ALBANIAN JOURNAL OF MATHEMATICS
Volume 8, Number 1, Pages 49–53
ISSN: 1930-1235; (**2014**)

ON THE CONGRUENT NUMBER PROBLEM OVER INTEGERS OF REAL NUMBER FIELDS

Albertas Zinevičius

Department of Mathematics and Informatics,
Vilnius University,
Naugarduko 24, Vilnius, LT-03225,
Lithuania
and
Institute of Mathematics and Informatics,
Akademijos 4, Vilnius, LT-08663,
Lithuania
Email: albertas.zinevicius@mif.vu.lt

Abstract. Given a real finite field extension $K/\mathbb{Q}$ of degree d and class number h_K and a positive integer a, we show that there is a set of rational prime numbers of relative density at least $1/(2dh_K)$ that have a principal prime factor $\pi\mathcal{O}_K \subset \mathcal{O}_K$ of degree one such that the equation $a\pi^2 = x^4 - y^2$ has no nontrivial solutions in $\mathcal{O}_K$.

1. Introduction

The classical congruent number problem asks for an algorithm that would decide if a given positive integer n is the area of a right triangle with rational side lengths. The existence of such a triangle is equivalent to the solvability of the equation

$$y^2 = x^4 - 16n^2 \tag{1}$$

in rational numbers (x, y) with x nonzero. It is known that the existence of such a (surprisingly simple) algorithm would follow from the conjecture of Birch and Swinnerton-Dyer, as was shown in the work of Tunnell [12]. It was noted by Jedrzejak [6] that, under assumption of the same conjecture, Tunnell's theorem together with the work of Tada [10] imply that every positive integer is the area of some right triangle with side lengths in the quartic extension $\mathbb{Q}(\sqrt{3}, \sqrt{5})$.

It is difficult to expect, on the other hand, that the equation (1) could have solutions among the integers $\mathcal{O}_K$ of a fixed number field K for all n. Indeed, as it was remarked by Stoll [9], the conjecture of Bombieri-Lang suggests the opposite.

2010 *Mathematics Subject Classification.* 11D45, 11H06.
Key words and phrases. Congruent numbers, real number fields, rings of integers, prime ideals.

That this can never happen when K is a cyclic extension, can be concluded from the following statement that we showed in [13]:

Theorem A. *Let K be a finite Galois extension of the field of rational numbers with cyclic Galois group* $\mathrm{Gal}(K/\mathbb{Q})$ *and let a be a nonzero (rational) integer. Then the set of rational prime numbers p for which the equation*

$$ap^2 = x^4 - y^2 \tag{2}$$

in unknowns x, y does not have a solution $(x, y) \in \mathcal{O}_K \times \mathcal{O}_K$ with $x \neq 0$, has lower relative density at least $1/2$ in the set of (rational) prime numbers that remain inert in K.

The conjectural solvability of (1) in some number fields for all positive integers n raises the question of whether one could expect to find a number field K in which all the equations (1) were solvable when the parameter n also varies over K (rather than $\mathbb{Q}$). This still has the same geometric interpretation when the extension K is real. The analogous question for integers of number fields becomes easier and can be settled:

Theorem 1. *Let K be a finite real extension of the field of rational numbers, of degree d and class number h_K, and let a be a positive integer. Then there is a set of rational prime numbers p of relative density at least $1/(2dh_K)$, such that the principal ideal $p\mathcal{O}_K$ has a principal prime factor $\pi\mathcal{O}_K$ of degree one for which the equation*

$$a\pi^2 = x^4 - y^2 \tag{3}$$

in unknowns x, y does not have a solution $(x, y) \in \mathcal{O}_K \times \mathcal{O}_K$ with $x \neq 0$.

Most of the proof of this observation translates *mutatis mutandis* from the proof of Theorem A, which is indebted to the results of Jarden-Narkiewicz and Green-Tao. Additionally, a fundamental result of class field theory is employed in Lemma 3. The proof does not suggest that the density $1/(2dh_K)$ could be precise for some number fields K. The author of this note would find it interesting to see a demonstration that (1) does not have solutions over $\mathcal{O}_K$ for many rational integer values of the parameter n.

2. Proof of Theorem 1

For the proof of the theorem we borrow two statements from [4] and [5], respectively, that we state here as lemmas:

Lemma 1. *Let A be any subset of the prime numbers of positive relative upper density. Then A contains infinitely many arithmetic progressions of length l for all l.*

Lemma 2. *If R is a finitely generated integral domain of zero characteristic and l is an integer, then there exists a constant $A_l(R)$ such that every arithmetic progression in R having more than $A_l(R)$ elements contains an element which is not a sum of l units.*

In addition, we will use the following lemma:

Lemma 3. *The relative density of prime numbers $p \subset \mathbb{Z}$ such that the principal ideal $p\mathcal{O}_K \subset \mathcal{O}_K$ has a principal prime factor $\mathfrak{p} = \pi\mathcal{O}_K$ of degree one that remains inert in the quadratic extension $K(\sqrt{-a})/K$, is at least $1/(2dh_K)$.*

Proof of Lemma 3. Notice first that, since K is a subfield of the real numbers, its Hilbert class field $\mathrm{Cl}(K)$ is also a subfield of the real numbers (as $\mathrm{Cl}(K)/K$ must be unramified at the infinite prime). Therefore there is an element $\sigma \in \mathrm{Gal}(\mathrm{Cl}(K)(\sqrt{-a})/K)$ that fixes $\mathrm{Cl}(K)$ but is not the identity automorphism.

Let L be the Galois closure of the extension $\mathrm{Cl}(K)(\sqrt{-a})/\mathbb{Q}$. Since the extension $L/\mathrm{Cl}(K)(\sqrt{-a})$ is Galois and $\sigma \in \mathrm{Aut}(\mathrm{Cl}(K)(\sqrt{-a}))$, one can extend σ to an element of $\mathrm{Gal}(L/\mathrm{Cl}(K))$. More precisely, there are $[L : \mathrm{Cl}(K)(\sqrt{-a})]$ distinct elements $\sigma_j \in \mathrm{Gal}(L/\mathrm{Cl}(K)), j = 1, \ldots, [L : \mathrm{Cl}(K)(\sqrt{-a})]$, that coincide with σ on the subfield $\mathrm{Cl}(K)(\sqrt{-a})$.

Recall that for any tower of number fields $E \subset E' \subset E''$, where E''/E is Galois, the decomposition type of a prime ideal $\mathfrak{q} \subset \mathcal{O}_E$, that does not divide $\Delta_{E''/E}$, in the extension E'/E coincides with the cycle structure of the permutation of $\mathrm{Gal}(E''/E)/\mathrm{Gal}(E''/E')$ that is induced by the action of (any) Frobenius element $\mathrm{Frob}_{\mathfrak{q}}$ of the prime ideal $\mathfrak{q}$.

When $E = \mathbb{Q}, E' = K, E'' = L$ and p is a rational prime that does not divide the discriminant $\Delta_{L/\mathbb{Q}}$, it follows that the ideal $p\mathcal{O}_K \subset \mathcal{O}_K$ has a prime factor $\mathfrak{p} \subset \mathcal{O}_K$ of degree one if and only if the conjugacy class of the Frobenius element $\mathrm{Frob}_p \in \mathrm{Gal}(L/\mathbb{Q})$ intersects the subgroup $\mathrm{Gal}(L/K)$ (see, e.g., [7]). In particular, when the conjugacy class of Frob_p contains one of σ_j as above, $p\mathcal{O}_K$ has a prime factor $\mathfrak{p}$ of degree one.

Likewise, when $E = K, E' = \mathrm{Cl}(K), E'' = L$, it follows that a prime ideal $\mathfrak{p} \subset \mathcal{O}_K$ as above splits completely in the extension $\mathrm{Cl}(K)/K$. Indeed, we may assume, without a loss of generality, that

$$\mathrm{Frob}_p(x) \equiv x^{\#\mathbb{Z}/p\mathbb{Z}} \mod \mathfrak{q}$$

for all $x \in \mathcal{O}_L$ and a prime ideal $\mathfrak{q} \subset \mathcal{O}_L$ that lies over $\mathfrak{p}$ (by replacing Frob_p, if necessary, with another element from the conjugacy class of Frob_p). Since $\mathfrak{p}$ is of degree 1, we have $\#\mathbb{Z}/p\mathbb{Z} = \#\mathcal{O}_K/\mathfrak{p}$. Hence holds

$$\mathrm{Frob}_p(x) \equiv x^{\#\mathcal{O}_K/\mathfrak{p}} \mod \mathfrak{q},$$

for all $x \in \mathcal{O}_L$. Thus Frob_p is also a Frobenius element $\mathrm{Frob}_{\mathfrak{p}}$ of $\mathfrak{p}$ (with respect to the extension L/K). The cycle structure of the permutation of the group $\mathrm{Gal}(L/K)/\mathrm{Gal}(L/\mathrm{Cl}(K))$ induced by $\mathrm{Frob}_{\mathfrak{p}}$ is then the same as that induced by any σ_j that is in the same conjugacy class as Frob_p. Consequently, it is the product of 1-cycles (since $\sigma_j \in \mathrm{Gal}(L/\mathrm{Cl}(K))$ acts on $\mathrm{Gal}(L/K)/\mathrm{Gal}(L/\mathrm{Cl}(K))$ trivially).

On the other hand, the permutation of $\mathrm{Gal}(L/K)/\mathrm{Gal}(L/K(\sqrt{-a}))$ induced by the σ_j is not the trivial one since $\sigma_j \notin \mathrm{Gal}(L/K(\sqrt{-a}))$. Consequently, the prime ideal $\mathfrak{p}$ remains inert in the extension $K(\sqrt{-a})/K$.

A fundamental result of class field theory asserts that prime ideals of K that split completely in the extension $\mathrm{Cl}(K)/K$ are principal [8]. Thus $\mathfrak{p} = \pi\mathcal{O}_K$ for some prime element $\pi \in \mathcal{O}_K$ that remains prime in $\mathcal{O}_{K(\sqrt{-a})}$.

By the Chebotarev density theorem [11], the density of rational prime numbers p with Frobenius symbol Frob_p (with respect to the extension $L/\mathbb{Q}$) in the same conjugacy class as some σ_j is equal to the number of elements in those conjugacy classes of $\mathrm{Gal}(L/\mathbb{Q})$ that contain some σ_j, divided by the size of the Galois group $\mathrm{Gal}(L/\mathbb{Q})$. It is therefore, at least

$$\#\{\sigma_j\}/\#\,\mathrm{Gal}(L/\mathbb{Q}) = ([L : \mathrm{Cl}(K)]/2)/([\mathrm{Cl}(K) : \mathbb{Q}][L : \mathrm{Cl}(K)]) = 1/(2dh_K).$$

□

Proof of Theorem 1. Let $\mathfrak{p} = \pi\mathcal{O}_K$ be a prime ideal as in Lemma 3. If the equation

$$a\pi^2 = x^4 - y^2 = (x^2 + y)(x^2 - y)$$

has a solution in $\mathcal{O}_K$ with $x \neq 0$ then either both $x^2 - y, x^2 + y$ are divisible by π or not. In the first case,

$$\begin{cases} x^2 - y = \pi r \\ x^2 + y = \pi a r^{-1} \end{cases}$$

for some $r \in \mathcal{O}_K$ that divides a. Denote by σ the generator of $\mathrm{Gal}(K(\sqrt{-a})/K)$. By adding the equations one obtains

$$2x^2 r = \pi(r^2 + a) = \pi(r + \sqrt{-1})(r - \sqrt{-a}) = \pi(r + \sqrt{-1})\sigma(r + \sqrt{-a}).$$

We thus can see that, since π is a prime element of the ring of integers of $K(\sqrt{-a})$ that is mapped to an associate of itself by σ , the highest power of π that divides the right-hand side must be odd. On the other hand, the highest power of any prime element that divides the left-hand side and does not divide $2a$ is even. Therefore, the first case may hold for at most finitely many prime ideals $\pi\mathcal{O}_K$. We thus may restrict ourselves to the second case, i.e., assume that

$$\begin{cases} x^2 - y = \pi^2 a r^{-1} \\ x^2 + y = r \end{cases}$$

holds for some $r \in \mathcal{O}_K$ that divides a. By adding the equations again, one obtains

$$2x^2 r = r^2 + \pi^2 a.$$

Let K' be a field extension of K that is generated by elements of the form $\sqrt{r}$, where $r \in \mathcal{O}_K$ divide a. Up to multiplication by units, there are only finitely many such r. Let $r_1, ..., r_v$ be their representatives. The Dirichlet unit theorem [2] tells also that the multiplicative group of units of $\mathcal{O}_K$ is finitely generated. Let $e_1, ..., e_s$ be its generators. Then $K' = K(\sqrt{2}, \sqrt{e_1}, ..., \sqrt{e_s}, \sqrt{r_1}, ..., \sqrt{r_v})$ is a finite extension of K. Over $\mathcal{O}_{K'}$ one can write

$$(x\sqrt{2r} - \pi\sqrt{a})(x\sqrt{2r} + \pi\sqrt{a}) = r^2.$$

Hence both $x\sqrt{2r} - \pi\sqrt{a}, x\sqrt{2r} + \pi\sqrt{a}$ are divisors of a^2 in $\mathcal{O}_{K'}$. Consequently, $2\pi\sqrt{a}$ is a sum of two divisors of a^2.

We claim that such ideals $\mathfrak{p} = \pi\mathcal{O}_K$ have density zero among the prime ideals of the ring $\mathcal{O}_K$. Let M denote the Galois closure of the field extension $K'/\mathbb{Q}$. Note that there is a subset $G_\pi \subset \mathrm{Gal}(M/\mathbb{Q})$ of cardinality d such that $Nm_{K/\mathbb{Q}}(\pi) =$

$\prod_{\sigma\in G_\pi}\sigma(\pi)$. Thus,

$$\prod_{\sigma\in G_\pi}\sigma(2\pi\sqrt{a}) = Nm_{K/\mathbb{Q}}(\pi)\prod_{\sigma\in G_\pi}\sigma(2\sqrt{a}).$$

On the other hand, $\sigma(2\pi\sqrt{a})$ is a sum of two divisors of a^2 in $\mathcal{O}_M$, and hence $\prod_{\sigma\in G_\pi}\sigma(2\pi\sqrt{a})$ is a sum of 2^d divisors of a^{2d} in $\mathcal{O}_M$. Furthermore, since $\mathfrak{p}$ is of degree one,

$$|Nm_{K/\mathbb{Q}}(\pi)| = \#\mathcal{O}_K/\mathfrak{p} = p.$$

Had prime ideals of the form $\mathfrak{p} = \pi\mathcal{O}_K$ positive upper density among the prime ideals of $\mathcal{O}_K$, then the upper density of rational prime numbers of the form $|Nm_{K/\mathbb{Q}}(\pi)|$ would also be positive in the set of rational prime numbers. Moreover, there would exist a fixed $G \subset \mathrm{Gal}(M/\mathbb{Q})$ such that $G_\pi = G$ for a positive fraction of the prime numbers $|Nm_{K/\mathbb{Q}}(\pi)|$. It would follow from the Lemma 1 that there must exist arbitrarily long arithmetic progressions with elements of the form $Nm_{K/\mathbb{Q}}(\pi)\prod_{\sigma\in G}\sigma(2\sqrt{a})$.

Let $r_1', \dots, r_l' \in \mathcal{O}_M$ be the representatives of the divisors of a^{2d} modulo the multiplicative group of units of $\mathcal{O}_M$. Notice that the ring $\mathcal{O}_M[1/r_1', \dots, 1/r_l']$ is finitely generated. Furthermore, any term of an arithmetic progression as above is a sum of 2^d units in this ring. However, by Lemma 2, the length of such arithmetic progressions cannot be arbitrarily large, a contradiction. Thus, prime ideals $\pi\mathcal{O}_K$ as in Lemma 3 for which (3) holds have density zero.

□

References

[1] Chandrasekar V., *The congruent number problem*, Resonance **3**(8), 33-45 (1998).
[2] Narkiewicz W., *Elementary and analytic theory of algebraic numbers*, 3rd ed., p. 98, Springer-Verlag, Berlin-Heidelberg (2004).
[3] Girondo E., Gonzalez-Diez G., Gonzalez-Jimenez E., Steuding R., Steuding J., *Right triangles with algebraic sides and elliptic curves over number fields*, Math. Slovaca **59**(3), 299-306 (2009).
[4] Green B., Tao T., *The primes contain arbitrarily long arithmetic progressions*, Annals of Mathematics **167**(2), 481-547 (2008).
[5] Jarden M., Narkiewicz W., *On sums of units*, Monatsh. Math. **150**(4), 327-332 (2006).
[6] Jedrzejak T., *Congruent numbers over real number fields*, Colloquium Mathematicum **128**(2), 179-186 (2012).
[7] Neukirch J., *Algebraische Zahlentheorie*, p. 570, Springer-Verlag, Berlin-Heidelberg (2007).
[8] Neukirch J., *Algebraische Zahlentheorie*, p. 429, Springer-Verlag, Berlin-Heidelberg (2007).
[9] Stoll M., personal communication (2014).
[10] Tada M., *Congruent numbers over real quadratic fields*, Hiroshima Math. J. **31**(2), 331-343 (2001).
[11] Tschebotareff N., *Die Bestimmung der Dichtigkeit einer Menge von Primzahlen, welche zu einer gegebenen Substitutionsklasse gehören*, Math. Ann. **95**, 191-228 (1925).
[12] Tunnell J.B., *A Classical Diophantine problem and modular forms of Weight 3/2*, Inventiones Mathematicae **72**, 323-334 (1983).
[13] Zinevičius A., *On the congruent number problem over integers of cyclic extensions* (to appear in Mathematica Slovaca).

