Lower bounds for the greatest prime factor of $ax^m + by^n$

Yann Bugeaud (Strasbourg)

Abstract. In the present work, we state our new lower bounds for the greatest prime factor of algebraic numbers of the form $ax^m + by^n$, together with a brief survey of related results.

Math. Subject Classification : 11D61.

Keywords : Greatest prime factor, binary form.

1. Introduction

The first important result about prime factors of integers of the form $ax^m + by^n$ goes back to Zsigmondy [17] and Birkhoff & Vandiver [1], who proved that $P[x^n - y^n] \geq n + 1$ for all integers $n > 6$ and all relatively coprime non-zero integers x and y, with $x \neq \pm y$. Here and throughout the paper, we denote by $P[z]$ the greatest prime factor of the norm of the algebraic integer z, with the convention that $P[0] = 1$ and $P[z] = 1$ when z is a unit.

Mahler [11] proved that the greatest prime factor of $ax^m + by^n$, where $m \geq 2$, $n \geq 3$, a and b are fixed non-zero 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 [10] gave an explicit version of the above theorem of Mahler, which, a year later, has been extended by Shorey *et al.* [13] as follows. If a, b and $n \geq 2$ 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 rational integers x and y. Shorey [12] derived an explicit form of this result, and Shorey & Tijdeman [14, Chapter 10] generalized it to the number field case.

Recently, Bugeaud & Győry [5, 6, 2] have developped a new approach for giving explicit upper bounds for the size of the solutions of classical diophantine equations. This turns out to have interesting applications to the questions considered here and it allows us to considerably sharpen the above-quoted explicit results of Kotov [10] and Shorey [12]. In the present work, we state our new lower bounds for the greatest prime factor of $ax^m + by^n$, together with a brief survey of related results.

2. Notation

In the sequel, $\mathbf{K}$ always denote a number field, and we write N for the norm from $\mathbf{K}$ to $\mathbf{Q}$. We refer the reader to [5] for the definitions of S-norm and S-regulator, where S is any finite set of places on $\mathbf{K}$ containing the set of infinite places. We also denote by $\mathrm{h}(\alpha)$

the absolute (multiplicative) height of the algebraic number α. We warn the reader that, in the proof of Theorem 3, we use results of [5] without recalling them here.

Further, by constant, we always mean effectively computable positive constant, and we specify into brackets the parameters from which it depends. Finally, we denote by $p_1 = 2, p_2, \dots, p_t, \dots$ the sequence of prime numbers in increasing order.

3. Lower bounds when the two exponents are fixed

Let $f(X,Y)$ be a binary form with coefficients in the ring of integers of a number field $\mathbf{K}$ and assume that the polynomial $f(X,1)$ has at least three distinct roots. Following the classical proof leading to explicit estimates for the size of the solutions of the Thue-Mahler equation, several authors obtained a lower bound for the greatest prime factor of $f(x,y)$, where x and y are algebraic integers in $\mathbf{K}$. In Theorem 1 below, we present a simple version of their results.

Theorem 1. *There exists a constant $c_1 = c_1(f)$ such that*

$$P\big[f(x,y)\big] \geq c_1(f)\, \log\log \max\big\{|\mathrm{N}(x)|, |\mathrm{N}(y)|, e^e\big\},$$

for all coprime algebraic integers x and y in $\mathbf{K}$.

Proof : See Shorey *et al.* [13] or Győry [7]. The main tool is Baker's theory and its p-adic analogue. □

When $f(X,Y) = aX^n + bY^n$, with a and b non-zero algebraic integers, Theorem 1 is a particular case of the following result.

Theorem 2. *Let a and b be non-zero algebraic integers, and let $m \geq 2$ and $n \geq 2$ be integers satisfying $mn \geq 6$. Suppose that x and y are coprime algebraic integers in $\mathbf{K}$. Then there exists a constant $c_2 = c_2(a,b,m,n)$ such that*

$$P[a\,x^m + b\,y^n] \geq c_2\, \log\log \max\big\{|\mathrm{N}(x)|, |\mathrm{N}(y)|, e^e\big\}.$$

Proof : See Bugeaud [3]. Notice that Kotov's result [10] involves the function $(\log\log)^{1/2} \times (\log\log\log)^{1/2}$ instead of $\log\log$. □

4. Lower bounds when only one exponent is fixed

As mentioned in the introduction, Shorey *et al.* [13] and Shorey [12] were the first to prove that $P[ax^m + by^n]$ tends to infinity when only one exponent is fixed. It is interesting to note that the Thue-Siegel-Roth-Schmidt method seems to fail to prove an ineffective version of Theorem 3.

Theorem 3. *Let a and b be non-zero algebraic integers and let $n \geq 2$ be an integer. Then there exists a constant $c_3 = c_3(a,b,n)$ such that*

$$P[a\,x^m + b\,y^n] \geq c_3\, \log m,$$

for every non-zero coprime algebraic integers x and y, where x is not a root of unity.

Proof : See Bugeaud [4]. Notice that Shorey's result [12] involves the function $(\log)^{1/2} \times (\log\log)^{1/2}$ instead of log. □

5. Lower bounds for $P[ax^m + by^m]$ in terms of m

In the case of binary recurring sequences, Theorem 3 has been considerably refined by Kunrui Yu and Ling-kei Hung [16] (see also the works of Stewart and Pethő quoted therein). Let a, b, x and y be algebraic integers such that $abxy \neq 0$ and x/y is not a root of unity. Further, set $\mathbf{K} := \mathbf{Q}(a, b, x, y)$ and denote by d the degree of $\mathbf{K}$ and by $h_{\mathbf{K}}$ its class number.

Theorem 4. *There exists a constant $c_{16} = c_{16}(d, a, b, h_{\mathbf{K}})$ such that*

$$P[ax^m + b\,y^m] > c_{16}\, m^{1/(d+1)}.$$

Proof : See Kunrui Yu and Ling-kei Hung [16]. The main tool is a precise lower bound for linear forms in two p-adic logarithms. However, they also need an estimate for linear forms in three archimedean logarithms. □

When the sequence $(ax^m + by^m)$ is a Lucas-Lehmer sequence, Theorem 4 can be considerably refined, as shown by *e.g.* Schinzel and Stewart (for references, see the Notes at the end of Chapter 3 in the book of Shorey & Tijdeman [14]).

Let α and β be algebraic integers such that $\alpha + \beta$ (*resp.* $(\alpha + \beta)^2$) and $\alpha\beta$ are relatively prime non-zero algebraic integers and α/β is not a root of unity. For $n > 0$, we define the Lucas (*resp.* Lehmer) sequence (u_n) by $u_n = (\alpha^n - \beta^n)/(\alpha - \beta)$ (*resp.* by $u_n = (\alpha^n - \beta^n)/(\alpha^\delta - \beta^\delta)$, with $\delta = 1$ or 2, according as n is odd or even).

Theorem 5. *For any Lucas or Lehmer sequence (u_m), we have*

$$P[u_m] \geq m - 1 \quad \text{for} \quad m > e^{452}\, 4^{67}.$$

Proof : See Győry, Kiss & Schinzel [8]. The proof highly depends on properties of cyclotomic polynomials. Note that we can replace $e^{452}\, 4^{67}$ by the much smaller constant 30030 (see the recent work of Voutier [14]). □

6. An upper bound

Let a, b, x and y be non-zero integers. There is a wide gap between Theorem 2 and the trivial estimate $P[ax^m + by^n] \leq \exp\{c_{17} \log(|x| + |y|)\}$, and it seems difficult to conjecture which is the true order of magnitude. Nevertheless, using an idea due to Győry and Sárközy [9], we are able to refine the trivial upper bound for $P[ax^m + by^n]$ in a particular case.

Theorem 6. *Put $Q_t = p_1 \dots p_t$. There exists an absolute constant c_{18} such that for every non-zero integers x and y and for every $t \geq 1$, we have*

$$P[x^{Q_t} - y^{Q_t}] \leq \big(|x| + |y|\big)^{c_{18}\, Q_t / \log\log Q_t}.$$

Proof : We follow the argument of Theorem 3 of [9]. Denote by $\Phi_n(X,Y)$ the n-th homogeneized cyclotomic polynomial and let x, y be non-zero integers. Since for every integer $n \geq 1$ we have

$$X^n - Y^n = \prod_{d|n} \Phi_d(X,Y),$$

we deduce that

$$\begin{aligned} P[x^n - y^n] &= \max_{d|n}\ P\big[\Phi_d(x,y)\big] = \max_{d|n}\ P\Big[\prod_{1 \leq j \leq d, (j,d)=1} (x - e^{2i\pi j/d}\, y)\Big] \\ &\leq \max_{d|n}\ P\Big[\prod_{1 \leq j \leq d, (j,d)=1} \big(|x| + |y|\big)\Big] \\ &\leq \max_{d|n}\ \big(|x| + |y|\big)^{\varphi(d)}, \end{aligned}$$

where φ is the Euler totient function. To conclude, it is sufficient to note that there exists an absolute constant c_1 such that $\varphi(Q_t) \leq c_{18}\, Q_t / \log\log Q_t$ for every $t \geq 1$ (see [9]). $\square$

Acknowledgement. The author would like to thank the CCCI for providing him a financial support to attend the Conference in Ostravice.

References

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

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

[3] Y. Bugeaud, On the greatest prime factor of $ax^m + by^n$, In : Number Theory (ed. by K. Győry, A. Pető and V. T. Sós), Walter de Gruyter, Berlin - New-York (1998), 115-122.

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

[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] K. Győry, P. Kiss and A. Schinzel, A note on Lucas and Lehmer sequences, Colloq. Math. 45 (1981), 75–80.

[9] K. Győry and A. Sárközy, On prime factors of integers of the form $(ab+1)(bc+1)(ca+1)$, Acta Arith. 79 (1997), 163–171.

[10] 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.

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

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

[13] 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.

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

[15] P. Voutier, On primitive divisors of Lucas and Lehmer sequences *III*, Math. Proc. Cambridge Phil. Soc. 123 (1998), 407–419.

[16] K. Yu and L. Hung, On binary recurrence sequences, Indag. Math. N. S. 6 (1995), 341–354.

[17] K. Zsigmondy, Zur Theorie der Potenzreste, Monatsh. Math. 3 (1892), 256–284.

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

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