RIGHT TRIANGLES WITH ALGEBRAIC SIDES AND ELLIPTIC CURVES OVER NUMBER FIELDS

E. Girondo* ** — G. González-Diez* — E. González-Jiménez* ** — R. Steuding*** — J. Steuding***

(*Communicated by Stanislav Jakubec*)

ABSTRACT. Given any positive integer n, we prove the existence of infinitely many right triangles with area n and side lengths in certain number fields. This generalizes the famous congruent number problem. The proof allows the explicit construction of these triangles; for this purpose we find for any positive integer n an explicit cubic number field $\mathbb{Q}(\lambda)$ (depending on n) and an explicit point P_λ of infinite order in the Mordell-Weil group of the elliptic curve $Y^2 = X^3 - n^2 X$ over $\mathbb{Q}(\lambda)$.

1. Congruent numbers over the rationals

A positive integer n is called a congruent number if there exists a right triangle with rational sides and area equal to n, i.e., there exist $a, b, c \in \mathbb{Q}^*$ with

$$a^2 + b^2 = c^2 \qquad \text{and} \qquad \tfrac{1}{2}ab = n. \qquad (1)$$

It is easy to decide whether there is a right triangle of given area and integral sides (thanks to Euclid's characterization of the Pythagorean triples). The case of rational sides, known as the congruent number problem, is not completely

Springer

understood. Fibonacci showed that 5 is a congruent number (since one may take $a = \frac{3}{2}$, $b = \frac{20}{3}$ and $c = \frac{41}{6}$). Fermat found that 1, 2 and 3 are not congruent numbers. Hence, there is no perfect square amongst the congruent numbers since otherwise the corresponding rational triangle would be similar to one with area equal to 1. By the same reason one can restrict to square-free positive integers, a condition we will assume in the sequel.

There is a fruitful translation of the congruent number problem into the language of elliptic curves. Suppose n is a congruent number. It follows from (1) that there exist three squares in arithmetic progression of distance n, namely $x - n, x, x + n$, where $x = c^2/4$. Therefore their product $(x - n)x(x + n)$ is again a rational square. In other words, a right triangle of area n and rational sides a, b, c corresponds to the rational point $(c^2/4, c(a^2 - b^2)/8)$ on the elliptic curve

$$E_n : \ Y^2 = X^3 - n^2 X.$$

Conversely, given a rational point (x, y) on E_n such that $y \neq 0$, one may define

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

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

Therefore, n is a congruent number if and only if the elliptic curve E_n has a rational point with non-vanishing y-coordinate. The correspondence between rational points on E_n and right triangles with rational sides and area n is not bijective. For instance, solving x and y with respect to a, b and c in equation (2) gives the two points

$$x = \frac{1}{2} a(a \pm c), \qquad y = ax. \tag{3}$$

The points (x, y) with $y \neq 0$ have infinite order in the Mordell-Weil group $E_n(\mathbb{Q})$, since it is known (see [6]) that the torsion subgroup of $E_n(\mathbb{Q})$ consists only of points of order 2, that are $(0, 0)$, $(\pm n, 0)$, and the point at infinity. From this one can deduce the fact, already known to Fermat, that there are in fact infinitely many right triangles with rational sides a, b, c verifying equation (1) for a given congruent number n, since scalar multiplication of the points corresponding to (3) on E_n yields new right triangles of area n.

T u n n e l l [8] found an intruiging approach towards the congruent number problem. He showed that if n is an odd square-free congruent number then

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

and that the converse implication is also true provided the yet unsolved Birch & Swinnerton-Dyer conjecture holds (i.e., the rank of an elliptic curve E is positive if and only if the associated L-function vanishes at the central point: $L(E, 1) = 0$). A similar criterion exists when n is even. This conjectural equivalent statement for the congruent number problem in terms of the number of representations of n by certain ternary quadratic forms allows to determine by computation whether a given integer n is congruent or not.

2. Congruent numbers over number fields

A natural generalization of the congruent number problem is to allow the sides of the triangles to belong to an algebraic number field. The idea to study the congruent number problem over algebraic extensions dates back at least to T a d a [7] who considered real quadratic fields.

DEFINITION 1. Let $\mathbb{K}$ be a number field and let n be a positive integer. We say that n is a $\mathbb{K}$-*congruent number* if there exist $a, b, c \in \mathbb{K}$ such that (1) holds.

Note that $\mathbb{Q}$-congruent numbers are nothing but the usual congruent numbers. When $\mathbb{K}$ is a subfield of $\mathbb{R}$ the geometric meaning still holds, since n being $\mathbb{K}$-congruent implies the existence of a right triangle with real sides in $\mathbb{K}$ and area equal to n.

It is easy to see that any positive integer n is a congruent number for some quadratic extension of $\mathbb{Q}$. For instance, $a = b = \sqrt{2}$ yields a right triangle with area equal to $n = 1$. However, equation (3) leads to the points $(1 \pm \sqrt{2}, \sqrt{2} \pm 2)$ on the curve E_1 which are all torsion points over $\mathbb{Q}(\sqrt{2})$. 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 $\mathbb{K}$-congruent number n is *properly $\mathbb{K}$-congruent* if (1) has infinitely many solutions $a, b, c \in \mathbb{K}$.

This definition is not interesting for $\mathbb{K} = \mathbb{Q}$, since all $\mathbb{Q}$-congruent numbers are properly $\mathbb{Q}$-congruent. But the example above shows that things may be different over number fields.

2.1. Congruent numbers over quadratic fields

THEOREM 1. *Every positive integer n is properly $\mathbb{K}$-congruent over some real quadratic field $\mathbb{K}$.*

P r o o f. Consider the system

$$\begin{cases} a^2 + b^2 = c^2\,, \\ \qquad ab = 2n\,. \end{cases}$$

Substituting a by $2n/b$ in the first equation yields

$$4n^2 + b^4 = c^2 b^2.$$

Therefore

$$c = \frac{\sqrt{4n^2 + b^4}}{b}.$$

It follows that n is congruent over $\mathbb{Q}(\sqrt{m})$, where $m = 4n^2 + b^4$ (and b is any chosen rational point).

Given such a triple $(a, b, c) \in \mathbb{Q}(\sqrt{m})^3$, the corresponding $\mathbb{Q}(\sqrt{m})$-rational point P on the curve E_n is given by (3). It is known (see [7], [3]) that the torsion subgroup of $E_n(\mathbb{Q}(\sqrt{m}))$ reduces to the 2-torsion, namely $\{\infty, (0,0), (\pm n, 0)\}$, except for the cases $(n, m) = (1, 2)$ or $(n, m) = (2, 2)$.

We can choose $b \in \mathbb{Q}$ such that $m \neq 2$, and therefore P is a non-torsion point. This finishes the proof. $\qquad\square$

Remark 2. T a d a [7] showed that if n is not $\mathbb{Q}$-congruent, then it is congruent over $\mathbb{Q}(\sqrt{m})$ if and only if nm is $\mathbb{Q}$-congruent. This fact has applications of the following kind.

Since it is known that 1 and 11 are not $\mathbb{Q}$-congruent numbers, it follows that 1 is not $\mathbb{Q}(\sqrt{11})$-congruent. According to the proof above, $4n^2 + b^4 = 4 + b^4$ cannot be of the form $11 \cdot d^2$ with $d \in \mathbb{Q}$ for any choice of $b \in \mathbb{Q}$. That is, the genus 1 curve

$$11y^2 = x^4 + 4$$

is not an elliptic curve over $\mathbb{Q}$, i.e. it has no nonsingular $\mathbb{Q}$-rational point.

The same argument applied to a general pair $n, m \in \mathbb{Z}^*$ leads to the following generalization. Denote by $C_{n,m}$ the genus 1 curve $C_{n,m} : \ my^2 = x^4 + 4n^2$. Then this curve has a $\mathbb{Q}$-rational point if and only if n is $\mathbb{Q}(\sqrt{m})$-congruent, or equivalently, if and only if nm is $\mathbb{Q}$-congruent.

Note that the curve $C_{n,m}$ is the twist by m of the curve $C_{n,1} : \ y^2 = x^4 + 4n^2$, that is another parametrization of the congruent number problem.

2.2. Congruent numbers over cubic fields

Next we shall construct an explicit non-torsion point on E_n over certain cubic fields (depending on n).

Theorem 3. *Every positive integer n is properly congruent over some real cubic field. More precisely, for a positive integer n let $\lambda = \lambda(n)$ be the unique real solution of the cubic equation*

$$32\lambda^3 - 32\lambda^2 + 8\lambda + n^2 = 0.$$

Then the point $P_\lambda = (x_\lambda, y_\lambda)$ with coordinates given by (6) and (7) below is of infinite order in the Mordell-Weil group of the elliptic curve $Y^2 = X^3 - n^2 X$ over $\mathbb{Q}(\lambda)$.

P r o o f. We use an idea of C h a h a l [1]. Starting from an old identity of D e s b o v e s [2],

$$(\mathscr{Y}^2 + 2\mathscr{X}\mathscr{Y} - \mathscr{X}^2)^4 + (2\mathscr{X}^3\mathscr{Y} + \mathscr{X}^2\mathscr{Y}^2)(2\mathscr{X} + 2\mathscr{Y})^4$$
$$= (\mathscr{X}^4 + \mathscr{Y}^4 + 10\mathscr{X}^2\mathscr{Y}^2 + 4\mathscr{X}\mathscr{Y}^3 + 12\mathscr{X}^3\mathscr{Y})^2,$$

the substitution $\mathscr{X} = 1 - 2\lambda$, $\mathscr{Y} = 4\lambda$ yields

$$(1 - 12\lambda + 4\lambda^2)^4 + 8\lambda(2\lambda - 1)^2(2(1 + 2\lambda))^4$$
$$= (1 + 40\lambda - 104\lambda^2 + 160\lambda^3 + 16\lambda^4)^2.$$

This gives the point (x, y) with coordinates

$$x \quad = \quad x(\lambda) = \frac{(1 - 12\lambda + 4\lambda^2)^2}{4(1 + 2\lambda)^2}, \tag{4}$$

$$y \quad = \quad y(\lambda) = \frac{(1 - 12\lambda + 4\lambda^2)(1 + 40\lambda - 104\lambda^2 + 160\lambda^3 + 16\lambda^4)}{8(1 + 2\lambda)^3} \tag{5}$$

on the elliptic curve $y^2 = x^3 + dx$, where $d = d(\lambda) = 8\lambda(2\lambda - 1)^2$. Now let n be a positive integer and consider the equation $-n^2 = 8\lambda(2\lambda - 1)^2$. It is easy to see that there is a unique real solution, explicitly given by

$$\lambda = \lambda(n) = \frac{1}{3} + \frac{1}{12}\kappa + \frac{1}{3\kappa},$$

where

$$\kappa = \kappa(n) = \sqrt[3]{-8 - 27n^2 + 3\sqrt{48n^2 + 81n^4}}.$$

303

Here we choose κ as the unique real third root which is negative for all n. By computation, we obtain a point $P_\lambda = (x_\lambda, y_\lambda)$ on $E_n(\mathbb{Q}(\lambda))$, where the coordinates are given by

$$
\begin{aligned}
x = x_\lambda \;=\;\; & \frac{1}{4(n^2-16)^2}\big\{256 + 992n^2 + 65n^4 + (1024 - 2688n^2 - 28n^4)\lambda \\
& + (1024 + 1920n^2 + 4n^4)\lambda^2\big\}, \hspace{4cm} (6)
\end{aligned}
$$

$$
\begin{aligned}
y = y_\lambda \;=\;\; & \frac{1}{32(n^2-16)^3}\big\{-16384 + 72704n^2 + 80960n^4 + 2868n^6 - n^8 \\
& + (196608 - 462848n^2 - 145152n^4 - 1456n^6)\lambda \hspace{1.5cm} (7) \\
& + (196608 + 421888n^2 + 100608n^4 + 208n^6)\lambda^2\big\}.
\end{aligned}
$$

This can be checked by use of a computer algebra package or by hand computation as follows: firstly, multiply the numerator and denominator of the coordinates (4) and (5) by the conjugates of $(1 + 2\lambda)^2$ and $(1 + 2\lambda)^3$, respectively, then the coordinates are given as rational polynomials in the variable λ; secondly, since $\mathbb{Q}(\lambda)$ is a cubic field, these polynomials turn out to have degree at most two, which yields (6) and (7).

It remains to show that the point P_λ has infinite order on $E_n(\mathbb{Q}(\lambda))$. Note that the map that sends (x, y) to $\big(-x, \sqrt{-1}y\big)$ is an endomorphism on the elliptic curve E_n, hence E_n has complex multiplication by $\mathbb{Z}\big[\sqrt{-1}\big]$. There are bounds [4], [5] for the order of the subgroup of torsion points on a elliptic curve with complex multiplication defined over a number field. Applying these results to the elliptic curve E_n over the cubic number field $\mathbb{Q}(\lambda)$ we obtain that if M is the order of a torsion point of $E_n(\mathbb{Q}(\lambda))$, then $\phi(M) \le 6$, where ϕ is Euler's ϕ-function. Therefore $M \in \mathscr{B} = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12, 14, 18\}$. Hence it is sufficient to prove that the order of P_λ is not in $\mathscr{B}$. For this purpose we use the m-division polynomial $\Psi_m(x)$ associated with the elliptic curve E_n. It suffices to check that x_λ is not a root of $\Psi_m(x)$ for $m \in \mathscr{B}$ over $\mathbb{Q}(\lambda)$. We have

$$
\Psi_m(x_\lambda) = P_{0,m}(n) + P_{1,m}(n)\lambda + P_{2,m}(n)\lambda^2,
$$

where $P_{k,m} \in \mathbb{Q}[n]$ has no integer roots for $k = 0, 1, 2$ and $m \in \mathscr{B}$. Thus $\Psi_m(x_\lambda) \ne 0$ for any integer n and $m \in \mathscr{B}$. This proves that $P_{\lambda(n)}$ has infinite order and so the Mordell-Weil group of $E_n(\mathbb{Q}(\lambda(n)))$ has positive rank. The theorem is proved. $\qquad\square$

2.2.1. An example

The integer $n = 1$ is a congruent number over the cubic field $\mathbb{Q}(\alpha)$, where

$$\alpha = \frac{1}{3} + \frac{1}{12}\sqrt[3]{-35 + 3\sqrt{129}} + \frac{1}{3\sqrt[3]{-35 + 3\sqrt{129}}}.$$

The following picture shows a right triangle with area 1 and sides in $\mathbb{Q}(\alpha)$:
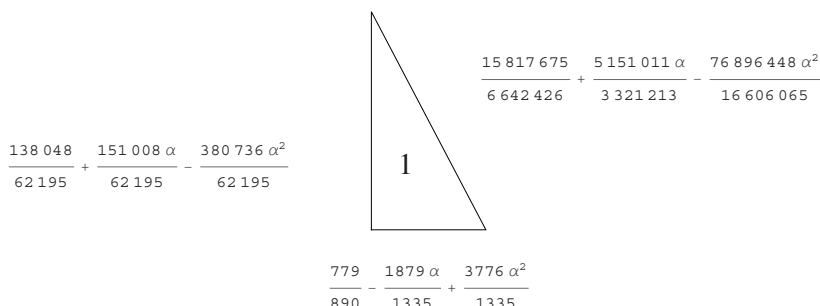
We conclude with an interesting but difficult question:

Given a number field $\mathbb{K}$, what are the congruent numbers over $\mathbb{K}$?

REFERENCES

[1] CHAHAL, J. S.: *Congruent numbers and elliptic curves*, Amer. Math. Monthly **113** (2006), 308–317.

[2] DESBOVES, A.: *Sur l'emploi des identités algébriques dans la résolution, en nombres entiers, des équations d'un degré supérieur au second*, Comptes Rendus **LXXXVII** (1879), 159–161, 321-322.

[3] KWON, S.: *Torsion subgroups of elliptic curves over quadratic extensions*, J. Number Theory **62** (1997), 144–162.

[4] PRASAD, D.—YOGANANDA, C. S.: *Bounding the torsion in CM elliptic curves*, C. R. Math. Acad. Sci. Soc. R. Can. **23** (2001), 1–5.

[5] SILVERBERG, A.: *Points of finite order on Abelian varieties*. In: Contemp. Math. 133, Amer. Math. Soc., Providence, RI, 1992, pp. 175–193.

[6] SILVERMAN, J-H.: *The Arithmetic of Elliptic Curves*. Grad. Texts in Math. 106, Springer-Verlag, New York, 1986.

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

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

Departamento de Matemáticas
Universidad Autónoma de Madrid
C. Universitaria de Cantoblanco
ES–28 049 Madrid
SPAIN
E-mail: ernesto.girondo@uam.es
    gabino.gonzalez@uam.es
    enrique.gonzalez.jimenez@uam.es

**Instituto de Ciencias Matemáticas*
CSIC-UAM-UC3M-UCM
Madrid
SPAIN
E-mail: ernesto.girondo@uam.es
    enrique.gonzalez.jimenez@uam.es

***Institut für Mathematik*
Universität Würzburg
Am Hubland
DE–97 218 Würzburg
GERMANY
E-mail: steuding@mathematik.uni-wuerzburg.de