PORTUGALIAE MATHEMATICA
Vol. 58 Fasc. 2 – 2001
Nova Série

INTEGER POINTS UNUSUALLY CLOSE TO ELLIPTIC CURVES

M. Vâjâitu and A. Zaharescu

Abstract: We consider an elliptic curve $E_{\alpha,\beta}$ given by the equation $Y^2 = X^3 + \alpha X + \beta$, where α, β are real numbers, and look for integer points close to the curve. In case the diophantine type of α is larger than 4 we find infinitely many integer points unusually close to $E_{\alpha,\beta}$ or to the curve $E_{-\alpha,\beta}$.

1 – Introduction

For any real numbers α, β such that $4\,\alpha^3 + 27\,\beta^2 \neq 0$ we denote by $E_{\alpha,\beta}$ the elliptic curve given by the equation:

$$Y^2 \;=\; X^3 + \alpha\,X + \beta~. \tag{1}$$

In case $\beta = 0$ we write E_α for $E_{\alpha,0}$. From Siegel's integer point theorem we know that the set of integer points on the curve $E_{\alpha,\beta}$ is finite. There are however infinitely many integer points near the curve $E_{\alpha,\beta}$. To be precise, let us denote by $\theta(E_{\alpha,\beta}) \in \mathbb{R} \cup \{-\infty\}$ the lower bound of those $\theta \in \mathbb{R}$ for which the inequality

$$|\,Y^2 - X^3 - \alpha\,X - \beta\,| \;\leq\; X^\theta \tag{2}$$

has infinitely many solutions $X, Y \in \mathbb{Z}$. By choosing $X = n \in \mathbb{N}$ and $Y = [\sqrt{n^3 + \alpha\,n + \beta}]$, where $[\,\cdot\,]$ denotes the integer part function, one sees immediately that $\theta(E_{\alpha,\beta}) \leq 3/2$. Reasoning heuristically we would expect that as n takes the values $1, 2, ..., N$, some of the fractional parts $\{\sqrt{n^3 + \alpha\,n + \beta}\}$ are smaller than $1/N^{1-\varepsilon}$, which leads us to conjecture that

$$\theta(E_{\alpha,\beta}) \;\leq\; 1/2 \tag{3}$$

Received: December 10, 1999; *Revised*: April 27, 2000.

for any $\alpha, \beta \in \mathbb{R}$. A general method to produce small fractional parts is to provide upper bounds for the corresponding exponential sums and then to use the Erdös–Turán inequality to obtain information on the discrepancy of the above set of fractional parts, see [Mo], Chapter 1. This method has been applied to produce small fractional parts of polynomials, see [Sc] and [Ba], which in turn provide integer points close to curves $Y = P(X)$ with $P(X) \in \mathbb{R}[X]$. In principle, a result based on exponential sums only, will not surpass the so called "square root type barrier" which is right in the middle between the "trivial upper bound" and the "expected upper bound". In order to break the square root type barrier one needs to find an alternative method. This is done in [Za] in the case of fractional parts of $\alpha\, n^2$, where $\alpha \in \mathbb{R}$, i.e. in the case of integer points close to the parabola $Y = \alpha\, X^2$. Another class of algebraic curves for which the square root type barrier is broken is the class of hyperelliptic curves C given by an equation of the form

$$Y^2 \;=\; X^{2d+1} + P(X)$$

where $P(X)$ is a polynomial of degree d with real coefficients, see [VZ]. In particular when $d = 1$ we have the class of elliptic curves defined in (1). Here the square root barrier is $\theta = 1$, in the middle between the "trivial upper bound" $\theta(E_{\alpha,\beta}) \le 3/2$ and the "expected upper bound" given by (3). Theorem 1 of [VZ] states in this case that

$$\theta(E_{\alpha,\beta}) \;\le\; 2/3 \tag{4}$$

for any $\alpha, \beta \in \mathbb{R}$ and a proof of this result will be given in the appendix. In this paper we are interested in elliptic curves $E_{\alpha,\beta}$ for which there are infinitely many integer points unusually close to $E_{\alpha,\beta}$. Precisely, by this we mean elliptic curves $E_{\alpha,\beta}$ for which $\theta(E_{\alpha,\beta}) < 1/2$. There are such curves, in fact the set of pairs (α, β) for which $\theta(E_{\alpha,\beta}) < 1/2$ is dense in $\mathbb{R}^2$. We prove the following stronger result:

Theorem 1. *For any $\beta \in \mathbb{R}$ there exists a dense subset A_β of $\mathbb{R}$ such that for any $\alpha \in A_\beta$ one has $\theta(E_{\alpha,\beta}) = -\infty$.*

For certain elliptic curves $E_{\alpha,\beta}$ one has $\theta(E_{\alpha,\beta}) < 1/2$ because of the existence of a rational curve defined over $\mathbb{Q}$ which is unusually close to $E_{\alpha,\beta}$. One such curve was discovered by Stark, see [La]. He found the parametrization

$$\begin{cases} X \,=\, t^6 + 2\,t^2 \\ Y \,=\, t^9 + 3\,t^5 + 3/2\,t \end{cases} \tag{5}$$

which produces integer points unusually close to E_1, showing that $\theta(E_1) \le 1/3$. By an appropriate modification of (5) one sees that $\theta(E_{\alpha,\beta}) \le 1/3$ for any rational number α. Note that when both α, β are rational one also has the lower bound $\theta(E_{\alpha,\beta}) \ge 0$. If α is rational while β is an irrational number of diophantine type k then one has the lower bound $\theta(E_{\alpha,\beta}) \ge 1 - k$. The diophantine type of α is defined as the upper bound of those $\sigma \in \mathbb{R}$ for which

$$|\alpha - a/q| \, < \, 1/q^\sigma \tag{6}$$

for infinitely many rational numbers a/q. For any rational number α, Vojta's General Conjecture, see [Vo], implies that the integer points responsible for the inequality $\theta(E_\alpha) < 1$ lie on the union of a finite set of rational curves. In the particular case $\alpha = 0$ one has the more precise conjecture of Hall, which states that there are only finitely many integer points (X, Y) such that

$$0 \, < \, |Y^2 - X^3| \, < \, \sqrt{X} \; .$$

Hall's Conjecture is essentially best possible as follows from the work of Danilov [Da] who proved that there are infinitely many pairs (X, Y) of integers for which

$$0 \, < \, |Y^2 - X^3| \, \le \, 433 \sqrt{2} \, |X|^{1/2} \; .$$

Returning to the case α rational, $\alpha \ne 0$ we saw that Vojta's Conjecture does not imply any nontrivial lower bound for $\theta(E_\alpha)$ because of the possible existence of several rational curves exceptionally close to E_α. Such a lower bound follows from the Hall–Lang–Stark Conjecture on integer points on elliptic curves [La], [Vo]. The conjecture states that for any elliptic curve E given by the equation

$$Y^2 \, = \, X^3 + a\,X + b$$

with $a, b \in \mathbb{Z}$, any integer point (X, Y) on E satisfies:

$$|X| \, \ll_\varepsilon \, \max\Big\{|a|^3, \, |b|^2\Big\}^{5/3+\varepsilon} \; .$$

Lang originally posed the conjecture with an unknown exponent, then Stark suggested on probabilistic grounds that the exponent should be 5/3. The Hall–Lang–Stark Conjecture provides us with a lower bound for $\theta(E)$, namely

$$\theta(E_\alpha) \, \ge \, 3/10$$

for any nonzero rational number α. We now consider the case α irrational. Using Stark's parametrization one can show that given $\varepsilon > 0$ there exists $k(\varepsilon)$ such that for any α of diophantine type $k > k(\varepsilon)$ one has

$$\theta(E_\alpha) \, < \, 1/3 + \varepsilon \; . \tag{7}$$

A sharper upper bound is provided by the following

Theorem 2. *For any irrational number α of diophantine type $k > 4$ one has*

$$\min\Big\{\theta(E_\alpha),\, \theta(E_{-\alpha})\Big\} \;\le\; 1/6 + 2/(3\,k)\ . \tag{8}$$

The Right Hand Side of (8) is $< 1/3$ for any $k > 4$. A little bit surprising, for $k > 5$ it is $< 3/10$, an upper bound which should not be obtainable for nonzero rational numbers α by the Hall–Lang–Stark Conjecture.

2 – Proof of Theorem 1

Fix $\alpha_0, \beta \in \mathbb{R}$ and $\varepsilon_0 > 0$. We need to find an $\alpha \in (\alpha_0 - \varepsilon_0,\, \alpha_0 + \varepsilon_0)$ for which $\theta(E_{\alpha,\beta}) = -\infty$. Let $2/3 < \theta < 1$. By (4) it follows that there exists an integer point (X_0, Y_0) with $X_0^{1-\theta} > 2/\varepsilon_0$ such that

$$|\, Y_0^2 - X_0^3 - \alpha_0\, X_0 - \beta\,| \;\le\; X_0^\theta\ .$$

Note that if one defines α_1 by

$$Y_0^2 \;=\; X_0^3 + \alpha_1\, X_0 + \beta\ ,$$

one has $\alpha_1 \in (\alpha_0 - \varepsilon_0/2,\, \alpha_0 + \varepsilon_0/2)$. Next, choose $\varepsilon_1 > 0$ such that $(\alpha_1 - \varepsilon_1,\, \alpha_1 + \varepsilon_1) \subset (\alpha_0 - \varepsilon_0/2,\, \alpha_0 + \varepsilon_0/2)$ and such that

$$|\, Y_0^2 - X_0^3 - \alpha\, X_0 - \beta\,| \;\le\; 1/X_0 \tag{9}$$

for any $\alpha \in [\alpha_1 - \varepsilon_1,\, \alpha_1 + \varepsilon_1]$. We now repeat the above reasoning with α_0, β and ε_0 replaced by α_1, β and ε_1. There are $\alpha_2 \in (\alpha_1 - \varepsilon_1/2,\, \alpha_1 + \varepsilon_1/2)$, $\varepsilon_2 > 0$ and an integer point (X_1, Y_1) such that

$$Y_1^2 \;=\; X_1^3 + \alpha_2\, X_1 + \beta\ ,$$

$(\alpha_2 - \varepsilon_2,\, \alpha_2 + \varepsilon_2) \subset (\alpha_1 - \varepsilon_1/2,\, \alpha_1 + \varepsilon_1/2)$ and such that instead of (9) one has

$$|\, Y_1^2 - X_1^3 - \alpha\, X_1 - \beta\,| \;\le\; 1/X_1^2$$

for any $\alpha \in [\alpha_2 - \varepsilon_2,\, \alpha_2 + \varepsilon_2]$. By repeating the same reasoning we obtain four sequences $\{\alpha_k\}_{k\in\mathbb{N}}$, $\{\varepsilon_k\}_{k\in\mathbb{N}}$, $\{X_k\}_{k\in\mathbb{N}}$ and $\{Y_k\}_{k\in\mathbb{N}}$ such that for any $k \ge 1$ one has: $\varepsilon_k > 0$, $X_k, Y_k \in \mathbb{N}$, $(\alpha_k - \varepsilon_k,\, \alpha_k + \varepsilon_k) \subseteq (\alpha_{k-1} - \varepsilon_{k-1}/2,\, \alpha_{k-1} + \varepsilon_{k-1}/2)$,

$$Y_k^2 \;=\; X_k^3 + \alpha_{k+1}\, X_k + \beta$$

and

$$|Y_k^2 - X_k^3 - \alpha X_k - \beta| \le 1/X_k^{k+1} \tag{10}$$

for any $\alpha \in [\alpha_{k+1} - \varepsilon_{k+1}, \alpha_{k+1} + \varepsilon_{k+1}]$. The sequence $\{\alpha_k\}_{k\in\mathbb{N}}$ is convergent. Denote by α its limit and consider the elliptic curve $E_{\alpha,\beta}$. By (10) it follows that for any $\theta \in \mathbb{R}$ there are infinitely many integer points satisfying (2), namely the points (X_k, Y_k) with $k \ge -\theta - 1$. Therefore $\theta(E_{\alpha,\beta}) = -\infty$ and Theorem 1 is proved. ∎

3 – Proof of Theorem 2

Let α be an irrational number of type $k > 4$ and fix a small number $0 < \delta < k-4$. There are infinitely many pairs of integers (a_n, q_n) such that for any n one has

$$|\alpha - a_n/q_n| < 1/q_n^{k-\delta} . \tag{11}$$

Replacing if necessary α by $-\alpha$ we may assume in the following that $\beta_n = \alpha - a_n/q_n$ is positive for infinitely many n. Let us fix an n with $\beta_n > 0$ and use Stark's parametrization to find integer points close to the curve E_{a_n/q_n}. With X, Y given by (5) one has

$$Y^2 = X^3 + X + t^2/4 .$$

We now replace (5) by the parametrization

$$\begin{cases} X = (a_n/q_n)^2\, t^6 + 2\,(a_n/q_n)\, t^2 \\ Y = (a_n/q_n)^3\, t^9 + 3\,(a_n/q_n)^2\, t^5 + 3/2\,(a_n/q_n)\, t \end{cases} \tag{12}$$

and obtain

$$Y^2 = X^3 + a_n/q_n\, X + a_n^2\, t^2/4\, q_n^2 . \tag{13}$$

Here if we let t be a relatively small positive integer which is divisible by $2\,q_n$ then on one hand X and Y given by (12) will be integers and on the other hand the point (X,Y) will be close to the curve E_{a_n/q_n} by (13). Since this curve is close to E_α we get an integer point (X,Y) close to E_α. This line of reasoning proves (7) only. Now the main point in the proof of Theorem 2 is to use the error β_n which appears in the approximation (11) in order to cancel or at least decrease the contribution of the last term in (13). The details are as follows.

We set $t = 2q_n u$ with $u \in \mathbb{N}$ to be chosen later. This will ensure that X, Y given by (12) are integers. Next, we write (13) in the form

$$Y^2 = X^3 + \alpha X + a_n^2 u^2 - 64\beta_n a_n^2 q_n^4 u^6 - 8\beta_n a_n q_n u^2 . \tag{14}$$

Here we want to make the quantity

$$|a_n^2 u^2 - 64\beta_n a_n^2 q_n^4 u_n^6| = 64\beta_n a_n^2 q_n^4 u^2 |1/(64\beta_n q_n^4) - u^4|$$

as small as possible and for this reason we let

$$u = u_n = \left[1/(2\sqrt{2}\, q_n \beta_n^{1/4})\right] .$$

Then set $t = t_n = 2q_n u_n$ and define $X = X_n$ and $Y = Y_n$ by (12). Note that $u_n \approx 1/(q_n \beta_n^{1/4}) > q_n^{(k-4-\delta)/4}$ which goes to infinity as $n \to \infty$. We derive

$$1/(64 q_n^4 \beta_n) = u_n^4 + O(u_n^3) = u_n^4 + O\Big(1/(q_n^4 \beta_n u_n)\Big) \tag{15}$$

from which we obtain

$$|a_n^2 u_n^2 - 64\beta_n a_n^2 q_n^4 u_n^6| = O(a_n^2 u_n) = O_\alpha(q_n^2 u_n) . \tag{16}$$

By (15) the last term in (14) satisfies

$$\begin{aligned} 8\beta_n q_n a_n u_n^2 &= O_\alpha(\beta_n q_n^2 u_n^{-2} u_n^4) \\ &= O_\alpha(\beta_n q_n^2 u_n^{-2} q_n^{-4} \beta_n^{-1}) = O_\alpha\Big(1/(q_n^2 u_n^2)\Big) . \end{aligned} \tag{17}$$

From (14), (16) and (17) we get

$$Y_n^2 = X_n^3 + \alpha X_n + O_\alpha(q_n^2 u_n) . \tag{18}$$

Here one has

$$q_n u_n \approx t_n \approx X_n^{1/6} \tag{19}$$

from which we deduce

$$q_n = (q_n q_n^{(k-4-\delta)/4})^{4/(k-\delta)} \ll (q_n u_n)^{4/(k-\delta)} \approx X_n^{2/3(k-\delta)} . \tag{20}$$

By (18), (19) and (20) we have

$$Y_n^2 = X_n^3 + \alpha X_n + O_{\alpha,\delta}(X_n^{1/6+2/3(k-\delta)}) . \tag{21}$$

Since (21) holds true for infinitely many integer points (X_n, Y_n) it follows that

$$\min\Big\{\theta(E_\alpha), \theta(E_{-\alpha})\Big\} \;\le\; 1/6 + 2/3\,(k-\delta) \;.$$

We now let $\delta \to 0$ and obtain (8), which concludes the proof of Theorem 2. ∎

4 – Appendix

Proposition. $\theta(E_{\alpha,\beta}) \le 2/3$.

Proof: The equation $Y^2 = X^3 + \alpha\,X + \beta$ defines implicitly Y as a function of X. One needs to find integer values for X such that the fractional part of $Y(X)$ is small. We take this algebraic function $Y(X)$ and look at its expansion at ∞. We have

$$Y(X) \;=\; (X^3 + \alpha\,X + \beta)^{1/2} \;=\; X^{3/2} + \alpha/2X^{-1/2} + O(X^{-3/2}) \;.$$

The statement will be proved if we show that the inequality

$$\|X^{3/2} + \alpha/2X^{-1/2}\| \;\ll_\varepsilon\; X^{-5/6+\varepsilon}$$

holds true for infinitely many integers X, where $\|\cdot\|$ stands for the distance to the nearest integer. We split up X as $X = u^2 + v$, where $u, v \in \mathbb{N}$ and v is bounded by $u^{2/3+\varepsilon}$. Since $X \approx u^2$, what we need to show is that one has

$$\Big\|(u^2+v)^{3/2} + \;\alpha/2(u^2+v)^{-1/2}\Big\| \;\ll_\varepsilon\; u^{-5/3+\varepsilon} \tag{22}$$

for infinitely many pairs $(u, v) \in \mathbb{N}^2$. We have

$$(u^2+v)^{-1/2} \;=\; u^{-1} - v\,u^{-3}/2 + O(u^{-3}) \;=\; u^{-1} + O(u^{-7/3+\varepsilon})$$

and

$$(u^2+v)^{3/2} \;=\; u^3 + 3/2\,v\,u + 3/8\,v^2\,u^{-1} - 1/16\,v^3\,u^{-3} + O_\varepsilon(u^{-7/3+4\varepsilon}) \;.$$

Therefore, if we choose u and v such that v^2 is divisible by $8u$ then we get

$$\|Y(X)\| \;=\; \|-1/16\,v^3\,u^{-3} + \alpha/2\,u^{-1}\| + O_\varepsilon(u^{-7/3+4\varepsilon}) \;.$$

If $\alpha \ne 0$ is rational we achieve (22) by arranging u and v such that

$$-1/16\,v^3\,u^{-3} + \alpha/2\,u^{-1} \;=\; 0 \;. \tag{23}$$

To do this, we take any large integer w divisible by the denominator of α and set

$$u \;=\; 8\,\alpha\,w^3\,, \qquad v \;=\; 8\,\alpha\,w^2 \;. \tag{24}$$

Then (23) holds true, u, v are integers and moreover v^2 is divisible by $8u$ as required. This solves the case α rational, in the stronger form: $\theta(E_{\alpha,\beta}) \leq 1/3$.

If α is irrational we take the convergents b_n/q_n to the continued fraction of α and for each n we replace α by b_n/q_n in (24). We choose $w = w_n \in \mathbb{N}^*$ to be a small multiple of q_n. This w_n produces a pair (u_n, v_n) which gives us further an integer point (X_n, Y_n). Using the inequality $|\alpha - b_n/q_n| < q_n^{-2}$ we see that $|-1/16\, v_n^3\, u_n^{-3} + \alpha/2\, u_n| \ll 1/(u_n\, q_n^2)$. Now $q_n \approx w_n$, $w_n^3 \approx u_n$, $u_n^2 \approx X_n$ and we find that $\|Y(X_n)\| \ll X_n^{-5/6}$. This gives $\theta(E_{\alpha,\beta}) \leq 2/3$ which completes the proof. ∎

REFERENCES

[Ba] Baker, R.C. – *Diophantine Inequalities,* Oxford Univ Press, New York, 1986.

[Da] Danilov, L.V. – Diophantine equation $x^3 - y^2 = k$ and Hall's conjecture, *Math. Zametki,* 32 (1982), 273–275; English translation, *Math. Notes of the USSR,* 32 (1982), 617–618.

[La] Lang, S. – *Conjectured diophantine estimates on elliptic curves*, in "Arithmetic and Geometry" (M. Artin and J. Tate, Eds.), Birkhauser, Boston, 1983, 155–172.

[Mo] Montgomery, H.L. – *Ten lectures on the interface Between Analytic Number Theory and Harmonic Analysis*, Regional Conference Series in Math., Amer. Math. Soc., Providence, 1994.

[Sc] Schmidt, W.M. – *Small fractional parts of polynomials*, Regional Conference Series in Math., 32, Amer. Math. Soc., Providence, 1977.

[VZ] Vâjâitu, M. and Zaharescu, A. – *Integer points near hyperelliptic curves*, preprint.

[Vo] Vojta, P. – *Diophantine approximations and value distribution theory,* Lecture Notes in Mathematics 1239, Springer-Verlag, Berlin, Heidelberg, 1987.

[Za] Zaharescu, A. – Small values of $n^2\,\alpha\,(\mathrm{mod}\,1)$, *Invent. Math.,* 121 (1995), 379–388.

Marian Vâjâitu,
Institute of Mathematics of the Romanian Academy,
P.O. Box 1-764, RO-70700, Bucharest – ROMANIA
E-mail: mvajaitu@stoilow.imar.ro

and

Alexandru Zaharescu,
Institute of Mathematics of the Romanian Academy,
P.O. Box 1-764, RO-70700, Bucharest – ROMANIA
and
Institute for Advanced Study, School of Mathematics,
Math. Building, Olden Lane, Princeton, New Jersey 08540 – USA
E-mail: zaharesc@ias.edu