ACTA ARITHMETICA
128.2 (2007)

Ratios of congruent numbers

by

ASHVIN RAJAN (Baltimore, MD) and
FRANÇOIS RAMAROSON (Washington, DC)

1. Introduction. A *rational right triangle* is a right triangle whose sides are all positive rational numbers. Such a triangle is denoted $\{a, b, c\}$ where a and b are the legs, and c is the hypotenuse. Throughout this paper, a *square-free integer* is understood to be a positive integer which is not divisible by the square of an integer greater than 1. A *congruent number* is a square-free integer which is the area of a rational right triangle. A square-free integer N is a congruent number if and only if the elliptic curve $Ny^2 = (x^2 - 1)x$ has positive rank. For details, see Koblitz [7].

In the spirit of Euclid's proof of the infinitude of prime numbers, one can also show that there are infinitely many congruent numbers as follows: If there were only finitely many of them, say $N_1, \ldots, N_r$, all greater than 1, then consider $N = N_1 \cdots N_r$. Elementary number theory shows that $\mathrm{sqf}(N^3 - N)$, the *square-free part* of $N^3 - N$, cannot be 1. Moreover, it is a congruent number which cannot be any of the N_i's. Indeed, if it were N_1, say, let $M = N_2 \cdots N_r$ and $d = \gcd(N_1, M)$. Writing $N_1 = dn$ and $M = dm$ with $\gcd(m, n) = 1$, one sees that $\mathrm{sqf}(m)\,\mathrm{sqf}(N_1^2M^2 - 1) = d$. This last equality implies that $\mathrm{sqf}(N_1^2M^2 - 1)$ divides d, and hence M, but at the same time, since it divides $N_1^2M^2 - 1$, it must be 1, and this is impossible.

Chahal [2] established that the residue classes of $1, 2, 3, 5, 6, 7$ modulo 8 contain infinitely many congruent numbers. Bennett [1] extended Chahal's result by showing that if a and m are positive integers such that $\gcd(a, m)$ is square-free, then the residue class of a modulo m contains infinitely many congruent numbers.

In this paper we prove the following:

2000 *Mathematics Subject Classification*: Primary 11G05; Secondary 14G05.
The authors wish to thank J. S. Chahal and the referee for useful suggestions.

Main Theorem. *If k and l are positive, square-free, coprime integers, then there exist infinitely many pairs (M, N) of congruent numbers such that $lN = kM$.*

Corollary. *If k and l are positive, square-free, coprime integers, then there exist infinitely many square-free integers N such that both kN and lN are congruent numbers.*

2. Holm's curve and its jacobian. We consider the following non-singular curve of genus one:

$$H: \quad lx(x^2-1) = ky(y^2-1),$$

where k and l are coprime, square-free integers. In a slightly different form, this curve was considered by Holm [5], in his work on right triangles whose areas are in a given ratio. The jacobian of H is the elliptic curve

$$E: \quad Y^2 = X^3 - 3k^2l^2X + k^2l^2(k^2+l^2).$$

The following proposition is easily proved.

Proposition 2.1.

(i) *The discriminant of E is $-3^3k^4l^4(k^2-l^2)^2$.*

(ii) *The j-invariant of E is $-2^8 3^3 k^2l^2/(k^2-l^2)^2$.*

(iii) *The following integral points lie on E:*

$$(-kl, \pm kl(k+l)),\ (k^2, \pm k(k^2-l^2)),\ (kl, \pm kl(k-l)),\ (l^2, \pm l(k^2-l^2)).$$

(iv) *E has positive rank, since $(l^2, l(k^2-l^2))$ is a point of infinite order.*

(v) *The rational transformations relating H and E are*

$$x = \frac{k(X-l^2)}{Y}, \qquad y = \frac{l(X-k^2)}{Y},$$
$$X = \frac{kl(kx-ly)}{lx-ky}, \qquad Y = \frac{kl(k^2-l^2)}{lx-ky}.$$

Let $A_x = x(x^2-1)$ and $A_y = y(y^2-1)$. Then every *rational* point (x, y) on H, that is, not in the set

$$\{(0,0), (\pm 1, \pm 1), (\pm 1, 0), (0, \pm 1)\},$$

gives rise to two rational right triangles whose areas are in the ratio

$$\frac{A_x}{A_y} = \frac{k}{l}.$$

Indeed, if both A_x and A_y are positive, the rational right triangles $\{x^2-1, 2x, x^2+1\}$ (for $x > 0$), or $\{1-x^2, -2x, x^2+1\}$ (for $x < 0$), will have area A_x, and similarly for A_y, while if A_x and A_y are both negative, the rational right triangles $\{x^2-1, -2x, x^2+1\}$ (for $x > 0$), or $\{1-x^2, 2x, x^2+1\}$ (for $x < 0$), will have area $-A_x$, and similarly for $-A_y$. Therefore, every rational point

(x, y) on H which is not in the set mentioned above produces a pair of congruent numbers, (N_x, N_y), when we take the square-free parts N_x of A_x and N_y of A_y respectively.

If we choose a rational point (X, Y) in $E(\mathbb{Q})$ different from those listed in Proposition 2.1(iii) and employ the transformations, we get "areas" $A_x(X, Y)$ and $A_y(X, Y)$. We will show that there are infinitely many points (X, Y) in $E(\mathbb{Q})$ for which l is prime to the square-free part of $A_x(X, Y)$ and k is prime to the square-free part of $A_y(X, Y)$. In order to do this, we will use well-known properties of p-adic filtrations.

3. The p-adic filtration on global points. Let E be an elliptic curve given as a Weierstrass model with coefficients in $\mathbb{Z}$, and p a prime at which the model is minimal. We then have the p-adic filtration

$$E(\mathbb{Q}_p) \supset E_0(\mathbb{Q}_p) \supset E_1(\mathbb{Q}_p) \supset E_2(\mathbb{Q}_p) \supset \cdots$$

The following facts on p-adic filtrations are well-known (see Knapp [6] or Silverman [8], for instance).

(1) $E_0(\mathbb{Q}_p)$ is the set of points whose reduction mod p is non-singular.
(2) $E_1(\mathbb{Q}_p)$ is the kernel of reduction mod p.
(3) $E(\mathbb{Q}_p)/E_0(\mathbb{Q}_p)$ and $E_0(\mathbb{Q}_p)/E_1(\mathbb{Q}_p)$ are finite groups.
(4) For each $n \geq 1$, $E_n(\mathbb{Q}_p) = \{P \mid \mathrm{ord}_p(x(P)) \leq -2n\}$.
(5) For each $n \geq 1$, $E_n(\mathbb{Q}_p)/E_{n+1}(\mathbb{Q}_p) \cong \mathbb{F}_p$.

Let

$$E_n(\mathbb{Q}) = E_n(\mathbb{Q}_p) \cap E(\mathbb{Q}) \quad \text{for each } n \geq 1.$$

The proofs of the following propositions are well-known.

PROPOSITION 3.1. *For each $m \geq 1$, if $E_m(\mathbb{Q})/E_{m+1}(\mathbb{Q}) \cong \mathbb{F}_p$, then*

$$E_{m+1}(\mathbb{Q})/E_{m+2}(\mathbb{Q}) \cong \mathbb{F}_p.$$

More generally, for any $n \geq m$, and for any $P \in E_m(\mathbb{Q}) - E_{m+1}(\mathbb{Q})$,

$$p^{n-m} P \in E_n(\mathbb{Q}) - E_{n+1}(\mathbb{Q}).$$

PROPOSITION 3.2. *If E has positive rank over $\mathbb{Q}$, then there is an integer $N \geq 1$ such that $E_n(\mathbb{Q})/E_{n+1}(\mathbb{Q}) \cong \mathbb{F}_p$ for all $n \geq N$.*

Next, we investigate the relationship between the filtrations on global points for a set of primes at each of which the model is minimal.

Let $S = \{p_1, \ldots, p_s\}$ be a set of distinct primes such that E is minimal at each p_i. For each prime p_i, there is a p_i-adic filtration

$$E(\mathbb{Q}_{p_i}) \supset E_0(\mathbb{Q}_{p_i}) \supset E_1(\mathbb{Q}_{p_i}) \supset \cdots .$$

As before, we put $E_{n,p_i}(\mathbb{Q}) = E_n(\mathbb{Q}_{p_i}) \cap E(\mathbb{Q})$. Proposition 3.2 implies that for each i, $1 \le i \le s$, there exists an integer N_i such that

$$E_{n,p_i}(\mathbb{Q})/E_{n+1,p_i}(\mathbb{Q}) \cong \mathbb{F}_{p_i} \quad \text{for all } n \ge N_i.$$

Let $N = \max\{N_1, \ldots, N_s\}$, and for each $n \ge N$, let

$$U_n = \bigcap_{i=1}^{s} (E_{n,p_i}(\mathbb{Q}) - E_{n+1,p_i}(\mathbb{Q})).$$

Although somewhat lengthy, the proof of the following proposition is straightforward.

PROPOSITION 3.3. *If E has positive rank over $\mathbb{Q}$, then there exists an integer $m \ge N$ such that $U_m \ne \emptyset$.*

COROLLARY 3.4. *If E has positive rank over $\mathbb{Q}$, then there exists an integer m_0 such that for all $m \ge m_0$, $U_m \ne \emptyset$.*

4. Applications to the elliptic curve E. We now apply the general results of the previous section to the curve

$$E: \quad Y^2 = X^3 - 3k^2l^2X + k^2l^2(k^2 + l^2),$$

which has positive rank over $\mathbb{Q}$. Recall that k and l are square-free, coprime positive integers.

PROPOSITION 4.1. *There exists an integer n and an infinite set $\mathcal{P}$ of rational points in $E(\mathbb{Q})$ such that if $(X,Y) \in \mathcal{P}$ then, for any prime divisor q of l and for any prime divisor p of k,*

$$\operatorname{ord}_q(X) = \operatorname{ord}_p(X) = -4n, \qquad \operatorname{ord}_q(Y) = \operatorname{ord}_p(Y) = -6n.$$

Proof. In the notation of the previous section, let S be the set of all prime divisors of k and l. By Proposition 2.1(i), and the assumptions on k and l, E is minimal at all primes in S. Applying Corollary 3.4, we find an integer n such that $U_{2n} \ne \emptyset$. Let $P \in U_{2n}$, and consider the set of points $\mathcal{P} = \{P_a = r^a P \mid a \in \mathbb{N}\}$. Since $r \notin S$,

$$\mathcal{P} \subset U_{2n} \subset E(\mathbb{Q}).$$

Moreover, $\mathcal{P}$ is infinite since P is of infinite order. The conclusions about the orders directly follow from the definition of U_{2n}. ∎

For each point $(X,Y) \in \mathcal{P}$, we form the "areas" $A_x = x(x^2 - 1)$ and $A_y = y(y^2 - 1)$ where

$$x = \frac{k(X - l^2)}{Y}, \qquad y = \frac{l(X - k^2)}{Y}.$$

THEOREM 4.2. *For each $(X,Y) \in \mathcal{P}$, let N_x (resp. N_y) be the square-free part of A_x (resp. A_y). Then*

$$lN_x = kN_y.$$

Proof. Proposition 4.1 implies that $(l, N_x) = (k, N_y) = 1$. Since the point (X, Y) is on E, the point (x, y) is on H, and hence $lA_x = kA_y$. Taking the square-free parts of both sides yields the result. ∎

Theorem 4.2 associates to every point (X, Y) in the set $\mathcal{P}$ a pair of square-free integers (N_x, N_y). We next establish that there are infinitely many such pairs (N_x, N_y) associated to the infinite set $\mathcal{P}$. It is clear that if there were only a finite number of N_x, there would also be only a finite number of N_y, and *vice versa*.

THEOREM 4.3. *Associated with the infinite set of points* (X, Y) *in* $\mathcal{P}$, *there are infinitely many pairs of square-free integers* (N_x, N_y).

Proof. Assume that there are only finitely many such pairs. Then there must exist a pair (N, M) of square-free integers which is associated with infinitely many rational points (X, Y) in $\mathcal{P}$. Using (x, y) instead of (X, Y), we find that in an $xyzw$-space, the algebraic variety

$$(\mathcal{C}): \quad \begin{cases} lx(x^2-1) = ky(y^2-1), \\ x(x^2-1) = Nz^2, \\ y(y^2-1) = Mw^2 \end{cases}$$

is a non-singular algebraic curve, defined over $\mathbb{Q}$, having infinitely many rational points.

LEMMA 4.4. *In the* xyz*-space*, *the curve*

$$(\mathcal{C}_1): \quad \begin{cases} lx(x^2-1) = ky(y^2-1), \\ x(x^2-1) = Nz^2 \end{cases}$$

has only finitely many rational points.

Proof. In the projective space $P^3(\overline{\mathbb{Q}})$, with x, y, z, t coordinates, the curve $(\mathcal{C}_1)$ has equations

$$\begin{cases} lx(x^2-t^2) = ky(y^2-t^2), \\ x(x^2-t^2) = Nz^2t. \end{cases}$$

Let $(\mathcal{C}_2)$ be the elliptic curve $x(x^2-t^2) = Nzt^2$, and consider the projection along y

$$(\mathcal{C}_1) \to (\mathcal{C}_2), \qquad (x, y, z, t) \mapsto (x, z, t).$$

This is a finite morphism of curves, of degree 3, which is ramified over the point $(x, z, t) = (0, 1, 0)$. If we let $g((\mathcal{C}_1))$ be the genus of $(\mathcal{C}_1)$, the Hurwitz formula implies that $g((\mathcal{C}_1)) > 1$. Faltings' theorem ([3]) now implies that $(\mathcal{C}_1)$ only has a finite number of rational points. ∎

NOTE. One could also work out Exercise 7.2(d) in Hartshorne [4].

To finish the proof of Theorem 4.3, we observe that the projection from the curve $(\mathcal{C})$ to the curve $(\mathcal{C}_1)$ along w is a rational map, defined over $\mathbb{Q}$, between curves, and is of degree 2. Since $(\mathcal{C}_1)$ only has a finite set of rational points, so does $(\mathcal{C})$. This contradiction ends the proof of Theorem 4.3. ∎

THEOREM 4.5. *If k and l are positive, square-free, coprime integers, then there exist infinitely many pairs (N, M) of congruent numbers such that $lN = kM$.*

Proof. Consider the elliptic curve $E : Y^2 = X^3 - 3k^2l^2X + k^2l^2(k^2 + l^2)$, the infinite set of rational points $\mathcal{P} \subset E(\mathbb{Q})$, and apply Theorems 4.2 and 4.3. ∎

The case $l = 1$ is worth pointing out.

COROLLARY 4.6. *Given a positive, square-free integer k, there exist infinitely many pairs (N, M) of congruent numbers such that $N = kM$.* ∎

References

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

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

[3] G. Faltings, *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern*, Invent. Math. 73 (1983), 349–366.

[4] R. Hartshorne, *Algebraic Geometry*, Grad. Texts in Math. 52, Springer, New York, 1977.

[5] A. Holm, *Some points in Diophantine analysis*, Proc. Edinburgh Math. Soc. 22 (1903), 40–48.

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

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

[8] J. H. Silverman, *The Arithmetic of Elliptic Curves*, Grad. Texts in Math. 106, Springer, New York, 1986.

3935 Cloverhill Road
Baltimore, MD 21218, U.S.A.
E-mail: AshvinRj@aol.com

Department of Mathematics
Howard University
Washington, DC 20059, U.S.A.
E-mail: framaroson@howard.edu

Received on 20.5.2005
and in revised form on 21.10.2006 (4991)