ON CONGRUENT NUMBERS WITH THREE PRIME FACTORS

Lindsey Reinholz
Department of Mathematics and Statistics, University of British Columbia Okanagan, Kelowna, BC, Canada, V1V 1V7.
reinholz@interchange.ubc.ca

Blair K. Spearman
Department of Mathematics and Statistics, University of British Columbia Okanagan, Kelowna, BC, Canada, V1V 1V7.
blair.spearman@ubc.ca

Qiduan Yang
Department of Mathematics and Statistics University of British Columbia Okanagan, Kelowna, BC, Canada, V1V 1V7.
qiduan.yang@ubc.ca

Received: 9/7/10, Accepted: 1/12/10, Published: 3/18/11

Abstract

A method is given for constructing congruent numbers with three prime factors of the form $8k+3$. A family of such numbers is given for which the Mordell-Weil rank of their associated elliptic curves equals 2, the maximal rank and expected rank for a congruent number curve of this type.

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 rank of the elliptic curve

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

is positive. Otherwise n is non-congruent. We use the notation $p_i, q_i, r_i, \ldots$ to denote prime numbers of the form $8k + i$. In certain cases, congruent numbers or non-congruent numbers are characterized in terms of their prime factors. For example, Monsky [5] showed that p_5 and p_7 are congruent numbers, while Gennochi [3] and Tunnell [8] showed that p_3 and p_3q_3 are non-congruent. Kida [4] noticed that $1419 = 3 \cdot 11 \cdot 43$ is the only congruent number less that 4500 of the form $p_3q_3r_3$ and that quite often a 2-descent shows that a number of the form $p_3q_3r_3$ is non-congruent. Other congruent numbers $p_3q_3r_3$ less than $10,000$ include $4587 = 3{\cdot}11{\cdot}139$, $4731 = 3{\cdot}19{\cdot}83$, $6963 = 3{\cdot}11{\cdot}211$, $7611 = 3{\cdot}43{\cdot}59$ and $9339 = 3{\cdot}11{\cdot}283$. Our main purpose in this paper is to give a family of congruent numbers $n = p_3q_3r_3$ for which we can prove that the Mordell-Weil rank of (1) is equal to 2, the maximal rank for a congruent number curve of this type. It is also the expected rank according to parity conjectures on the rank as described by Dujella, Janfada and Salami in the introduction of [2]. This family is obtained by specialization of a larger family which we use to generate congruent numbers $p_3q_3r_3$. Both of these families are conjecturally infinite. We prove the following theorem.

Theorem 1. *Suppose that the prime numbers q and r have the form*

$$q = 3u^4 + 3v^4 - 2u^2v^2,$$
$$r = 3u^4 + 3v^4 + 2u^2v^2,$$

for nonzero integers u and v. Set $n = 3qr$. Then $q \equiv r \equiv 3 (\mathrm{mod}\, 8)$, n is a congruent number and the congruent number elliptic curve given by (1) has rank equal to 2.

In Section 2, we give our method of construction for congruent numbers $p_3q_3r_3$, and give the background material necessary for the proof of our theorem. In Section 3, we discuss the generation of $p_3q_3r_3$ congruent numbers and give the proof of our theorem.

2. Preliminary Results

Since the definition of a congruent integer can be immediately extended to rational numbers we can give the following lemma.

Lemma 2. *Let v be a rational number with $v \notin (-\infty - 1] \cup [0, 1]$. Then*

$$v(v-1)(v+1) \tag{2}$$

is a congruent number.

Proof. The restriction on v ensures that it is positive. If v is an integer, the congruent number $v(v-1)(v+1)$ is a special case of a formula in [1]. It is sufficient to note that if $n = v(v-1)(v+1)$ is a rational number then the congruent number curve (1) has the non-torsion point

$$(x, y) = \left(\frac{(1+v^2)^2}{4}, \frac{(v^2+1)(v^2+2v-1)(v^2-2v-1)}{8}\right)$$

□

Lemma 3. *Suppose that the prime numbers $p_3, q_3,$ and r_3 satisfy*

$$q_3 = p_3a^2 - 16b^2,$$
$$r_3 = p_3a^2 + 16b^2,$$

for integers a and b. Then $n = p_3q_3r_3$ is a congruent number.

Proof. Put $v = p_3a^2/16b^2$ in (2) to give the congruent number

$$p_3a^2/16b^2(p_3a^2/16b^2 - 1)(p_3a^2/16b^2 + 1). \tag{3}$$

This number is positive if we impose the restrictions stated in Lemma 1. Since congruent numbers scaled by squares are still congruent, we multiply by $2^{12}b^6/a^2$ to obtain the stated congruent number $p_3q_3r_3$. $\square$

Lemma 4. *If*

$$n = 3(3 + 3z^4 - 2z^2)(3 + 3z^4 + 2z^2) \tag{4}$$

for a rational number $z \neq 0, \pm 1$ then the rank of the congruent number curve (1) is at least 2 with at most finitely many exceptions.

Proof. This formula for n is obtained from the congruent number formula in Lemma 1 where we set

$$v = \frac{3z^4 - 2z^2 + 3}{4z^2},$$

noting that $z \neq 0, \pm 1$ implies that $v > 1$. Then we scale to remove squares. For this value of n, the congruent number curve (1) over $\mathbb{Q}(z)$ possesses the two points

$$(x_1, y_1) = \left(-9(3 + 3z^4 - 2z^2)\,(z^2 - 1)^2, 36(3 + 3z^4 - 2z^2)^2 z(z^2 - 1)\right) \tag{5}$$

and

$$(x_2, y_2) = \left(\frac{3(3 + 3z^4 + 2z^2)^2(3 + 3z^4 - 2z^2)}{4z^2}, \frac{9(3 + 3z^4 - 2z^2)^2(3 + 3z^4 + 2z^2)^2(z^2 + 1)}{8z^3}\right) \tag{6}$$

If $z = 2$, then our formula (4) yields the congruent number $n = 7611 = 3 \cdot 43 \cdot 59$ while (5) and (6) give two points on $y^2 = x(x^2 - 7611^2)$, namely

$$(x_1, y_1) = (-3483, 399384)$$

and

$$(x_2, y_2) = \left(\frac{449049}{16}, \frac{289636605}{64}\right).$$

Magma confirms that these two non-torsion points are independent in the group of rational points on $y^2 = x(x^2 - 7611^2)$. By Silverman's specialization theorem [7], the points (5) and (6) are independent over $\mathbb{Q}(z)$ and are therefore independent for all rational values of z with at most finitely many exceptions. $\square$

Remark 5. Under the further restriction that $3+3z^4-2z^2 = p_3c^2$ and $3+3z^4+2z^2 = q_3d^2$ for distinct primes p_3 and q_3 different from 3, and rational numbers, $z, c,$and d, then a longer argument using a 2-descent would show that the points (5) and (6) are always independent. This statement applies to our main theorem.

In order to bound the rank $r(n)$ of the congruent curves in our theorem, we need Monsky's formula for $s(n)$, the 2-Selmer rank [2], [5]. The quantity $s(n)$ is an upper bound for $r(n)$. Let n be a squarefree positive integer with odd prime factors $P_1, P_2, \ldots, P_t$. We define diagonal $t \times t$ matrices $D_l = (d_i)$ for $l \in \{-2,-1,2\}$, and the square $t \times t$ matrix $A = (a_{ij})$ by

$$d_i = \begin{cases} 0, & \text{if } \left(\frac{l}{P_i}\right) = 1, \\ 1, & \text{if } \left(\frac{l}{P_i}\right) = -1, \end{cases}$$

$$a_{ij} = \begin{cases} 0, & \text{if } \left(\frac{P_j}{P_i}\right) = 1,\ j \neq i, \\ 1, & \text{if } \left(\frac{P_j}{P_i}\right) = -1,\ j \neq i, \end{cases} \qquad a_{ii} = \sum_{j:j\neq i} a_{ij}.$$

Then

$$s(n) = \begin{cases} 2t - \operatorname{rank}_{\mathbb{F}_2}(M_o), & \text{if } n = P_1P_2\cdots P_t, \\ 2t - \operatorname{rank}_{\mathbb{F}_2}(M_e), & \text{if } n = 2P_1P_2\cdots P_t, \end{cases} \tag{7}$$

where M_o and M_e are the $2t \times 2t$ matrices:

$$M_o = \left[\begin{array}{c|c} A + D_2 & D_2 \\ \hline D_2 & A + D_{-2} \end{array}\right], \quad M_e = \left[\begin{array}{c|c} D_2 & A + D_2 \\ \hline A^T + D_2 & D_{-1} \end{array}\right]. \tag{8}$$

Lemma 6. *If $n = p_3q_3r_3$ then $s(n) \leq 2$.*

Proof. We calculate $s(n)$ using formulas (7) and (8) with $P_1 = p_3$, $P_2 = q_3$ and $P_3 = r_3$ for all possible choices of values of the Legendre symbols $\left(\frac{p_3}{q_3}\right)$, $\left(\frac{p_3}{r_3}\right)$ and $\left(\frac{q_3}{r_3}\right)$. For example if

$$\left(\frac{p_3}{q_3}\right) = +1, \left(\frac{p_3}{r_3}\right) = -1 \text{ and } \left(\frac{q_3}{r_3}\right) = +1$$

then M_o is given by

$$\begin{bmatrix} 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix}.$$

Its rank over $\mathbb{F}_2$ is equal to 4 so that (7) gives $s(n) = 2$. We record the results for all 8 cases in the following table.

Values of $s(n)$

$\left(\frac{p_3}{q_3}\right)$	$\left(\frac{p_3}{r_3}\right)$	$\left(\frac{q_3}{r_3}\right)$	$s(n)$
$+1$	$+1$	$+1$	0
$+1$	$+1$	-1	0
$+1$	-1	$+1$	2
$+1$	-1	-1	0
-1	$+1$	$+1$	0
-1	$+1$	-1	2
-1	-1	$+1$	0
-1	-1	-1	0

$\square$

Remark 7. In the proof of Lemma 4, the six cases where $s(n) = 0$ are related by permutation of the primes p_3, q_3 and r_3. The cases where $s(n) = 2$ are similarly related.

3. Generating Congruent Numbers $p_3q_3r_3$ and Proof of Theorem

We recall Schinzel's hypothesis H [6], which states if a finite product $Q(x) = \prod_{i=1}^{m} f_i(x)$ of polynomials $f_i(x) \in \mathbb{Z}[x]$ has no fixed divisors, then all of the $f_i(x)$ will be simultaneously prime, for infinitely many integral values of x. From this hypothesis we deduce that for any fixed prime p_3 the two forms

$$p_3a^2 - 16b^2 \quad \text{and} \quad p_3a^2 + 16b^2 \tag{9}$$

will assume prime values infinitely often. In order to obtain q_3, r_3 prime numbers from these two forms, we must have a odd. By Lemma 2 the number $n = p_3q_3r_3$ will be congruent. All of the examples of congruent numbers mentioned in the introduction have $p_3 = 3$, but we can generate examples for any fixed prime p_3 using (9). For example if $p_3 = 43$ then using (9) with $a = 9$ and $b = 1$ yields the value

$$n = p_3q_3r_3 = 43 \cdot 3467 \cdot 3499,$$

which by Lemma 2 is a congruent number. Now we give the proof of our theorem.

Proof. If the formulas for q and r given in our theorem assume prime values, then u and v must have opposite parity from which it follows that $p \equiv q \equiv 3(\bmod 8)$. From Lemma 3, the congruent number curve

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

with $n = 3(3 + 3z^4 - 2z^2)(3 + 3z^4 + 2z^2)$ has rank at least 2 for all but finitely many values of the rational number z. Hence, setting $z = u/v$ and scaling by v^8 shows that $n = 3qr$ is a congruent number. By the remark just after Lemma 3, the curve (1) with $n = 3qr$ has rank at least 2. However Lemma 4 shows that $s(n) \leq 2$, and since the rank is bounded above by $s(n)$ the rank is at most 2. Thus the rank equals 2 and the theorem is proved. $\square$

Example 8. A few smaller congruent numbers whose associated congruent number curves have rank 2 and which are generated by the formulas in our theorem include $7611 = 3 \cdot 43 \cdot 59$, $1021683291 = 3 \cdot 13219 \cdot 25763$ and $2700420027 = 3 \cdot 30203 \cdot 29803$.

Acknowledgements Research supported by the Natural Sciences and Engineering Research Council of Canada.

References

[1] R. Alter, The Congruent Number Problem. *Amer. Math. Monthly*, **87** (1) (1980), 43-45.

[2] A. Dujella, A.S. Janfada and S. Salami, A search for high rank congruent number elliptic curves. *J. Integer Seq.*, **12** (5) (2009), Article 09.5.8.

[3] A. Gennochi, Note analitche sopra tre scritti. *Annali di Scienze Matematische e Fisiche*, **6** (1855).

[4] M. Kida, On the Rank of an Elliptic Curve in Elementary 2-extensions. *Proc. Japan. Acad.*, **69** (10) (1993), 422-425.

[5] P. Monsky, Mock Heegner points and congruent numbers. *Math. Z.,* **204** (1) (1990), 45-68.

[6] A. Schinzel and W. Sierpiński, Sur certain hypothèses concernant les nombres premiers. *Acta Arith.,* **4** (1958), 185-208.

[7] J.H. Silverman, *The Arithmetic of Elliptic Curves.* Graduate Texts in Mathematics. 106, Springer, New York (1986).

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