due to Baker and Wüstholz [1].

Theorem BW. *Let $\alpha_1, \ldots, \alpha_n$ be algebraic numbers different from 0 and 1. Let $d \geq [\mathbb{Q}(\alpha_1, \ldots, \alpha_n) : \mathbb{Q}]$ and define the modified height h' by*

$$h'(\alpha) = \max\left\{h(\alpha), \frac{|\log \alpha|}{d}, \frac{1}{d}\right\},$$

for every non-zero α in $\mathbb{Q}(\alpha_1, \dots, \alpha_n)$. Let $b_1, \dots, b_n$ be rational integers not all 0, and with absolute values less than $B \geq 3$. Setting

$$\Lambda = b_1 \log \alpha_1 + \cdots + b_n \log \alpha_n,$$

we have

$$\log |\Lambda| > -C(n,d)\ h'(\alpha_1) \dots h'(\alpha_n)\ \log B,$$

with

$$C(n,d) = 18\ (n+1)!\ n^{n+1}\ (32\ d)^{n+2}\ \log(2nd).$$

Proof. This is the Theorem of Baker and Wüstholz [1]. □

We deduce Theorem 2 from Theorem 1 by using an explicit upper bound for the size of the solutions of superelliptic equations.

Theorem B. *Let f be a monic polynomial of degree $n \geq 2$ with non-zero discriminant Δ_f, and denote by H its height, i.e. the maximum of the absolute values of its coefficients. Let b and m be non-zero integers with $m \geq 3$. Then all the solutions $(x,y) \in \mathbb{Z}^2$ of the diophantine equation*

$$f(x) = b\, y^m$$

satisfy

$$|x| \leq H^{m+1} \exp\left\{ (c_2\, n\, m)^{c_3\, n^2\, m}\, |\Delta_f|^{5\, n\, m}\, |b|^{n^2\, m}\, (\log_* |b\, \Delta_f|)^{2\, n^2\, m} \right\},$$

where c_2 and c_3 are effectively computable numerical constants.

Proof. This easily follows from the Proposition of Bugeaud [6]. □

4. Proofs

Let a and k be non-zero integers and put $f(x) = ax^n - k$. Denote by Δ_f the discriminant of f. The following Proposition is a variant of a result of Brindza, Evertse and Győry, cf. [3], who delt with the case where $b = 1$ and f is an arbitrary monic, irreducible polynomial with rational integer coefficients. Other versions can also be found in [4] and [2]. Here we formulate this result in the form which is the most suitable for our application.

Proposition. *Let b denote a non-zero integer and m a positive integer. Using the previous notation, the equation*

$$f(x) = by^m \tag{6}$$

in integers x, y with $|y| \geq 2$ implies

$$m \leq 20^{5n+17} n^{5n+27} |ak|^{\frac{5n}{2}} (\log_* |b|)^{\frac{7}{3}}.$$

Proof of the Proposition. We will more or less follow the proof of the similar results given in [3], [4] and [2]. Put $g(t) = t^n - a^{n-1}k$, and let Δ_g denote the discriminant of g. It is easy to verify that $|\Delta_f| = |ak|^{n-1}n^n$ and $|\Delta_g| = |a|^{n^2-3n+2}|\Delta_f|$. By the definitions of f and g, putting $t = ax$, equation (6) is clearly equivalent to

$$g(t) = a^{n-1}by^m. \tag{7}$$

First suppose that either $\deg(g) > 2$ or $a^{n-1}k$ is not a perfect square, and let β_1 be a non-rational root of g. Set $\mathbb{K} = \mathbb{Q}(\beta_1)$, and denote by $d_{\mathbb{K}}$, $D_{\mathbb{K}}$, $R_{\mathbb{K}}$, $h_{\mathbb{K}}$ and $r_{\mathbb{K}}$ the degree, discriminant, regulator, class number and unit rank of $\mathbb{K}$, respectively. Further, we denote by β_i, $i = 1, \ldots, d_{\mathbb{K}}$ the conjugates of β_1. Combining the inequality

$$d_{\mathbb{K}} \leq \frac{2}{\log 3} \log |D_{\mathbb{K}}|,$$

due to Győry [7], with a result of Lenstra [8], we have

$$h_{\mathbb{K}}R_{\mathbb{K}} \leq \frac{1}{(d_{\mathbb{K}}-1)!}|D_{\mathbb{K}}|^{\frac{1}{2}} \log^{d_{\mathbb{K}}-1} |D_{\mathbb{K}}|. \tag{8}$$

Further, we clearly have

$$r_{\mathbb{K}} \leq d_{\mathbb{K}}/2 \leq n/2. \tag{9}$$

Let (t, y) be a fixed solution to (7). The g.c.d. of the principal ideals $\langle t - \beta_1 \rangle$ and $\langle g(t)/(t - \beta_1) \rangle$ divides Δ_g, hence there are integral ideals A, B, C in $\mathbb{K}$ with

$$A\langle t - \beta_1 \rangle = BC^m \tag{10}$$

and

$$\max\{N_{\mathbb{K}/\mathbb{Q}}(A), N_{\mathbb{K}/\mathbb{Q}}(B)\} \leq |a^{n-1} \cdot b \cdot \Delta_g|.$$

Hence, using (8), the Lemma, and the fact that the discrminant of $\mathbb{K}$ divides $|\Delta_f|$, we obtain by a simple calculation that the ideals $A^{h_{\mathbb{K}}}$ and $B^{h_{\mathbb{K}}}$ have generators α and β, respectively, with

$$\max\{h(\alpha), h(\beta)\} \leq c_4 \log_* |a| \log_* |b| |\Delta_f|^{\frac{1}{2}} \log_*^{d_{\mathbb{K}}} |\Delta_f|, \tag{11}$$

where $c_4 = \frac{4(n-1)^2(r_{\mathbb{K}}+1)^{r_{\mathbb{K}}+1}(\log(3d_{\mathbb{K}}))^{3r_{\mathbb{K}}+3}}{(d_{\mathbb{K}}-1)!}$. Thus, equation (10) can be written as

$$\alpha(t - \beta_1)^{h_{\mathbb{K}}} = \varepsilon\beta\gamma^m, \tag{12}$$

where γ is a generator of $C^{h_{\mathbb{K}}}$ and ε is a unit.

We may assume that $\mathbb{K}$ is not an imaginary quadratic field, otherwise the following argument would be much simpler. To obtain a better estimate than in [4], we work with an independent system of units in $\mathbb{K}$, instead of a fundamental one. Let $\varepsilon_1, \ldots, \varepsilon_{r_{\mathbb{K}}}$ be an independent system of units for $\mathbb{K}$ provided by the Lemma. Using (5), we can express ε as $\varepsilon = \varepsilon' \varepsilon_1^{l_1} \ldots \varepsilon_{r_{\mathbb{K}}}^{l_{r_{\mathbb{K}}}}$, where ε' is a unit with $h(\varepsilon') \leq (r_{\mathbb{K}}+1)^{r_{\mathbb{K}}+1}(\log(3d_{\mathbb{K}}))^{3r_{\mathbb{K}}+3}R_{\mathbb{K}}$, and, modifying γ if necessary, we may assume that $\max\limits_{1 \leq i \leq r_{\mathbb{K}}} |l_i| < m$.

We can suppose that $|t| > |a^{n-1}k|^{\frac{1}{n}}+1$, for otherwise we obtain $m \leq 2n\log(2ak)$, and the Proposition is proved. Hence, $|t-\beta_i| > 1$ for $i = 1, \dots, d_{\mathbb{K}}$, and (12) implies

$$|a^{n-1}by^m|^{h_{\mathbb{K}}} \geq \max_{1\leq i\leq d_{\mathbb{K}}} |t-\beta_i|^{h_{\mathbb{K}}} \geq \overline{|\varepsilon'|}^{-d_{\mathbb{K}}+1}\overline{|\varepsilon_1|}^{-m}\dots\overline{|\varepsilon_{r_{\mathbb{K}}}|}^{-m}\overline{|\alpha|}^{-1}\overline{|\beta|}^{-d_{\mathbb{K}}+1}\overline{|\gamma|}^{m},$$

where $\overline{|x|}$ denotes the house of the algebraic number x, *i.e.* the maximum of the absolute values of its conjugates.

Using (4) together with (8), we obtain

$$\prod_{i=1}^{r_{\mathbb{K}}}\overline{|\varepsilon_i|} \leq \exp\left(c_5\ |\Delta_f|^{\frac{1}{2}}\log_*^{d_{\mathbb{K}}-1}|\Delta_f|\right) \text{ and } \overline{|\varepsilon'|} \leq \exp\left(c_5 d_{\mathbb{K}}\ |\Delta_g|^{\frac{1}{2}}\log_*^{d_{\mathbb{K}}-1}|\Delta_g|\right),$$

with $c_5 = c_4/(4(n-1)^2)$. Supposing $m \geq n-1$ (otherwise the Proposition follows), the last two inequalities and (11) yield

$$h(\gamma) \leq 6c_4 d_{\mathbb{K}} \log_*|a|\log_*|b||\Delta_f|^{\frac{1}{2}}\log_*^{d_{\mathbb{K}}}|\Delta_f|\log_*|y|.$$

We may assume that $|t| \geq \frac{1}{2}|y|^{\frac{m}{n}}$, or else we obtain $m \leq 2n\log(2ak)$, and the Proposition is proved. Hence we get $|t-\beta_i| \geq \frac{1}{4}|y|^{\frac{m}{n}}$ for $i = 1, \dots, d_{\mathbb{K}}$. We can suppose that for all $1 \leq i \neq j \leq d_{\mathbb{K}}$, β_1 and β_2 satisfy the inequality

$$\frac{|\beta_i-\beta_j|}{|t-\beta_i|} \geq \frac{|\beta_2-\beta_1|}{|t-\beta_2|}.$$

Thus we have

$$\prod_{\substack{1\leq i,j\leq d_{\mathbb{K}}\\ i\neq j}} \frac{|\beta_i-\beta_j|}{|t-\beta_i|} \leq \frac{4^{d(d-1)}\cdot|\Delta_g|}{|y|^{\frac{md(d-1)}{n}}}.$$

Hence, provided that $|y|^{m/2n} \geq 2|\Delta_g|h_{\mathbb{K}}$ (otherwise we would obtain a much better estimate for m), we get

$$\log\left|\left(\frac{t-\beta_1}{t-\beta_2}\right)^{h_{\mathbb{K}}}-1\right| \leq \log_*\left(h_{\mathbb{K}}\left|\frac{t-\beta_1}{t-\beta_2}-1\right|\right) \leq -\frac{m}{2n}\log_*|y|.$$

In the trivial case $\left(\frac{t-\beta_1}{t-\beta_2}\right)^{h_{\mathbb{K}}} = 1$ one can easily obtain a very good bound for m, as well as in the case $\left|\left(\frac{t-\beta_1}{t-\beta_2}\right)^{h_{\mathbb{K}}}-1\right| > \frac{1}{3}$. Otherwise, using Theorem BW, (3), (8) and (9), we get

$$0 \neq \left|\left(\frac{t-\beta_1}{t-\beta_2}\right)^{h_{\mathbb{K}}}-1\right| = \left|\left(\frac{\varepsilon_1}{\varepsilon_1^{(2)}}\right)^{l_1 h_{\mathbb{K}}}\cdots\left(\frac{\varepsilon_{r_{\mathbb{K}}}}{\varepsilon_{r_{\mathbb{K}}}^{(2)}}\right)^{l_{r_{\mathbb{K}}}h_{\mathbb{K}}}\frac{\beta/\alpha}{\beta^{(2)}/\alpha^{(2)}}\left(\frac{\gamma}{\gamma^{(2)}}\right)^{mh_{\mathbb{K}}}-1\right| \geq$$

$$\geq \frac{1}{2}\left|b_0\log(-1)+l_1h_{\mathbb{K}}\log\left(\frac{\varepsilon_1}{\varepsilon_1^{(2)}}\right)+\dots+l_{r_{\mathbb{K}}}h_{\mathbb{K}}\log\left(\frac{\varepsilon_{r_{\mathbb{K}}}}{\varepsilon_{r_{\mathbb{K}}}^{(2)}}\right)\right.$$

$$\left.+\log\left(\frac{\varepsilon'\beta/\alpha}{\varepsilon'^{(2)}\beta^{(2)}/\alpha^{(2)}}\right)+mh_{\mathbb{K}}\log\left(\frac{\gamma}{\gamma^{(2)}}\right)\right|$$

$$\geq \exp\left(-c_6(n)\log_*^2|a|\log_*^2|b|\Delta_f^{\frac{3}{2}}\log_*^{3n-1}|\Delta_f|\log_*|y|\log_*(m)\right),$$

where b_0 is an integer with $|b_0| \leq mh_{\mathbb{K}}(r+1)$, and $c_6(n) = 1.35\cdot 10^{19}\cdot 33^{3n}\cdot n^{25}$. Here the superscript $^{(2)}$ denotes the image by the isomorphism $\mathbb{Q}(\beta_1)\to\mathbb{Q}(\beta_2)$. The comparision of the upper and lower bounds, using the explicit form of Δ_f, completes the proof of the Proposition in this case.

If $\deg(g) = 2$ and $a^{n-1}k$ is a perfect square, then $g(t)$ is of the form $t^2 - s^2$. Now we can repeat the whole process for the factors $t+s$ and $t-s$, and we get a much better bound for m than stated. Hence, the Proposition is proved. $\square$

Proof of Theorem 1. Put $k = ax^n - by^m$. Using the Lemma we have

$$m \leq 20^{5n+17}n^{5n+27}|ak|^{\frac{5n}{2}}\log_*^{\frac{7}{3}}|b|,$$

which leads to (2), and Theorem 1 is proved. $\square$

Proof of Theorem 2. Set $k = ax^n - by^m$. By Theorem B we obtain a bound for $|x|$, hence for $|a\,x^n|$, in terms of a, b, n, k and m. Namely, we get

$$\log_*\log_*|ax^n| \leq c_7 n^3 m\log(m)\log_*|a|\log_*|b|\log_*|k|,$$

where c_7 is an effectively computable absolute constant. Further, we can derive an upper estimate for m in terms of a, b, n and k. Indeed, by the Proposition we have

$$m \leq 20^{5n+17}n^{5n+27}|ak|^{\frac{5n}{2}}(\log_*|b|)^{\frac{7}{3}}.$$

Combining these estimates, Theorem 2 easily follows. $\square$

Acknowledgements. This work was prepared while the first author visited the University of Debrecen. He wishes to thank the Institute of Mathematics and Informatics for its hospitality. The authors are also grateful to Professor K. Győry for his valuable remarks and suggestions.

References

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

[2] A. Bérczes, B. Brindza and L. Hajdu, *On power values of polynomials*, Publ. Math. Debrecen (to appear).

[3] B. Brindza, J.-H. Evertse and K. Győry, *Bounds for the solutions of some diophantine equations in terms of the discriminants*, J. Austral Math. Soc. **51** (1991), 8–26.

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

[5] Y. Bugeaud, *Bornes effectives pour les solutions des equations en S-unites et des equations de Thue-Mahler*, J. Number Theory **71** (1998), 227–244.

[6] Y. Bugeaud, *On the greatest prime factor of $ax^m + by^n$*, Number Theory: Diophantine, Computational and Algebraic Aspects (K. Győry, A. Pethő and V. T. Sós, eds.), Walter de Gruyter, Berlin–New York, 1998, pp. 115–122.

[7] K. Győry, *Sur les polynômes à coefficients entiérs et de discriminant donné II.*, Publ. Math. Debrecen **21** (1974), 125–144.

[8] H. W. Lenstra Jr., *Algorithms in algebraic number theory*, Bull. Amer. Math. Soc. **26** (1992), 211–244.

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

[10] J. Turk, *On the difference between perfect powers*, Acta Arith. **45** (1986), 289–307.

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

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

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

Lajos Hajdu
Kossuth Lajos University
Institute of Mathematics and Informatics
P.o. box 12.
H–4010 DEBRECEN (HUNGARY)

e-mail : hajdul@math.klte.hu