COLLOQUIUM MATHEMATICUM

VOL. 128 2012 NO. 2

CONGRUENT NUMBERS OVER REAL NUMBER FIELDS

BY

TOMASZ JĘDRZEJAK (Szczecin)

Abstract. It is classical that a natural number n is congruent iff the rank of $\mathbb{Q}$-points on $E_n : y^2 = x^3 - n^2x$ is positive. In this paper, following Tada (2001), we consider generalised congruent numbers. We extend the above classical criterion to several infinite families of real number fields.

1. Introduction. A positive integer n is called a *congruent number* if it is the area of a right triangle all of whose sides have rational lengths, i.e. if there are positive rationals a, b, c with

$$a^2 + b^2 = c^2 \quad \text{and} \quad ab = 2n. \tag{1}$$

Without loss of generality we may (and will) assume that n is squarefree. The problem of determining whether or not a given positive integer is a congruent number is very old. Thanks to Euclid's characterization of the Pythagorean triples it is easy to decide whether there exists a right triangle of given area and integer sides. However, the case of rational sides, called the congruent number problem, is not completely understood. Immediately we can see that 6 is a congruent number. Fibonacci showed that also 5 is a congruent number (one may take $a = 3/2$, $b = 20/3$, $c = 41/6$). Fermat found that 1, 2 and 3 are not congruent numbers.

In the spirit of Euclid's proof of the infinitude of prime numbers, one can also show that there are infinitely many (squarefree) congruent numbers. Chahal [Ch] established that the residue classes of $1, 2, 3, 5, 6, 7$ modulo 8 contain infinitely many congruent numbers. Bennett [Be] extended this result by showing that if k and m are positive integers such that $\gcd(k, m)$ is squarefree then the residue class of a modulo m contains infinitely many congruent numbers. Next Rajan and Ramaroson [RR] proved that if k and m are positive, squarefree, coprime integers then there exist infinitely many squarefree integers n such that both nk and nm are congruent numbers.

There is a fruitful translation of the congruent number problem into the language of elliptic curves (see Koblitz [Ko] for details). If n is a congruent

2010 *Mathematics Subject Classification*: Primary 11G05; Secondary 14H52.
Key words and phrases: congruent numbers, elliptic curves, number fields.

DOI: 10.4064/cm128-2-3

number then it follows from (1) that there exist three rational squares in arithmetic progression of common difference n, namely $x-n, x, x+n$ where $x = c^2/4$. Therefore we obtain the rational point $(c^2/4, c(a^2-b^2)/8)$ on the elliptic curve

$$E_n : y^2 = x^3 - n^2 x. \tag{2}$$

Conversely, given a rational point (x, y) on E_n with $y \neq 0$, one may take

$$a = \left|\frac{y}{x}\right|, \quad b = 2n\left|\frac{x}{y}\right|, \quad c = \frac{x^2+n^2}{|y|} \tag{3}$$

to obtain a right triangle with rational sides a, b, c and area n.

The rational points (x, y) with $y \neq 0$ have infinite order in the Mordell–Weil group $E_n(\mathbb{Q})$, since it is well known that its torsion subgroup consists only of points of order 2, namely $(0,0), (\pm n, 0)$, and the point at infinity ∞. This is the key point in the proof of the following criterion.

Criterion 0. *A positive integer n is a congruent number if and only if $E_n(\mathbb{Q})$ has a point of infinite order.*

From this one can deduce the fact (already known to Fermat) that for a given congruent number n there are infinitely many right triangles with rational sides a, b, c satisfying (1), since scalar multiplication of that point in the Mordell–Weil group $E_n(\mathbb{Q})$ yields new right triangles of area n.

Note that the correspondence between rational points on E_n and right triangles with rational sides is not bijective. Solving (3) for x and y with given a, b and c gives the two points

$$x = \frac{1}{2}a(a \pm c), \quad y = ax. \tag{4}$$

The congruent number problem has been solved almost completely by Tunnell [Tu] who gave a simple equivalence criterion, which however, depends on the truth of a weak form of the Birch and Swinnerton-Dyer conjecture for the family of elliptic curves $E_n : y^2 = x^3 - n^2 x$ (the conjecture has been checked by Nemenzo [Ne] for $n < 42553$). More precisely, Tunnell showed that if n is an odd congruent number then

$$\#\{x, y, z \in \mathbb{Z} : 2x^2 + y^2 + 8z^2 = n\} = 2\#\{x, y, z \in \mathbb{Z} : 2x^2 + y^2 + 32z^2 = n\},$$

and the converse is also true provided the Birch and Swinnerton-Dyer conjecture for the family E_n holds (i.e. the rank of the elliptic curve E_n is positive if and only if the associated L-function vanishes at the central point 1). He gave a similar criterion when n is even.

If n is not a congruent number, one can ask if n is the area of a right triangle with three sides in some number field. This leads to the following natural generalization:

Definition 1. We say that a positive integer n is a *congruent number over a number field* K (or for short, a K*-congruent number*) if there exist $a, b, c \in K$ such that (1) holds.

The idea to study the congruent number problem over algebraic extensions dates back at least to Tada [Ta] who considered real quadratic fields. Note that when K is a subfield of $\mathbb{R}$ the geometric interpretation still holds. Also other generalizations are possible. For example Fujiwara [Fu] extended the concept of congruent numbers by considering not necessarily right triangles with rational sides and an angle θ (so called θ-congruent numbers). However this generalization is not a topic of our paper.

It is easy to see that, for instance, 1 is a congruent number over $\mathbb{Q}\left(\sqrt{2}\right)$ (one may take $a = b = \sqrt{2}$, $c = 2$). But equations (4) lead to the points $\left(1 \pm \sqrt{2}, 2 \pm \sqrt{2}\right)$ which are all torsion points in $E_1\left(\mathbb{Q}\left(\sqrt{2}\right)\right)$. Therefore we do not get infinitely many different right triangles from these points. This example motivates the following definition:

Definition 2. We say that a positive integer n is a *properly* K*-congruent number* if (1) has infinitely many solutions $a, b, c \in K$.

In this paper we give infinite families of real number fields K for which all K-congruent numbers are properly K-congruent. Of course all $\mathbb{Q}$-congruent numbers are properly $\mathbb{Q}$-congruent. Note that n is properly K-congruent if and only if $E_n(K)$ has a point of infinite order. Hence we also obtain a variant of Criterion 0 for such fields.

2. Congruent numbers over number fields of type $(2, \dots, 2)$**.** For a number field K let $T_n(K)$ denote the group of K-rational torsion points of E_n defined in (2), with $n \in \mathbb{N}$ squarefree. It is well known that $T_n(\mathbb{Q}) = E_n[2] = \{\infty, (0,0), (\pm n, 0)\}$.

Let $K_{2,d}$ denote the real number field of type $(2, \dots, 2)$, i.e. $K_{2,d} = \mathbb{Q}(\sqrt{m_1}, \dots, \sqrt{m_d})$, m_i positive integers. Without loss of generality we may assume that $[K_{2,d} : \mathbb{Q}] = 2^d$, m_i are squarefree ($1 \le i \le d$) and no m_i, divides any other. Tada [Ta, Theorem 1] showed that n is $\mathbb{Q}(\sqrt{m})$-congruent (where $m \neq 2$) if and only if $E_n(\mathbb{Q}(\sqrt{m}))$ has a point of infinite order. We have the following generalizations of this (and of Criterion 0).

Theorem 1. *Assume that* $\sqrt{2} \notin K_{2,d}$*. Then* n *is a congruent number over* $K_{2,d}$ *if and only if* $E_n(K_{2,d})$ *has a point of infinite order.*

Remark 2. It is easy to see that the above assumption is satisfied if all m_i are odd. Moreover it is easy to check that $\sqrt{2} \notin K_{2,2}$ if and only if $m_1 \neq 2$ and $m_2 \neq 2$.

The proof of Theorem 1 is divided into a few lemmas.

Lemma 3. *For every subfield K of $\mathbb{R}$ a positive integer n is a congruent number over K if and only if $E_n(K) \setminus E_n[2] \neq \emptyset$.*

Proof. This is a well known result. See, for instance, the beginning of the proof of Theorem 1 in [Ta]. ■

Lemma 4. *Assume that $T_n(K) = E_n[2]$. Then n is a congruent number over K if and only if $E_n(K)$ has a point of infinite order.*

Proof. This follows easily from Lemma 3. ■

Therefore, it is important to know $T_n(K)$ for fields mentioned in Theorem 1. For example, the assumptions of Lemma 4 are satisfied for $K = \mathbb{Q}(\sqrt{m})$ for squarefree integers $m > 2$ (see [Ta]). The next lemma generalizes this result.

Lemma 5. *If $\sqrt{2} \notin K_{2,d}$ then $T_n(K_{2,d}) = E_n[2]$.*

Proof. Observe that the quadratic twist $E_n^m : y^2 = x^3 - m^2n^2x$ of the curve E_n is isomorphic (over $\mathbb{Q}$) to E_{mn}. Therefore $E_n^m(\mathbb{Q})_{\mathrm{tors}} = T_{mn}(\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$. Then from [QZ, remark after Theorem 2 and Lemma 3] we know that $T_n(K_{2,d})$ is a 2-group, i.e. has no point of an odd order. Hence to finish the proof we must show that $T_n(K_{2,d})$ has no point of order 4. It is clear that $P \in E_n(K_{2,d})$ is of order 4 if and only if $2P = (0,0), (n,0)$ or $(-n,0)$. By [Kn, Theorem 4.2, p. 85] we have the following cases to consider:

(a) $2P = (0,0) \Leftrightarrow -n$ and n are perfect squares in $K_{2,d}$,
(b) $2P = (n,0) \Leftrightarrow n$ and $2n$ are perfect squares in $K_{2,d}$,
(c) $2P = (-n,0) \Leftrightarrow -n$ and $-2n$ are perfect squares in $K_{2,d}$.

In cases (a) and (c) we have $\sqrt{-n} \in K_{2,d}$ for some positive integer n, which is impossible because $K_{2,d} \subset \mathbb{R}$. In case (b) we conclude that $\sqrt{2}$ belongs to $K_{2,d}$, and the assertion follows. ■

Proof of Theorem 1. This follows immediately from Lemmas 4 and 5. ■

Corollary 6. *Assume that $\sqrt{2} \notin K_{2,d}$. Then n is a congruent number over $K_{2,d}$ if and only if at least one of the 2^d numbers $nm_1^{e_1} \cdots m_d^{e_d}$ $(e_i = 0,1)$ is a congruent number over $\mathbb{Q}$.*

To prove this corollary we need the following proposition.

Proposition 7 (Theorem B in [Ta]). *Assume that E is an elliptic curve over a number field k and $D \in k \setminus k^2$. Then*

$$\mathrm{rank}(E(k(\sqrt{D}))) = \mathrm{rank}(E(k)) + \mathrm{rank}(E^D(k)),$$

where E^D is the twist of E over $k(\sqrt{D})$.

Proof. See for example [Se, p. 63]. ■

Proof of Corollary 6. By easy induction, from Proposition 7 and the first sentence of the proof of Lemma 5 we conclude that

$$\operatorname{rank}(E_n(K_{2,d})) = \sum \operatorname{rank}(E_{nm_1^{e_1}\cdots m_d^{e_d}}(\mathbb{Q})),$$

where summation is over all d-tuples $e_i \in \{0,1\}$, $i = 1,\dots,d$. By Theorem 1 we know that n is a congruent number over $K_{2,d} \Leftrightarrow \operatorname{rank}(E_n(K_{2,d})) > 0$. Hence in particular at least one summand in this sum is positive. Using Criterion 0 we are done. ∎

REMARK 8. From Tunnell's criterion ([Tu]) it follows, in particular, that any squarefree $n \equiv 5,6,7 \pmod 8$ is conditionally a congruent number over $\mathbb{Q}$. Corollary 6 then implies that, conjecturally, every odd positive integer is a congruent number over $\mathbb{Q}(\sqrt{5})$ and every even positive integer is a congruent number over $\mathbb{Q}(\sqrt{3})$. Therefore, hypothetically every squarefree positive integer is a congruent number over $\mathbb{Q}(\sqrt{3},\sqrt{5})$.

COROLLARY 9. *Assume that $\sqrt{2} \notin K_{2,d}$. If n is a congruent number over $K_{2,d}$, then n is a congruent number over $\mathbb{Q}$ or over some real quadratic subfield $\mathbb{Q}(\sqrt{m_1^{e_1}\cdots m_d^{e_d}}) \subset K_{2,d}$.*

Proof. This follows easily from Corollary 6. ∎

REMARK 10. Any positive integer n is a congruent number over the field $\mathbb{Q}(\sqrt{2},\sqrt{n})$. Indeed, it is enough to take $a = b = \sqrt{2n}$ and $c = 2\sqrt{n}$. Then equations (4) lead to the points $P = (n(1\pm\sqrt{2}), n\sqrt{2n}(1\pm\sqrt{2})) \in E_n(\mathbb{Q}(\sqrt{2},\sqrt{n}))$ such that $2P = (n,0)$. Taking an odd n such that neither n nor $2n$ are congruent numbers over $\mathbb{Q}$ (e.g. $n = 1, 33$) we see that the assumption $\sqrt{2} \notin K_{2,d}$ in Theorem 1 and in Corollaries 6 and 9 is necessary. In particular such an n is not properly $\mathbb{Q}(\sqrt{2},\sqrt{n})$-congruent.

3. Congruent numbers over other real number fields. Now we consider real number fields of degree $\neq 2^d$ (or $= 4$). We obtain the following counterpart of Theorem 1.

THEOREM 11. *Let $K \subset \mathbb{R}$ be a number field such that $\sqrt{2},\sqrt{3},\sqrt{5} \notin K$. Suppose that $[K:\mathbb{Q}]$ is odd or $[K:\mathbb{Q}] = 2p$, where p is a prime. Then n is a congruent number over K if and only if $E_n(K)$ has a point of infinite order.*

To prove Theorem 11 we require a bound on the torsion subgroup of $E_n(K)$. We write down the following two general results about torsion of CM elliptic curves.

THEOREM 12 (SPY-bounds). *Let E be an elliptic curve over a number field K of degree d with CM by an order O in an imaginary quadratic field L.*

Let $P \in E(K)$ be a point of order N, let M be the order of the torsion subgroup of $E(K)$ and μ be the number of roots of unity in O. Then

(i) $\varphi(N) \le (\mu/2)d$ *if* $L \subset K$,
(ii) $\varphi(M) \le 2d$ *if* $K \cap L = \mathbb{Q}$,

where φ denotes Euler's totient function.

Proof. See the papers of Silverberg [Si] or Prasad and Yogananda [PY]. ∎

THEOREM 13. *With the above notation and assumptions suppose furthermore that O is a maximal order in $L = \mathbb{Q}(\sqrt{D})$, $K \cap L = \mathbb{Q}$ and N is an odd prime. Then be the number of roots of unity in O. Then*

(i) *if* $\left(\frac{D}{N}\right) = 1$, *then* $(N-1)\frac{2h(L)}{\mu} \mid d$,
(ii) *if* $\left(\frac{D}{N}\right) = 0$, *then* $(N-1)\frac{h(L)}{\mu} \mid d$,
(iii) *if* $\left(\frac{D}{N}\right) = -1$, *then* $(N^2-1)\frac{h(L)}{\mu} \mid d$,

where $h(L)$ is the class number of L.

Proof. See [CCS, Theorem 2]. ∎

LEMMA 14. *If a number field $K \subset \mathbb{R}$ satisfies the assumptions of Theorem 11 then $T_n(K) = E_n[2]$.*

Proof. Let $[K : \mathbb{Q}] = s$. It is obvious that the curve E_n has complex multiplication by $\mathbb{Z}[i]$. From Theorem 12 we get $\varphi(\#T_n(K)) \le 2[K : \mathbb{Q}] = 2s$. Since $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \subset T_n(K)$ we have $T_n(K) \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2N\mathbb{Z}$ for some positive integer N. Next for any squarefree positive integer $n > 1$ we have $\sqrt{-n}, \sqrt{2} \notin K$, hence (see the proof of Lemma 5) $T_n(K)$ has no point of order 4. Therefore N is odd and we obtain $\varphi(N) \le s$. Thus in order to finish the proof it will be sufficient to check that $T_n(K)$ has no point of order N, where N is an odd prime $\le s+1$.

Now we use Theorem 13 which in some cases refines SPY-bounds. Assume that $T_n(K)$ has a point of an odd prime order $N \le s+1$. Then $N \equiv 1 \pmod 4$ implies $\frac{N-1}{2} \mid s$, and $N \equiv 3 \pmod 4$ implies $\frac{N^2-1}{4} \mid s$. In either case, we have a contradiction if s is odd. Hence we can assume that $s = 2p$.

Let $N \equiv 1 \pmod 4$. Note that $\frac{N-1}{2} \mid 2p$ if and only if $N = 5$. Similarly for $N \equiv 3 \pmod 4$ we have $\frac{N^2-1}{4} \mid 2p$ if and only if $N = 3$. Hence it will be sufficient to consider $N = 3, 5$.

If $P \in E_n(K)$ has an odd order N, then $x\big(\big[\frac{N+1}{2}\big]P\big) = x\big(\big[-\frac{N-1}{2}\big]P\big)$. So using the group law formulas we obtain homogeneous polynomial equations $F_N(x,n) = 0$ (for $N = 3, 5$) where

$$F_3(x,n) = n^4 + 6n^2x^2 - 3x^4,$$

$$F_5(x,n) = n^{12} + 50n^{10}x^2 - 125n^8x^4 + 300n^6x^6 - 105n^4x^8 - 62n^2x^{10} + 5x^{12}$$

(we have used Mathematica for symbolic computations). Let $f_N(x) := F_N(x,1)$ be the dehomogenization of $F_N(x,n)$. We find that $\pm\sqrt{(3+2\sqrt{3})/3}$ are all real roots of polynomials f_3 and check that if $\sqrt{3} \notin K$ then f_3 has no roots in K. Similarly we can compute all real roots of f_5 and check that they do not belong to K if $\sqrt{5} \notin K$. The assertion follows. ∎

Proof of Theorem 11. This follows immediately from Lemmas 4 and 14. ∎

COROLLARY 15. *If a real number field K satisfies the assumptions of Theorems* 1 *or* 11 *then a number n is K-congruent if and only if n is properly K-congruent.*

Proof. For such fields K a number n is K-congruent if and only if $\mathrm{rank}(E_n(K)) > 0$. The correspondence between K-rational points on E_n and right triangles with sides in K (cf. (3)) finishes the proof. ∎

QUESTIONS. 1) One can ask whether there exists a real number field F such that any $n \in \mathbb{N}$ is a congruent number over F. Such a field must have the following property: for every $n \in \mathbb{N}$ either the group $T_n(F)$ is strictly larger than $E_n[2]$ or $\mathrm{rank}(E_n(F)) > 0$. Of course the field $F = \mathbb{Q}(\sqrt{n} : n \in \mathbb{N})$ has the desired property unconditionally but $[F : \mathbb{Q}] = \infty$. Hypothetically, we may take $F = \mathbb{Q}(\sqrt{3}, \sqrt{5})$ (see Remark 8).

2) One can ask whether for any positive integer d there exists a number field F of degree d over $\mathbb{Q}$ such that $T_n(F) = E_n[2]$ for all squarefree n. We have proved that the answer is positive when d is a power of 2 or an odd number or $d = 2p$, where p is a prime.

3) In [GGGSS] it is proved that any number n is properly congruent over some real quadratic and some real cubic field. One can ask whether for a given positive integer d every $n \in \mathbb{N}$ is properly congruent over some real field of degree d.

4) It would be of interest to characterize all real number fields with the property given in Corollary 15.

Acknowledgements. I would like to thank Andrzej Dąbrowski for helpful conversations and suggestions.

REFERENCES

[Be] M. A. Bennett, *Lucas' square pyramid problem revisited*, Acta Arith. 105 (2002), 341–347.

[Ch] J. S. Chahal, *On the identity of Desboves*, Proc. Japan Acad. Ser. A Math. Sci. 60 (1984), 105–108.

[CCS] P. Clark, B. Cook and J. Stankiewicz, *Torsion points on elliptic curves with complex multiplication*, Int. J. Number Theory, to appear; http://math.uga.edu/~pete/torspaper.pdf.

[Fu] M. Fujiwara, *θ-congruent numbers*, in: Number Theory, de Gruyter, 1997, 235–241.

[GGGSS] E. Girondo, G. González-Diez, E. González-Jiménez, R. Steuding and J. Steuding, *Right triangles with algebraic sides and elliptic curves over number fields*, Math. Slovaca 59 (2009), 299–306.

[Kn] A. Knapp, *Elliptic Curves*, Math. Notes 40, Princeton Univ. Press, NJ, 1992.

[Ko] N. Koblitz, *Introduction to Elliptic Curves and Modular Forms*, Grad. Texts in Math. 97, Springer, New York, 1984.

[Ne] F. R. Nemenzo, *All congruent numbers less than* 40000, Proc. Japan. Acad. Ser. A Math. Sci. 74 (1998), 144–162.

[PY] D. Prasad and C. S. Yogananda, *Bounding the torsion in CM elliptic curves*, C. R. Math. Rep. Acad. Sci. Canada 23 (2001), 1–5.

[QZ] D. Qui and X. Zhang, *Elliptic curves and their torsion subgroups over number fields of type* $(2, 2, \ldots, 2)$, Sci. China 44 (2001), 159–167.

[RR] A. Rajan and F. Ramaroson, *Ratios of congruent numbers*, Acta Arith. 128 (2007), 101–106.

[Se] P. Serf, *The rank of elliptic curves over real quadratic number fields of class number 1*, PhD Thesis, Univ. Saarbrücken, 1995.

[Si] A. Silverberg, *Points of finite order on abelian varieties*, in: Contemp. Math. 133, Amer. Math. Soc., 1992, 175–193.

[Ta] M. Tada, *Congruent numbers over real quadratic fields*, Hiroshima Math. J. 31 (2001), 331–343.

[Tu] J. Tunnell, *A classical Diophantine problem and modular forms of weight* 3/2, Invent. Math. 72 (1983), 323–334.

Tomasz Jędrzejak
Institute of Mathematics
University of Szczecin
Wielkopolska 15
70-451 Szczecin, Poland
E-mail: tjedrzejak@gmail.com

Received 21 November 2011;
revised 28 August 2012 (5577)