C. R. Math. Rep. Acad. Sci. Canada Vol. **32** (2) 2010, pp. 33–39

ELLIPTIC CURVES AND FAMILIES OF CONGRUENT AND θ-CONGRUENT NUMBERS

SCOTT SITAR

Presented by David Boyd, FRSC

Abstract. We show that for any integer $M > 1$, any integer k, and any admissible angle θ, there are infinitely many θ-congruent numbers which are congruent to k modulo M. Our method is inspired by an argument used by Chahal for an analogous result on congruent numbers modulo 8. Since congruent numbers are $\pi/2$-congruent numbers, this also includes as a special case the parallel statement for congruent numbers, originally due to Bennett.

Résumé. Soit M un entier tel que $M > 1$, soit k un entier, et soit θ un angle admissible, nous montrons qu'il y a une infinité de nombres θ-congruents dans la classe de k modulo M. Notre méthode est inspirée par cela de Chahal, où il a montré le résultat analogue pour les nombres congruents modulo 8. Car les nombres congruents sont aussi des nombres $\pi/2$-congruents, notre travail contient aussi le résultat analogue pour les nombres congruents, démontré initialement par Bennett.

1. Introduction.

A rational number n is called *congruent* if it is the area of a right triangle whose sides are also rational numbers. If such a triangle exists, we may always scale its sides so that its area becomes an integer. This means that to classify all rational numbers which are congruent, it suffices to classify all integers which are congruent. We call an integer which is congruent a *congruent number.*

The study of congruent numbers is very old, and an excellent account of its history is given in [3]. What makes the problem so intriguing, however, is that although the statement is elementary, the only test for determining whether a given integer is congruent relies on one of the central conjectures in the theory of elliptic curves, namely the conjecture of Birch and Swinnerton-Dyer. In particular, this conjecture would also imply that every integer which is congruent to 5, 6, or 7 modulo 8 would be a congruent number. For an exposition of the techniques used in connecting congruent numbers to elliptic curves, see [7].

Our first focus will be to illuminate and extend the argument given by Chahal in [2] and [3]. He uses a polynomial identity due to Desboves [4] to explicitly construct infinitely many congruent numbers in each residue class modulo 8.

Received by the editors on June 22, 2009.
The author was supported in part by an NSERC fellowship.
AMS Subject Classification: Primary: 11D25; secondary: 11G05.

While this is interesting in light of the above conjecture, it is not the complete story. We will use the identity of Desboves to show that, in fact, we can obtain another proof of the much stronger result, originally proved by Bennett in [1].

Theorem 1.1. *Let $M > 1$ be any integer. Then for any integer k, there are infinitely many congruent numbers n which satisfy $n \equiv k \pmod{M}$.*

While this is an easy corollary of Theorem 1.2 below, it is instructive to write down a proof in the spirit of Chahal's original argument, since this brings to light a direct connection between Desboves' identity and the "congruent number curve". In particular, we will show that in a certain sense, this identity can in fact be used to generate *all* congruent numbers.

As a generalization of congruent numbers, Fujiwara in [5] defined the notion of a θ-congruent number for angles $0 < \theta < \pi$ such that $\cos\theta = \frac{s}{r}$ where r and s are integers satisfying $|s| \leq r$ and $(r, s) = 1$. For such a θ, a number n is called *θ-congruent* if $n\sqrt{r^2 - s^2}$ is the area of a triangle having rational sides and an angle θ. Note that for $r = 1$ and $s = 0$, this reduces to the usual notion of a congruent number. In a similar spirit to our generation of congruent numbers, we will be able to produce families of θ-congruent numbers for all moduli and residue classes by making particular choices for an arbitrary parametrizing function. In particular, we prove the following.

Theorem 1.2. *Fix r, s, and θ as above. For any integer $M > 1$ and any integer k, there are infinitely many θ-congruent numbers n which satisfy $n \equiv k$ $\pmod{M}$.*

If we choose $r = 1$ and $s = 0$, we recover the result of Theorem 1.1. Also, by picking $r = 2$ and $s = -1$, we obtain infinitely many $2\pi/3$-congruent numbers in each residue class for each modulus, which is interesting in light of the conjectures stated in [6].

2. Using the identity of Desboves.

It is well known [7] that in order to demonstrate that an integer N is congruent, one need only produce a rational point on the elliptic curve $Y^2 = X^3 - N^2X$ such that the Y-coordinate is nonzero. In order to generate this point, we follow Chahal in turning to the identity of Desboves [4]:

$$(y^2 + 2xy - x^2)^4 + (2x^3y + x^2y^2)(2x + 2y)^4 = (x^4 + y^4 + 10x^2y^2 + 4xy^3 + 12x^3y)^2. \tag{2.1}$$

Our particular use for this identity will be to generate solutions to the equation $s^4 + At^4 = u^2$, where A has the form $x^2y(2x + y)$. If we can generate such a solution with $t \neq 0$, then we can in fact generate a rational point on the elliptic curve $Y^2 = X^3 + AX$ through the equations

$$X = \frac{s^2}{t^2} \quad \text{and} \quad Y = \frac{su}{t^3}.$$

Moreover, if our solution leads to a choice of A such that $-A$ is a perfect square and $Y \neq 0$, then we will have succeeded in showing that $\sqrt{-A}$ is a congruent number. Therefore, we set ourselves with the following task: substitute rational numbers for x and y in (2.1) such that in the resulting solution of the equation $s^4 + At^4 = u^2$, we have $stu \neq 0$ and $-A$ being a perfect rational square.

This is where our argument begins to deviate from [2]. We wish to ensure that $-A = -x^2y(2x + y)$ is a square, but we do not want to accomplish this by imposing the condition that $-x^2y = 2x + y$, which was a consequence of the choices made in [2]. Instead, we will avoid triviality by supposing that both x and y are non-zero, and we will write $x = \frac{a}{b}$ and $y = \frac{c}{d}$ for integers a, b, c, and d, giving

$$-A = -\Big(\frac{a}{b^2d}\Big)^2 bc(2ad + bc).$$

This will be a rational square if and only if $-bc(2ad + bc)$ is an integral square. By writing the factors as

$$(2.2) \qquad 2ad + bc = v^2u \quad \text{and} \quad -bc = w^2u$$

with u, v, and w integers and u square free, we can solve for ad and bc, giving

$$ad = \frac{u(v^2 + w^2)}{2} \quad \text{and} \quad bc = -w^2u.$$

When these are substituted back into $-A$, we obtain

$$-A = \Big(\frac{a}{b^2d}\Big)^2 v^2w^2u^2,$$

and so our candidate congruent number will be

$$\frac{avwu}{b^2d} = \frac{advwu}{b^2d^2} = 2vw(v^2 + w^2)\Big(\frac{u}{2bd}\Big)^2,$$

where this will be congruent if and only if $2vw(v^2 + w^2)$ is congruent. Note that given a pair (v, w), we can recover x and y up to a scalar multiple by dividing the two equations (2.2):

$$\frac{2ad + bc}{-bc} = \Big(\frac{v}{w}\Big)^2 \implies \frac{a}{b}\frac{d}{c} = -\frac{1}{2} - \frac{1}{2}\Big(\frac{v}{w}\Big)^2 \implies x = \frac{1}{2}\bigg(-1 - \Big(\frac{v}{w}\Big)^2\bigg)y.$$

In particular, we cannot have $x = -y$ unless $v = \pm w$, so in what follows we will always pick v and w so that $x \neq -y$. We will call this our non-degeneracy condition.

Next, we must ensure that with these choices, we have a solution to the equation $s^4 + At^4 = u^2$ such that $stu \neq 0$. To guarantee that $t \neq 0$, it is necessary and sufficient to have $x \neq -y$, which we have already done. However, once this is enforced, s and u will automatically be non-zero. To see this, we notice that the constituent pieces of equation (2.1) are homogeneous polynomials, and we are making choices so that both x and y are non-zero. Therefore, having $s = 0$ is equivalent to the polynomial $z^2 + 2z - 1$ having a rational root, which it does not. Similarly, the condition $u = 0$ would mean that the polynomial $z^4 + 4z^3 + 10z^2 + 12z + 1$ has a rational root, which it does not.

To ensure that the prime 2 does not cause undue difficulty, we will further suppose that v is even, so writing $v = 2v'$ makes our candidate congruent number

$$4v'w(4(v')^2 + w^2),$$

which will be congruent if and only if $v'w(4(v')^2+w^2)$ is congruent. This disposes of the inconvenient leading factor of 2 without compromising the generality of the method. Reverting back to using v instead of v', this means that we must investigate the possible values of the quartic form $vw(4v^2+w^2)$ modulo arbitrary integers M to see which congruent numbers can be so constructed. Our non-degeneracy condition now becomes $w \neq \pm 2v$, which we can always guarantee to be satisfied by adding a multiple of our modulus to either w or v, if necessary.

3. Generating congruent numbers in arbitrary residue classes.

The proof of Theorem 1.1 now follows swiftly from our above discussion. Let us choose any integer $M > 1$ and any integer k. If we substitute $w = 1$ and $v = kM^2$ into our congruent number producing quartic form $vw(4v^2 + w^2)$, we obtain the congruent number

$$kM^2(1 + 4k^2M^4) \equiv kM^2 \pmod{M^3}.$$

Therefore, by scaling the corresponding triangle to remove the square factor M^2, we obtain a congruent number which is congruent to k modulo M. Since k and M were chosen arbitrarily, and since we may add arbitrary multiples of M^3 to v and w to ensure our non-degeneracy condition is satisfied, this completes the proof of Theorem 1.1.

4. Generating all congruent numbers.

In order to justify the attention we are giving to this method of constructing congruent numbers and to explain its effectiveness at generating them, let us look slightly more carefully at the quartic form $vw(4v^2 + w^2)$, which was obtained as one of the components of a specialization of Desboves' identity. We have already seen that substituting non-zero values for v and w such that $w \neq \pm 2v$ yields congruent numbers, but the numbers we are generating will most likely not be squarefree. Let us therefore look at the equation

$$vw(4v^2 + w^2) = Nz^2,$$

where for non-zero values of v and w, we can find corresponding values for N and z, with N squarefree. However, on making the change of variables

$$X = \frac{Nw}{v} \quad \text{and} \quad Y = \frac{N^2 z}{v^2}, \tag{4.1}$$

we see that we have a point on the curve $Y^2 = X^3 + (2N)^2X$ where both X and Y are non-zero. Then, by applying the standard 2-isogeny which is used in the proof of the Mordell–Weil theorem over $\mathbb{Q}$ for elliptic curves with a rational 2-torsion point, namely

$$\phi(X,Y) = \Big(\frac{Y^2}{X^2}, \frac{Y\big(X^2 - (2N)^2\big)}{X^2}\Big) = (S,T),$$

we obtain a rational point on the curve

$$T^2 = S^3 - 4(2N)^2S = S^3 - 16N^2S,$$

where we certainly have $S \neq 0$. However, $T = 0$ if and only if $X^2 - (2N)^2 = 0$, but after filling in the values of the variables, this means that $w = \pm 2v$, which violates our non-degeneracy condition. Finally, we can eliminate the factor of 16 by a simple scaling of variables, giving us a non-2-torsion point on the congruent number curve for N.

The key observation is that this process can be reversed. Let N be a squarefree congruent number. This means we can find non-zero rational numbers S and T such that $T^2 = S^3 - N^2S$. By rescaling to reintroduce the factor of 16, we then apply the dual isogeny to ϕ, which is obtained from ϕ by replacing $-(2N)^2$ in the numerator of the second component with $16N^2$. This leads to a point on $Y^2 = X^3 + (2N)^2X$ with $X, Y \neq 0$. Then, by using (4.1), we can find integers v, w, and z such that $vw(4v^2 + w^2) = Nz^2$. Therefore, N occurs as the squarefree part of a value of $vw(4v^2 + w^2)$, so in this way, this quartic form essentially generates all congruent numbers.

We should also mention that the polynomial identity employed by Bennett in [1] can also be brought to the congruent number curve by a similar rational transformation.

5. θ-congruent numbers.

We will now start afresh and attempt a similar approach to generate families of θ-congruent numbers. We will fix our notation so that r and s are integers with $|s| < r$ and $(r,s) = 1$. Also, we will have an angle $0 < \theta < \pi$ such that $\cos\theta = \frac{s}{r}$. The key ingredient to our previous argument was a characterization of congruent numbers in terms of rational points on elliptic curves. Fortunately, we have a similar resource for θ-congruent numbers. In particular, Fujiwara proves in [5] that a number n will be a θ-congruent number if and only if the elliptic curve

$$Y^2 = X\big(X + (r+s)n\big)\big(X - (r-s)n\big) \tag{5.1}$$

has a rational point other than a 2-torsion point. This means we just need to find a rational point on this curve with $Y \neq 0$.

In the spirit of Chahal's original argument, we will try to accomplish this by means of an algebraic identity which will give us a parametrized family of θ-congruent numbers, for any admissible θ we wish. Since Desboves' identity was an identity between homogeneous polynomials, it is reasonable for us to search for a similar single-variable identity and then "projectivize" to introduce the second variable.

To find rational solutions to equation (5.1) with $Y \neq 0$, let us try to choose $X = f(x)$ and $X + (r+s)n = g(x)$ in such a way that $X - (r-s)n = f(x)g(x)$, where x will be an arbitrary parameter. If we can do this, then the product of the three factors will be a perfect square. On eliminating X and n from these equations, we are led to the choices:

$$g(x) = \frac{2rf(x)}{(r-s)+(r+s)f(x)}, \quad n = \frac{f(x)\bigl(1-f(x)\bigr)}{(r-s)+(r+s)f(x)},$$
$$Y = f(x)g(x), \qquad X = g(x) - (r+s)n.$$

Each of the quantities defined above depends only on the quantities that have already been defined, and thus give a formal solution of equation (5.1). Therefore, if we make a particular choice of $f(x)$ and x such that $f(x) \neq \frac{s-r}{s+r}$ and $f(x) \neq 0$, then the corresponding n will be a θ-congruent number. We will call these our non-degeneracy conditions. One particular choice gives us the following stepping stone towards the proof of Theorem 1.2:

Lemma 5.1. *Let $N > 1$ be an integer, and let ℓ be any integer. Then there are infinitely many θ-congruent numbers congruent to $\ell(r+s)N^2$ modulo N^3.*

Proof. We will make the choice $f(x) = \frac{ax+b}{cx+d}$, where $a \equiv c \equiv 0 \pmod{N^3}$, $b \equiv 1 \pmod{N^3}$, and $d \equiv -\ell N^2 \pmod{N^3}$. We then let $x = p/q$ where $p \equiv 0 \pmod{N^3}$ and $q \equiv 1 \pmod{N^3}$. When these choices are substituted into our expression for n, we can clear denominators by introducing square factors to find that we obtain a θ-congruent number which is congruent to $\ell(r+s)N^2$ modulo N^3. Note that we may satisfy all of the non-degeneracy conditions above by adjusting our choices by multiples of N^3, if necessary. □

To finish the proof of Theorem 1.2 using this lemma, pick any integer $M > 1$ and any integer k. If we let $N = M(r+s)^2$ and $\ell = k(r+s)$, then the previous lemma tells us that there are infinitely many congruent numbers n such that

$$n \equiv kM^2(r+s)^6 \bigl(\operatorname{mod} M^3(r+s)^6\bigr).$$

Therefore, we may now scale by the square factor $M^2(r+s)^6$ to obtain infinitely many θ-congruent numbers congruent to k modulo M, as desired.

We should mention that quartic forms have been associated to θ-congruent numbers before. In [6], Kan proves that a squarefree integer n will be θ-congruent if and only if it is the squarefree part of $pq(p+q)\big(2rq+p(r-s)\big)$ for some integers p and q. This result is the exact analogue of our observation that the quartic form which is produced by our extension to Chahal's argument can be brought to the congruent number curve by a rational transformation.

However, while this quartic form will generate all θ-congruent numbers in a certain sense, the actual numbers represented by the form will miss quite a few residue classes. For example, it will only generate numbers which are congruent to 0, 2, 6, 8, 12, 14, 18, or 20 (mod 24). With the choice of parametrizing functions

$$f(x) = \frac{4x}{4x+1} \quad \text{and} \quad f(x) = \frac{864x+1}{864x+604},$$

we can produce two quartic forms, which taken together produce infinitely many $2\pi/3$-congruent numbers in every residue class modulo 24, without needing to adjust by square factors.

References

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

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

3. ———, *Congruent numbers and elliptic curves.* Amer. Math. Monthly **113** (2006), no. 4, 308–317.

4. A. Desboves, *Sur l'emploi des identités algébriques dans la résolution, en nombres entiers, des équations d'un degré supérieur au second.* Comptes Rendus Paris **87** (1878), 159–161.

5. M. Fujiwara, *θ-congruent numbers.* In: Number Theory, de Gruyter, Berlin, 1998, pp. 235–241.

6. M. Kan, *θ-congruent numbers and elliptic curves.* Acta Arith. **94** (2000), no. 2, 153–160.

7. N. Koblitz, *Introduction to elliptic curves and modular forms.* Graduate Texts in Mathematics, 97, Springer-Verlag, New York, 1984.

Department of Mathematics
University of British Columbia
Vancouver, BC
V6T 1Z2
email: scottsitar@gmail.com