EXPLICIT BOUNDS FOR THE SOLUTIONS OF ELLIPTIC EQUATIONS WITH RATIONAL COEFFICIENTS

L. Hajdu* and T. Herendi**

Abstract. In this paper we give new, improved explicit upper bounds for the absolute values of the integer solutions and for the heights of S-integer solutions of elliptic equations over $\mathbb{Q}$.

1. Introduction

The first general effective bound for the integral solutions of elliptic equations was established by A. Baker [2]. In proving his result he deduced the problem to give a bound for the integral solutions of quartic Thue-equations. Then he used his effective bound for the solutions of Thue-equations (cf. [1]) which was obtained by means of his famous method concerning linear forms in logarithms. Later, Baker's bound on the solutions of elliptic equations has been improved and generalized by several authors, for references see eg. [3], [4], [15], [16] and [5]. The best known bounds for the integral solutions and S-integral solutions of elliptic equations are due to Y. Bugeaud [5]. However, his result is valid in a more general context, for the integral and S-integral solutions of superelliptic equations over number fields. In its proof the author followed an approach different from that of Baker mentioned above.

The aim of this paper is to considerably improve the previous estimates concerning the solutions of elliptic equations over $\mathbb{Q}$. In our paper we will use an extension of Baker's approach to the case of S-integral solutions. Generalizing a classical result of Mordell, we reduce the problem of estimating the S-integral solutions to a quartic Thue-Mahler equation. Then the use of the best known bounds, due to Bugeaud and Győry [6] and Győry [9] on Thue-Mahler equations enables us to derive sharper bounds for the S-integral solutions of elliptic equations (cf. Theorem 2). In particular, we give a bound for the rational integral solutions, too (cf. Theorem 1). In contrast to the previous estimates, our bounds are explicitly given in terms of each parameter.

Recently, J. Gebel, A. Pethő and H. G. Zimmer [8] and R. J. Stroeker and N. Tzanakis [17] elaborated efficient algorithms for solving elliptic equations in rational integers. Our improved and completely explicit bounds might be useful in extending these algorithms for determining S-integral solutions.

*Research supported in part by the Hungarian Academy of Sciences and by Grants 014245 and T 016 975 from the Hungarian National Foundation for Scientific Research.

**Research supported in part by 016791 from the Hungarian National Foundation for Scientific Research and by the Universitas Foundation of Kereskedelmi Bank RT.

2. Notation

Let $F(x,y)=a_0x^4+4a_1x^3y+6a_2x^2y^2+4a_3xy^3+a_4y^4$ be a binary quartic form with $a_i\in\mathbb{Z}$ for $0\leq i\leq 4$. By the invariants of F we mean the following expressions

$$g_2(F)=a_0a_4-4a_1a_3+3a_2^2\ ,\qquad g_3(F)=a_0a_2a_4+2a_1a_2a_3-a_0a_3^2-a_1^2a_4-a_2^3\ .$$

The quartic covariant H_F and the sextic covariant G_F of F are defined by

$$H_F(x,y)=(a_1^2-a_0a_2)x^4+(2a_1a_2-2a_0a_3)x^3y+$$

$$+(-a_0a_4-2a_1a_3+3a_2^2)x^2y^2+(2a_2a_3-2a_1a_4)xy^3+(a_3^2-a_2a_4)y^4$$

and

$$G_F(x,y)=(a_0^2a_3-3a_0a_1a_2+2a_1^3)x^6+(a_0^2a_4+2a_0a_1a_3+6a_1^2a_2-9a_0a_2^2)x^5y+$$

$$+(5a_0a_1a_4-15a_0a_2a_3+10a_1^2a_3)x^4y^2+(10a_1^2a_4-10a_0a_3^2)x^3y^3+$$

$$(15a_1a_2a_4-5a_0a_3a_4-10a_1a_3^2)x^2y^4+(-a_0a_4^2-2a_1a_3a_4-6a_2a_3^2+9a_2^2a_4)xy^5+$$

$$+(-a_1a_4^2+3a_2a_3a_4-2a_3^3)y^6\ .$$

It is well known (cf. e.g. [13], Chapter 25, Theorem 1) that

$$G_F^2(x,y)=4H_F^3(x,y)-g_2(F)H_F(x,y)F^2(x,y)-g_3(F)F^3(x,y)\ .$$

Let $f\in\mathbb{Z}[x]$ be a polynomial. By the height of f we mean the maximum of the absolute values of the coefficients of f, and we denote it by $H(f)$. The discriminant of f will be denoted by Δ_f.

If $S=\{p_1,\dots,p_t\}$ is a set of rational primes, then the rational number α is called an S-integer, if all the prime divisors of the denominator of α belong to S. The set of S-integers will be denoted by $\mathbb{Z}_S$. If in particular $S=\emptyset$ (i.e. $t=0$), then $\mathbb{Z}_S$ coincides with $\mathbb{Z}$.

By the height $h(\alpha)$ of a rational number $\alpha=a/b$ with $a,b\in\mathbb{Z}$, $(a,b)=1$, we mean $\max(|a|,|b|)$.

Throughout the paper we set $\log^*(r)=\max\{\log(r),1\}$ for $r\in\mathbb{R}$ with $r>0$.

3. Results

Theorem 1. *Let $f(x)=x^3+ax+b$ be a polynomial with coefficients in $\mathbb{Z}$ and with nonzero discriminant Δ_f. Then all solutions $(x,y)\in\mathbb{Z}^2$ of the equation*

$$y^2=x^3+ax+b \tag{1}$$

satisfy

$$\max\{|x|,|y|\}\leq\exp\{5\cdot 10^{64}c_1\log(c_1)(c_1+\log(c_2))\}$$

with

$$c_1=\frac{32|\Delta_f|^{1/2}(8+\frac{1}{2}\log(|\Delta_f|))^4}{3}\ ,\qquad c_2=10^4\max\{16a^2,\ 256|\Delta_f|^{2/3}\}\ .$$

Theorem 2. *Let $S = \{p_1, \dots, p_t\}$ be a set of rational primes, and put $P = \max\{p_1, \dots, p_t\}$. All solutions $(x, y) \in \mathbb{Z}_S^2$ of (1) satisfy*

$$\max\{h(x), h(y)\} \le \exp\{7 \cdot 10^{38t+86}(t+1)^{20t+35} P^{24} \cdot$$

$$\cdot (\log^*(P))^{4t+2} c_1 (\log(c_1))^2 (c_1 + 20tc_1 + \log(ec_2))\} \ ,$$

where c_1 and c_2 are the same constants as in Theorem 1.

Remark. The formerly known best result concerning the solutions of (1) in $\mathbb{Z}$ and $\mathbb{Z}_S$, respectively, is due to Y. Bugeaud [5]. His result is more general, that is he considered (1) over a number field K. Using the above notation, in the case $K = \mathbb{Q}$ his estimate yields

$$h(x) \le (H(f))^2 \exp\{c(t) P^{108} (\log^* P)^{36t} {\Delta_f}^{36} (\log \Delta_f)^{54} \log\log H(f)\} \ ,$$

where $c(t)$ is an effective constant depending only on t; however, this constant is not explicitely given in [5].

We mention that if $t = 0$, then in some special cases the estimate of Á. Pintér [14] gives a better bound than our Theorem 1.

4. Proofs of the Theorems

For the proof of Theorem 1 we need two lemmas.

Lemma 1. *Let $(x, y) \in \mathbb{Z}^2$ be a solution of (1). Then there exists a binary quartic form $F_{(x,y)}(u, v)$ with rational integer coefficients and with height and discriminant*

$$H(F_{(x,y)}) \le 10^4 \max\{16a^2, 256|\Delta_f|^{2/3}\} = E_1 \text{ and } \Delta_{F_{(x,y)}} = 4^6 \Delta_f \ ,$$

respectively, such that if the equation

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

implies $\max\{|p|, |q|\} \le E_2$, then

$$\max\{|x|, |y|\} \le 70 E_1^4 E_2^{10} \ .$$

Proof. This result is proved in [2], p. 8. □

Lemma 2. *Let $F(x, y) \in \mathbb{Z}[x, y]$ denote a binary quartic form with nonzero discriminant Δ_F and with height not exceeding H. Then the solutions $(x, y) \in \mathbb{Z}^2$ of the equation*

$$|F(x, y)| = 1$$

satisfy

$$\max\{|x|, |y|\} \le \exp\{4 \cdot 10^{63} E_3 \log(E_3)(E_3 + \log^*(H))\} \ ,$$

where $E_3 = |\Delta_F|^{1/2}(3 + \log(|\Delta_F|)/2)^4/6$.

Proof. If F is irreducible over $\mathbb{Q}$, then using an estimate concerning the regulator of a number field (see [10], Lemma 6.5), Lemma 2 follows from Theorem 3 of [6]. If F is not irreducible, then F has a factorization of the type $F(x, y) = F_1(x, y)F_2(x, y)$

over $\mathbb{Z}$, and here $\max\{H(F_1), H(F_2)\} \leq 4\sqrt{5}H(F)$. (For the case $\deg F_1 = \deg F_2 = 2$, cf. [11], Chapter 7; the other case can be treated easily.) Hence we have the following system of equations:

$$F_1(x,y) - \varepsilon_1 = 0,\ F_2(x,y) - \varepsilon_2 = 0,\ \varepsilon_1, \varepsilon_2 \in \{-1, 1\}\ .$$

Taking the resultant, we can obtain a much better estimate for the absolute values of x and y than stated above, and Lemma 2 follows. □

Proof of Theorem 1. Simply combining the estimates of Lemma 1 and Lemma 2, we obtain

$$\max\{|x|,\ |y|\} \leq \exp\{\log(70) + 4 \cdot \log(c_2) + 4 \cdot 10^{64} c_1 \log(c_1)(c_1 + \log(c_2))\}\ ,$$

and Theorem 1 follows. □

To prove Theorem 2, we will use three lemmas. The following Lemma 4 in fact is a theorem of Mordell, cf. [12] or [13]. As usual, the binary quartic forms $F_1(x,y)$ and $F_2(x',y')$ with integer coefficients are called equivalent, if there exist $u_1, u_2, u_3, u_4 \in \mathbb{Z}$ such that $x = u_1x' + u_2y'$, $y = u_3x' + u_4y'$ and $u_1u_4 - u_2u_3 = \pm 1$. We mention that the above defined invariants and covariants of the quartic forms are invariant under this equivalence (cf. [7]).

Lemma 3. *Let F(x,y) denote the binary quartic form*

$$a_0x^4 + 4a_1x^3y + 6a_2x^2y^2 + 4a_3xy^3 + a_4y^4$$

with rational integers $a_0 \neq 0, a_1, a_2, a_3, a_4$ and with invariants $g_2(F)$ and $g_3(F)$. Suppose that the discriminant $\Delta_F = 256((g_2(F))^3 - 27(g_3(F))^2)$ of F is nonzero. Then there exists a binary quartic form F', which is equivalent to F, with height

$$H(F') \leq 10^4 \max\{(g_2(F))^2,\ |\Delta_F|^{2/3}\}\ .$$

Proof. This assertion is proved in section 2 of [2]. □

Lemma 4. *Let $(X,Y,Z) \in \mathbb{Z}^3$ be a solution of the equation*

$$Y^2 = X^3 - G_2XZ^2 - G_3Z^3 \text{ with } G_2,\ G_3 \in \mathbb{Z}$$

and suppose that $\gcd(X,Z) = 1$. *Then there exists a binary quartic form $F(p,q)$ such that for some $p,\ q \in \mathbb{Z}$ we have*

$$X = H_F(p,q)\ ,\quad Z = F(p,q) \text{ and } 2Y = G_F(p,q)\ .$$

Moreover,

$$g_2(F) = 4G_2\ ,\quad g_3(F) = 4G_3 \text{ and } \gcd(p,q) = 1$$

hold.

Proof. This is Theorem 2 of Mordell [13] (page 233). □

Lemma 5. *Let S be a set of distinct rational primes $p_1, \dots, p_t$ not exceeding P and let $F(x,y) \in \mathbb{Z}[x,y]$ be a binary quartic form with height at most H and with nonzero discriminant Δ_F. Let $b \in \mathbb{Q}$ with height at most $B \geq e$. All solutions of the Thue-Mahler equation*

$$F(x,y) = bp_1^{z_1} \dots p_t^{z_t} \text{ in } x, y, z_1, \dots, z_t \in \mathbb{Z}$$

with $\gcd(x, y, p_1, \dots, p_t) = 1$, $z_1, \dots, z_t \geq 0$ *satisfy*

$$\max\{|x|, |y|, p_1^{z_1} \cdots p_t^{z_t}\} \leq \exp\{10^{38t+86}(t+1)^{20t+35} P^{24} \cdot$$

$$\cdot (\log^*(P))^{4t+2} E_3 (\log(E_3))^2 (E_3 + 20tE_3 + \log(BH))\} = C(F,S,B) \ ,$$

where E_3 has the same meaning as in Lemma 2.

Proof. If F is irreducible over $\mathbb{Q}$, then Lemma 5 follows from Theorem 4 of [6]. If F is not irreducible but has an irreducible factor F_1 (over $\mathbb{Q}$) of degree 3, then one can use again Theorem 4 of [6] to get a much better estimate. If F is reducible, and has no irreducible factor of degree 3, then the degree of the splitting field of F is at most 4, and by using Corollary 1 of [9] we can obtain a better bound for the heights of the solutions than stated above, and Lemma 5 follows. □

Proof of Theorem 2. Let $(x,y) \in \mathbb{Z}_S^2$ be an arbitrary solution of (1). We show that there exist integers X, Y and u such that $\gcd(XY, u) = 1$, the prime divisors of u belong to S, and $x = X/u^2$, $y = Y/u^3$. Indeed, put $x = X_1/(u_1 u^2)$, where u_1 is square-free with $\gcd(X_1, u_1 u) = 1$, and put $y = Y_1/v$ with $\gcd(Y_1, v) = 1$. Now we have

$$Y_1^2 \frac{u_1^3 u^6}{v^2} = X_1^3 + a u_1^2 u^4 X_1 + b u_1^3 u^6 \ . \tag{2}$$

If p is a prime divisor of u_1, then the order of p on the left hand side of (2) is odd, which is impossible by $\gcd(X_1, u_1) = 1$, whence $u_1 = \pm 1$. Now by $\gcd(Y_1, v) = 1$ we obtain $v = \pm u^3$, and we may set $X = X_1/u_1$ and $Y = Y_1 \cdot \operatorname{sgn}(v/u^3)$. Introducing the notation $Z = u^2$, we have

$$Y^2 = X^3 + aXZ^2 + bZ^3 \ ,$$

where $\gcd(X, Z) = 1$. By Lemma 3 and Lemma 4 there exists a binary quartic form $F(p,q)$ with height

$$H(F) \leq 10^4 \max\{16a^2, \ |4^6 \Delta_f|^{2/3}\} \ ,$$

such that for some rational integers p, q with $\gcd(p,q) = 1$

$$X = H_F(p,q), \ Z = F(p,q) \text{ and } 2Y = G_F(p,q)$$

hold. Using Lemma 5 one can derive the following estimate

$$\max\{u^2, |p|, |q|\} \leq C(F,S,e).$$

Moreover, by the definition of H_F and G_F we have

$$h(x) \leq 18(H(F))^2 (C(F,S,e))^4 \text{ and } h(y) \leq 64(H(F))^3 (C(F,S,e))^6 \ ,$$

whence

$$h(x) \leq 20^9 \max\{a^4, \ 2^8 |\Delta_f|^{4/3}\} (C(F,S,e))^4 \ ,$$

and

$$h(y) \leq 2^6 20^{12} \max\{a^6, \ 2^{12} \Delta_f^2\} (C(F,S,e))^6 \ ,$$

and Theorem 2 follows. □

Acknowledgements

We would like to thank Professors K. Győry, A. Pethő and H. G. Zimmer for their help and valuable suggestions. We are grateful to the Referees for their valuable and inspiring remarks, which helped us to improve the estimates of Theorem 2 considerably.

References

[1] A. Baker, *Contributions to the theory of diophantine equations. I, On the representation of integers by binary forms*, Phil. Trans. Royal Soc. London **A 263** (1968), 173–191.
[2] A. Baker, *The diophantine equation* $y^2 = ax^3+bx^2+cx+d$, J. London Math. Soc. **43** (1968), 1–9.
[3] A. Baker, *Transcendental Number Theory*, Cambridge Univ. Press, Cambridge, 1975.
[4] B. Brindza, *On S-integral solutions of the equation* $y^m = f(x)$, Acta Math. Hung. **44** (1984), 133–139.
[5] Y. Bugeaud, *Bounds for the solutions of superelliptic equations*, Comp. Math. (to appear).
[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] E. B. Elliot, *An Introduction to the Algebra of Quantics*, Oxford Univ. Press, 1913.
[8] J. Gebel, A. Pethő and H. G. Zimmer, *Computing integral points on elliptic curves*, Acta Arith. **68** (1994), 171–192.
[9] K. Győry, *Bounds for the solutions of decomposable form equations* (to appear).
[10] H. W. Lenstra Jr., *Algorithms in algebraic number theory*, Bull. Amer. Math. Soc. **26** (1992), 211–244.
[11] M. Mignotte, *Mathematics for computer algebra*, Springer, New York, 1992.
[12] L. J. Mordell, *Indeterminate equations of the third and fourth degrees*, Q. J. Pure Appl. Maths. **45** (1914), 170-186.
[13] L. J. Mordell, *Diophantine Equations*, Academic Press, London and New York, 1969.
[14] Á. Pintér, *On the magnitude of integer points on elliptic curves*, Bull. Austral. Math. Soc. **52** (1995), 195–199.
[15] T. N. Shorey and R. Tijdeman, *Exponential diophantine equations*, Cambridge Univ. Press, Cambridge, 1986.
[16] V. G. Sprindžuk, *Classical Diophantine Equations*, Lecture Notes in Mathematics 1559, Springer-Verlag, Germany, 1993.
[17] R. J. Stroeker and N. Tzanakis, *Solving elliptic diophantine equations by estimating linear forms in elliptic logarithms*, Acta Arith. **67** (1994), 177–196.