On the size of integer solutions of elliptic equations, *II*

Yann Bugeaud (Strasbourg)

Abstract

Let $\mathbf{K}$ be a number field and let a and b be coprime algebraic integers in $\mathbf{K}$. We give an upper bound for the size of the integer solutions of the elliptic equation $y^2 = x^3 + ax + b$ depending only on the prime factors of the discriminant of the polynomial $X^3 + aX + b$ and not on its height.

Mathematics Subject Classification : 11D25, 14H52.

1. Introduction

Let $\mathbf{K}$ be a number field of degree d and denote by $O_{\mathbf{K}}$ its ring of integers. Let a and b be in $O_{\mathbf{K}}$ such that $4a^3 + 27b^2 \neq 0$ and set $f(X) = X^3 + aX + b$. We consider the elliptic equation

$$y^2 = f(x) \qquad \text{in } x, y \in O_{\mathbf{K}}. \tag{1}$$

The first effective bound for the size of the integer solutions of (1) is due to Baker [1] in the case $\mathbf{K} = \mathbf{Q}$. Indeed, as a consequence of his powerful estimates for linear forms in logarithms, he showed that

$$\max\{|x|, |y|\} \leq \exp\Big\{ \big(10^6 \max\{|a|, |b|\}\big)^{10^6} \Big\}.$$

Later, this bound was considerably improved and generalized to arbitrary $\mathbf{K}$ by several authors, including Sprindžuk [10], Schmidt [9], Poulakis [8], Pintér [7], Voutier [11], Bugeaud [2] and Hajdu & Herendi [6]. For instance, the dependence on the height H_f of the polynomial f (see [2] for the definition) was considerably refined : Pintér [7] obtained in the rational case an upper bound polynomial on the height of f, but which takes into account the discriminant $\Delta_f := -4a^3 - 27b^2$ of f (see also Bugeaud [2]). Then, he deduced from his result an estimate for the size of the solutions of (1) depending only on $|\Delta_f|$. We point out that the height of a polynomial can be arbitrarily large compared with the absolute value of its discriminant.

The purpose of the present work is to refine Pintér's bound in giving an upper estimate depending only on the prime factors of $|\Delta_f|$, in the important case when a and b are coprime. A first step towards this result has already been done in [2] where, unfortunately, the height of f also slightly occured in the bounds.

Acknowledgement : This work has been done while the author was visiting the Aristotle University of Thessaloniki. He would like to express his warmest gratitude to Dimitrios Poulakis for his invitation.

2. Statement of the results

We keep the notation of the Introduction and we let $\mathrm{N}_{\mathbf{K}/\mathbf{Q}}$, or simply N, stand for the norm from $\mathbf{K}$ to $\mathbf{Q}$. The greatest prime factor (*resp.* the greatest square-free part) of $\mathrm{N}z$, the norm of the algebraic integer z, is denoted by $P[z]$ (*resp.* by $Q[z]$), and we use the convention that $P[0] = Q[0] = 1$ and $P[z] = Q[z] = 1$ when z is a unit.

As in [2], we denote by $\mathrm{h}(\alpha)$ the (absolute) height of the algebraic number α, and we stand the notation $\log^+ x$ for $\max\{\log x, 1\}$. Our main result is the following.

Theorem. *Let $\mathbf{K}$ be a number field of degree d. Let a and b be coprime algebraic integers in $\mathbf{K}$. Set $f(X) = X^3 + a\,X + b$ and denote by $\Delta_f := -4a^3 - 27b^2$ the discriminant of f. Assume that Δ_f is non–zero. Then there exist effective absolute constants $c_1 > 0$ and $c_2 > 0$ and an effective constant c_3 depending only on $\mathbf{K}$ such that*

$$P[\Delta_f] \geq c_1 \, \frac{\log^+ \log^+ \max\{|\mathrm{N}x|, |\mathrm{N}y|\}}{d}$$

and

$$Q[\Delta_f] \geq \big(2 \log^+ \max\{|\mathrm{N}x|, |\mathrm{N}y|\}\big)^{c_2/d}$$

for all algebraic integers x and y in $\mathbf{K}$ satisfying $y^2 = f(x)$, provided that $|\mathrm{N}\Delta_f| \geq c_3$.

Remark : We observe that in the case $a = 0$ the lower bound for $P[\Delta_f]$ follows from the Theorem of [4] (see also [3] for a slightly weaker result).

As an immediate corollary, we improve Corollary 1 of [2], where the given upper bound for $|x|$ and $|y|$ also depends on the height of the polynomial f.

Corollary. *Under the hypothesis of the Theorem, assume further that $\mathbf{K} = \mathbf{Q}$. There exist effective absolute constants $c_4 > 0$ and $c_5 > 0$ such that if the rational integers x and y satisfy $y^2 = f(x)$, then*

$$\max\{|x|, |y|\} \leq \exp\big\{\exp(c_4 \, P[\Delta_f])\big\}$$

and

$$\max\{|x|, |y|\} \leq \exp\bigg\{ \big(2\, Q[\Delta_f]\big)^{c_5} \bigg\}.$$

Remarks : For an arbitrary number field $\mathbf{K}$, one cannot obtain an upper estimate for the solutions of (1) depending only on $P[\Delta_f]$. Indeed, if $y^2 = x^3 + ax + b$, then, for every unit η in $O_{\mathbf{K}}$, we have $(\eta^3\, y)^2 = (\eta^2\, x)^3 + a\,\eta^4 (\eta^2\, x) + b\,\eta^6$, hence $(\eta^2\, x, \eta^3\, y)$ is a solution of

$$Y^2 = X^3 + (a\,\eta^4)\,X + (b\,\eta^6) =: f_\eta(X).$$

Therefore, $P[\Delta_f] = P[\Delta_{f_\eta}]$ while $\mathrm{h}(\eta^3\, y)$ and $\mathrm{h}(\eta^2\, x)$ can be arbitrarily large.

The hypothesis a and b coprime in the Corollary cannot be dropped since, for instance, for any integer $m \geq 1$, we have

$$(2^{3m})^2 = (2^{2m})^3 + 2^{4m}\,(2^{2m}) - 2^{6m},$$

and the greatest prime factor of the discriminant of the polynomial $X^3 + 2^{4m}\, X - 2^{6m}$ is equal to 23. However, we infer from the proof of the Theorem of [4] that there exists an effective absolute positive constant c_6 such that the Corollary remains valid under the weaker hypothesis

$$|4a^3 + 27b^2| \geq \exp\Bigl\{\bigl(\gcd(a,b)\bigr)^{c_6} - 1\Bigr\}.$$

3. Proof

Denote by $D_{\mathbf{K}}$ the discriminant of $\mathbf{K}$. Let a and b be coprime algebraic integers in $\mathbf{K}$ and let $(x,y) \in O_{\mathbf{K}}^2$ be such that $y^2 = x^3 + ax + b$. According to inequality (5) and Lemma 2 of [5], there exists a unit $\eta \in \mathbf{K}$ such that

$$\mathrm{h}\bigl(\eta^{12}(4a^3 + 27b^2)\bigr) \leq |\mathrm{N}(4a^3 + 27b^2)|^{1/d}\, \exp\{12\, d^{3d}\, |D_{\mathbf{K}}|\, (\log^+ |D_{\mathbf{K}}|)^{d-1}\}.$$

Set $a' = a\,\eta^4$ and $b' = b\,\eta^6$. Then, the discriminant Δ' of the polynomial $X^3 + a'X + b'$ satisfies $\Delta' = \eta^{12}\,\Delta$, where $\Delta := -4a^3 - 27b^2$ is the discriminant of $X^3 + aX + b$. Since we have

$$(\eta^3\, y)^2 = (\eta^2\, x)^3 + a'(\eta^2\, x) + b',$$

Theorem 2 of [2] yields

$$\max\{\mathrm{h}(\eta^3 y), \mathrm{h}(\eta^2 x)\} \leq \mathrm{h}(a')^{35}\, \mathrm{h}(b')^{35}\, \exp\bigl\{\exp\{c_7\, d\, (P + \log^+ |d\, D_{\mathbf{K}}|)\}\bigr\} \tag{2}$$

and

$$\max\{\mathrm{h}(\eta^3 y), \mathrm{h}(\eta^2 x)\} \leq \mathrm{h}(a')^{35}\, \mathrm{h}(b')^{35}\, \exp\bigl\{|D_{\mathbf{K}}|^6\, (2\, d\, Q\, \log^+ |D_{\mathbf{K}}|)^{c_8\, d}\bigr\}, \tag{3}$$

where $P = P[\Delta]$ and $Q = Q[\Delta]$. Here and below, $c_7, \ldots, c_{15}$ denote effective absolute positive constants.

Further, we observe that

$$(108\, b')^2 = (-12\, a')^3 + (-16 \times 27)\, \Delta',$$

and we can apply once more Theorem 2 of [2] to get

$$\begin{aligned} \max\{\mathrm{h}(108\, b'), \mathrm{h}(12\, a')\} &\leq \mathrm{h}(432\, \Delta')^{35}\, \exp\bigl\{\exp\{c_9\, d(P + \log^+ |d\, D_{\mathbf{K}}|)\}\bigr\}, \\ &\leq |\mathrm{N}\Delta'|^{35/d}\, \exp\bigl\{\exp\{c_9\, d(P + \log^+ |d\, D_{\mathbf{K}}|)\}\bigr\} \end{aligned} \tag{4}$$

and

$$\max\{\mathrm{h}(108\,b'), \mathrm{h}(12\,a')\} \le |\mathrm{N}\Delta'|^{35/d} \exp\bigl\{|D_{\mathbf{K}}|^6 \,(2\,d\,Q\,\log^+|D_{\mathbf{K}}|)^{c_{10}\,d}\bigr\}. \tag{5}$$

Since a and b are coprime, the Theorem of [4] (see also [3] for a slightly weaker result) asserts that $P[-4a^3 - 27b^2]$ tends to infinity with $\max\{|\mathrm{N}a|, |\mathrm{N}b|\}$. In the course of the proof, it is shown that there exists $\rho \in O_{\mathbf{K}}$ such that $\mathrm{h}(a\rho^{-2})$ is bounded in terms of P. This upper bound remains clearly valid (up to the numerical constants) for $\mathrm{h}(b\rho^{-3})$ and for $\mathrm{h}\bigl((4a^3+27b^2)\rho^{-6}\bigr) = \mathrm{h}(\Delta\,\rho^{-6})$, and, arguing as in [4], we deduce that

$$\log^+\log^+|\mathrm{N}\Delta| \le c_{11}\,(d\,P + d\,\log^+|d\,D_{\mathbf{K}}|),$$

whence

$$P \ge c_{12}\,\frac{\log^+\log^+|\mathrm{N}\Delta|}{d}, \tag{6}$$

provided that $|\mathrm{N}\Delta|$ is large enough in terms of $|D_{\mathbf{K}}|$. It is quite easy to see that the same proof also yields that

$$Q \ge \bigl(2\,\log^+|\mathrm{N}\Delta|\bigr)^{c_{13}/d} \tag{7}$$

when $|\mathrm{N}\Delta|$ is large enough in terms of $|D_{\mathbf{K}}|$. Combining (2), (4) and (6) on the one hand, and (3), (5) and (7) in the other hand, and using that $\max\{\mathrm{h}(\eta^3 y), \mathrm{h}(\eta^2 x)\} \ge \max\{|\mathrm{N}x|, |\mathrm{N}y|\}^{1/d}$, we get that

$$P \ge c_{14}\,\frac{\log^+\log^+\max\{|\mathrm{N}x|, |\mathrm{N}y|\}}{d}$$

and

$$Q \ge \bigl(2\,\log^+\max\{|\mathrm{N}x|, |\mathrm{N}y|\}\bigr)^{c_{15}/d},$$

provided that $|\mathrm{N}\Delta|$ is large enough, as claimed. $\square$

References

[1] A. Baker, *The diophantine equation $y^2 = ax^3 + bx^2 + cx + d$*, J. London Math. Soc. 43 (1968), 1–9.

[2] Y. Bugeaud, *On the size of integer solutions of elliptic equations*, Bull. Austral. Math. Soc. 57 (1998), 199–206.

[3] 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.

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

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

[6] L. Hajdu and T. Herendi, *Explicit bounds for the solutions of elliptic equations with rational coefficients*, J. Symbolic Comput. 25 (1998), 361–366.

[7] A. Pintér, *On the magnitude of integer points on elliptic curves*, Bull. Austral. Math. Soc. 52 (1995), 195–199.

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

[9] W. M. Schmidt, *Integer points on curves of genus 1*, Compositio Math. 81 (1992), 33–59.

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

[11] P. M. Voutier, *An Upper Bound for the Size of Integer Solutions to* $Y^m = f(X)$, J. Number Theory 53 (1995), 247–271.

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

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