On the size of integer solutions of elliptic equations

Yann Bugeaud (Strasbourg)

Abstract

We improve upon earlier effective bounds for the magnitude of integer points on an elliptic curve $\mathcal{E}$ defined over a number field $\mathbf{K}$. We slightly refine the dependence on the discrminant of $\mathbf{K}$. In most of the previous papers, the estimates obtained are exponential in the height of $\mathcal{E}$. In this work, taking also into consideration the prime ideals dividing the discriminant of $\mathcal{E}$, we provide a totally explicit bound which is only polynomial in the height.

Mathematics Subject Classification : 11D25, 14H52.

On the size of integer solutions of elliptic equations

Yann Bugeaud (Strasbourg)

1. Introduction

Let $\mathbf{K}$ be a number field and denote by $O_{\mathbf{K}}$ its ring of integers. The first effective bound for the integer solutions $(x, y) \in O_{\mathbf{K}}^2$ of the elliptic equation

$$y^2 = x^3 + ax + b,$$

where a, $b \in O_{\mathbf{K}}$ satisfy $4a^3 + 27b^2 \neq 0$ was given by Baker [1] in the case $\mathbf{K} = \mathbf{Q}$, as a consequence of its powerful estimates for linear forms in logarithms. He showed that

$$\max\{|x|, |y|\} \leq \exp\Big\{(10^6\, H)^{10^6}\Big\},$$

where H denotes the height of the polynomial $f(X) = X^3 + aX + b$, i.e., here, $\max\{|a|, |b|\}$. Later, this bound was considerably improved and generalized to arbitrary $\mathbf{K}$ by several authors, including Sprindžuk [13], Schmidt [10], Poulakis [9], Pintér [8] and Hajdu & Herendi [5]. The approach followed in [13] and [10] goes back to Siegel [11] and can easily be adapted to the study of superelliptic equations (cf. Voutier [14] and Bugeaud [2]), while the other two methods are specific to the case of elliptic equations. Indeed, Poulakis uses the "multiplication by 2" on an elliptic curve and Pintér and Hajdu & Herendi argue as Baker, reducing the problem to the study of Thue equations.

In the present work, we rework the approach of Poulakis [9] and improve upon his estimate thanks to a careful study of the unit equation involved in the proof. Our main improvement concerns the dependence on the discriminant of the ground field $\mathbf{K}$. Moreover, we show (cf. also [2]) that the dependence on the height of f is only polynomial if we take also the discriminant of f (and, even, only the prime ideals dividing it) into consideration, and we make explicit all the numerical constants.

2. Statement of the results

Let $\mathbf{K}$ be a number field of degree d and denote by $D_{\mathbf{K}}$ its discriminant and by $O_{\mathbf{K}}$ its ring of integers. Let a and b be algebraic integers in $\mathbf{K}$ satisfying $4a^3 + 27b^2 \neq 0$ and consider the elliptic equation

$$y^2 = x^3 + ax + b \ \text{ in } \ (x, y) \in O_{\mathbf{K}}^2. \qquad (E)$$

The main motivation of this work is to give a detailed presentation of the less known method introduced by Chabauty [4] (see also Lang [6, page 140] and Poulakis [9]), which is based on the group law defined over the points on an elliptic curve. We deduce two new upper bounds for the size of the solutions of (E), which slightly improve the results of

Schmidt [10], obtained by the "classical" method, and those of Poulakis. We pay particular attention to the dependence on the parameters of the field $\mathbf{K}$ and also on the height H (for the definition, see Section 3) and on the discriminant $\Delta_f = -4a^3 - 27b^2$ of the polynomial $f(X) = X^3 + aX + b$.

Throughout this paper, we denote by $\mathrm{h}(\alpha)$ the absolute multiplicative height of the algebraic number α (for the definition, see Section 3). Further, we stand the notation $\log^* x$ for $\max\{\log x, 1\}$.

Theorem 1. *All the solutions (x, y) of (E) satisfy*

$$\max\{\mathrm{h}(x), \mathrm{h}(y)\} \leq H^{35} \exp\Big\{(100d)^{100d}\, |D_{\mathbf{K}}|^{12} |\mathrm{N}_{\mathbf{K}/\mathbf{Q}}(\Delta_f)|^7 \left(\log |D_{\mathbf{K}}\, \mathrm{N}_{\mathbf{K}/\mathbf{Q}}(\Delta_f)|\right)^{24d-1}\Big\}.$$

Thanks to a precise estimate of the different of a number field extension (see Lemma 1), we are able to refine the dependence on $|\mathrm{N}_{\mathbf{K}/\mathbf{Q}}(\Delta_f)|$ and to produce a bound involving only the prime numbers dividing it.

Denote by $\mathfrak{p}_1, \ldots, \mathfrak{p}_t$ the distinct prime ideals in $O_{\mathbf{K}}$ dividing Δ_f and let P (resp. Q) be the greatest prime factor (resp. the greatest square-free divisor) of $|\mathrm{N}_{\mathbf{K}/\mathbf{Q}}(\Delta_f)|$. Theorem 2 below considerably improves and generalizes to the number field case the estimate of Pintér [8].

Theorem 2. *All the solutions (x, y) of (E) satisfy*

$$\max\{\mathrm{h}(x), \mathrm{h}(y)\} \leq H^{35} \exp\Big\{\big(100(t+d)\big)^{100(t+d)}\, P^{24d}\, Q^{9d}\, |D_{\mathbf{K}}|^6 \left(\log |D_{\mathbf{K}}|\right)^{12d+1}\Big\}.$$

Remarks : • With the classical approach we obtain slightly weaker results than the above theorems. Precisely, we are able to get alternatively $|D_{\mathbf{K}}|^{24}$ or $|D_{\mathbf{K}}|^{12} \log^* \log^* H$ instead of $|D_{\mathbf{K}}|^{12}$ in Theorem 1 (to see this, follow carefully the proof of [2, Theorem 1]) and $|D_{\mathbf{K}}|^{12}$ instead of $|D_{\mathbf{K}}|^6$ in Theorem 2. These improvements are due to the particular form of the unit equation we deduce here. We point out that the numerical constants computed in Theorems 1 and 2 are not too big : this is a consequence of recent improvements of Waldschmidt [15] and Kunrui Yu [16] concerning linear forms in logarithms.

• The method used here also allows us to produce bounds for the S-integer solutions of (E), but the dependence on $P_{\max}$, the greatest prime number lying below the prime ideals involved in S is not very satisfactory : indeed, the exponent of $P_{\max}$ is then linear in t, rather to be independent of t (see [2, Theorem 1]). The same remark applies to the method used by Baker [1] (see [5]), which, however, does not seem to be applicable when the field $\mathbf{K}$ is not the rational field $\mathbf{Q}$.

• Unlike the classical method, it seems, unfortunately, that the one of Chabauty cannot be applied to practical resolutions of elliptic equations.

In the rational case, using $t + 1 \leq P$ and $Q \leq P^t$, we crudely deduce from Theorem 2 a considerable sharpening of the main result of Pintér [8].

Corollary 1. *If $\mathbf{K}=\mathbf{Q}$, all the solutions (x,y) of (E) satisfy*

$$\max\{|x|,|y|\} \le H^{35}\exp\Big\{(100P)^{124(t+1)}\Big\},$$

Remark : Pintér [8] shows that, under the hypotheses of Corollary 1, there exists a (very large) effectively computable numerical constant c_1 such that $\max\{|x|,|y|\} \le H^{23}\exp\Big\{(2P)^{c_1(t+1)^2}\Big\}$. Our improvement is mainly due to the new approach of Bugeaud & Győry [3] in giving new explicit upper bounds for the solutions of S-unit equations, which allows us to replace the factor $(t+1)^2$ by $(t+1)$.

3. Notations and a lemma

For a number field $\mathbf{K}$ we will always use the notation $M_{\mathbf{K}}$, $D_{\mathbf{K}}$, $R_{\mathbf{K}}$ and $O_{\mathbf{K}}$ for, respectively, the set of places on $\mathbf{K}$, the discriminant of $\mathbf{K}$, its regulator and its ring of integers. If S is a finite set of places on $\mathbf{K}$, including the set of infinite places, we denote by R_S the S-regulator of $\mathbf{K}$ (see [3] for the definition). We normalize the valuations in the same way as in [3], then the (absolute) height of an algebraic number α contained in $\mathbf{K}$ is defined by

$$\mathrm{h}(\alpha)=\Big(\prod_{v\in \mathbf{M_K}}\max(1,|\alpha|_v)\Big)^{1/[\mathbf{K}:\mathbf{Q}]}.$$

For a polynomial $F(X)=X^l+b_{l-1}X^{l-1}+\ldots+b_0\in\mathbf{K}[X]$, we define its height $\mathrm{h}(F)$ by

$$\mathrm{h}(F)=\Big(\prod_{v\in \mathbf{M_K}}\max\big\{1,|b_0|_v,\ldots,|b_{l-1}|_v\big\}\Big)^{1/[\mathbf{K}:\mathbf{Q}]}.$$

It is well-known (cf. [12], Chapter *VIII*, Theorem 5.9) that

$$2^{-l}\prod_{\alpha\ \text{root of}\ F}\mathrm{h}(\alpha)\le \mathrm{h}(F)\le 2^{l-1}\prod_{\alpha\ \text{root of}\ F}\mathrm{h}(\alpha).$$

In course of our proofs, we often refer the reader to lemmas and propositions stated in [3]. However, we need an additional result.

Lemma 1. *Let $\mathbf{K}$ be a number field and let $a\notin\mathbf{K}$ be an algebraic integer, with minimal defining polynomial f over $\mathbf{K}$. Put $\mathbf{L}=\mathbf{K}(a)$ and $n=[\mathbf{L}:\mathbf{K}]$. Denote by Δ_f the discriminant of f and by $\mathrm{diff}_{\mathbf{L}/\mathbf{K}}$ the different of the extension $\mathbf{L}/\mathbf{K}$. Then we have*

$$|D_{\mathbf{L}}|\le |D_{\mathbf{K}}|^n\,|\mathrm{N}_{\mathbf{L}/\mathbf{Q}}(\mathrm{diff}_{\mathbf{L}/\mathbf{K}})|\le |D_{\mathbf{K}}|^n\,|\mathrm{N}_{\mathbf{K}/\mathbf{Q}}(\Delta_f)|.$$

More precisely, let $\mathfrak{p}$ be a prime ideal in $\mathbf{K}$ dividing $\mathrm{N}_{\mathbf{L}/\mathbf{K}}(\mathrm{diff}_{\mathbf{L}/\mathbf{K}})$ and write

$$\mathfrak{p}\,O_{\mathbf{L}}=\mathfrak{p}_1^{e_1}\ldots\mathfrak{p}_r^{e_r}.$$

Then we have $\mathrm{ord}_{\mathfrak{p}}\big(\mathrm{N}_{\mathbf{L}/\mathbf{K}}(\mathrm{diff}_{\mathbf{L}/\mathbf{K}})\big) \leq (n-1) + n \max_i \mathrm{ord}_{\mathfrak{p}}(e_i)$.

Proof : This follows from [7, Proposition 4.9] & [7, Proposition 6.3]. $\square$

4. Proofs

- **Reduction to a unit equation.**

As previously mentioned, our approach goes back to Chabauty [4] (see Lang [6, page 140]) and has also been used by Poulakis [9]. It is based on the group law defined over the set of rational points on (E). Although all we need can be found in [9], it is convenient for the reader to give here a detailed account of the method.

Let $(x,y) \in O_{\mathbf{K}}^2$ be a non-zero point on (E). In order to compute $(s,t) \in \mathbf{K}^2$ such that $2\,(s,t) = (x,y)$, where

$$2\,(s,t) := \left(-2s + \left(\frac{3s^2+a}{2t}\right)^2, -t + \left(\frac{3s^2+a}{2t}\right)\left(3s - \left(\frac{3s^2+a}{2t}\right)^2\right)\right),$$

we set $u := (3s^2+a)/(2t)$ and we consider the equation

$$(x,y) = \left(-2s + u^2, -\frac{3s^2+a}{2u} + u(3s-u^2)\right). \tag{1}$$

Eliminating s between the two equalities induced by (1), we get

$$u^4 - 6xu^2 - 8yu - 3x^2 - 4a = 0, \tag{2}$$

which allows us to determine u, $s = (u^2 - x)/2$ and t. Moreover, substituting the values of x and y given by (1) in equation (2) and replacing u^2 by $2s + x$, we get

$$s^4 - 4xs^3 - 2as^2 - 4axs - 8bs - 4bx + a^2 = 0, \tag{3}$$

hence s is an algebraic integer and $\mathbf{K}(s) = \mathbf{K}(u)$.

Further, Sublemma 4.3 of [12, Chapter *VIII*] with $Z = 1$ and $X = s$ yields

$$(3s^2+4a)(s^4 - 2as^2 - 8bs + a^2) - (3s^3 - 5as - 27s)(s^3 + as + b) = 4a^3 + 27b^2,$$

and we infer from (3) that $\mathrm{N}_{\mathbf{K}(s)/\mathbf{Q}}(s^3+as+b)$ divides $\mathrm{N}_{\mathbf{K}(s)/\mathbf{Q}}(4a^3+27b^2)$. Setting $L := \mathbf{K}(u) = \mathbf{K}(s)$, we have proved that

$$\mathrm{N}_{\mathbf{L}/\mathbf{Q}}(s^3+as+b) \mid \mathrm{N}_{\mathbf{K}/\mathbf{Q}}(\Delta_f)^{[\mathbf{L}:\mathbf{K}]}. \tag{4}$$

In all what follows we assume that $f(X)$ is irreducible over $\mathbf{L}$. However, our bounds remain clearly valid if this is not the case. Let e_1, e_2 and e_3 be the roots of the polynomial f and denote by σ an embedding satisfying $\sigma|_{\mathbf{L}} \equiv \mathrm{Id}|_{\mathbf{L}}$ and $\sigma(e_1) = e_2$. In the field $\mathbf{L}(e_1, e_2)$, we have

$$(s-e_1) + (e_2 - s) + (e_1 - e_2) = 0. \tag{5}$$

We will work with equation (5) under two distinct ways.

- **Proof of Theorem 1.**

By [3, Lemma 2] and (4) we obtain a unit $\eta_1 \in \mathbf{L}(e_1)$ and an algebraic integer $u_1 \in \mathbf{L}(e_1)$ satisfying

$$s - e_1 = u_1\eta_1 \quad \text{and} \quad \mathrm{h}(u_1) \leq |\mathrm{N}_{\mathbf{K}/\mathbf{Q}}(\Delta_f)| \exp\{(600d)^{24d}\, R_{\mathbf{L}(e_1)}\}. \tag{6}$$

Equation (5) now becomes

$$u_1\eta_1 - u_1^{(\sigma)}\,\eta_1^{(\sigma)} + (e_1 - e_2) = 0.$$

Let $\varepsilon_1, \ldots, \varepsilon_r$ be a fundamental system of units in $O_{\mathbf{L}(e_1)}$ satisfying the properties stated in [3, Lemma 1]. We can write

$$\eta_1 = \zeta\, \varepsilon_1^{b_1} \ldots \varepsilon_r^{b_r},$$

where ζ is a root of unity and the b_i's are rational integers. Notice that, in view of [3, (iii) of Lemma 1], we have

$$\max\{|b_i|\} \leq (12d)^{24d}\, \log \mathrm{h}(\eta_1). \tag{7}$$

Applying an estimate of Waldschmidt [15] (see [3, Proposition 1]) to give a lower bound for

$$\left|\frac{e_2 - e_1}{u_1\eta_1}\right| = \left|1 - \frac{u_1^{(\sigma)}}{u_1} \cdot \frac{\eta_1^{(\sigma)}}{\eta_1}\right| = \left|1 - \frac{u_1^{(\sigma)}}{u_1} \cdot \left(\frac{\varepsilon_1^{(\sigma)}}{\varepsilon_1}\right)^{b_1} \ldots \left(\frac{\varepsilon_r^{(\sigma)}}{\varepsilon_r}\right)^{b_r}\right|,$$

we use that $\mathrm{h}(\varepsilon_i^{(\sigma)}/\varepsilon_i) \leq \mathrm{h}(\varepsilon_i)^2$ for $1 \leq i \leq r$ and we argue as in [3, Section 5, see the displayed inequality after (33)] to deduce from $r \leq 12d$ and (7) that

$$\mathrm{h}\left(\frac{e_2 - e_1}{u_1\eta_1}\right) \leq \exp\left\{(50d)^{72d}\, R_{\mathbf{L}(e_1)}\, \log \mathrm{h}(u_1)\, \log \frac{\log \mathrm{h}(\eta_1)}{\log \mathrm{h}(u_1)}\right\},$$

whence

$$\mathrm{h}(s - e_1) = \mathrm{h}(u_1\,\eta_1) \leq H^2\, \exp\{(52d)^{72d}\, R_{\mathbf{L}(e_1)}\, \log^* R_{\mathbf{L}(e_1)}\, \log \mathrm{h}(u_1)\}. \tag{8}$$

Using $\mathrm{h}(s) \leq 2\mathrm{h}(e_1 - s)\,\mathrm{h}(e_1)$, $t^2 = (s - e_1)(s - e_2)(s - e_3)$ and (6), we deduce from (8) the upper bound

$$\max\{\mathrm{h}(x), \mathrm{h}(y)\} \leq H^{35}\, \exp\{(82d)^{100d}\, R_{\mathbf{L}(e_1)}\, \log^* R_{\mathbf{L}(e_1)}\, (R_{\mathbf{L}(e_1)} + \log |\mathrm{N}_{\mathbf{K}/\mathbf{Q}}(\Delta_f)|)\}. \tag{9}$$

Further, we infer from [9, proof of Theorem 3] that

$$|D_{\mathbf{L}(e_1)}| \leq 2^{36d}\, |D_{\mathbf{K}}|^{12} |\mathrm{N}_{\mathbf{K}/\mathbf{Q}}(\Delta_f)|^7. \tag{10}$$

Theorem 1 now follows from (8), (9), (10) and [3, inequality (5)].

- **Proof of Theorem 2.**

Denote by $\mathfrak{p}_1, \ldots, \mathfrak{p}_t$ the distinct prime ideals in $O_{\mathbf{K}}$ dividing Δ_f and let S be the set of places of $\mathbf{K}$ composed by the infinite places and those places induced by the ideals $\mathfrak{p}_i$, $1 \le i \le t$. Further, denote by S_1 (resp. S_2, S_{12}) the set of all extensions to $\mathbf{L}(e_1)$ (resp. $\mathbf{L}(e_2)$, $\mathbf{L}(e_1, e_2)$) of the places in S and let P (resp. Q) be the greatest prime factor (resp. the greatest square-free divisor) of $|\mathrm{N}_{\mathbf{K}/\mathbf{Q}}(\Delta_f)|$.

Let $\varepsilon_1, \ldots, \varepsilon_u$ be a fundamental system of S_1-units in $\mathbf{L}(e_1)$. Obviously, $u \le 12(d+t)$ and $\varepsilon_1^{(\sigma)}, \ldots, \varepsilon_u^{(\sigma)}$ is a fundamental system of S_2-units in $\mathbf{L}(e_2)$. In view of (4), $e_1 - s$ (resp. $e_2 - s$) is an S_1-unit in $\mathbf{L}(e_1)$ (resp. an S_2-unit in $\mathbf{L}(e_2)$) and we derive from (5) the equality

$$\frac{e_1 - e_2}{e_1 - s} = 1 - \frac{e_2 - s}{e_1 - s} =: \Lambda.$$

We proceed as in [3, Section 5, see the displayed inequality before (42)] in order to compute a lower bound for $|\Lambda|_v$, where v denotes any place in S_{12}. Omitting details, we obtain

$$\mathrm{h}\left(\frac{e_1 - e_2}{e_1 - s}\right) \le \exp\Big\{ \big(60(t+d)\big)^{88(t+d)} P^{24d} R_{S_1} \log^* R_{S_1} \log\log \mathrm{h}(e_1 - s) \Big\}. \tag{11}$$

It remains us to give a precise estimate of R_{S_1}. To this end, we first apply Lemma 1 to bound the differents of the extensions $\mathbf{L}/\mathbf{K}$ and $\mathbf{L}(e_1)/\mathbf{L}$, and we obtain

$$|\mathrm{N}_{\mathbf{L}/\mathbf{Q}}(\mathrm{diff}_{\mathbf{L}/\mathbf{K}})| \le 7^{8d} \prod_{p | v_p(\Delta_f) \neq 0} p^{3d} = 7^{8d} Q^{3d}$$

and

$$|\mathrm{N}_{\mathbf{L}/\mathbf{Q}}(\mathrm{diff}_{\mathbf{L}(e_1)/\mathbf{L}})| \le 6^{20d} Q^{8d}.$$

Further, using Lemma 1 together with

$$|\mathrm{N}_{\mathbf{L}(e_1)/\mathbf{Q}}(\mathrm{diff}_{\mathbf{L}(e_1)/\mathbf{K}})| = |\mathrm{N}_{\mathbf{L}/\mathbf{Q}}(\mathrm{diff}_{\mathbf{L}/\mathbf{K}})|^3 \cdot |\mathrm{N}_{\mathbf{L}(e_1)/\mathbf{Q}}(\mathrm{diff}_{\mathbf{L}(e_1)/\mathbf{L}})|$$

(cf. [7, Proposition 4.9]), we get after a few calculations that

$$|D_{\mathbf{L}(e_1)}| \le 8^{40d} |D_{\mathbf{K}}|^{12} Q^{17d}. \tag{12}$$

We infer from [3, inequalities (16) and (5)] that

$$R_{S_1} \le 12^{12t} |D_{\mathbf{L}(e_1)}|^{1/2} \left(\log |D_{\mathbf{L}(e_1)}|\right)^{12d-1} \prod_{i=1}^{t} \log^* \mathrm{N}_{\mathbf{K}/\mathbf{Q}}(\mathfrak{p}_i). \tag{13}$$

Hence, by (11), (12) and (13), we get

$$\mathrm{h}(e_1 - s) \le H^2 \exp\Big\{ \big(90(t+d)\big)^{100(t+d)} P^{24d} Q^{9d} |D_{\mathbf{K}}|^6 \left(\log |D_{\mathbf{K}}|\right)^{12d+1} \Big\}.$$

To conclude, we argue as at the end of the proof of Theorem 1. $\square$

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, *Bounds for the solutions of superelliptic equations*, Compositio Math., to appear.

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

[4] C. Chabauty, *Démonstration de quelques lemmes de rehaussement*, C.R.A.S. Paris 217 (1943), 413–415.

[5] L. Hajdu and T. Herendi, *Explicit bounds for the solutions of elliptic equations with rational coefficients*, submitted.

[6] S. Lang, Elliptic Curves, Diophantine Analysis, New York-Berlin, Springer-Verlag, 1978.

[7] W. Narkiewicz, Elementary and Analytic Theory of Algebraic Numbers, Springer-Verlag, Berlin, 1990.

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

[9] D. Poulakis, *Integer points on algebraic curves with exceptional units*, J. Austral. Math. Soc., to appear.

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

[11] C. L. Siegel (Under the pseudonym X), *The integer solutions of the equation* $y^2 = ax^n + bx^{n-1} + \ldots + k$, J. London Math. Soc. 1 (1926), 66–68.

[12] J. H. Silverman, The arithmetic of elliptic curves, Graduate Texts in Math. 106, Springer-Verlag, Berlin, 1986.

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

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

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

[16] 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@pari.u-strasbg.fr