ROMANIAN JOURNAL OF MATHEMATICS AND COMPUTER SCIENCE, 2012, VOLUME 2, ISSUE 2, p.11-16

The congruence number problem over real quadratic fields

Sever Achimescu[1]

Abstract

Classically, a congruent number is a positive integer equal to the area of a right triangle ABC such that the segments AB, BC, CA have rational lengths. The congruent number problem asks for criteria to decide if a given positive integer is a congruent number. This problem has been solved in 1983 by Tunnel. In this paper we prove a generalization to real quadratic fields of the first step of the proof in the rational case.

AMS Subject Classification (2010): 11R11, 11G05, 11F37
Key words: generalized congruent number problem

1 Introduction

Classically, a congruent number is a positive integer equal to the area of a right triangle ABC such that the segments AB, BC, CA have rational lengths. The congruent number problem asks for criteria to decide if a given positive integer is a congruent number. This problem has been solved (assuming a weak version of the Birch-Swinnerton-Dyer conjecture) in 1983 by Tunnel, who proved the last step and gave explicit criteria. The steps are the following:

Step1. (proved in [3]) Let n be a positive integer and let $E_n(\mathbf{Q})$ be the elliptic curve $y^2 = x^3 - nx^2$ over $\mathbf{Q}$. Then n is a congruent number iff $E_n(\mathbf{Q})$ has a point of infinite order.

Step2. (assuming the Birch-Swinnerton-Dyer conjecture; one direction being proved in this case by the work of Coates-Wiles) $E_n(\mathbf{Q})$ has a point of infinite order iff $L(E_n(\mathbf{Q}), 1) = 0$ where $L(E, s)$ denotes the L-function of the elliptic curve E.

Step3. $L(E_n(\mathbf{Q}), s) = L(f \otimes \chi_n, s)$, where f is the unique normalized newform of level 32, weight 2 and trivial character and χ_n is the quadratic character corresponding to $\mathbf{Q}(\sqrt{\mathbf{n}})$.

Step4. Let c_n be the n^{th} coefficient of the modular form of weight 3/2 which maps to f via the Shimura lift. Then $L(E_n(\mathbf{Q}), 1)$ can be expressed in terms of c_n^2.

Step5. Using [5], Tunnel proved in [6] that f equals to a product of a theta series and a modular form of weight one (both with known coefficients), thus the condition $L(E_n(\mathbf{Q}), 1) = 0$ became equivalent to a simple algebraic formula easy to be tested on computers. Tables with (non)congruent numbers are now available.

We suggest the reader to consult [3] for details.

Our long-term goal is to generalize and the congruent number problem to totally real number fields F and solve it. In the next section we define the concept of F-congruent number, which will take the place of the usual concept of (rational) congruent number. Instead of (half integral weight) modular forms we will deal with (half integral weight) Hilbert modular forms. Hoping to generalize the solution step by step, we notice that the generalization of the Serre-Stark theorem (from [5]) to Hilbert modular forms of weight 1/2 has been done in [2].

The goal of this paper is to prove a generalization of Step1 in the case of real quadratic fields.

2 Definitions and notations

Let $F = \mathbf{Q}(\sqrt{d})$ be a real quadratic field, $d \geq 2$ being a square-free integer. The positiveness of the elements of F depends on the embedding of F in $\mathbf{R}$. There are two embeddings: $\tau_1(a + b\sqrt{d}) = a + b\sqrt{d}$ and $\tau_{-1}(a + b\sqrt{d}) = a - b\sqrt{d}$. Let $\tau \in \{\tau_1, \tau_{-1}\}$.

Definition 1 *$\alpha \in F$ is said to be an F-congruent number with respect to τ iff $\exists X, Y, Z \in F$ such that:*

$$\tau(X) > 0, \tau(Y) > 0, \tau(Z) > 0$$

$$\tau(X)^2 + \tau(Y)^2 = \tau(Z)^2$$

$$2\tau(X)\tau(Y) = \tau(\alpha)$$

Note that if α is an F-congruent number with respect to τ then $\tau(\alpha) > 0$. We quote from [1] the following example of a $\mathbf{Q}(\sqrt{2})$-congruent number with respect to τ_1 which is not a $\mathbf{Q}(\sqrt{2})$-congruent number with respect to τ_{-1} : $\alpha = 78 + 58\sqrt{2}$ satisfies Definition 1 with $X = 3 + 4\sqrt{2}, Y = 20 + 12\sqrt{2}, Z = 21 + 12\sqrt{2}$ but $\tau_{-1}(\alpha) < 0$.

We study the congruence with respect to τ_1. The case τ_{-1} is similar.

In the classical (rational) case there are a few results leading to the statement of the Step1. We now state the analogues of some of them, their proofs being very similar to those in the rational case which may be found in [3].

Proposition 1 *$\alpha \in F^*$ is an F-congruent number $\Rightarrow \forall x \in F^*$, $x^2\alpha$ is an F-congruent number.*

Corollary 1 *Instead of studying the F-congruence of $\alpha \in F^*$ it suffices to study the F-congruence of $\alpha \in \mathcal{O}_F, \alpha > 0, \alpha$ square free, where $\mathcal{O}_F$ denotes the ring of integers of F.*

Let $E_\alpha(F)$ denote the elliptic curve $y^2 = x^3 - \alpha^2 x$ over F. Recall that $E_\alpha(F)$ is an abelian group and the null element is the point at infinity denoted O.

Proposition 2 *All the points of order 2 of $E_\alpha(F)$ are $\{(0,0),(\alpha,0),(-\alpha,0)\}$.*

Proposition 3 *If $\exists P \in E_\alpha(F)$ such that $2P \neq O$ then α is an F-congruent number.*

Remark 1 *If $P = (x_P, y_P) \in E_\alpha(F)$ the coordonates of $2P = (x_{2P}, y_{2P})$ are given by the same formulae as those in the rational case ([3], pp 34). It is a critical observation that $x_{2P} = (\frac{x_P^2+\alpha^2}{2y_P})^2$ is a square in F.*

Let us denote $F^2 = \{x^2, x \in F\}$.

Proposition 4 *The below two maps are inverse each other and they define bijections between the following two sets:*

$$S := \{(X,Y,Z) \in F \times F \times F\,,\, 0 < X < Y < Z\,,\, X^2 + Y^2 = Z^2, XY = 2\alpha\}$$

$$T := \{x \in F^*\,,\, x, x+\alpha, x-\alpha \in F^2\}$$

$$S \longrightarrow T\,,\, (X,Y,Z) \mapsto x = \frac{Z^2}{4}$$

$$T \longrightarrow S\,,\, x \mapsto (X = \sqrt{x+\alpha} - \sqrt{x-\alpha}, \sqrt{x+\alpha} + \sqrt{x-\alpha}, 2\sqrt{x})$$

The following proposition has a trivial analogue over rationals. Note that in totally real number fields we have plenty of squares which are square-free, namely the squares of units.

Proposition 5 *If α is not a square in F then there are no elements of order 4 in $E_\alpha(F)$.*

Proof: By contradiction if P has order 4 then $2P$ has order 2 and by applying Prop. 2 we get α is a square contradiction .□

3 Main result

In this section F denotes a totally real number field.

Proposition 6 *If $F/\mathbf{Q}$ is a Galois extension then*

$$\phi(|E_\alpha(F)_{tors}|) \leq 2[F:\mathbf{Q}]$$

where ϕ denotes the totient Euler function.

Proof:

Let us denote the points on the elliptic curve with projective coordinates (x, y, z) satisfying $y^2z = x^3 - n^2xz^2$ so that we may assume that $E_\alpha(F)_{tors} = E_\alpha(\mathcal{O}_F)_{tors}$. For any prime ideal P of $\mathcal{O}_F$ define the reduction mod P map as follows:

$$\psi_P : E_\alpha(F)_{tors} = E_\alpha(\mathcal{O}_F)_{tors} \longrightarrow E_\alpha(\mathcal{O}_F/P)_{tors}$$

$$(x, y, z) \mapsto (\bar{x}, \bar{y}, \bar{z})$$

Denote $Y = \{(p)$ prime ideal of $\mathbf{Z}$ such that $p \equiv 3(mod\, 4)$ and p splits completely in $\mathcal{O}_F\}$. For every $(p) \in Y$ fix P ideal of $\mathcal{O}_F$ dividing $p\mathcal{O}_F$ and denote $\psi_p = \psi_P$. Since p splits completely in $\mathcal{O}_F$ we have $\mathcal{O}_F/P = \mathbf{F}_p$. As in [3] pp 40-45 we obtain:

(1)$|E_\alpha(\mathbf{F}_p)_{tors}| = p + 1$

(2) $(\bar{x}_1, \bar{y}_1, \bar{z}_1) = (\bar{x}_2, \bar{y}_2, \bar{z}_2)$ iff P divides the $gcd(y_1z_2 - y_2z_1, x_2z_1 - x_1z_2, x_1y_2 - y_2x_1)$

(3) since only finitely many P's divide the above gcd, we conclude that ψ_p is injective for all but finitely many p's.

Denote $m = |E_\alpha(F)_{tors}|$. We proved that $p \equiv -1(mod\, m)$, $\forall (p) \in Y$ but finitely many.

Denote $A = \{p \in \mathbf{Z}, p \equiv -1(mod\, m)\}$. Let d be the density function as defined in [4]. Since A contains all the elements of Y but finitely many we have that $d(A) \geq d(Y)$. Now let $K = \mathbf{Q}(i)$. Since $F \cap K = \mathbf{Q}$ we obtain that $d(Y) = \frac{1}{2}\frac{1}{[F:\mathbf{Q}]}$ using cor(13.6) p. 547 from [4]. Finally, by applying the Dirichlet density theorem ([4]) we conclude $d(A) = \frac{1}{\phi(m)}$.□

Corollary 2 *If* $[F:\mathbf{Q}]=2$ *then* $|E_\alpha(F)_{tors}|\in\{4,8,12\}$.

Proof: It follows from Prop. 6 and Prop. 2 .□

Proposition 7 3 *does not divide* $|E_\alpha(F)_{tors}|$.

Proof: Since 3 is inert in $\mathbf{Q}[i]$ the associated elliptic curve is supersingular there. Looking at the representation of G_F on $E[3]$ one has two possibilities: either 3 is inert in F, in which case the representation is irreducible; or 3 splits in F, in which case the representation splits as $\chi\oplus\chi$ with χ a nontrivial character of G_F. In any way, no nonzero vector is fixed by G_F therefore there is no nonzero point of order 3 in $E_\alpha(F)_{tors}$.□

Corollary 3 *If* $[F:\mathbf{Q}]=2$ *and* α *is not a square in* F *then* $|E_\alpha(F)_{tors}|$=*4*.

Proof: It follows from Cor. 2, Prop. 5 Prop. 7 .□

Proposition 8 *If* $[F:\mathbf{Q}]=2$ *and* α *is not a square in* F *then the following are equivalent:*
(1) $E_\alpha(F)$ *has a point of infinite order;*
(2) $E_\alpha(F)$ *has a nonzero point of order distinct from* 2*;*
(3) α *is an* F*-congruent number.*

Proof.
(1) $\Rightarrow$ (2) is trivial;
(2) $\Rightarrow$ (3) follows from Prop. 3
(3) $\Rightarrow$ (1)

If α is an F-congruent number then by Prop. 4 one gets that $\exists x\in F^*\cap F^2$ such that $y:=\sqrt{x(x+\alpha)(x-\alpha)}\in F$ thus $(x,y)\in E_\alpha(F)$. We claim that (x,y) has infinite order. Assume by contradiction that $(x,y)\in E_\alpha(F)_{tors}$ which by Prop. 2 and Cor. 3 is $\{O,(0,0),(\alpha,0),(-\alpha,0)\}$. It follows that $\alpha=x\in F^2$ contradiction .□

References

[1] S. Achimescu, *Hilbert Modular Forms of weight 1/2*, Ph.D. thesis, 2004.

[2] S. Achimescu and A, Saha , *Hilbert Modular Forms of weight 1/2 and theta functions*, Journal of Number Theory, 2008.

[3] N. Koblitz, *Introduction to Elliptic Curves and Modular Forms*, Springer-Verlag, New York, 1984.

[4] J. Neukirch, *Algebraic Number Theory*, Springer, 1999.

[5] J.P. Serre and H.M. Stark, *Modular Forms of weight 1/2*, Modular functions of one variable VI, Lecture Notes on Mathematics, vol. 627, pp 27-68, Springer, Berlin Heidelberg New York 1977.

[6] J.B. Tunnel, *A classical Diophantine Problem and Modular Forms of Weight 3/2*, Inventiones mathematicae 72 pp 323-334, 1983.

[1] *Institute of Mathematics of the Romanian Academy,*
P.O. Box 1-764, Bucharest, Romania,
E-mail: sachimescu@yahoo.com