On the distribution of τ-congruent numbers

By Chad Tyler Davis and Blair Kenneth Spearman

Department of Mathematics and Statistics, University of British Columbia Okanagan, Science Building 115, 1177 Research Road, Kelowna, BC, Canada, V1V 1V7

(Communicated by Masaki Kashiwara, m.j.a., June 12, 2015)

Abstract: It is known that a positive integer n is the area of a right triangle with rational sides if and only if the elliptic curve $E^{(n)} : y^2 = x(x^2 - n^2)$ has a rational point of order different than 2. A generalization of this result states that a positive integer n is the area of a triangle with rational sides if and only if there is a nonzero rational number τ such that the elliptic curve $E_\tau^{(n)} : y^2 = x(x - n\tau)(n + n\tau^{-1})$ has a rational point of order different than 2. Such n are called τ-congruent numbers. It is shown that for a given integer $m > 1$, each congruence class modulo m contains infinitely many distinct τ-congruent numbers.

Key words: Elliptic curve; τ-congruent number.

1. Introduction. A positive integer n is called a congruent number if it is equal to the area of a right triangle with rational sides. Equivalently, n is congruent if and only if the elliptic curve

$$E^{(n)} : y^2 = x(x^2 - n^2)$$

has a rational point which is not of order 2. The idea of a congruent number can be generalized by requiring only that n be equal to the area of a triangle with rational sides. Such triangles are called Heron triangles. Goins and Maddox [5] proved that a positive integer n is the area of a Heron triangle if and only if for some nonzero rational number τ the elliptic curve

$$E_\tau^{(n)} : y^2 = x(x - n\tau)(x + n\tau^{-1}) \tag{1}$$

has a rational point which is not of order 2. In this case we call n a τ-congruent number. If (x, y) is such a point on $E_\tau^{(n)}$ then transformations, in terms of x, y and τ which produce a rational triangle with area n or indeed a rational right triangle in the case of congruent numbers, are given by Goins and Maddox in [5, p. 1516]. Chahal, [2,3] studied the connection between elliptic curves and congruent numbers, and employed an identity of Desboves to show that there are infinitely many congruent numbers in each residue class modulo 8. Bennett [1], extended this result, by showing that for any positive integer m, there exist infinitely many congruent numbers in each residue class modulo m.

The purpose of this paper is to prove an analog of Bennett's theorem for τ-congruent numbers. We will make use of another identity of Desboves [4]. We state our result in the following theorem.

Theorem 1. *Let τ be a fixed nonzero rational number, $m > 1$ a positive integer and a any integer. Then there exist infinitely many τ-congruent numbers n, inequivalent modulo squares of rational numbers and satisfying $n \equiv a \pmod m$.*

To prove our theorem we introduce in Section 1, an identity of Desboves that we shall use. Additionally we give a preliminary description of τ-congruent numbers. Then we give the proof of our theorem in Section 2.

2. An identity of Desboves. We begin with a simple lemma describing a relation concerning τ-congruent numbers.

Lemma 1. *Let n, n', e be positive integers and suppose that $n = n'e^2$. If n is a τ-congruent number then n' is a τ-congruent number.*

Proof. If n is a τ-congruent number then there is a rational point (x_0, y_0) which is not of order 2 on $E_\tau^{(n)}$. It follows that $(x_0/e^2, y_0/e^3)$ is a rational point which is not of order 2 on $E_\tau^{(n')}$ proving that n' is a τ-congruent number. □

Desboves [4] obtained a solution in integers of the following quadratic equation.

Proposition 1 (Desboves [4])**.** *Let n, u, v, w be integers. If we set*

$$X = u^2 + n^2v^2, \tag{2}$$

2010 Mathematics Subject Classification. Primary 14H52; Secondary 11G05.

doi: 10.3792/pjaa.91.101

$$Y = 2uv + wv^2,$$
$$Z = u^2 + wuv - n^2v^2,$$

then

$$X^2 + wXY - n^2Y^2 = Z^2. \tag{3}$$

As an identity, equation (3) using the expressions given in (2) remains valid if n, u, v, w are rational numbers. We shall apply the previous proposition with this fact in mind. Our next lemma gives a general formula for a τ-congruent number.

Lemma 2. *Let τ be a fixed nonzero rational number so that we may write $\tau = c/d$ for relatively prime integers c and d with $d > 0$. Suppose that n, r and s are integers with $\gcd(r, s) = 1$ and $n > 0$ such that*

$$n = cdrs(cr + ds)(dr - cs). \tag{4}$$

Then n is a τ-congruent number with at most finitely many exceptions.

Proof. To construct a rational point on $E_\tau^{(n)}$ given by (1), consider the quadratic equation

$$X^2 + (n/\tau - n\tau)XY - n^2Y^2 = Z^2. \tag{5}$$

We set

$$X = u^2 + n^2v^2, \tag{6}$$
$$Y = 2uv + wv^2,$$
$$Z = u^2 + wuv - n^2v^2,$$

where n, u and v are integers and w is the rational number given by

$$w = (n/\tau - n\tau), \tag{7}$$

bearing in mind the remark stated just before this lemma. By Proposition 1, equation (5) holds with these choices of X, Y, Z and w. If we substitute

$$u = n(r^2 - s^2), \quad v = 2rs, \quad \tau = c/d$$

and

$$n = cdrs(cr + ds)(dr - cs) \tag{8}$$

in (6) and (7), then we obtain

$$X = (cdrs)^2(r^2 + s^2)^2(cr + ds)^2(cs - dr)^2, \tag{9}$$
$$Y = 4r^2s^2(cr + ds)^2(cs - dr)^2,$$
$$Z = -cdr^2s^2(2drs + cr^2 - cs^2)$$
$$(2crs - dr^2 + ds^2)(cr + ds)^2(cs - dr)^2.$$

We now have a solution to the quartic equation

$$x^4 + (n/\tau - n\tau)x^2y^2 - n^2y^4 = z^2, \tag{10}$$

given by

$$x = cdrs(r^2 + s^2)(cr + ds)(cs - dr), \tag{11}$$
$$y = 2rs(cr + ds)(cs - dr),$$
$$z = -cdr^2s^2(2drs + cr^2 - cs^2)$$
$$(2crs - dr^2 + ds^2)(cr + sd)^2(cs - dr)^2.$$

Since we assumed that $n > 0$, equation (8) implies that r, s, $(cr + ds)$ and $(cs - dr)$ are nonzero, hence $x \neq 0$ and $y \neq 0$. If $z \neq 0$, then our solution (11) of equation (10) contributes a rational point P on $E_\tau^{(n)}$ given by

$$P = \left(\frac{x^2}{y^2}, \frac{xz}{y^3}\right).$$

P does not have order 2 as $xz \neq 0$. If however $z = 0$ then P would have order 2, and from equation (9) for z, either

$$2drs + cr^2 - cs^2 = 0 \tag{12}$$
or
$$2crs - dr^2 + ds^2 = 0.$$

Rearranging the equations in (12) yields

$$\frac{c}{d} = \frac{2rs}{s^2 - r^2} \quad \text{or} \quad \frac{c}{d} = \frac{r^2 - s^2}{2rs}. \tag{13}$$

Since $\gcd(c, d) = \gcd(r, s) = 1$ and c, d are constants, there are finitely many pairs of integers (r, s) satisfying (13) and for which P would have order 2. The proof of this lemma is complete. □

In the case where n is a congruent number, we have $c = d = 1$ in equation (4). If we further replace s by $4s$, set $r = 4s^2 + 1$ and scale the resulting integer expression by $4(2s - 1)^2(2s + 1)^2$, according to Lemma 1, we obtain the congruent number

$$s(4s^2 + 1),$$

used by Chahal [2,3]. Now we give the proof of our theorem.

3. Proof of Theorem.

Proof. We fix $\tau = c/d$ where c, d are relatively prime integers with $d > 0$. Define the set Λ by

$$\Lambda = \{\lambda \in \mathbf{N} \mid \lambda \equiv -a \pmod m\}.$$

We set

$$r = -1 \quad \text{and} \quad s = (cdm)^2\lambda,$$

noting that $\gcd(r, s) = 1$, as required by Lemma 2,

and substitute these values of r and s into (4). We obtain the integer $\tilde{n}$ given in (14).

$$\tilde{n} = c^4d^4m^2\lambda(c^3dm^2\lambda + 1)(cd^3m^2\lambda - 1). \tag{14}$$

As $m > 1$, we have $\tilde{n} > 0$ for all $\lambda \in \Lambda$. Lemma 2 implies that $\tilde{n}$ is a τ-congruent number with at most finitely many exceptions. By Lemma 1, we may scale $\tilde{n}$ by $(cd)^4m^2$, obtaining the τ-congruent number n given by

$$n = \lambda(c^3dm^2\lambda + 1)(cd^3m^2\lambda - 1). \tag{15}$$

From (15), we have

$$n \equiv -\lambda \equiv a \pmod{m}.$$

Finally, it is clear that infinitely many of these integers n are inequivalent modulo squares of rational numbers. Otherwise there would exist a finite set of integers $\{d_i\}$ such that for each value of λ with n given by (15) we would have nd_i equal to the square of an integer for some i. Thus there would exist infinitely many integral points lying on at least one of the nonsingular cubic curves

$$Y^2 = d_i\lambda(c^3dm^2\lambda + 1)(cd^3m^2\lambda - 1),$$

contradicting the theorem of Siegel [6]. □

References

[1] M. A. Bennett, Lucas' square pyramid problem revisited, Acta Arith. **105** (2002), no. 4, 341–347.

[2] J. S. Chahal, On an identity of Desboves, Proc. Japan Acad. Ser. A Math. Sci. **60** (1984), no. 3, 105–108.

[3] J. S. Chahal, Congruent numbers and elliptic curves, Amer. Math. Monthly **113** (2006), no. 4, 308–317.

[4] A. Desboves, Mémorie sur la Résolution en nombers entiers de l' équation $aX^m + bY^m = cZ^n$, Nouv. Ann. Math., Sér. II **18** (1879), 481–489.

[5] E. H. Goins and D. Maddox, Heron triangles via elliptic curves, Rocky Mountain J. Math. **36** (2006), no. 5, 1511–1526.

[6] C. L. Siegel, Über einige Anwendungen diophantischer Approximationen, Abh. Preuss. Akad. Der Wissenschaften Phys.-math. Kl. **1** (1929), 209–266.