GLASNIK MATEMATIČKI
Vol. 46(66)(2011), 333 – 338

A REMARK ON THE DIOPHANTINE EQUATION $f(x) = g(y)$

Ivica Gusić
University of Zagreb, Croatia

Abstract. Let K be an algebraic number field, and let $h(x) = x^3+ax$ be a polynomial over K. We prove that there exists infinitely many $b \in K$ such that the equation $dy^2 = x^3 + ax + b$ has no solutions over K for infinitely many $d \in K^*/K^{*2}$. The proof is based on recent results of B. Mazur and K. Rubin on the 2-Selmer rank in families of quadratic twists of elliptic curves over number fields.

On the other side, it is known that if the parity conjecture is valid, then there exist a number field K and a cubic polynomial f irreducible over K, such that the equation $dy^2 = f(x)$ has infinitely many solutions for each $d \in K^*$.

1. Introduction

Yu. Bilu observed that if f is a polynomial over $\mathbb{Q}$ of degree $n \geq 2$ and m is a composite natural number, then there exists a polynomial g over $\mathbb{Q}$ of degree m, such that the equation $f(x) = g(y)$ has no rational solutions (see [4]). Therefore, it is reasonable to ask the following question.

Question 1.1. *Let f be a polynomial over $\mathbb{Q}$ of degree $n \geq 2$ and let m be a prime number. Does there exist a polynomial g over $\mathbb{Q}$ of degree m, such that the equation $f(x) = g(y)$ has no rational solutions?*

The answer to Question 1.1. is positive for $n = 2$, for $(m, n) = (2, 3)$ and if $m|n$. Using a result from [3], it can be proved that the answer is positive for all (m, n), provided the abc-conjecture is true (see [5]).

The positive answer in the case $(m, n) = (2, 3)$ follows from the fact that there are infinitely many zero rank curves in the family of quadratic twists of arbitrary elliptic curve E over $\mathbb{Q}$ (see, for example, [8]), and that there are

2010 *Mathematics Subject Classification.* 11G05, 14G05.
Key words and phrases. Elliptic curve, quadratic twist, 2-Selmer rank, number field.

only finitely many square-free d such that E_d has a rational torsion point of order > 2 (see [6, Lemma 5.5] for a proof over number fields).

All proofs of the existence of infinitely many zero rank curves in the family of quadratic twists of a fixed elliptic curve over $\mathbb{Q}$ were analytical and based on the modularity and special values of L-functions. Therefore they were not applicable to elliptic curves over general algebraic number fields. Moreover, it is known that if the parity conjecture holds, then there is an algebraic number field K and an elliptic curve E/K such that all quadratic twists of E/K have positive K-rank (Remark 2.1). This hypothetic curve provides an example of irreducible polynomial f over K such that the equation

$$dy^2 = f(x)$$

has infinitely many solutions over K for each $d \in K^*$.

Recently, B. Mazur and K. Rubin ([6]) obtained several general results on the rank of the quadratic twists of E/K based on a detailed analysis of the 2-Selmer groups (Lemma 2.2). Using their results and a characterization of elliptic curves with constant 2-Selmer parity from [2], we show that the answer to Question 1.1. for $(m, n) = (2, 3)$ is positive over algebraic number fields (Theorem 2.3.).

2. The case $(m, n) = (2, 3)$ over algebraic number fields.

Let K be a number field (of a finite degree over $\mathbb{Q}$) and let E be an elliptic curve over K. The global root number $\omega(E/K)$ of E/K is defined to be the product of local root numbers each equal to ±1. The parity conjecture states that

$$\omega(E/K) = (-1)^{r(E/K)}, \tag{2.1}$$

where $r(E/K)$ denotes the $\mathbb{Z}$-rank of the group $E(K)$. Let E^F denote the quadratic twist of E corresponding to the quadratic extension F/K. Note that

$$r(E/F) = r(E/K) + r(E^F/K). \tag{2.2}$$

Remark 2.1. ([1]) If the parity conjecture holds then there exist a number field K and a cubic polynomial f irreducible over K, such that the equation $dy^2 = f(x)$ has infinitely many solutions for each $d \in K^*$. For example, let E be the elliptic curve given with $y^2 = f(x) := x^3 + \frac{5}{4}x^2 - 2x - 7$. Then E has everywhere good reduction over $K := \mathbb{Q}(\zeta_3, \sqrt[3]{11})$, where ζ_3 is a primitive 3rd root of unity. Therefore all local root numbers of E/K at non-Archimedean primes are equal to 1, and so the global root number $\omega(E/K)$ is $(-1)^3 = -1$. By (2.1) the rank $r(E/K)$ is odd and so $r(E/K) \geq 1$. Let L be any quadratic extension of K. Since the good reduction is stable, E has everywhere good reduction over L, too. Now we have $\omega(E/L) = 1$. By the parity conjecture $r(E/L)$ is even, and so, by (2.2), $r(E^L/K)$ is odd. We see that f is an irreducible cubic polynomial over K and that the equation $dy^2 = f(x)$ has infinitely many solutions over K for all $d \in K^*$.

Let $d_2(E/K)$ denote the 2-Selmer rank of E/K, i.e., the $\mathbb{F}_2$-dimension of the 2-Selmer group of E/K (see [6, section 2.]). Note that $d_2(E/K)$ is finite and that $d_2(E/K) \geq r(E/K)$. It is said that E/K has constant 2-Selmer parity if $d_2(E^F/K) \equiv d_2(E/K) \pmod 2$ for all quadratic extensions F/K ([6, Definition 9.1]). Let us formulate the results from [6] which are crucial for the proof of Theorem 2.3.

Lemma 2.2. *Let K be a field of algebraic numbers and let E be an elliptic curve over K such that $E(K)[2] = 0$. Then:*

(i) *There are infinitely many quadratic extensions F/K such that $d_2(E^F/K) = d_2(E/K)$.*
(ii) *If $d_2(E/K) \geq 2$ then there is a quadratic extension F/K such that $d_2(E^F/K) = d_2(E/K) - 2$.*
(iii) *Assume that K has a real place or that E/K has multiplicative bad reduction at some non-Archimedean place. Then there is a quadratic extension F/K such that $d_2(E^F/K)$ and $d_2(E/K)$ have different parity.*

Proof of Lemma 2.2. See [6, Proposition 4.2, Lemma 4.1, Proposition 5.2. and Proposition 5.3.]. □

Theorem 2.3. *Let K be a number field and let $f(x) = x^3 + ax$ be a polynomial over K. Then there exist infinitely many $b \in K$ such that the equation $dy^2 = x^3 + ax + b$ has no solutions over K for infinitely many $d \in K^*/K^{*2}$.*

Proof of Theorem 2.3. The case $a \neq 0$. Let E be the elliptic curve given by $y^2 = x^3 + ax + b$ for $b \in K$. Then the discriminant of E is $\Delta = -16(4a^3 + 27b^2)$ and $c_4 = -48a$ (see [10, III. sect. 1.]). We claim that there are infinitely many $b \in K$ such that E has multiplicative bad reduction at some non-archimedean place of K. Without loss of generality we may assume that a is K-integral. By the Hilbert irreducibility theorem ([9, Theorem 46., p. 298]) there exist a natural number α and a rational integer β such that for each rational integer n the polynomial

$$f(x) := x^3 + ax + (\alpha n + \beta)$$

is irreducible over K. We need n such that there exists a valuation v of K with $v(\Delta) > 0$ and $v(c_4) = 0$. It would imply that E has multiplicative reduction at v (see [10, VII, Proposition 5.1. and Remark 1.1.]). In fact, we will show that there is a v such that $v(\Delta)$ is odd and $v(c_4) = 0$. Note that the family of prime ideals $\mathcal{P}$ of K such that the congruence $27(\alpha n + \beta)^2 + 4a^3 \equiv 0 \pmod{\mathcal{P}}$

has a solution is infinite. In order to prove it, put

$$h(n) := \prod_{\sigma}[27(\alpha n+\beta)^2+4(\sigma a)^3],$$

where σ ranges over all embeddings of a in $\mathbb{C}$. Then h is a nonconstant polynomial over $\mathbb{Z}$. Let H denote the Galois field of h and $\tilde{K}$ the Galois closure of K over $\mathbb{Q}$. Then there are infinitely many rational primes p that split completely both in H and $\tilde{K}$. For almost all such p the equation $h(n)\equiv 0 \pmod{p}$ has a solution. Therefore, there is at least one prime $\mathcal{B}$ of $\tilde{K}$ over p such that $27(\alpha n+\beta)^2+4a^3\equiv 0 \pmod{\mathcal{B}}$ has a solution. Let $\mathcal{P}$ denote the prime of K under $\mathcal{B}$. Since $a\in K$, the congruence $27(\alpha n+\beta)^2+4a^3\equiv 0 \pmod{\mathcal{P}}$ also has a solution. Hence we may fix $\mathcal{P}$ over p that is relatively prime to $2, 3, a, \alpha$, and $\alpha n_0+\beta$, where n_0 is a solution of the congruence. Let v denote the (normalized) discrete valuation corresponding to $\mathcal{P}$. Replacing n_0 by n_0+p, if it is necessary, we may assume that $v(\Delta)=1$ and $v(c_4)=0$, and so E has multiplicative bad reduction at v. By Lemma 2.2 (iii), we see that E/K has not constant 2-Selmer parity. Therefore, by Lemma 2.2 (ii) we get that there is a quadratic twist of E/K with trivial 2-Selmer group. Finally, by Lemma 2.2 (i) we see that there are infinitely many quadratic twists of E/K with trivial 2-Selmer group (hence with trivial Mordell-Weil rank over K, too). Since all but finitely many quadratic twists of an elliptic curve over K have no K-rational torsion points of odd order (see [6, Proposition 5.5]), the equation $dy^2=x^3+ax+b$ has no K-rational solutions for infinitely many integers b and infinitely many $d\in K^*/K^{*2}$.

The case $a=0$. Assume first that $\sqrt{-3}\in K$, and look at any elliptic curve

$$E: y^2=x^3+b$$

over K such that $\sqrt[3]{b}\notin K$. Note that E has complex multiplication and that $End(E)\otimes\mathbb{Q}\cong\mathbb{Q}(\sqrt{-3})\subseteq K$. Therefore $E(K)\otimes\mathbb{Q}$ is a $\mathbb{Q}(\sqrt{-3})$-vector space, and so the rank of $E(K)$ is even. By Lemma 2.2 (ii) and (i), we have to consider only the case when $d_2(E/K)$ is odd. Then, by Lemma 2.2 (ii), there are infinitely many quadratic extensions F/K such that $d_2(E^F/K)=1$. Since $r(E^F/K)$ is even for all F, we get that $r(E^F/K)=0$, for infinitely many F.

Assume now that $\sqrt{-3}\notin K$. Then the polynomial $h(x):=x^2+3$ is irreducible over K. By the Chebotarev density theorem the set of primes $\mathcal{P}$ of K such that $h(x)$ modulo $\mathcal{P}$ remains irreducible, has the Dirichlet density equal to $\frac{1}{2}$. Since almost all primes of K have the degree over $\mathbb{Q}$ equal to 1, we see that there are infinitely many primes of K of degree 1 such that $h(x)$ modulo $\mathcal{P}$ remains irreducible. Therefore there are infinitely many rational primes p with $p\equiv 2 \pmod{3}$ such that there is a prime $\mathcal{P}$ of K over p of degree 1. Let us fix such odd prime p and a prime $\mathcal{P}$ over p and look at the elliptic curve

$$E: y^2=x^3+p.$$

Let v denote the valuation at $\mathcal{P}$. Since the discriminant of E is $\Delta = -16\cdot 27p^2$ we see that $v(\Delta) = 2 < 12$, and so E has bad reduction at v. We claim that this bad reduction remains bad over each finite abelian extension of K. It is sufficient to prove that the reduction remains bad over each finite abelian extension of the completion $K_v \cong \mathbb{Q}_p$ (in fact we have to consider only ramified extensions). By the local Kronecker-Weber theorem each finite abelian extension of $\mathbb{Q}_p$ is contained in a cyclotomic extension. The ramification index of a ramified cyclotomic extension L of $\mathbb{Q}_p$ is equal to $p^{n-1}(p-1)$ for some natural number n. Hence $w(\Delta) = 2p^{n-1}(p-1)$ where w denotes the unique extension of v from K_v to L. Since $p \equiv 2 \pmod 3$ we see that $w(\Delta)$ is not divisible by 3, and so the reduction remains bad. Therefore the reduction remains bad over each finite abelian extension of K_v. By [2, Remark 4.9.], an elliptic curve over K has constant 2-Selmer parity if and only if it acquires everywhere good reduction over an abelian extension of K and K has no real place. Therefore E/K has not constant 2-Selmer parity, and we can proceed as above. □

As it has already said, the fact that each elliptic curve over $\mathbb{Q}$ has infinitely many quadratic twists with rank zero does not generalize to elliptic curves over number fields generally (provided the parity conjecture holds). Nevertheless, the statement of Theorem 2.3. (the case $a = 0$) is the full generalization of the fact that there are infinitely many integers b such that the equation $y^2 = x^3 + b$ has no rational solutions (see [7], where the result over $\mathbb{Q}$ is proved as a consequence of a refinement of the Davenport-Heilbronn theorem). Let us note, that from the proof of Theorem 2.3. (the case $a = 0$), it follows that there are infinitely many $b \in K^*/K^{*3}$ such that the equation $dy^2 = x^3 + b$ has no solutions over K for infinitely many $d \in K^*/K^{*2}$.

References

[1] T. Dokchitser and V. Dokchitser, *Elliptic curves with all quadratic twists of positive rank*, Acta Arith. **137** (2009), 193–197.

[2] T. Dokchitser and V. Dokchitser, *Root numbers and parity of ranks of elliptic curves*, J. Reine Angew. Math. **2011**, 658, 39–64.

[3] A. Granville, *Rational and integral points on quadratic twists of a given hyperelliptic curve*, Int. Math. Res. Not. IMRN 2007, Art. ID 027, 24 pp. (2007).

[4] I. Gusić, *A characterization of linear polynomials*, J. Number Theory **115** (2005), 343–347.

[5] I. Gusić, *Some applications of the abc-conjecture to the diophantine equation $qy^m = f(x)$*, Glas. Mat. Ser III., to appear.

[6] B. Mazur and K. Rubin, *Ranks of twists of elliptic curves and Hilbert's tenth problem*, Invent. Math. **181** (2010), 541–575.

[7] J. Nakagawa and K. Horie, *Elliptic curves with no rational points*, Proc. Amer. Math. Soc. **104** (1988), 20–24.

[8] K. Ono and C. Skinner, *Non-vanishing of quadratic twists of modular L-functions*, Invent. Math., **134** (1998), 651–660.

[9] A. Schinzel, Polynomials with special regard to reducibility, Cambridge University Press, Cambridge, 2000.

[10] J. H. Silverman, The Arithmetic of Elliptic Curves, Graduate Texts in Mathematics, **106**, Springer, Berlin, 1986.

I. Gusić
Faculty of Chemical Engin. and Techn.
University of Zagreb
Marulićev trg 19, 10000 Zagreb
Croatia
E-mail: igusic@fkit.hr

Received: 21.6.2010.
Revised: 6.11.2010.