ON BINOMIAL THUE–MAHLER EQUATIONS

YANN BUGEAUD and KÁLMÁN GYŐRY *)

To the memory of Professor P. Kiss

Abstract

We give a rather sharp upper bound for the degree of a binomial Thue-Mahler equation in terms of the coefficients and the primes involved. Further, we establish explicit lower bounds for the greatest prime factor of a binomial binary form at integral points. Our estimates considerably generalize and improve the earlier results obtained in this direction.

1. Introduction

Let a, b, x and y be non-zero rational integers with $|x| \neq |y|$, and let n be a positive integer. Then, by a theorem of Stewart [10], we have

$$P(ax^n + by^n) > c_1\left(\frac{n}{\log n}\right)^{1/2} \quad \text{if} \quad n \geq c_2, \tag{1}$$

where c_1, c_2 are positive, effectively computable numbers which depend only on a and b. Later, Győry, Mignotte and Shorey [7] (see also Yu and Hung [11]) improved (1) to

$$P(ax^n + by^n) > c_3 n^{1/2} \quad \text{if} \quad n \geq c_4, \tag{2}$$

where the constants c_3, c_4 are positive and effectively computable numbers depending only on a and b. It is known that for $n = 0, 1, 2, \dots, ax^n + by^n$ can be regarded as a special binary recurrence sequence. In [10] and [7], the authors deduced (1) and (2) as consequences of more general results concerning recurrence sequences.

Bugeaud [2] showed that if

$$ax^n + by^n = p^z, z \in \mathbf{N}, \tag{3}$$

Mathematics Subject Classification number: Primary 11D57, Secondary 11D41, 11D61.

Key words and phrases: Thue-Mahler equation, exponential equation, greatest prime factor of binomial binary form.

*) Research supported in part by the Netherlands Organization for Scientific Research, the Hungarian Academy of Sciences, and by Grants 38225 and 42985 of the Hungarian National Foundation for Scientific Research.

where $\gcd(x,y)=1$ and p is a prime with $p \not| ab$, then

$$n \leq 34000 p (\log p) \log A \tag{4}$$

holds with $A=\max\{|a|,|b|,3\}$. The main tools used in [2] are sharp, effective estimates for linear forms in two logarithms, in the Archimedean and non-Archimedean cases.

We prove the following generalization of Bugeaud's theorem.

Theorem 1. *Let a, b, x and y be non-zero rational integers with $|x| \neq |y|$ and $\gcd(x,y) = 1$. Let $p_1, \ldots, p_s$ be primes not dividing a and b, and suppose that*

$$ax^n + by^n = \pm p_1^{z_1} \ldots p_s^{z_s} \tag{5}$$

with an integer $n \geq 3$ and non-negative integers $z_1, \ldots, z_s$. If a/b and x/y are multiplicatively independent, then

$$n \leq 39650 s P (\log P) \log A, \tag{6}$$

while if a/b and x/y are multiplicatively dependent, then

$$n \leq P + \log A. \tag{7}$$

Here, we have set $P = \max\{p_1, \ldots, p_s, 3\}$ and $A = \max\{|a|,|b|,3\}$.

Using that $s \leq 2P/\log P$ (cf. [9]), Theorem 1 immediately yields an explicit lower bound for P in terms of A and n, and so an explicit version of (2). However, it is possible to slightly improve it.

Theorem 2. *Suppose that $|y| > |x|$. Then we have*

$$P(ax^n + by^n) \geq 0.001 \left(\frac{n}{\log A}\right)^{1/2} \left(\log \min\left\{\frac{n}{\log A}, |y|^{1/\log 2}\right\}\right)^{1/2}.$$

Combining Theorem 2 with the best known bounds for the solutions of Thue-Mahler equations (cf. [4] and [6]), one can derive an explicit upper bound for $\max\{|ax^n|, |by^n|\}$ in terms of A and P, only. In [4], it is assumed that the binary form F involved is irreducible. However, in the present case F is the form $aX^n + bY^n$ which can be reducible. For this reason, we use results from [6] and not from [4], see Proposition 3 below. Together with Theorem 2 this gives the following.

Theorem 3. *Let a, b, x, y and n be as in Theorem 1 with $X = \max\{|ax^n|, |by^n|\} \geq e^{e^e}$. Then there exists an effectively computable positive absolute constant c_5 such that*

$$P(ax^n + by^n) \geq c_5 \, \frac{(\log\log X)^{1/4} \cdot (\log\log\log X)^{1/4}}{(\log A \cdot \log\log A)^{1/2}}.$$

We remark that Theorem 3 is not a consequence of Theorem 1 and Proposition 3. Using Theorem 1 (or results from [7] and [11]), it is possible to prove a weaker version of Theorem 3, essentially with $(\log\log\log X)^{1/4}$ replaced by $(\log\log\log X)^{-1/4}$.

Theorem 3 should be compared with the following consequence of Theorem 2 of [3].

Theorem A. *With the same notation as in Theorem 1, there exists an effectively computable positive constant c_6, depending only on n and A, such that*

$$P(ax^n + by^n) \geq \frac{\log\log \max\{|x|, |y|\}}{8n^3}$$

provided that $\max\{|x|, |y|\} \geq c_6$.

In terms of $\max\{|x|, |y|\}$, Theorem A is considerably sharper than Theorem 3; however, there is no dependence on n in the lower bound obtained in Theorem 3. To our knowledge, this is the first time when such a uniform result is established. As (1) and (2) in [10] and [7], our Theorems can also be easily extended to more general binary recurrences and to the number field case. This will be the subject of a forthcoming paper.

2. Auxiliary results

The proof of (6) in Theorem 1 will be based on the next two propositions concerning linear forms in two logarithms. Let $\alpha = \alpha_1$ be a non-zero algebraic number with minimal defining polynomial $a_0(X - \alpha_1)\dots(X - \alpha_n)$ over $\mathbf{Z}$. The logarithmic height of α, denoted by $\mathrm{h}(\alpha)$, is defined by

$$\mathrm{h}(\alpha) = \frac{1}{n} \log\Big(a_0 \prod_{i=1}^{n} \max\{1, |\alpha_i|\}\Big).$$

For any prime number p, let $\overline{\mathbf{Q}}_p$ be an algebraic closure of the field $\mathbf{Q}_p$ of p-adic numbers. We denote by v_p the unique extension to $\overline{\mathbf{Q}}_p$ of the standard p-adic valuation over $\mathbf{Q}_p$, normalized by $v_p(p) = 1$.

Proposition 1. *Let p be a prime number. Let α_1 and α_2 be two algebraic numbers which are p-adic units. Denote by f the residual degree of the extension $\mathbf{Q}_p \hookrightarrow \mathbf{Q}_p(\alpha_1, \alpha_2)$ and put $D = [\mathbf{Q}(\alpha_1, \alpha_2) : \mathbf{Q}]/f$. Let b_1 and b_2 be two positive integers and put*

$$\Lambda = \alpha_1^{b_1} - \alpha_2^{b_2}.$$

Denote by $A_1 > 1$ and $A_2 > 1$ two real numbers such that

$$\log A_i \geq \max\{\mathrm{h}(\alpha_i), (\log p/D)\}, \;\; i = 1, 2,$$

and put

$$b' = \frac{b_1}{D \log A_2} + \frac{b_2}{D \log A_1}.$$

If α_1 and α_2 are multiplicatively independent, then we have the upper bound

$$v_p(\Lambda) \leq \frac{24p(p^f - 1)}{(p-1)(\log p)^4} D^4 \left(\max\left\{\log b' + \log\log p + 0.4, \frac{10\log p}{D}, 5\right\}\right)^2 \log A_1 \, \log A_2.$$

Proof : This is Théorème 4 of Bugeaud and Laurent [5] with the choice $(\mu, \nu) = (10, 5)$. $\square$

Proposition 2. *Let $\alpha_1 \geq 1$ and $\alpha_2 \geq 1$ be two real algebraic numbers. Let b_1 and b_2 be two positive integers and put*

$$\Lambda = b_1 \log \alpha_1 - b_2 \log \alpha_2.$$

Set $D = [\mathbf{Q}(\alpha_1, \alpha_2) : \mathbf{Q}]$ and denote by $A_1 > 1$ and $A_2 > 1$ two real numbers satisfying

$$\log A_i \geq \max\{\mathrm{h}(\alpha_i), 1/D\}, \quad i = 1, 2.$$

Finally, put

$$b' = \frac{b_1}{D \log A_2} + \frac{b_2}{D \log A_1}.$$

If α_1 and α_2 are multiplicatively independent, then we have the lower bound

$$\log |\Lambda| \geq -32.31\, D^4 \left(\max\{\log b' + 0.18, 0.5, 10/D\}\right)^2 \log A_1 \log A_2.$$

Proof : This is Corollaire 2 of Laurent, Mignotte and Nesterenko [8], where the numerical constants are given in Tableau 2 and correspond to the choice $h_2 = 10$. Notice that the hypotheses of the Proposition imply that $\mathrm{h}(\alpha_i) \leq |\log \alpha_i|/D$. $\square$

The proof of Theorem 3 depends on an upper estimate for the size of the solutions of Thue–Mahler equations, due to Győry [6].

Proposition 3. *Let a, b and n be non-zero integers with $n \geq 3$. Let $p_1, \ldots, p_s$ $(s > 0)$ be distinct rational primes not dividing a and b. All solutions of the Thue–Mahler equation*

$$ax^n + by^n = p_1^{z_1} \ldots p_s^{z_s} \quad \text{in } x, y, z_1, \ldots, z_s \in \mathbf{Z},$$

with $\gcd(x, y) = 1$ and $z_1, \ldots, z_s \geq 0$ satisfy

$$\log \log \max\{|ax^n|, |by^n|\} < c_7 n\big(s \log(ns) + n \log P + s \log \log P + \log A\big).$$

where $P = \max\{p_1, \ldots, p_s, 3\}$ and c_7 is an effectively computable absolute constant.

Proof : By means of a well-known argument the equation can be reduced to Thue equations of the form $F(x, y) = ax^n + by^n = \beta$ in S-integers x, y, where $S = \{p_1, \ldots, p_s\}$ and $\beta = p_1^{u_1} \cdots p_s^{u_s}$ with $0 \leq u_1, \ldots, u_s < n$. To these equations one can apply Theorem 2 of [6] with the choice $L = \mathbf{Q}$, $m = 2$, $k = 1$ and $d_3 \leq n(n-1)$ to derive an explicit upper bound for the height of x/y, and hence for $\max\{|ax^n|, |by^n|\}$. The bound so obtained depends not only on n, s, P and A, but also on some other parameters. However, all these parameters can be easily estimated from above in terms of n, s, P and A using (2.4) and Lemma 5 of [6], as well as

$$|D_{M_i}| \leq |D(F)| \leq n^{2n-1} A^{2n-2},$$

where $D(F)$ and D_{M_i} denote the discriminants of F and of the number field M_i generated by the i-th linear factor of $x^n+(b/a)y^n$ over $\overline{\mathbf{Q}}$. Finally, we get the upper bound requested. $\square$

3. Proofs of the Theorems

Proof of Theorems 1 and 2: We may assume without loss of generality that $y > x > 0$ with $\gcd(x, y) = 1$ and that $\gcd(a, b) = 1$.

First consider the case when a/b and x/y are multiplicatively dependent. Then there are positive integers x_1, y_1, u and an integer v such that

$$x = x_1^u, y = y_1^u, \pm a/b = (x_1/y_1)^v.$$

Put $n_1 = nu + v$. If $v \geq 0$, then

$$ax^n + by^n = \pm x_1^{n_1} \pm y_1^{n_1}.$$

If $v < 0$, then

$$a = \pm y_1^{|v|}, b = \pm x_1^{|v|},$$

whence

$$|v| \leq \log A.$$

Further,

$$ax^n + by^n = \pm(x_1y_1)^{|v|}(\pm x_1^{n_1} \pm y_1^{n_1}),$$

and so (5) gives

$$\pm x_1^{n_1} \pm y_1^{n_1} = \pm p_1^{z_1'} \dots p_s^{z_s'} \text{ with integers } z_i' \geq 0.$$

This means that it suffices to prove Theorem 1 for the case $a = 1, b = \pm 1$. If we have an upper bound, say N, for n_1, then in the first case $n \leq N$, while in the second case

$$n \leq n_1 + |v| \leq N + \log A$$

follows. But, by a classical theorem of Zsigmondy [12] (see also Birkhoff and Vandiver [1]), we have

$$P(x_1^{n_1} \pm y_1^{n_1}) \geq n_1 \text{ if } n_1 > 2. \tag{8}$$

Since $P \geq P(x_1^{n_1} \pm y_1^{n_1})$, inequality (8) gives (7).

Next consider the case when a/b and x/y are multiplicatively independent. In view of Bugeaud's result (4), it is enough to deal with the case $s \geq 2$.

Put

$$R_n = ax^n + by^n. \tag{9}$$

First suppose that

$$|R_n| \leq y^{0.9n}. \tag{10}$$

Let

$$\Lambda = \frac{a}{b}\left(\frac{x}{y}\right)^n + 1. \tag{11}$$

Then (9),(10) and (11) give

$$\log|\Lambda| \leq -0.1n\log y. \tag{12}$$

Hence, by (11),

$$\left|n\log\frac{y}{x} - \log\left|\frac{a}{b}\right|\right| \leq |\log(\Lambda - 1)| \leq 1.001|\Lambda|. \tag{13}$$

We apply now Proposition 2 above. Let

$$\alpha_1 = y/x, \alpha_2 = \left|\frac{a}{b}\right|, b_1 = n, b_2 = 1.$$

Using the notation of Proposition 2, we can choose

$$\log A_1 = \log y,\ \ \log A_2 = \log A,\ \ b' = \frac{n}{\log A} + \frac{1}{\log y},$$

where $b' \leq 2n/\log A$, provided that $n \geq \log A$. We deduce now that if $\alpha_2 \geq 1$, then

$$\log|\Lambda| \geq -0.001 - 32.31\max\left\{\log\left(\frac{2n}{\log A}\right) + 0.18, 10\right\}^2 \log A\log y \tag{14}$$

which, together with (12), gives

$$n \leq 323.2\max\left\{\log\left(\frac{2n}{\log A}\right) + 0.18, 10\right\}^2 \log A, \tag{15}$$

whence

$$n \leq 135080\log A. \tag{16}$$

If $\alpha_2 < 1$, then in (13) the left hand side is

$$n\log\frac{y}{x} + \log\left|\frac{b}{a}\right|$$

which is positive. Then (13) and (12) imply that

$$\log\left|\frac{b}{a}\right| \leq 1.001|\Lambda| \leq 1.001y^{-0.1n} \leq 1.001\cdot 2^{-0.1n}$$

which yields again (16).

In what follows, we suppose that

$$|R_n| > y^{0.9n}. \tag{17}$$

If p divides R_n for some prime p, then in view of $\gcd(x,y)=1$ we have $p \nmid xy$. Further,

$$v_p(R_n) \le v_p\left(\left(\frac{y}{x}\right)^n - \left(-\frac{a}{b}\right)\right). \tag{18}$$

We apply Proposition 1 above. Let

$$\alpha_1 = \frac{y}{x}, \alpha_2 = -\frac{a}{b}, b_1 = n, b_2 = 1, f = D = 1.$$

Recall that we have $y > x > 0$. We fix ϵ with $0 \le \epsilon \le 1$ and we distinguish two cases.

First case: Assume first that every prime divisor p of R_n satisfies

$$\frac{\log y}{\log 2} \ge (\log p)^{\epsilon}.$$

This always holds if $\epsilon = 0$. Since $p \ge 2$ and $y \ge 2$, we may apply Proposition 1 with the choice

$$\log A_1 = \frac{\log y}{\log 2} \cdot (\log p)^{1-\epsilon}, \ \log A_2 = 2\frac{\log p}{\log 2} \log A$$

and

$$b' = \frac{n}{\log A_2} + \frac{1}{\log A_1} \le \frac{n \log 2}{\log p \log A},$$

provided that $n \ge (2\log A)/\log 2$. Then we get

$$v_p\left(\left(\frac{y}{x}\right)^n - \left(-\frac{a}{b}\right)\right) \le 100\frac{p}{(\log p)^{2+\epsilon}} \log y \cdot \log A \cdot \max\left\{10\log p, \log\left(\frac{n}{\log A}\right)\right\}^2,$$

whence

$$v_p(R_n) \le 100\frac{p}{(\log p)^{2+\epsilon}} \log y \cdot \log A \cdot \max\left\{10\log p, \log\left(\frac{n}{\log A}\right)\right\}^2. \tag{19}$$

It follows now that

$$\begin{aligned} \log|R_n| &= \sum_{p|R_n} v_p(R_n)\log p \\ &\le 100\log y \cdot \log A \cdot \max\left\{10\log P, \log\left(\frac{n}{\log A}\right)\right\}^2 \cdot \sum_{p|R_n} \frac{p}{(\log p)^{1+\epsilon}}. \end{aligned} \tag{20}$$

Comparing (20) with (17), we deduce that

$$\frac{n}{\log A} < 111\max\left\{10\log P, \log\left(\frac{n}{\log A}\right)\right\}^2 \cdot \sum_{p|R_n} \frac{p}{(\log p)^{1+\epsilon}}. \tag{21}$$

Except possibly for the case when $P = 3$ and $s = 2$, we infer from (21) that either

$$n < 11100 sP(\log P)\log A \tag{22}$$

or

$$\frac{n}{\log A} < 111 s \frac{P}{(\log P)^{1+\epsilon}} \log^2\left(\frac{n}{\log A}\right),$$

whence, using that

$$s \leq \pi(P) \leq 1.25506 \frac{P}{\log P} \tag{23}$$

(cf. [9]), we get

$$n < 39650 sP(\log P)^{1-\epsilon}\log A. \tag{24}$$

It is easy to check that for $s = 2, p_1 = 2, p_2 = 3$, (21) also implies (24). Taking $\epsilon = 0$ in (24), this yields (6) and completes the proof of Theorem 1.

If a/b and x/y are multiplicatively dependent, a sharper version of Theorem 2 follows immediately from (7). Hence we consider the case when a/b and x/y are multiplicatively independent. Then, in the first case inequalities (23) and (24) imply that

$$n < 49764 P^2(\log P)^{-\epsilon}\log A, \tag{25}$$

thus

$$P \geq 0.001\left(\frac{n}{\log A}\right)^{1/2}\left(\log\left(\frac{n}{\log A}\right)\right)^{\epsilon/2}. \tag{26}$$

Second case: Assume now that there exists a prime divisor p of R_n such that $(\log y)/(\log 2) < (\log p)^\epsilon$. This trivially implies that

$$(\log P)^\epsilon > \frac{\log y}{\log 2}.$$

Hence the estimate $P \geq n/\log A$ and, a fortiori, (26) hold as soon as

$$(\log(n/\log A))^\epsilon \leq (\log y)/(\log 2),$$

thus for any ϵ such that

$$\epsilon \leq \frac{\log((\log y)/(\log 2))}{\log\log(n/\log A)}. \tag{27}$$

Conclusion: We choose for ϵ the largest possible value given by (27). If this value is ≥ 1, we put $\epsilon = 1$. Then (26) holds with $\epsilon = 1$. If $\epsilon < 1$ (that is, if $(\log y)/(\log 2) < \log(n/\log A)$), we infer from (26) and (27)that

$$P \geq 0.001\left(\frac{n}{\log A}\right)^{1/2}\left(\frac{\log y}{\log 2}\right)^{1/2}.$$

Consequently, we get

$$P \geq 0.001 \left(\frac{n}{\log A} \right)^{1/2} \left(\log \min \left\{ \frac{n}{\log A}, y^{1/\log 2} \right\} \right)^{1/2}.$$

This proves Theorem 2. □

Proof of Theorem 3:

If $(\log y)/(\log 2) \geq \log(n/\log A)$, we use (7) or (25) with $\epsilon = 1$ to bound n, according as a/b and x/y are multiplicatively dependent or not. Then, it follows from (23) and Proposition 3 that there exists an effectively computable positive absolute constant c_8 such that

$$\log \log \max\{|a|x^n, |b|y^n\} \leq c_8 \frac{P^4}{\log P} \log^2 A. \tag{28}$$

It is easily checked that (28) remains true if $(\log y)/(\log 2) < \log(n/\log A)$. Indeed, in this case $\max\{|a|, |b|\}y^n$ is bounded above in terms of A and n only. Then we can use Theorem 1 to bound n. Hence, we get a lower bound for P independent of n, and Theorem 3 is an immediate consequence of (28). □

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.

References

[1] G. D. Birkhoff and H. S. Vandiver *On the integral divisors of* $a^n - b^n$, Annals of Math. (2) 5 (1904), 173–180.

[2] Y. Bugeaud, *On the diophantine equation* $x^2 - p^m = \pm y^n$, Acta Arith. 80 (1997), 213–223.

[3] Y. Bugeaud, *On the greatest prime factor of* $ax^m + by^n$*, II*, Bull. London Math. Soc. 32 (2000), 673–678.

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

[5] Y. Bugeaud et M. Laurent, *Minoration effective de la distance p-adique entre puissances de nombres algébriques*, J. Number Theory 61 (1996), 311–342.

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

[7] K. Győry, M. Mignotte and T. N. Shorey, *On some arithmetical properties of weighted sums of* S*-units*, Math. Pannonica 1/2 (1990), 25–43.

[8] M. Laurent, M. Mignotte et Yu. Nesterenko, *Formes linéaires en deux logarithmes et déterminants d'interpolation*, J. Number Theory 55 (1995), 285–321.

[9] J. B. Rosser and L. Schoenfeld, *Approximate formulas for some functions of prime numbers*, Illionis J. Math. 6 (1962), 64–94.

[10] C. L. Stewart, *On divisors of terms of linear recurrence sequences*, J. Reine Angew. Math. 333 (1982), 12–31.

[11] Kunrui Yu and Ling-kei Hung, *On binary recurrence sequences*, Indag. Math. 6 (1995), 341–354.

[12] K. Zsigmondy, *Zur Theorie der Potenzerste*, Monatsh. Math. 3 (1892), 265–284.

Yann Bugeaud
Université Louis Pasteur
7, rue René Descartes
67084 STRASBOURG (FRANCE)

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

Kálmán Győry
Number Theory Research Group of the Hungarian Academy of Sciences,
Institute of Mathematics
University of Debrecen
4010 DEBRECEN (HUNGARY)

e-mail : gyory@math.klte.hu