Bull. Aust. Math. Soc. **96** (2017), 191–195
doi:10.1017/S0004972717000375

A NOTE ON SCHMIDT'S CONJECTURE

DIMITRIOS POULAKIS

(Received 19 December 2016; accepted 24 March 2017; first published online 9 June 2017)

Abstract

Schmidt ['Integer points on curves of genus 1', *Compos. Math.* **81** (1992), 33–59] conjectured that the number of integer points on the elliptic curve defined by the equation $y^2 = x^3 + ax^2 + bx + c$, with $a, b, c \in \mathbb{Z}$, is $O_\epsilon(\max\{1, |a|, |b|, |c|\}^\epsilon)$ for any $\epsilon > 0$. On the other hand, Duke ['Bounds for arithmetic multiplicities', *Proc. Int. Congress Mathematicians*, Vol. II (1998), 163–172] conjectured that the number of algebraic number fields of given degree and discriminant D is $O_\epsilon(|D|^\epsilon)$. In this note, we prove that Duke's conjecture for quartic number fields implies Schmidt's conjecture. We also give a short unconditional proof of Schmidt's conjecture for the elliptic curve $y^2 = x^3 + ax$.

2010 *Mathematics subject classification*: primary 11G05; secondary 11D25, 11D45.

Keywords and phrases: elliptic curve, discriminant, quartic number field.

1. Introduction

Let $f(X) = X^3 + aX^2 + bX + c$ be a cubic polynomial with integer coefficients and discriminant $\Delta \neq 0$. We denote by E the elliptic curve defined by the equation $y^2 = f(x)$ and we set $H(f) = \max\{1, |a|, |b|, |c|\}$. In 1986, Evertse and Silverman [7] obtained an explicit upper bound for the number of integer points on E. In 1992, as a consequence of the result of Evertse and Silverman, Schmidt [14] proved that, for every $\epsilon > 0$, the number of integer points on E is $O_\epsilon(H(f)^{2+\epsilon})$. Furthermore, he stated the following conjecture.

Conjecture 1.1. For every $\epsilon > 0$, the number of integer points on E is $O_\epsilon(H(f)^\epsilon)$.

In 2011, Draziotis [4] proved Schmidt's conjecture for the case of the elliptic curves $y^2 = x^3 + ax$, where a is a fourth-power-free integer. In 2006, Helfgott and Venkatesh [9, Corollary 3.12] proved that, for every $\epsilon > 0$, the elliptic curve E has $O_\epsilon(|\Delta|^{\tau+\epsilon})$ integer points, where $\tau = 0.20070\ldots.$ Recently, Bhargava *et al.* [2] improved the result of Helfgott and Venkatesh, reducing the exponent to $\tau = 0.1117\ldots.$ In the case of Mordell's equation $y^2 = x^3 + b$, Helfgott and Venkatesh obtained the estimate $O(|b|^{\rho+\epsilon})$, where $\rho = 0.22377\ldots.$ Denote by $P(b)$ the product of the prime divisors of b. The author [13, Theorem 1] showed that the equation $y^2 = x^3 + b$ has $O(P(b)^{1/2+\epsilon})$ integer solutions which may be a better bound for certain b.

On the other hand, in 1998, Duke [5] stated the following conjecture.

CONJECTURE 1.2. The number of algebraic number fields of given degree n and discriminant D is $O_\epsilon(|D|^\epsilon)$.

The conjecture is still open for $n \geq 3$. The conjecture is valid for the cubic abelian and the quartic abelian and dihedral extensions of $\mathbb{Q}$ (see Lemma 2.4).

In this note we prove the following result.

THEOREM 1.3. *Conjecture 1.2 for $n = 4$ implies Conjecture 1.1.*

For the proof of this theorem, we apply an idea that goes back to Chabauty [3]. As in [12], we use the multiplication-by-two map on the elliptic curve E to reduce the problem to the same problem for the solutions of a family of unit equations in a number field K of degree at most four with discriminant dividing a fixed integer. Then Conjecture 1.2 implies the result. Since Conjecture 1.2 is valid for the quartic abelian and dihedral extensions of $\mathbb{Q}$, we are able to give a short proof of Draziotis' result without any hypothesis on a.

THEOREM 1.4. *The elliptic curves of the form $y^2 = x^3 + ax$ satisfy Conjecture 1.1.*

2. Auxiliary results

Let K be a number field of degree d. We denote by O_K the ring of algebraic integers of K, by O_K^* the group of units of O_K and by N_K the norm map from K to $\mathbb{Q}$. Two elements $x, y \in O_K$ are called associates if there is $u \in O_K^*$ such that $x = uy$. If I is a nonzero integer, we denote by $\omega(I)$ the number of distinct prime divisors p of I, and we denote by $\mathrm{ord}_p(I)$ the exponent of p in the prime factorisation of I.

LEMMA 2.1 [1, Lemma 4]. *Let I be a nonzero integer. The number of nonassociated elements $x \in O_K$ such that $N_K(x)|I$ is at most*

$$d^{\omega(I)} \prod_{p|I} \frac{(\mathrm{ord}_p(I) + d - 1)\cdots(\mathrm{ord}_p(I) + 1)}{(d-1)!},$$

where the product is taken over all the distinct primes dividing I.

LEMMA 2.2 [6, Theorem 1]. *Let $a, b \in K \setminus \{0\}$. The number of solutions (u, v) in $O_K^* \times O_K^*$ of the unit equation $au + bv = 1$ is at most 3×7^{3d}.*

LEMMA 2.3 [10, Theorem 3]. *Let $h(X) = X^4 + aX^2 + b$ be an irreducible polynomial of $\mathbb{Q}[X]$. Then the Galois group of the splitting field of $h(X)$ is either the Klein 4-group, V, the cyclic group of order four, C_4, or the dihedral group of order eight, D_4.*

LEMMA 2.4. *The number of quartic abelian and dihedral extensions of $\mathbb{Q}$ of discriminant D is $O_\epsilon(|D|^\epsilon)$.*

PROOF. By [16, Théorème 2], there are $O(4^{\omega(|D|)})$ abelian extensions. From [8, page 355], $\omega(|D|) = O(\log|D|/\log\log|D|)$, so the number of abelian quartic extensions of $\mathbb{Q}$ of discriminant D is $O_\epsilon(|D|^\epsilon)$. Further, in the proof of [11, Theorem 3], it is noted that there are at most $O_\epsilon(|D|^\epsilon)$ dihedral quartic fields of discriminant D. □

3. Proof of Theorem 1.3

It is sufficient to consider the case where E is an elliptic curve defined by the equation $y^2 = x^3 + ax + b$. Let $(x, y) \in \mathbb{Z}^2$ be an integer point of E. Then there is $(s, t) \in E(\bar{\mathbb{Q}})$ such that $[2](s, t) = (x, y)$. On the other hand, $[2](s, t) = (\phi(s, t), \psi(s, t))$, where

$$\phi(s,t) = -2s + \left(\frac{3s^2 + a}{2t}\right)^2, \quad \psi(s,t) = -t + \left(\frac{3s^2 + a}{2t}\right)(s - \phi(s,t)).$$

Putting $\eta = (3s^2 + a)/2t$,

$$x = -2s + \eta^2, \quad y = -\frac{3s^2 + a}{2\eta} + \eta(3s - \eta^2). \tag{3.1}$$

Eliminate s between these two equations. We deduce that η satisfies the equation

$$h(U) = U^4 - 6xU^2 - 8yU - 3x^2 - 4a = 0. \tag{3.2}$$

Next, substituting the values of x and y given by (3.1) in (3.2) and replacing η^2 by $2s + x$, we see that s is a root of the equation

$$s^4 - 4xs^3 - 2as^2 - 4axs - 8bs - 4bx + a^2 = 0.$$

Thus

$$4x = \frac{s^4 - 2as^2 + a^2 - 8bs}{s^3 + as + b}.$$

Let $K = \mathbb{Q}(s)$ so that $[K : \mathbb{Q}] \le 4$. By [15, Ch. VIII, Sublemma 4.3],

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

It follows that

$$N_K(s^3 + as + b) \quad \text{divides } |\Delta|^{[K:\mathbb{Q}]}. \tag{3.3}$$

Suppose that $K = \mathbb{Q}$. Since the number of divisors of Δ is $O_\epsilon(\Delta^\epsilon)$, there are at most $O_\epsilon(\Delta^\epsilon)$ equations of the form $s^3 + as + b = \delta$, where δ is a divisor of $|\Delta|$. Every such equation has at most three distinct solutions and so there are at most $O_\epsilon(\Delta^\epsilon)$ values for s and hence for x.

Suppose now that $K \neq \mathbb{Q}$. Denote by ρ_1, ρ_2, ρ_3 the roots of the polynomial $T^3 + aT + b$ and put $M = K(\rho_1, \rho_2, \rho_3)$. Let Ω denote a maximal set of pairwise nonassociated elements of O_M with norm dividing $|\Delta|^{[M:\mathbb{Q}]}$. By (3.3), there are $k_1, k_2 \in \Omega$ and units of M, say u_1 and u_2, such that

$$s - \rho_i = k_i u_i \quad (i = 1, 2).$$

It follows that (u_1, u_2) is a solution of the unit equation

$$\frac{k_1}{\rho_2 - \rho_1} U_1 - \frac{k_2}{\rho_2 - \rho_1} U_2 = 1.$$

The number of these equations is $|\Omega|^2$. By Lemma 2.1, this number is bounded above by

$$24^{2\omega(\Delta)} \prod_{p|\Delta} (\log\log|\Delta|^{24})^{46\omega(\Delta)} = O_\epsilon(\Delta^\epsilon).$$

By Lemma 2.2, each such equation yields $O(1)$ solutions over M. Thus, for every K, there are $O_\epsilon(|\Delta|^\epsilon)$ values for s, and hence also for x.

Denote the discriminant of K by D_K. Since $s = (\eta^2 - x)/2$, we see that $s \in \mathbb{Q}(\eta)$ and $K \subseteq \mathbb{Q}(\eta)$. The discriminant of $h(U)$ is equal to $2^{12}\Delta$, so D_K divides $2^{12}\Delta$.

Suppose that $[K : \mathbb{Q}] = 2$. The number of quadratic fields with discriminant dividing $2^{12}\Delta$ is bounded by the number of integer divisors of $2^{12}\Delta$ which is $O_\epsilon(|\Delta|^\epsilon)$. Thus, we have $O_\epsilon(\Delta^\epsilon)$ choices for K.

Finally, let $[K : \mathbb{Q}] = 4$. Then $K = \mathbb{Q}(\eta) = \mathbb{Q}(s)$. Conjecture 1.2 for $n = 4$ implies that there are at most $O_\epsilon(|\Delta|^\epsilon)$ choices for K. Since $\Delta = O(H(f)^4)$, the result follows.

Remark 3.1. Suppose that $a = 0$. From [17], we deduce that K has signature $(2, 1)$.

4. Proof of Theorem 1.4

Suppose that E is the elliptic curve defined by the equation $y^2 = x^3 + ax$. From the general case considered in Section 3, for every number field K, there are $O_\epsilon(\Delta^\epsilon)$ values for s and hence for x. We shall give an upper bound for the number of the fields K. It suffices to consider the case $[K : \mathbb{Q}] = 4$. Then $f(T)$ is irreducible. Now

$$0 = \frac{f(s)}{s^2} = \left(s + \frac{a}{s}\right)^2 - 4x\left(s + \frac{a}{s}\right) - 4a,$$

and hence

$$s + \frac{a}{s} = 2(x \pm \sqrt{x^2 + a}).$$

It follows that

$$s^2 - 2(x \pm \sqrt{x^2 + a})s + a,$$

and hence

$$s = x \pm \sqrt{x^2 + a} \pm \sqrt{2x^2 \pm 2x\sqrt{x^2 + a}}.$$

Therefore $K = \mathbb{Q}(\sqrt{2x^2 \pm 2x\sqrt{x^2 + a}})$ and $x^2 + a$ is not a square. The irreducible polynomial of $\sqrt{2x^2 \pm 2x\sqrt{x^2 + a}}$ is

$$h(T) = T^4 - 4x^2T^2 - 4x^2a.$$

By Lemma 2.3, the Galois group of the splitting field of $h(T)$ over $\mathbb{Q}$ is one of V, C_4 and D_4. Thus, Lemma 2.4 implies that there are $O_\epsilon(a^\epsilon)$ choices for K. Therefore the number of integer solutions of $y^2 = x^3 + ax$ is $O_\epsilon(a^\epsilon)$.

https://doi.org/10.1017/S0004972717000375 Published online by Cambridge University Press

References

[1] A. Berczes, 'On the number of solutions of norm form equations', *Period. Math. Hungar.* **43**(1–2) (2001), 165–176.

[2] M. Bhargava, A. Shankar, T. Taniguchi, F. Thorne, J. Tsimerman and Y Zhao, 'Bounds on 2-torsion in class groups of number fields and integral points on elliptic curves', Preprint 2017, arXiv:1701.02458v1.

[3] C. Chabauty, 'Démonstration de quelques lemmes de rehaussement', *C. R. Acad. Sci. Paris* **217** (1943), 413–415.

[4] K. Draziotis, 'On the number of integer points on the elliptic curve $y^2 = x^3 + Ax$', *Int. J. Number Theory* **7**(3) (2011), 611–621.

[5] W. Duke, 'Bounds for arithmetic multiplicities', in: *Proceedings of the International Congress of Mathematicians,* Vol. II (Berlin, 1998), 163–172 (electronic supplement).

[6] J.-H. Evertse, 'On equations in S-units and the Thue–Mahler equation', *Invent. Math.* **75** (1984), 561–584.

[7] J.-H. Evertse and J.-H. Silverman, 'Uniform bounds for the number of solutions to $Y^n = f(X)$', *Math. Proc. Cambridge Philos. Soc.* **100** (1986), 237–248.

[8] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, 5th edn (Oxford University Press, Oxford, 1979).

[9] H. A. Helfgott and A. Venkatesh, 'Integral points on elliptic curves and 3-torsion in class groups', *J. Amer. Math. Soc.* **19**(3) (2006), 527–550.

[10] L.-C. Kappe and B. Warren, 'An elementary test for the Galois group of a quartic polynomial', *Amer. Math. Monthly* **96**(2) (1989), 133–137.

[11] J. Klüner, 'The number of S_4-fields with given discriminant', *Acta Arith.* **122**(2) (2006), 185–194.

[12] D. Poulakis, 'Integer points on algebraic curves with exceptional units', *J. Aust. Math. Soc.* **63** (1997), 145–164.

[13] D. Poulakis, 'The number of solutions of the Mordell equation', *Acta Arith.* **88**(2) (1999), 173–179; Corrigendum, *Acta Arith.* **92**(4) (2000), 387–388.

[14] W. Schmidt, 'Integer points on curves of genus 1', *Compos. Math.* **81**(1) (1992), 33–59.

[15] J. H. Silverman, *The Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics, 106 (Springer, New York, 1986).

[16] A. Travesa, 'Nombre d'extensions abéliennes sur $\mathbb{Q}$', *Sémin. Théor. Nombres Bordeaux* **2** (1990), 413–423.

[17] L. Yang, X. R Hou and Z. B. Zeng, 'A complete discrimination system for polynomials', *Sci. China E* **39** (1996), 628–646.

DIMITRIOS POULAKIS, Department of Mathematics,
Aristotle University of Thessaloniki, 54124 Thessaloniki, Greece
e-mail: poulakis@math.auth.gr