On the distribution of congruent numbers

By Jennifer Ann JOHNSTONE and Blair Kenneth SPEARMAN

Mathematics and Statistics, University of British Columbia Okanagan, Kelowna, BC, Canada, V1V 1V7

(Communicated by Shigefumi MORI, M.J.A., April 12, 2010)

Abstract: For an integer $m > 1$, it is shown that each congruence class modulo m contains infinitely many congruent numbers whose associated elliptic curves have rank at least two.

Key words: Congruent numbers; elliptic curve; rank.

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

$$y^2 = x(x^2 - n^2) \tag{1}$$

has positive rank. Congruent numbers, scaled by squares of integers, retain the property of being congruent and their associated scaled elliptic curves have the same rank. Tables of congruent numbers can be found in the papers of Noda and Wada [8] and Nemenzo [7]. Chahal [4] has proved that there exist infinitely many congruent numbers in each congruence class modulo 8. In other words, there exist infinitely many positive integers n in each congruence class modulo 8 such that the curve given in (1) has rank at least 1. Bennett [2] showed that there exist infinitely many congruent numbers in any congruence class modulo the integer $m > 1$. The purpose of this paper is to prove a related result where the ranks of the congruent number curves are shown to be at least 2. We prove the following theorem.

Theorem 1. *If $m > 1$ is an integer then any congruence class modulo m contains infinitely many congruent numbers n, inequivalent modulo squares, such that the rank of $y^2 = x(x^2 - n^2)$ is greater than or equal to 2.*

In Section 2 we outline the computational method we will use and give a lemma which is necessary for the proof of our theorem. In Section 3 we prove our theorem.

2. Preliminary Results. The proof of the lemma in this section utilizes Silverman's specialization theorem [9, Theorem 11.4, p. 271] in the following form. If $P_1(t), P_2(t), \ldots, P_r(t)$ are independent points on the elliptic curve

$$y^2 = x^3 + A(t)x + B(t)$$

over $\mathbf{Q}(t)$ then these points remain independent over $\mathbf{Q}$ for all but finitely many values of t. For our purpose, we require a suitable formula for congruent numbers. We began with the form $n = a^4 - b^4$ given by Alter and Curtz [1] and specialized variables $(a, b) = \left(\dfrac{3t^2+6t+1}{2}, \dfrac{3t^2+2t+1}{2}\right)$ so that the elliptic curve (1) has at least two independent points. We were led to this specialization by formally carrying out a 2 descent on the congruent number curve with $n = a^4 - b^4$. We state this in a lemma.

Lemma 1. *Let $t \neq 0, -1, -1/3$ be a rational number and define $f(t)$ by*

$$f(t) = t(t+1)(3t+1)(9t^4 + 24t^3 + 26t^2 + 8t + 1). \tag{2}$$

Then the elliptic curve

$$y^2 = x\left(x^2 - f(t)^2\right) \tag{3}$$

has rank greater than or equal to 2, for all but finitely many values of t.

Proof. The elliptic curve $y^2 = x(x^2 - f(t)^2)$ has the nontorsion points (x_1, y_1) and (x_2, y_2) where

$$x_1 = -\frac{4t^2(t+1)^2(3t+1)^2(9t^4+24t^3+26t^2+8t+1)}{(3t^2+2t+1)^2}, \tag{4}$$

$$y_1 = \frac{2t^2(t+1)^2(3t+1)^2(3t^2-1)(9t^4+24t^3+26t^2+8t+1)^2}{(1+2t+3t^2)^3}.$$

and

$$x_2 = \frac{(9t^4+24t^3+26t^2+8t+1)^2}{4}, \tag{5}$$

$$y_2 = \frac{(9t^4+24t^3+26t^2+8t+1)^2(3t^2+2t+1)(3t^2+6t+1)}{8}.$$

2000 Mathematics Subject Classification. Primary 11G05.

doi: 10.3792/pjaa.86.89

We claim that in $\mathbf{Q}(t)$ these two points are independent. By Silverman's specialization theorem, it suffices to demonstrate this with a single rational value of t since any dependence relation between these two points in $\mathbf{Q}(t)$ would remain a dependence relation under a specialization to $\mathbf{Q}$. If we choose $t = 1$, then (3), (4) and (5) give the elliptic curve

$$y^2 = x(x^2 - 544^2)$$

together with the points on this curve

$$(x_1, y_1) = \left(\frac{-4352}{9}, \frac{147968}{27}\right)$$

and

$$(x_2, y_2) = (1156, 34680).$$

We can use the canonical height regulator as described by Cohen [5] to show that these points are independent. A procedure for this calculation is available in mwrank, PARI or Magma [3]. This regulator is equal to $7.099\ldots$, which is nonzero, confirming that these points are independent and thereby proving the lemma. □

3. Proof of Theorem.

Proof. Let $m > 1$ be an integer and the integer $a \in \{1, 2, \ldots, m\}$ be a representative of a congruence class modulo m. For $x = 1, 2, \ldots$ define the integer n by

$$n \doteqdot n(x, m, a) = \frac{f(am^2x^2)}{m^2x^2}. \tag{6}$$

We can easily determine from (2) and (6) that $n > 0$, and from Lemma 1 followed by scaling, that n is a congruent number whose associated elliptic curve has rank at least 2 with at most finitely many exceptions. Furthermore this congruent number n satisfies $n \equiv a (\mathrm{mod}\, m)$. Moreover we can find an infinite subset of these numbers n which are inequivalent modulo squares. Otherwise there would exist a finite set of nonzero rational numbers $\{d_i, i = 1, \ldots, k\}$ which are inequivalent modulo squares, such that for each value of x in (6) we would have,

$$\frac{f(am^2x^2)}{m^2x^2} = d_i y^2,$$

for some rational numbers y, d_i depending on x. Our infinitely many distinct values of x would give rise to an infinite set of distinct points on the set of algebraic curves

$$d_i Y^2 = \frac{f(am^2X^2)}{m^2X^2}.$$

However this is impossible since we have finitely many curves of genus 5, each of which has only finitely many points from Faltings' theorem [6]. This completes the proof. □

Acknowledgement. This research is supported by the Natural Sciences and Engineering Research Council of Canada.

References

[1] R. Alter and T. B. Curtz, A note on congruent numbers, Math. Comp. **28** (1974), 303–305.

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

[3] W. Bosma, J. Cannon and C. Playoust, The Magma algebra system. I. The user language, J. Symbolic Comput. **24** (1997), no. 3–4, 235–265.

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

[5] H. Cohen, *A course in computational algebraic number theory*, Springer, Berlin, 1993.

[6] G. Faltings, Endlichkeitssätze für abelsche Varietäten über Zahlkörpern, Invent. Math. **73** (1983), no. 3, 349–366.

[7] F. R. Nemenzo, All congruent numbers less than 40000, Proc. Japan Acad. Ser. A Math. Sci. **74** (1998), no. 1, 29–31.

[8] K. Noda and H. Wada, All congruent numbers less than 10 000, Proc. Japan Acad. Ser. A Math. Sci. **69** (1993), no. 6, 175–178.

[9] J. H. Silverman, *Advanced topics in the arithmetic of elliptic curves*, Springer, New York, 1994.