BULL. AUSTRAL. MATH. SOC. 11D25, 14H52
VOL. 52 (1995) [195–199]

# ON THE MAGNITUDE OF INTEGER POINTS ON ELLIPTIC CURVES

ÁKOS PINTÉR

The known effective bounds for the magnitude of integer points on elliptic curves are exponential in the "height" of curve. The bound given in this note is polynomial in the height and depends slightly on the discriminant.

## INTRODUCTION

One of the most classical diophantine problems is to describe the structure of rational or integer points on elliptic curves. For the rational case we refer to [3] and [11]. The first effective bound for the integer solutions $x, y$ to the elliptic equation

$$(1) \qquad y^2 = x^3 + ax + b = f(x) \qquad \left(a, b \in \mathbb{Z},\ 4a^3 + 27b^2 \neq 0\right)$$

was derived by Baker [1] in 1968. As usual, let $H(f)$ and $D(f)$ denote the height and the discriminant of the polynomial $f$, respectively. Baker proved that all the solutions $x, y$ of (1) satisfy

$$\max(|x|, |y|) \leqslant \exp\{(10^6 H(f))^{10^6}\}.$$

Later, this bound was improved by several authors (see [9, 12, 13]), but those estimates are still exponential in $H(f)$. Corresponding to certain related results in the function field case (see [7] and [8]), Lang [6] conjectured that if $(x, y)$ is an integral point on the elliptic curve (1) then

$$\max(|x|, |y|) \leqslant c \cdot H(f)^k,$$

where $c$ and $k$ are absolute constants. We remark that an affirmative answer to Lang's conjecture would solve Pillai's conjecture, for instance, and some other classical polynomial-exponential diophantine equations (see [10, Chapters 11, 12]). However, Lang's conjecture seems well beyond the reach of current techniques.

The purpose of this note is to point out that a recent result of [2] on Thue equations gives a reasonable bound which is polynomial in the height of $f$.

Received 25th October, 1994.
Research supported in part by Grants T4055 and W015355 from the Hungarian National Foundation for Scienctific Research, Foundation for Hungarian Higher Education and Research and Kereskedelmi Bank Rt. Universitas Foundation.

https://doi.org/10.1017/S000497270001460X Published online by Cambridge University Press

**Theorem.** *All the rational integer solutions $x, y$ to the equation (1) satisfy*

$$\max(|x|, |y|) \leqslant H(f)^{23} \exp\{(2P)^{c_1(\omega+1)^2}\},$$

*where $P = P(D(f))$ and $\omega = \omega(D(f))$ denote the greatest prime factor and the number of distinct prime factors of $D(f)$, respectively, and $c_1$ is an effectively computable absolute constant.*

By the Nagell-Lutz theorem, Lang's conjecture is true for trivial elliptic curves (when the Mordell-Weil group of the curve is trivial). We construct an infinite parametric family of non-trivial curves for which Lang's conjecture is true. Let $a$ and $b$ be fixed in (1) and suppose that there exists a solution $(x_0, y_0)$ to equation (1) such that $y_0^2$ does not divide the discriminant of $f$ (for example, $a = -1, b = 1$ and $(x_0, y_0) = (56, 419)$). By using the Nagell-Lutz theorem again it is easy to see that the curves

$$y^2 = x^3 + an^2x + bn^3 = f_n(x), \tag{2}$$

with $(n, y_0) = 1$ are non-trivial. Supposing $n$ satisfies the inequality

$$n > \exp\{2P(nD(f))^{c_1(\omega(nD(f))+1)^2}\},$$

our Theorem implies

$$y_0 \cdot H(f_n)^{1/2} \leqslant \max(|x|, |y|) \leqslant H(f_n)^{24}.$$

## Proof of the Theorem

The proof of the Theorem is a straightforward consequence of the following lemmas.

**Lemma 1.** *Let $(x, y) \in \mathbb{Z}^2$ be an arbitrary but fixed solution to (1). Then there exists a binary form $F_{x,y}(X, Y) \in \mathbb{Z}[X, Y]$ of degree 4 with*

$$H(F_{x,y}) \leqslant 10^4 \max\left(a^2, |D(f)|^{2/3}\right) = \mathcal{M} \quad \text{and} \quad D(F_{x,y}) = 4^6 D(f),$$

*furthermore, if the equation*

$$F_{x,y}(p, q) = \pm 1 \quad \text{in integers } p, q$$

*implies* $\max(|p|, |q|) \leqslant M$, *then*

$$\max(|x|, |y|) \leqslant 70\mathcal{M}^4 M^{10}.$$

**Proof:** This result is essentially proved in [1, p.8], with the same constants.

https://doi.org/10.1017/S000497270001460X Published online by Cambridge University Press

**Lemma 2.** *Let $F(X,Y)$ be a binary form of degree $n \geqslant 3$ with non-zero discriminant $D(F)$. The equation*

$$F(x,y) = \pm 1 \quad \textit{in integers } x,y$$

*implies*

$$\max(|x|,|y|) \leqslant H(f)^{3/n} \exp\{(2P(D(F)))^{c_2(n)(\omega(D(F))+1)^2}\},$$

*where $c_2(n)$ is an effectively computable constant depending only on $n$.*

Proof: Using an effective result of Evertse and Győry [**4**, Lemma 11] on homogeneous $S$-unit equations in three variables and the argument of the proof of Theorem 1 in [**2**] one can see that

$$\max(|x|,|y|) \leqslant H(F)^{3/n} \exp\left\{((\omega(D(F))+2)\cdot P(D(F))\cdot |D|)^{c_3(n)(\omega(D(F))+1)}\right\},$$

where $D$ denotes the discriminant of the splitting field of the polynomial $F(X,1)$ and $c_3(n)$ is an effectively computable constant depending only on $n$. Finally, inequality (9) of [**2**] completes the proof of Lemma 2.

## Corollaries

In the sequel $c_4, \dots, c_9$ will denote effectively computable absolute constants. Applying the Theorem to the relation $-27b^2 - 4a^3 = D(f)$, we have

$$H(f) = \max(|a|,|b|) \leqslant D(f)^{23} \exp\{(2P)^{c_4(\omega+1)^2}\}$$

and it leads to a bound independent of $H(f)$.

**Corollary 1.** *The equation (1) in integers $x,y$ implies*

$$\max(|x|,|y|) \leqslant D(f)^{529} \exp\{(2P)^{c_5(\omega+1)^2}\}.$$

Let $g(X) = a_0X^3 + a_1X^2 + a_2X + a_3 \in \mathbb{Z}[X]$ be a cubic polynomial with distinct zeros. By a simple transformation, the equation

$$(2) \qquad y^2 = a_0x^3 + a_1x^2 + a_2x + a_3 \qquad \text{in integers } x,y$$

can be written as

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

where $y' = 27a_0y$, $x' = 9a_0x + 3a_1$, $a' = 27(3a_0a_2 - a_1^2)$ and $b' = 27\left(27a_0^2a_3 + 2a_1^3 - 9a_0a_1a_2\right)$. A simple calculation gives

$$(3) \quad \max(|x|,|y|) \leqslant \max(|x'|,|y'|) + \left|\frac{a_1}{3a_0}\right|, H(h) \leqslant 10^4 H(g)^3, D(h) = 3^{12}a_0^2D(g),$$

and we obtain

**Corollary 2.** *All the rational integer solutions $x, y$ to the equation (2) satisfy*

$$\max(|x|,|y|) \leqslant \min_{1\leqslant i\leqslant 3} B_i,$$

*where*

$$B_1 = H(g)^{69} \exp\left\{(2P_1)^{c_6(\omega_1+1)^2}\right\},$$

$$B_2 = \left(a_0^2 D(g)\right)^{529} \exp\left\{(2P_1)^{c_7(\omega_1+1)^2}\right\} + \left|\frac{a_1}{3a_0}\right|,$$

$$B_3 = \exp\left\{2\left((2P_1)^{c_6(\omega_1+1)^2} + \left(c_8 a_0^2 D(g)\right)^{690}\right)\right\} + |a_0 a_3|,$$

*and* $P_1 = P(a_0 D(g)), \omega_1 = \omega(a_0 D(g))$.

Proof: From the Theorem, Corollary 1 and (3) it follows that

$$\max(|x|,|y|) \leqslant \min(B_1, B_2). \tag{4}$$

By a theorem of Győry [5, Theorem 1] we get $g(X) = g^*(X+a)$ with some $a \in \mathbb{Z}$ and $g^* \in \mathbb{Z}[X]$ satisfying

$$H(g^*) \leqslant \exp\{c_9\left(a_0^2 D(g)\right)^{10}\}. \tag{5}$$

The equation (2) implies $g^*(x+a) = y^2$ for each solution, and inequalities (4) and (5) yield

$$|a_0 y| \leqslant \exp\left\{(2P_1)^{c_6(\omega_1+1)^2} + \left(c_8 a_0^2 D(g)\right)^{690}\right\}.$$

Since $|a_0 x| \leqslant (a_0 y)^2 + \left|a_0^2 a_3\right|$, Corollary 2 is proved.

As the following example shows, the dependence upon the coefficients is necessary. Let $m \neq 0$ be a fixed rational integer and consider the family of elliptic equations

$$g_n(x) = x^3 - 3nx^2 + \left(3n^2 - 1\right)x - n^3 + n + m^2 = y^2 \quad \text{in integers } x, y, \tag{6}$$

where $n \geqslant 3$. One can verify that $D(g_n) = 4 - 27m^4$ and

$$(x, y) = \left(64m^6 - 8m^2 + n, 512m^9 - 96m^5 + 3m\right)$$

is a solution to (6) (see [14]); that is, $x > (1/5)\left|D(g_n)\right|^{3/2} + n$.

https://doi.org/10.1017/S000497270001460X Published online by Cambridge University Press

## REFERENCES

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

[2] B. Brindza, J.H. Evertse and K. Győry, 'Bounds for the solutions of some diophantine equations in terms of discriminant', *J. Austral. Math. Soc. Ser. A* **51** (1991), 8–26.

[3] J.W.S. Cassels, 'Diophantine equations with special reference to elliptic curves', *J. London Math. Soc.* **41** (1966), 193–291.

[4] J.H. Evertse and K. Győry, 'Effective finiteness results for binary forms with given discriminant', *Compositio Math.* **79** (1991), 169–204.

[5] K. Győry, 'On polynomials with integer coefficients and given discriminant', IV, *Publ. Math. Debrecen* **25** (1978), 155–167.

[6] S. Lang, 'Conjectured diophantine estimates on elliptic curves', in *Arithmetic and Geometry, Papers Dedicated I.R.Shafarevich on the Occasion of His Sixtieth Birthday, Volume I, Arithmetic*, (M. Artin and J. Tate, Editors), Progress in Math. **35**, (Birkhäuser, Boston, Basel, Stuttgart, 1983), pp. 155–171.

[7] R.C. Mason and B. Brindza, 'LeVeque's superelliptic equation over function fields', *Acta Arith.* **47** (1986), 167–173.

[8] W.M. Schmidt, 'Thue's equation over function fields', *J. Austral. Math. Soc. Ser. A* **25** (1978), 385–422.

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

[10] T.N. Shorey and R. Tijdeman, *Exponential diophantine equations*, Cambridge tracts in math. **87**, (Cambridge University Press, Cambridge, 1986).

[11] J.H. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Math. **106** (Springer-Verlag, Berlin, Heidelberg, New York, 1986).

[12] V.G. Sprindžuk, *Classical diophantine equations*, Lecture Notes in Math. **1559** (Springer-Verlag, Berlin, Heidelberg, New York, 1993).

[13] H.M. Stark, 'Effective estimates of solutions of some diophantine equations', *Acta Arith.* **24** (1973), 251–259.

[14] D. Zagier, 'Large integral points on elliptic curves', *Math.Comp.* **48** (1987), 425–436.

Kossuth Lajos University
Mathematical Institute
Debrecen
4010-Hungary
e-mail: apinter@math.klte.hu

https://doi.org/10.1017/S000497270001460X Published online by Cambridge University Press