On the distribution of rank two τ-congruent numbers

By Chad Tyler Davis

Mathematics and Statistics, Irving K. Barber School of Arts and Sciences, University of British Columbia Okanagan Campus, 3333 University Way, Kelowna, BC, Canada, V1V 1V7

(Communicated by Masaki Kashiwara, m.j.a., April 12, 2017)

Abstract: A positive integer n is the area of a Heron triangle if and only if there is a non-zero rational number τ such that the elliptic curve

$$E_\tau^{(n)} : Y^2 = X(X - n\tau)(X + n\tau^{-1})$$

has a rational point of order different than two. Such integers n are called τ-congruent numbers. In this paper, we show that for a given positive integer p, and a given non-zero rational number τ, there exist infinitely many τ-congruent numbers in every residue class modulo p whose corresponding elliptic curves have rank at least two.

Key words: Elliptic curve; τ-congruent number; rank.

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. It is well-known that a given positive integer n is congruent if and only if the elliptic curve

$$E^{(n)} : Y^2 = X(X^2 - n^2)$$

has a rational point of order different than two. In [6], Goins and Maddox proved that a positive integer n is the area of a Heron triangle (a triangle with rational sides) if and only if there exists a non-zero rational number τ such that the elliptic curve

$$E_\tau^{(n)} : Y^2 = X(X - n\tau)(X + n\tau^{-1})$$

has a rational point of order different than two, thus generalizing the congruent number problem. Such an integer n is called a τ-congruent number. In [2] and [3], Chahal showed that there exist infinitely many congruent numbers contained in every residue class modulo 8. In [1], Bennett generalized this result to show that there are infinitely many congruent numbers contained in every residue class modulo m for any positive integer m. In [5], Davis and Spearman generalized Bennett's result to τ-congruent numbers for any non-zero rational number τ.

The purpose of this paper is to expand upon the result in [5] to *rank two τ-congruent numbers*; that is τ-congruent numbers whose associated elliptic curves have rank at least two.

2. Some useful lemmas. We begin by proving three lemmas that will be imperative to the proof of our main result.

Lemma 1. *Let $a, b, p \in \mathbf{Z}$ be fixed with $\gcd(a, b) = 1$. Let $0 \neq \lambda \in \mathbf{Z}$. Define the following quantities*

$$\begin{aligned} G(\lambda) &= ((4a^6b^4p^4)(a^2 + b^2)\lambda^2 + 1) \\ &\quad ((4a^4b^6p^4)(2a^2 + b^2)\lambda^2 + 4a^3b^3p^2\lambda + 1) \\ &\quad ((abp^2)(a^4 - a^2b^2 - b^4)\lambda - 1), \\ H(\lambda) &= ((4a^4b^6p^4)(2a^2 + b^2)\lambda^2 + 4a^3b^3p^2\lambda + 1) \\ &\quad ((abp^2)(a^4 - a^2b^2 - b^4)\lambda - 1), \\ K(\lambda) &= ((4a^6b^4p^4)(a^2 + b^2)\lambda^2 + 1) \\ &\quad ((abp^2)(a^4 - a^2b^2 - b^4)\lambda - 1). \end{aligned}$$

Then there are at most finitely many values of λ such that $(\lambda ab)G(\lambda), (\lambda ab)H(\lambda)$, and $(\lambda ab)K(\lambda)$ are rational squares.

Proof. The quantities (λab) and $G(\lambda)$ are relatively prime, hence it suffices to show that $G(\lambda)$ is a rational square for at most finitely many values of λ. Consider the equations

$$\tilde{G} : G(X) = \pm Y^2.$$

These two equations define genus 2 curves over $\mathbf{Q}$. Let $(\lambda, y) \in \tilde{G}(\mathbf{Q})$, the set of rational points on $\tilde{G}$, with $\lambda \in \mathbf{Z}$. The restriction of λ to the integers implies that y is also an integer. Thus (λ, y) is an

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

doi: 10.3792/pjaa.93.37

integral point on a genus 2 curve. Siegel's Theorem [7] implies that there are at most finitely many integral points on $\tilde{G}$, hence there are at most finitely many such pairs (λ, y).

The quantities (λab) and $H(\lambda)$ are relatively prime. Consider the equations

$$\tilde{H} : H(X) = \pm Y^2.$$

These two equations define elliptic curves over $\mathbf{Q}$. Let $(\lambda, y) \in \tilde{H}(\mathbf{Q})$ with $\lambda \in \mathbf{Z}$. The restriction of λ to the integers implies that y is also an integer. Hence (λ, y) is an integral point on $\tilde{H}$. Siegel's Theorem [7] implies that at most finitely many of these can exist.

The quantities (λab) and $K(\lambda)$ are relatively prime. As in the previous case,

$$\tilde{K} : K(X) = \pm Y^2$$

define elliptic curves over $\mathbf{Q}$. The argument is then the same. □

Lemma 2. *Let a, b, p, k be fixed, non-zero integers. Let $0 \neq \ell \in \mathbf{Z}$. Define the following quantities*

$$\begin{aligned} A(\ell) &= 4a^6b^4p^4k^2(a^2+b^2)(p\ell+1)^8 + 1, \\ B(\ell) &= 4a^4b^6p^4k^2(2a^2+b^2)(p\ell+1)^8 \\ &\quad + 4a^3b^3p^2k(p\ell+1)^4 + 1, \\ C(\ell) &= (k(p\ell+1)^4ab) \\ &\quad (abp^2k(a^4-a^2b^2-b^4)(p\ell+1)^4 - 1). \end{aligned}$$

Then there are at most finitely many values for ℓ such that the above expressions are rational squares.

Proof. It is clear that $A(\ell)$ is always positive. Consider the equation

$$\tilde{A} : A(X) = Y^2.$$

This equation defines a genus 3 curve over $\mathbf{Q}$. Let $(\ell, y) \in \tilde{A}(\mathbf{Q})$ with $\ell \in \mathbf{Z}$. The restriction of ℓ to the integers implies that y must also be an integer. Thus (ℓ, y) is an integral point on a genus 3 curve. As in Lemma 1, Siegel's Theorem [7] implies there can only be finitely many of these.

The equations

$$\tilde{B} : B(X) = \pm Y^2$$

define genus 3 curves over $\mathbf{Q}$. The same argument in the previous paragraph now applies.

The quantities $(k(p\ell+1)^4ab)$ and $(abp^2k(a^4 - a^2b^2 - b^4)(p\ell+1)^4 - 1)$ are relatively prime. Thus if the equation $C(\ell) = \pm y^2$ has a rational solution, then both $(k(p\ell+1)^4ab)$ and $(abp^2k(a^4 - a^2b^2 - b^4)(p\ell+1)^4 - 1)$ must be rational squares. The equations

$$\tilde{C} : (abp^2k)(a^4 - a^2b^2 - b^4)(pX+1)^4 - 1 = \pm Y^2$$

define elliptic curves over $\mathbf{Q}$. Let $(\ell, z) \in \tilde{C}(\mathbf{Q})$ with $\ell \in \mathbf{Z}$. The restriction of ℓ to the integers implies that z is an integer. Hence (ℓ, z) is an integral point on $\tilde{C}$. By Siegel's Theorem [7], there are only finitely many of these. □

Lemma 3. *Let a, b, p, k be fixed, non-zero integers with $p > 0$ and $\gcd(a, b) = 1$. Let $\lambda(\ell) = k(p\ell+1)^4$ and $n(\ell) = -\lambda(\ell)G(\lambda(\ell))$ where G is the same as in Lemma 1 and $\ell \in \mathbf{Z}$. Then there are infinitely many integers of the form $n(\ell)$ belonging to every residue class modulo p.*

Proof. We have that

$$n(\ell) \equiv -\lambda(\ell)(-1) \equiv \lambda(\ell) \equiv k(p\ell+1)^4 \equiv k \pmod{p}.$$

Varying ℓ implies that there are infinitely many integers of the form $n(\ell)$ congruent to k modulo p. As k in $\mathbf{Z}$ was fixed arbitrarily, the result follows. □

3. The main result. We now prove the main result which will come as a corollary to the next theorem. First we recall the fundamental 2-descent map given by Cohen in [4], Definition 8.2.3, p. 536, and Silverman and Tate in [8], Proposition, p. 85. Let $E : Y^2 = X^3 + aX^2 + bX$ be an elliptic curve over $\mathbf{Q}$, let $\mathcal{O}$ denote the point at infinity on E, and let $E(\mathbf{Q})$ denote the group of rational points on E. Let $(\mathbf{Q}^*)^2$ denote the set of all squared non-zero rational numbers. Then the *fundamental 2-descent map* $\alpha : E(\mathbf{Q}) \to \mathbf{Q}/(\mathbf{Q}^*)^2$ is given by

$$\alpha(P) = \begin{cases} 1 \pmod{(\mathbf{Q}^*)^2} & \text{if } P = \mathcal{O} \\ b \pmod{(\mathbf{Q}^*)^2} & \text{if } P = (0,0) \\ X(P) \pmod{(\mathbf{Q}^*)^2} & \text{otherwise} \end{cases}$$

where $X(P)$ denotes the X-coordinate of $P \in E(\mathbf{Q})$. The rank r of E then satisfies the relation

$$|\alpha(E(\mathbf{Q}))||2^{r+2}$$

(see [4], Proposition 8.2.8, p. 539). We now present our first theorem.

Theorem 1. *Let $0 \neq \tau = a/b \in \mathbf{Q}$ be a fixed rational number with $\gcd(a, b) = 1$. Let $p, k \in \mathbf{Z}$ be fixed, non-zero integers, and let $\ell \in \mathbf{Z}$ be any integer. Let $\lambda(\ell) = k(p\ell+1)^4$, and let $G(\lambda(\ell))$, $H(\lambda(\ell)), K(\lambda(\ell))$, $A(\ell), B(\ell), C(\ell)$ be as in Lemmas*

1 *and* 2. *Let* $n(\ell)$ *be defined as in Lemma* 3. *Consider*

$$E_\tau^{n(\ell)} : Y^2 = X(X - n(\ell)\tau)(X + n(\ell)\tau^{-1}).$$

Then $E_\tau^{n(\ell)}$ *is an elliptic curve and has rank at least two for all but finitely many values of* ℓ.

Proof. Let $\mathcal{O}$ denote the point at infinity on $E_\tau^{n(\ell)}$. The discriminant for $E_\tau^{n(\ell)}$ is zero if and only if either

$$4a^3b^3p^2(2a^3b^3p^2\lambda(\ell) + ab^5p^2\lambda(\ell) + 1)\lambda(\ell) + 1 = 0$$

or

$$abp^2(a^4 - a^2b^2 - b^4)\lambda(\ell) - 1 = 0.$$

The former equation is an octic polynomial in the variable ℓ and hence can have at most 8 possible integral solutions, and the latter is a quartic in ℓ and hence can have at most 4 possible integral solutions. Therefore $E_\tau^{n(\ell)}$ is an elliptic curve with at most finitely many exceptions.

We now proceed by descent via 2-isogeny. Let α denote the fundamental 2-descent map as in the beginning of Section 3. It will suffice to show that

$$|\alpha(E_\tau^{n(\ell)}(\mathbf{Q}))| \geq 16.$$

Notice that $(0,0) \in E_\tau^{n(\ell)}(\mathbf{Q})$ and

$$\alpha((0,0)) \equiv -(n(\ell))^2 \equiv -1 \pmod{(\mathbf{Q}^*)^2},$$

thus we have $\{\pm 1\} \subseteq \alpha(E_\tau^{n(\ell)}(\mathbf{Q}))$. We also have $(n(\ell)\tau, 0) \in E_\tau^{n(\ell)}(\mathbf{Q})$. If

$$\alpha((n(\ell)\tau, 0)) \equiv \pm 1 \pmod{(\mathbf{Q}^*)^2},$$

then

$$(\lambda(\ell)ab)G(\lambda(\ell)) \equiv \pm 1 \pmod{(\mathbf{Q}^*)^2}.$$

Lemma 1 implies that this equation is true for only finitely many values of $\lambda(\ell)$, hence for only finitely many values of ℓ. Thus

$$\{\pm 1, \pm\alpha((n(\ell)\tau, 0))\} \subseteq \alpha(E_\tau^{n(\ell)}(\mathbf{Q}))$$

and $|\alpha(E_\tau^{n(\ell)}(\mathbf{Q}))| \geq 4$ for all but finitely many values of ℓ. Henceforth, for simplicity, we will just list the generators of $\alpha(E_\tau^{n(\ell)}(\mathbf{Q}))$.

The equation

$$\begin{aligned} X(P_1) = -(\lambda(\ell))^2(4a^2b^4p^2)((4a^6b^4p^4)(a^2 + b^2) \\ (\lambda(\ell))^2 + 1)((abp^2)(a^4 - a^2b^2 - b^4) \\ (\lambda(\ell)) - 1)^2 \end{aligned}$$

is the X-coordinate of a point $P_1 \in E_\tau^{n(\ell)}(\mathbf{Q})$. We see that

$$\alpha(P_1) \equiv -A(\ell) \pmod{(\mathbf{Q}^*)^2}.$$

Lemma 2 implies the equation

$$\alpha(P_1) \equiv \pm 1 \pmod{(\mathbf{Q}^*)^2}$$

is true for at most finitely many values of ℓ. If

$$\alpha(P_1) \equiv \pm\alpha((n(\ell)\tau, 0)) \pmod{(\mathbf{Q}^*)^2},$$

then

$$\begin{aligned} \alpha(P_1)\alpha((n(\ell)\tau, 0)) &\equiv (\lambda(\ell)ab)H(\lambda(\ell)) \\ &\equiv \pm 1 \pmod{(\mathbf{Q}^*)^2}. \end{aligned}$$

Lemma 1 implies this equation is true for at most finitely many values of $\lambda(\ell)$, hence for only finitely many values of ℓ. Thus

$$\langle -1, \alpha((n(\ell), 0)), \alpha(P_1)\rangle \subseteq \alpha(E_\tau^{n(\ell)}(\mathbf{Q}))$$

and $|\alpha(E_\tau^{n(\ell)}(\mathbf{Q}))| \geq 8$ for all but finitely many values of ℓ.

The equation

$$\begin{aligned} X(P_2) = a^{-1} \cdot ((\lambda(\ell)b)((4a^6b^4p^4)(a^2 + b^2)(\lambda(\ell))^2 + 1) \\ (2a^5bp^2\lambda(\ell) - 1)^2 \\ ((abp^2)(a^4 - a^2b^2 - b^4)\lambda(\ell) - 1)) \end{aligned}$$

is the X-coordinate of a point $P_2 \in E_\tau^{n(\ell)}(\mathbf{Q})$. Applying α gives

$$\begin{aligned} \alpha(P_2) &\equiv \frac{(\lambda(\ell)b)K(\lambda(\ell))}{a} \\ &\equiv (\lambda(\ell)ab)K(\lambda(\ell)) \pmod{(\mathbf{Q}^*)^2}. \end{aligned}$$

Lemma 1 implies that

$$\alpha(P_2) \equiv \pm 1 \pmod{(\mathbf{Q}^*)^2}$$

is true for at most finitely many values of $\lambda(\ell)$, hence for only finitely many values of ℓ. If

$$\alpha(P_2) \equiv \pm\alpha((n(\ell)\tau, 0)) \pmod{(\mathbf{Q}^*)^2},$$

then

$$\alpha(P_2)\alpha((n(\ell)\tau, 0)) \equiv B(\ell) \equiv \pm 1 \pmod{(\mathbf{Q}^*)^2}.$$

Lemma 2 implies this equation is true for at most finitely many values of ℓ. If

$$\alpha(P_1) \equiv \pm\alpha(P_2) \pmod{(\mathbf{Q}^*)^2},$$

then

$$\alpha(P_1)\alpha(P_2) \equiv C(\ell) \equiv \pm 1 \pmod{(\mathbf{Q}^*)^2}.$$

Lemma 2 implies this equation is true for at most finitely many values of ℓ. Thus

$$\langle -1, \alpha((n(\ell)\tau, 0)), \alpha(P_1), \alpha(P_2)\rangle \subseteq \alpha(E_\tau^{n(\ell)}(\mathbf{Q}))$$

and $|\alpha(E_\tau^{n(\ell)}(\mathbf{Q}))| \geq 16$ for all but finitely many values of ℓ. Thus the rank of $E_\tau^{n(\ell)}$ is at least two with at most finitely many exceptions. □

Corollary 1. *Let $0 \neq \tau = a/b \in \mathbf{Q}$ be a fixed rational number with $\gcd(a, b) = 1$ and let $p, k \in \mathbf{Z}$ be fixed integers with p positive. Then there exist infinitely many rank two τ-congruent numbers n with $n \equiv k \pmod{p}$.*

Proof. Let $n = n(\ell)$ where $n(\ell)$ is the same as in Theorem 1. Then $E_\tau^{n(\ell)}$ is an elliptic curve with rank at least two, with at most finitely many exceptions by Theorem 1. Hence $n(\ell)$ is a rank two τ-congruent number for all but finitely many values of ℓ. Furthermore, $n(\ell) \equiv k \pmod{p}$ so that the result follows from Lemma 3. □

Acknowledgements. The author would like to thank Dr. Blair K. Spearman for the many helpful discussions and the anonymous referee(s) for their helpful suggestions in regards to the first draft of this paper.

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] H. Cohen, *Number theory. Vol. I. Tools and Diophantine equations*, Graduate Texts in Mathematics, 239, Springer, New York, 2007.

[5] C. T. Davis and B. K. Spearman, On the distribution of τ-congruent numbers, Proc. Japan Acad. Ser. A Math. Sci. **91** (2015), no. 7, 101–103.

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

[7] C. L. Siegel, Über einige Anwendungen diophantischer Approximationen [reprint of Abhandlungen der Preußischen Akademie der Wissenschaften. Physikalisch-mathematische Klasse 1929, Nr. 1, 1–41], in *On some applications of Diophantine approximations*, Quad./Monogr., 2, Ed. Norm., Pisa, 2014, pp. 81–138.

[8] J. H. Silverman and J. Tate, *Rational points on elliptic curves*, Undergraduate Texts in Mathematics, Springer-Verlag, New York, 1992.