THE CONGRUENT NUMBER PROBLEM

KEITH CONRAD

1. Introduction

A right triangle is called *rational* when its legs and hypotenuse are all rational numbers. Examples of rational right triangles include Pythagorean triples like $(3, 4, 5)$. We can scale such triples to get other rational right triangles, like $(3/2, 2, 5/2)$. Of course, usually when two sides are rational the third side is not rational, such as the $(1, 1, \sqrt{2})$ right triangle.

Any rational right triangle has a rational area, but not all (positive) rational numbers can occur as the area of a rational right triangle. For instance, no rational right triangle has area 1. This was proved by Fermat. The question we will examine here is: which rational numbers occur as the area of a rational right triangle?

Definition 1.1. A positive rational number n is called a *congruent number* if there is a rational right triangle with area n: there are rational $a, b, c > 0$ such that $a^2 + b^2 = c^2$ and $(1/2)ab = n$.

In Figure 1 are rational right triangles with respective areas 5, 6, and 7, so these three numbers are congruent numbers.

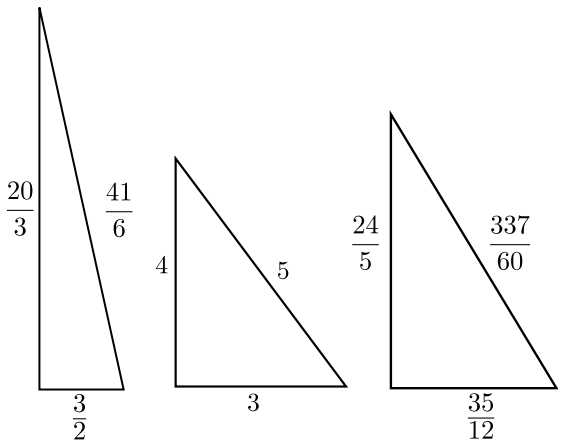

Figure 1. Rational right triangles with respective areas 5, 6, and 7.

This use of the word congruent has nothing to do (directly) with congruences in modular arithmetic. The etymology will be explained in Section 3. The history of congruent numbers can be found in [3, Chap. XVI], where it is indicated that an Arab manuscript called the search for congruent numbers the "principal object of the theory of rational right triangles."

The congruent number problem asks for a description of all congruent numbers. Since scaling a triangle changes its area by a square factor, and every rational number can be multiplied by a suitable rational square to become a squarefree integer (*e.g.*, $18/7 = 3^2 \cdot 2/7$,

so multiplying by $(7/3)^2$ produces the squarefree integer 14), we can focus our attention in the congruent number problem on squarefree positive integers. For instance, to say 1 is not a congruent number means no rational square is a congruent number.

When n is squarefree in $\mathbf{Z}^+$, to show n is a congruent number we just need to find an integral right triangle whose area has squarefree part n. Then writing the area as m^2n shows scaling the sides by m produces a rational right triangle with area n.

In Section 2, the parametrization of Pythagorean triples will be used to construct a lousy algorithm generating all congruent numbers. The equivalence of the congruent number problem with a problem about rational squares in arithmetic progressions is in Section 3. Section 4 gives an equivalence between the congruent number problem and the search for rational points on $y^2 = x^3 - n^2x$ where $y \neq 0$, which ultimately leads to a solution of the congruent number problem (depending in part on the Birch and Swinnerton-Dyer conjecture, a famous open problem in mathematics). In the appendices we explain some algebraically mysterious formulas from our treatment using projective geometry and give a relation between the congruent number problem and other Diophantine equations.

Acknowledgments. I thank Lucas David-Roesler for generating the pictures.

2. A bad algorithm

There is a parametric formula for primitive Pythagorean triples, and we will use it to make a small list of squarefree congruent numbers. A primitive triple (with even second leg) is $(k^2 - \ell^2, 2k\ell, k^2 + \ell^2)$ where $k > \ell > 0$, $(k, \ell) = 1$, and $k \not\equiv \ell \bmod 2$. In Table 1 we list such primitive triples where $k + \ell \leq 9$. The squarefree part of the area is listed in the last column. Each number in the fourth column is a congruent number and each number in the fifth column is also a congruent number. The final row of the table explains how a rational right triangle with area 5 can be found.

k	ℓ	(a, b, c)	$(1/2)ab$	Squarefree part
2	1	$(3, 4, 5)$	6	6
4	1	$(15, 8, 17)$	60	15
3	2	$(5, 12, 13)$	30	30
6	1	$(35, 12, 37)$	210	210
5	2	$(21, 20, 29)$	210	210
4	3	$(7, 24, 25)$	84	21
8	1	$(63, 16, 65)$	504	126
7	2	$(45, 28, 53)$	630	70
5	4	$(9, 40, 41)$	180	5

Table 1. Congruent Numbers.

Notice 210 shows up twice in Table 1. Do other numbers which occur once also occur again? We will return to this question later.

Table 1 can be extended as $k + \ell$ increases, and each squarefree congruent number eventually occurs in the last column: if the squarefree number m is the area of a rational right triangle with sides a/d, b/d, and c/d, using minimal common denominator d, then (a, b, c) is a primitive Pythagorean triple with area md^2, whose squarefree part is m. Alas, the table is *not* systematic in the appearance of the last column: we can't tell by building the table when

any particular number should occur, if at all, in the last column, so this method of generating (squarefree) congruent numbers is not a good algorithm. For instance, 53 is a congruent number, but it shows up for the first time when $k = 1873180325$ and $\ell = 1158313156$. (The corresponding right triangle has area $53 \cdot 297855654284978790^2$.)

Tables of congruent numbers are in 10th century Arabic manuscripts, where 5 and 6 appear [3, p. 459]. Fibonacci found in the 13th century that 7 is congruent and he stated that 1 is *not* congruent (no rational right triangle has area equal to a perfect square). The first proof of that is by Fermat and a proof likely due to him shows 2 is not congruent [12, pp. 75–77]. That 3 is not congruent is due to Genocchi [4, pp. 101-103], who showed primes $p \equiv 3 \bmod 8$ are not congruent. Hemenway [5, §1.3] translated the argument into English.

Theorem 2.1 (Fermat, 1640)**.** *The number* 1 *is not congruent.*

Proof. We will use the method of descent, which was discovered by Fermat on this very problem. Our argument is adapted from [2, pp. 658–659].

Assume a rational right triangle has area 1. Call the sides a/d, b/d, and c/d, where a, b, c, and d are positive integers, so $a^2 + b^2 = c^2$ and $(1/2)ab = d^2$. (In other words, if some rational right triangle has area 1 then some Pythagorean triangle has area equal to a perfect square. The converse is true too.) Clearing the denominator in the second equation,

$$a^2 + b^2 = c^2, \quad ab = 2d^2. \tag{2.1}$$

We will show (2.1) has no positive integer solutions.

Assume there is a solution to (2.1) in positive integers. Let's show there is then a solution where a and b are relatively prime. Set $g = (a, b)$, so $g \mid a$ and $g \mid b$. Then $g^2 \mid c^2$ and $g^2 \mid 2d^2$, so $g \mid c$ and $g \mid d$ (why?). Divide a, b, c, and d by g to get another 4-tuple of positive integers satisfying (2.1) with $(a, b) = 1$. So we may now focus on showing (2.1) has no solution in positive integers with the extra condition that $(a, b) = 1$.

We will do this using Fermat's method of descent: construct a new 4-tuple of positive integers a', b', c', d' satisfying (2.1) with $(a', b') = 1$ and $0 < c' < c$. Repeating this enough times, we reach a contradiction. Several times in the descent process we will use the following (or minor variations on it): two positive relatively prime integers whose product is a perfect square must each be perfect squares.

Now we start the descent. Since $ab = 2d^2$ and a and b are relatively prime, a or b is even but not both. Then $c^2 = a^2 + b^2$ is odd, so c is odd. Since ab is twice a square, $(a, b) = 1$, and a and b are positive, one is a square and the other is twice a square. The roles of a and b are symmetric, so without loss of generality a is even and b is odd. Then

$$a = 2k^2, \quad b = \ell^2$$

for some positive integers k and ℓ, with ℓ odd (because b is odd). The first equation in (2.1) now looks like $4k^4 + b^2 = c^2$, so $\frac{c+b}{2}\frac{c-b}{2} = k^4$. Because b and c are both odd and relatively prime, $(c + b)/2$ and $(c - b)/2$ are relatively prime. Therefore

$$\frac{c+b}{2} = r^4, \quad \frac{c-b}{2} = s^4$$

for some relatively prime positive integers r and s. Solve for b and c by adding and subtracting these equations:

$$b = r^4 - s^4, \quad c = r^4 + s^4,$$

so $\ell^2 = b = (r^2 + s^2)(r^2 - s^2)$. The factors $r^2 + s^2$ and $r^2 - s^2$ are relatively prime: any common factor would be odd (since ℓ is odd) and divides the sum $2r^2$ and the difference

$2s^2$, so is a factor of $(r^2, s^2) = 1$. Since the product of $r^2 + s^2$ and $r^2 - s^2$ is an odd square and one of these is positive, the other is positive and

$$r^2 + s^2 = t^2, \quad r^2 - s^2 = u^2 \tag{2.2}$$

for odd positive integers t and u which are relatively prime. Since $u^2 \equiv 1 \bmod 4$, $r^2 - s^2 \equiv 1 \bmod 4$, which forces r to be odd and s to be even.[1] Solving for r^2 in (2.2),

$$r^2 = \frac{t^2 + u^2}{2} = \left(\frac{t+u}{2}\right)^2 + \left(\frac{t-u}{2}\right)^2, \tag{2.3}$$

where $(t \pm u)/2 \in \mathbf{Z}$ since t and u are odd.

Equation (2.3) will give us a "smaller" version of (2.1). Setting

$$a' = \frac{t+u}{2}, \quad b' = \frac{t-u}{2}, \quad c' = r,$$

we have $a'^2 + b'^2 = c'^2$. From $(t, u) = 1$ we get $(a', b') = 1$. Moreover, using (2.2), $a'b' = (t^2 - u^2)/4 = 2s^2/4 = 2(s/2)^2$. Let $d' = s/2 \in \mathbf{Z}$, so we have a new solution (a', b', c', d') to (2.1). Since $0 < c' = r \leq r^4 < r^4 + s^4 = c$, by descent we get a contradiction. □

Theorem 2.1 leads to a weird proof that $\sqrt{2}$ is irrational. If $\sqrt{2}$ were rational then $\sqrt{2}$, $\sqrt{2}$, and 2 would be the sides of a rational right triangle with area 1. This is a contradiction of 1 not being a congruent number!

3. Relation to Arithmetic Progressions of Three Squares

The squares 1, 25, 49 form an arithmetic progression with common difference 24, whose squarefree part is 6. This is related to 6 being a congruent number, by the next theorem.

Theorem 3.1. *Let $n > 0$. There is a one-to-one correspondence between right triangles with area n and 3-term arithmetic progressions of squares with common difference n: the sets*

$$\{(a, b, c) : a^2 + b^2 = c^2, (1/2)ab = n\}, \quad \{(r, s, t) : s^2 - r^2 = n, t^2 - s^2 = n\}$$

are in one-to-one correspondence by

$$(a, b, c) \mapsto ((b - a)/2, c/2, (b + a)/2), \quad (r, s, t) \mapsto (t - r, t + r, 2s).$$

Proof. It is left to the reader to check the indicated functions take values in the indicated sets, and that the correspondences are inverses of one another: if you start with an (a, b, c) and make an (r, s, t) from it, and then form an (a', b', c') from this (r, s, t), you get back the original (a, b, c). Similarly, starting with an (r, s, t), producing an (a, b, c) from it and then producing an (r', s', t') from that returns the same (r, s, t) you started with. □

How could the correspondence in Theorem 3.1 be discovered? When $s^2 - r^2 = n$ and $t^2 - s^2 = n$, adding gives $t^2 - r^2 = 2n$, so $(t - r)(t + r) = 2n$. This suggests using $a = t - r$ and $b = t + r$. Then $a^2 + b^2 = 2(t^2 + r^2) = 2(2s^2) = (2s)^2$, so use $c = 2s$.

For rational $n > 0$, the correspondence in Theorem 3.1 preserves rationality and positivity/monotonicity: (a, b, c) is a rational triple if and only if (r, s, t) is a rational triple, and $0 < a < b < c$ if and only if $0 < r < s < t$. So n is congruent if and only if there is a rational square s^2 such that $s^2 - n$ and $s^2 + n$ are squares. Note the correspondence in Theorem 3.1 involves not the squares in arithmetic progression but their square roots r, s, and t.

[1] Odd squares are 1 mod 4 and even squares are 0 mod 4, so the only way $r^2 - s^2$ can be 1 mod 4 is for r to be odd and s to even,

Example 3.2. For $n = 6$, using $(a, b, c) = (3, 4, 5)$ in Theorem 3.1 produces $(r, s, t) = (1/2, 5/2, 7/2)$, whose termwise squares are the arithmetic progression $1/4, 25/4, 49/4$ with common difference 6.

Example 3.3. Taking $n = 5$ and $(a, b, c) = (3/2, 20/3, 41/6)$, the correspondence in Theorem 3.1 yields $(r, s, t) = (31/12, 41/12, 49/12)$: the rational squares $(31/12)^2$, $(41/12)^2$, $(49/12)^2$ are an arithmetic progression with common difference 5.

Example 3.4. Since Fermat showed 1 and 2 are not congruent numbers, there is no arithmetic progression of 3 rational squares with common difference 1 or 2 (or, more generally, common difference a nonzero square or twice a nonzero square).

We now can explain the origin of the peculiar name "congruent number." Fibonacci, in his book *Liber Quadratorum* (Book of Squares) from 1225, called an integer n a *congruum* if there is an integer x such that $x^2 \pm n$ are both squares. This means $x^2 - n, x^2, x^2 + n$ is a 3-term arithmetic progression of squares. Fibonacci's motivation for writing his book was the study of 3-term arithmetic progressions of integral (rather than rational) squares. Both words congruum and congruence come from the Latin *congruere*, which means "to meet together" (to congregate!). A congruum is a number related to three integer squares in a kind of agreement (having a common difference). Considering a congruum multiplied by rational squares (*e.g.*, $24 \cdot (1/2)^2 = 6$) gives the congruent numbers.

4. The Curve $y^2 = x^3 - n^2x$

Whether or not n is congruent is related to solvability of *pairs* of equations: first, by definition we need to solve $a^2 + b^2 = c^2$ and $(1/2)ab = n$ in positive rational numbers a, b, and c. In Section 3 we saw this is equivalent to solving a second pair of equations in positive rational numbers: $s^2 - r^2 = n$ and $t^2 - s^2 = n$. It turns out that the congruent number property is also equivalent to (nontrivial) rational solvability of the single equation $y^2 = x^3 - n^2x$.

This equation has three obvious rational solutions: $(0, 0)$, $(n, 0)$, and $(-n, 0)$. These are the solutions with $y = 0$.

Theorem 4.1. *For $n > 0$, there is a one-to-one correspondence between the following two sets:*

$$\{(a, b, c) : a^2 + b^2 = c^2, (1/2)ab = n\}, \quad \{(x, y) : y^2 = x^3 - n^2x, y \neq 0\}.$$

Mutually inverse correspondences between these sets are

$$(a, b, c) \mapsto \left(\frac{nb}{c - a}, \frac{2n^2}{c - a}\right), \quad (x, y) \mapsto \left(\frac{x^2 - n^2}{y}, \frac{2nx}{y}, \frac{x^2 + n^2}{y}\right).$$

Proof. This is a direct calculation left to the reader. We divide by $c - a$ in the first formula, and $c \neq a$ automatically since if $c = a$ then $b = 0$, but $(1/2)ab = n$ is nonzero. Restricting y to a nonzero value is necessary since we divide by y in the second formula. □

Remark 4.2. It is of course natural to wonder how the correspondence in Theorem 4.1 could be discovered in the first place. See the appendix.

The correspondence in Theorem 4.1 preserves positivity: if a, b, and c are positive then $(c-a)(c+a) = b^2 > 0$, so $c-a$ is positive and thus $x = nb/(c-a) > 0$ and $y = 2n^2/(c-a) > 0$. In the other direction, if x and y are positive then from $y^2 = x^3 - n^2x = x(x^2 - n^2)$ we see $x^2 - n^2$ has to be positive, so a, b, and c are all positive. Also, for rational $n > 0$, (a, b, c)

is rational if and only if (x, y) is rational. Any solution to $a^2 + b^2 = c^2$ and $(1/2)ab = n$ needs a and b to have the same sign (since $ab = 2n > 0$), and by a sign adjustment there is a rational solution with a, b, and c all positive if there is any rational solution at all. Therefore a rational number $n > 0$ is congruent if and only if the equation $y^2 = x^3 - n^2x$ has a rational solution (x, y) with $y \neq 0$; we don't have to pay attention to whether or not x and y are positive.

A positive rational number n is *not* congruent if and only if the only rational solutions to $y^2 = x^3 - n^2x$ have $y = 0$: $(0, 0)$, $(n, 0)$, and $(-n, 0)$. For example, since 1 is not congruent (Theorem 2.1), the only rational solutions to $y^2 = x^3 - x$ have $y = 0$.

Example 4.3. Since 6 is the area of a $(3, 4, 5)$ right triangle, the equation $y^2 = x^3 - 36x$ has a rational solution with $y \neq 0$. The solution corresponding to the $(3, 4, 5)$ right triangle by Theorem 4.1 is $(x, y) = (12, 36)$. See Figure 2.

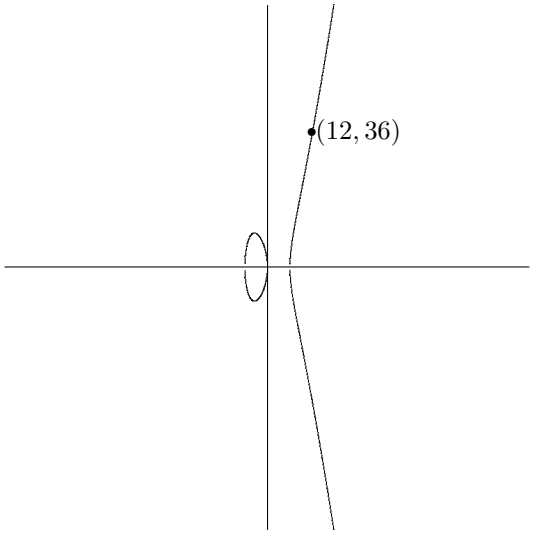

FIGURE 2. The rational point $(12, 36)$ on $y^2 = x^3 - 36x$.

Example 4.4. From the rational right triangle $(3/2, 20/3, 41/6)$ with area 5, Theorem 4.1 gives us a rational solution to $y^2 = x^3 - 25x$: $(x, y) = (25/4, 75/8)$. If we allow sign changes on the coordinates of $(3/2, 20/3, 41/6)$, Theorem 4.1 will give us new rational solutions to $y^2 = x^3 - 25x$. Using the triples of the form $(\pm 3/2, \pm 20/3, \pm 41/6)$ where the first two coordinates have the same sign, the new solutions we get to $y^2 = x^3 - 25x$ are collected in Table 2 and they are plotted on $y^2 = x^3 - 25x$ in Figure 3.

Example 4.5. A rational solution to $y^2 = x^3 - 49x$ is $(25, 120)$. Theorem 4.1 produces from this solution the rational right triangle $(24/5, 35/12, 337/60)$ with area 7, which we met already in Figure 1.

Example 4.6. In Table 1 we found two rational right triangles with area 210: $(35, 12, 37)$ and $(21, 20, 29)$. Using Theorem 4.1, these triangles lead to two rational solutions to $y^2 = x^3 - 210^2x$: $(1260, 44100)$ and $(525, 11025)$, respectively. In Figure 4, the line through $(1260, 44100)$ and $(525, 11025)$ meets the curve $y^2 = x^3 - 210^2x$ in a third point $(240, -1800)$.

Signs on $(3/2, 20/3, 41/6)$	(x, y)
$(+,+,+)$	$(25/4, 75/8)$
$(+,+,-)$	$(-4,-6)$
$(-,-,+)$	$(-4,6)$
$(-,-,-)$	$(25/4, -75/8)$

TABLE 2. Solutions to $y^2 = x^3 - 25x$.

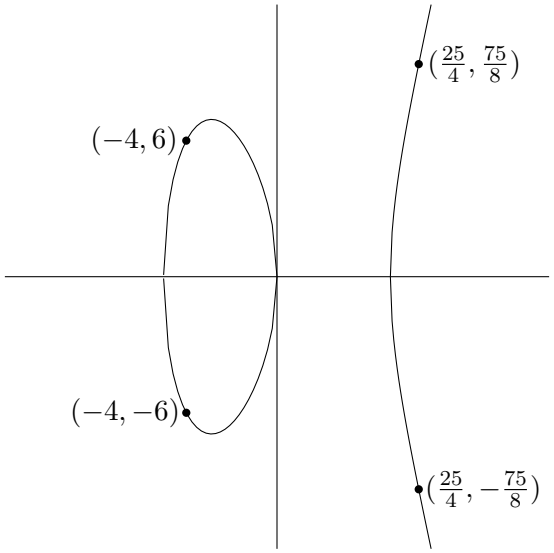

FIGURE 3. Some rational points on $y^2 = x^3 - 25x$.

Its second coordinate is negative, but the point $(240, 1800)$ is also on that curve, and it leads by Theorem 4.1 to the new rational right triangle $(15/2, 56, 113/2)$ with area 210.

Example 4.7. Suppose (a, b, c) satisfies $a^2 + b^2 = c^2$ and $(1/2)ab = n$. Such a solution gives rise to seven additional ones: $(-a, -b, -c)$ and

$$(a, b, -c), \quad (-a, -b, c), \quad (b, a, c), \quad (b, a, -c), \quad (-b, -a, c), \quad (-b, -a, -c).$$

These algebraic modifications have a geometric interpretation in terms of constructing new points from old ones on the curve $y^2 = x^3 - n^2x$ using secant lines. Say (a, b, c) corresponds to (x, y) by Theorem 4.1, so $y \neq 0$. From the point (x, y) on the curve we get automatically a second point: $(x, -y)$. This corresponds by Theorem 4.1 to $(-a, -b, -c)$. What points on the curve correspond to the six remaining algebraic modifications above?

Well, there are three obvious points on the curve which have nothing to do with our particular (x, y), namely $(0, 0)$, $(n, 0)$, and $(-n, 0)$. The line through (x, y) and $(0, 0)$ meets the curve in the point $(-n^2/x, -n^2y/x^2)$, which corresponds by Theorem 4.1 to $(a, b, -c)$. More generally, the three lines through (x, y) and each of $(0, 0)$, $(n, 0)$, and $(-n, 0)$ meet the curve in three additional points, and their reflections across the x-axis are an additional three points (which are where the lines through $(x, -y)$ and each of $(0, 0)$, $(n, 0)$, and $(-n, 0)$ meet the curve). See Table 3 and Figure 5. The corresponding triples from Theorem 4.1 are collected in Table 4 and are exactly what we were looking for.

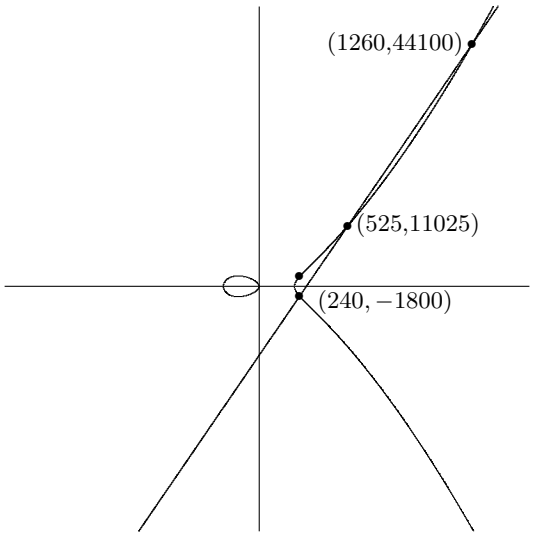

FIGURE 4. New rational point on $y^2 = x^3 - 210^2x$ from a secant line. (Not drawn to scale.)

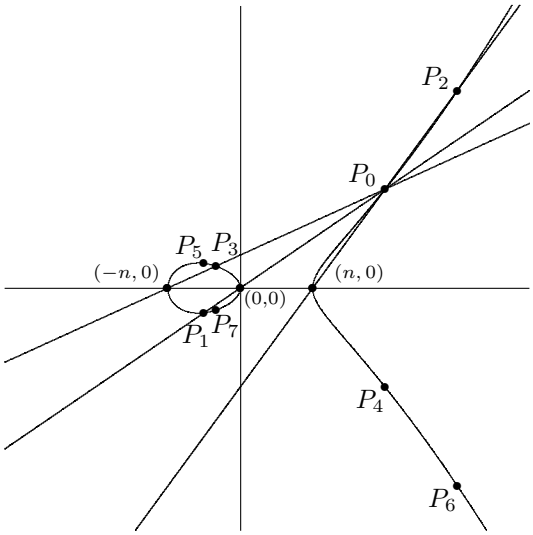

FIGURE 5. Intersecting $y^2 = x^3 - n^2x$ with lines through P_0 and $(0, 0)$, $(n, 0)$, $(-n, 0)$, and reflected points.

We have seen that the following properties of a positive rational number n are equivalent:

- there is a rational right triangle with area n,
- there is a 3-term arithmetic progression of rational squares with common difference n,
- there is a rational solution to $y^2 = x^3 - n^2x$ with $y \neq 0$.

First Point	Second Point	Third Point
(x, y)	$(0, 0)$	$(-n^2/x, -n^2y/x^2)$
$(x, -y)$	$(0, 0)$	$(-n^2/x, n^2y/x^2)$
(x, y)	$(n, 0)$	$(n(x+n)/(x-n), 2n^2y/(x-n)^2)$
$(x, -y)$	$(n, 0)$	$(n(x+n)/(x-n), -2n^2y/(x-n)^2)$
(x, y)	$(-n, 0)$	$(-n(x-n)/(x+n), 2n^2y/(x+n)^2)$
$(x, -y)$	$(-n, 0)$	$(-n(x-n)/(x+n), -2n^2y/(x+n)^2)$

TABLE 3. Third Intersection Point of a Line with $y^2 = x^3 - n^2x$.

Pair	Triple
(x, y)	(a, b, c)
$(x, -y)$	$(-a, -b, -c)$
$(-n^2/x, -n^2y/x^2)$	$(a, b, -c)$
$(-n^2/x, n^2y/x^2)$	$(-a, -b, c)$
$(n(x+n)/(x-n), 2n^2y/(x-n)^2)$	(b, a, c)
$(n(x+n)/(x-n), -2n^2y/(x-n)^2)$	$(-b, -a, -c)$
$(-n(x-n)/(x+n), 2n^2y/(x+n)^2)$	$(-b, -a, c)$
$(-n(x-n)/(x+n), -2n^2y/(x+n)^2)$	$(b, a, -c)$

TABLE 4. Theorem 4.1 and Sign Changes.

The viewpoint of the equation $y^2 = x^3 - n^2x$ lets us use the geometry of the curve to do something striking: produce a new rational right triangle with area n from two known triangles. We saw an instance of this in Example 4.6. Notice there is nothing in the definition of a congruent number which suggests it is possible to produce a new rational right triangle with area n from two known ones. We can even find a new rational right triangle with area n from just one such triangle, by using a tangent line in place of a secant line. Given a rational point (x_0, y_0) on $y^2 = x^3 - n^2x$ with $y_0 \neq 0$, draw the tangent line to this curve at the point (x_0, y_0). This line will meet the curve in a second rational point, and that can be converted into a new rational right triangle with area n using the correspondence of Theorem 4.1 (and removing any signs on a, b, c if they turn out negative.)

Example 4.8. In Example 4.6, we found a third rational right triangle from two known ones by intersecting the line through the points $(1260, 44100)$ and $(525, 11025)$ with $y^2 = x^3 - 210^2x$. We can find a new rational right triangle with area 210 from the single point $(1260, 44100)$ by using the tangent line to $y^2 = x^3 - 210^2x$ at $(1260, 44100)$. The tangent is

$$y = \frac{107}{2}x - 23310$$

and it meets the curve in the second point $(1369/4, -39997/8)$. See Figure 6. By Theorem 4.1, this point corresponds to $(a, b, c) = (-1081/74, -31080/1081, -2579761/79994)$, which after removing signs is the rational right triangle $(1081/74, 31080/1081, 2579761/79994)$, whose area is 210.

Example 4.9. The $(3, 4, 5)$ right triangle with area 6 corresponds to the point $(12, 36)$ on the curve $y^2 = x^3 - 36x$, as we saw already in Example 4.3. The tangent line to this curve at the point $(12, 36)$ is $y = (11/2)x - 30$, which meets the curve in the second point

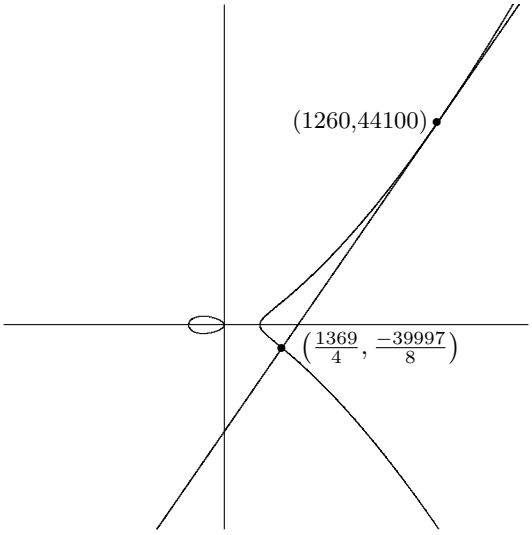

FIGURE 6. New rational point on $y^2 = x^3 - 210^2x$ from a tangent line. (Not drawn to scale.)

$(25/4, 35/8) = (6.25, 4.375)$. Let's repeat the tangent process on this new point. The tangent line to the curve at $(25/4, 35/8)$ has equation

$$y = \frac{1299}{140}x - \frac{6005}{112},$$

which meets the curve in the new point

$$\left(\frac{1442401}{19600}, \frac{1726556399}{2744000}\right) \approx (73.59, 629.21). \tag{4.1}$$

This is illustrated in Figure 7, where the second tangent line meets the curve outside the range of the picture.[2] A larger view, showing where the second tangent line meets the curve, is in Figure 8. (The axes in Figures 7 and 8 are not given equal scales, which is why the same tangent line in the two figures appears to have different slopes.) Using Theorem 4.1, $(25/4, 35/8)$ corresponds to the rational right triangle with area 6 having sides $(7/10, 120/7, 1201/70)$. The rational right triangle with area 6 corresponding to the point in (4.1) has sides

$$\left(\frac{1437599}{168140}, \frac{2017680}{1437599}, \frac{2094350404801}{241717895860}\right). \tag{4.2}$$

Armed with 3 rational right triangles with area 6, we can find 3 arithmetic progressions of rational squares using Theorem 3.1. The $(3, 4, 5)$ triangle, as we saw in Example 3.2, yields the arithmetic progression 1/4, 25/4, 49/4. The $(7/10, 120/7, 1201/70)$ right triangle yields the arithmetic progression

$$\left(\frac{1151}{140}\right)^2, \quad \left(\frac{1201}{140}\right)^2, \quad \left(\frac{1249}{140}\right)^2.$$

[2]The inflection points on the curve in Figure 7, for $x > 0$, occur where $x = \sqrt{12(3 + 2\sqrt{3})} \approx 8.8$.

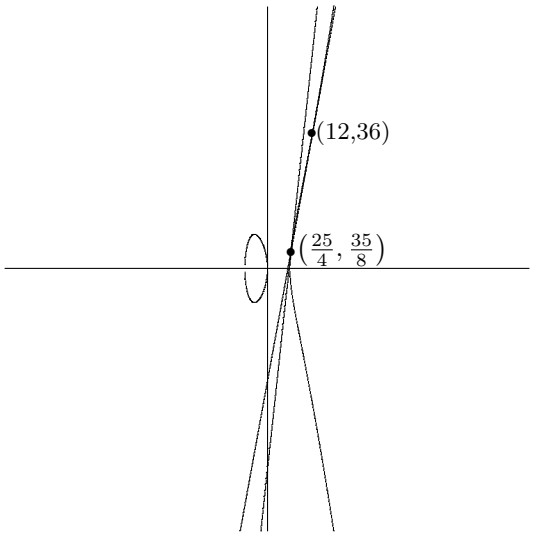

FIGURE 7. Close view of successive tangents to $y^2 = x^3 - 36x$ starting from $(12, 36)$.

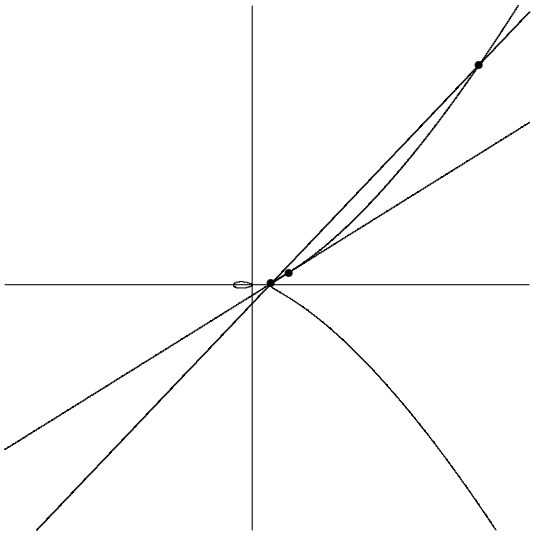

FIGURE 8. Far view of successive tangents to $y^2 = x^3 - 36x$ starting from $(12, 36)$. (Not drawn to scale.)

The right triangle with sides in (4.2) yields the arithmetic progression

$$\left(\frac{1727438169601}{483435791720}\right)^2, \quad \left(\frac{2094350404801}{483435791720}\right)^2, \quad \left(\frac{77611083871}{483435791720}\right)^2.$$

All of these arithmetic progressions of squares have common difference 6.

Remark 4.10. The secant method is a way to "add" points and the tangent method is essentially the special case of "doubling" a point.[3] These tangent and secant constructions can be used to give the rational points on $y^2 = x^3 - n^2x$ the structure of an abelian group in which, for rational $n > 0$, any rational point (x, y) with $y \neq 0$ has infinite order. (This is not at all obvious.) Therefore the curve $y^2 = x^3 - n^2x$ has infinitely many rational points as soon as it has just one rational point with $y \neq 0$, so there are infinitely many rational right triangles with area n provided there is one example and there are infinitely many 3-term arithmetic progressions of rational squares with common difference n provided there is one example. In terms of Table 1, this means any area arising in the table at least once will arise in the table infinitely often.[4]

The importance of thinking about congruent numbers in terms of the curves $y^2 = x^3 - n^2x$ goes far beyond this interesting construction of new rational right triangles with area n from old ones: this viewpoint in fact leads to a tentative solution of the whole congruent number problem! In 1983, Tunnell [10] used arithmetic properties of $y^2 = x^3 - n^2x$ (a particular example of an elliptic curve) to discover a previously unknown elementary necessary condition on congruent numbers and he was able to prove the condition is sufficient if a certain other conjecture is true.

Theorem 4.11 (Tunnell)**.** *Let n be a squarefree positive integer. Set*

$$\begin{aligned} f(n) &= \#\{(x,y,z) \in \mathbf{Z}^3 : x^2 + 2y^2 + 8z^2 = n\}, \\ g(n) &= \#\{(x,y,z) \in \mathbf{Z}^3 : x^2 + 2y^2 + 32z^2 = n\}, \\ h(n) &= \#\{(x,y,z) \in \mathbf{Z}^3 : x^2 + 4y^2 + 8z^2 = n/2\}, \\ k(n) &= \#\{(x,y,z) \in \mathbf{Z}^3 : x^2 + 4y^2 + 32z^2 = n/2\}. \end{aligned}$$

For odd n, if n is congruent then $f(n) = 2g(n)$. For even n, if n is congruent then $h(n) = 2k(n)$. Moreover, if the weak Birch and Swinnerton–Dyer conjecture is true for the curve $y^2 = x^3 - n^2x$ then the converse of both implications is true: $f(n) = 2g(n)$ implies n is congruent when n is odd and $h(n) = 2k(n)$ implies n is congruent when n is even.

The weak Birch and Swinnerton–Dyer conjecture, which we won't describe here, is one of the most important conjectures in mathematics. (It is on the list of Clay Millenium Prize problems.) Several years before Tunnell proved his theorem, Stephens [9] showed the weak Birch and Swinnerton–Dyer conjecture implies any positive integer $n \equiv 5, 6, 7 \bmod 8$ is a congruent number. Tunnell's achievement was discovering the enumerative criterion for congruent numbers and its relation to the weak Birch and Swinnerton–Dyer conjecture. For background on the ideas in Tunnell's theorem, see [6] and [7]. In [8, pp. 112–114] the particular case of prime congruent numbers is considered.

Tunnell's theorem provides an unconditional method of proving a squarefree positive integer n is not congruent (show $f(n) \neq 2g(n)$ or $h(n) \neq 2k(n)$, depending on the parity of n), and a conditional method of proving n is congruent (conditional, that is, on the weak Birch and Swinnerton-Dyer conjecture for the curve $y^2 = x^3 - n^2x$).

[3]The process of getting new rational points from known ones in the congruent number problem goes back to Turrière [11] in 1915, who worked with the points (r, s, t) lying on the two surfaces $s^2 + n = t^2$ and $s^2 - n = r^2$, which intersect in a curve that is essentially $y^2 = x^3 - n^2x$.

[4]The two rational points on $y^2 = x^3 - 210^2x$ which correspond to the repetition of 210 in Table 1 are independent in the group law: they do not have a common multiple.

Example 4.12. Since $f(1) = g(1) = 2$ and $f(3) = g(3) = 4$, we have $f(n) \neq 2g(n)$ for $n = 1$ and 3, so Tunnell's criterion shows 1 and 3 are not congruent.

Example 4.13. Since $h(2) = k(2) = 2$, we have $h(2) \neq 2k(2)$, so Tunnell's criterion shows 2 is not congruent.

Example 4.14. Since $f(5) = g(5) = 0$ and $f(7) = g(7) = 0$, we have $f(n) = 2g(n)$ for $n = 5$ and 7. Tunnell's theorem says 5 and 7 are congruent if the weak Birch and Swinnerton-Dyer conjecture is true for $y^2 = x^3 - 25x$ and $y^2 = x^3 - 49x$. Unconditionally, we saw earlier that 5 and 7 are congruent.

Example 4.15. Since $h(10) = 4$ and $k(10) = 4$, $h(10) \neq 2k(10)$, so Tunnell's theorem says 10 is not a congruent number.

Example 4.16. We will show (conditionally) that any squarefree positive integer n satisfying $n \equiv 5, 6, 7 \bmod 8$ is a congruent number. Tunnell's theorem tells us to check that $f(n) = 2g(n)$ when $n \equiv 5, 7 \bmod 8$ and $h(n) = 2k(n)$ when $n \equiv 6 \bmod 8$. Since $x^2 + 2y^2 \not\equiv 5, 7 \bmod 8$ for any integers x and y, $f(n) = 0$ and $g(n) = 0$ when $n \equiv 5, 7 \bmod 8$, so $f(n) = 2g(n)$. When $n \equiv 6 \bmod 8$ we have $n/2 \equiv 3 \bmod 4$, so $x^2 \not\equiv n/2 \bmod 4$ for any integer x. Therefore $h(n) = 0$ and $k(n) = 0$ when $n \equiv 6 \bmod 8$, so $h(n) = 2k(n)$. This shows n is congruent if the weak Birch and Swinnerton-Dyer conjecture is true for $y^2 = x^3 - n^2x$.

Appendix A. Discovering Theorem 4.1

Fix a real number $n \neq 0$. The real solutions (a, b, c) to each of the equations

$$a^2 + b^2 = c^2, \quad \frac{1}{2}ab = n, \tag{A.1}$$

describe a surface in $\mathbf{R}^3$, so it is reasonable to expect these two surfaces intersect in a curve. We want an equation for that curve, which will be $y^2 = x^3 - n^2x$ in the right choice of coordinates. Two approaches will be described, one algebraic and the other geometric. The sign on n will be irrelevant, so we allow any $n \neq 0$ rather than $n > 0$.

The algebra is simplified by introducing a cross-term in the equation $a^2 + b^2 = c^2$. Let $c = t + a$, which turns this equation into $b^2 = t^2 + 2at$, or equivalently

$$2at = b^2 - t^2. \tag{A.2}$$

Since $ab = 2n$ is nonzero, neither a nor b is 0, so we can write $a = 2n/b$ and substitute it into (A.2):

$$\frac{4nt}{b} = b^2 - t^2.$$

Multiplying through by b makes this

$$4nt = b^3 - t^2b.$$

Divide by t^3 ($t \neq 0$, as otherwise $a = c$ and then $b = 0$, but $ab = 2n \neq 0$):

$$\frac{4n}{t^2} = \left(\frac{b}{t}\right)^3 - \frac{b}{t}.$$

Multiply through by n^3:

$$\left(\frac{2n^2}{t}\right)^2 = \left(\frac{nb}{t}\right)^3 - n^2\left(\frac{nb}{t}\right).$$

Set $x = nb/t$ and $y = 2n^2/t$, so $y^2 = x^3 - n^2x$. Then $x = nb/(c-a)$ and $y = 2n^2/(c-a)$, as in Theorem 4.1.

We now turn to a geometric explanation of Theorem 4.1, taking greater advantage of the interpretation of the two equations in (A.1) as surfaces which meet in a curve. Rather than working with the equations as surfaces in $\mathbf{R}^3$, we will work in the projective space $\mathbf{P}^3(\mathbf{R})$ by homogenizing the two equations. This doesn't change the first equation in (A.1), but makes the second one $(1/2)ab = nd^2$.

Letting $[a, b, c, d]$ be the homogeneous coordinates of a typical point in $\mathbf{P}^3(\mathbf{R})$, the two equations

$$a^2 + b^2 = c^2, \quad \frac{1}{2}ab = nd^2 \tag{A.3}$$

each define surfaces in $\mathbf{P}^3(\mathbf{R})$. Let C be the intersection of these surfaces (a curve). There are points on C with $b = 0$, namely $[a, b, c, d] = [1, 0, \pm 1, 0]$. These points are not in the usual affine space inside $\mathbf{P}^3(\mathbf{R})$, and we will use one of these points in a geometric construction.

Let's project through the point $P := [1, 0, 1, 0]$ to map C to the plane

$$\Pi := \{[0, b, c, d]\}$$

and find the equation for the image of C in this plane. The point P lies on C and not in Π. For each $Q \in C$ other than P, the line $\overline{PQ}$ in $\mathbf{P}^3(\mathbf{R})$ meets Π in a unique point. Call this point $f(Q)$. When $Q = P$, intersect the tangent line to C at P with the plane Π to define $f(P)$. We have defined a function $f\colon C \to \Pi$.

Computing a formula for f necessitates a certain about of computation to see what happens. Suppose first that $Q = [a, b, c, d]$ is not P. The line through P and Q is the set of points

$$[\lambda + \mu a, \mu b, \lambda + \mu c, \mu d],$$

which meets Π where $\lambda = -\mu a$, making

$$f(Q) = [0, \mu b, \mu(c-a), \mu d] = [0, b, c-a, d].$$

As for $f(P)$, the tangent planes to each of the surfaces $a^2 + b^2 = c^2$ and $(1/2)ab = nd^2$ in $\mathbf{P}^3(\mathbf{R})$ at the point P are the planes $a = c$ and $b = 0$, so the tangent line at P is the set of points

$$[a, 0, a, d],$$

which meets Π in $[0, 0, 0, 1]$, so $f(P) = [0, 0, 0, 1]$. Thus

$$f([a, b, c, d]) = \begin{cases} [0, b, c-a, d], & \text{if } [a, b, c, d] \neq [1, 0, 1, 0], \\ [0, 0, 0, 1], & \text{if } [a, b, c, d] = [1, 0, 1, 0]. \end{cases}$$

As an exercise, check f is injective. (Hint: Since $(1/2)ab = nd^2$, b and d determine a if $b \neq 0$.)

All points in the plane Π have first coordinate 0. Identify Π with $\mathbf{P}^2(\mathbf{R})$ by dropping this coordinate, which turns f into the function $g\colon C \to \mathbf{P}^2(\mathbf{R})$ where

$$g([a, b, c, d]) = \begin{cases} [b, a-c, d], & \text{if } [a, b, c, d] \neq [1, 0, 1, 0], \\ [0, 0, 1], & \text{if } [a, b, c, d] = [1, 0, 1, 0]. \end{cases} \tag{A.4}$$

We have mapped our curve C to the projective plane $\mathbf{P}^2(\mathbf{R})$. What is an equation for the image $g(C)$? For $Q = [a, b, c, d]$ on C, write $g(Q) = [x, z, y]$. (This ordering of the coordinates will make formulas come out in close to the expected way more quickly.) When

$Q \neq [1,0,1,0]$ (that is, $a \neq c$), (A.4) says we can use $x = b$, $y = d$, and $z = c - a \neq 0$.[5] The equations in (A.3) become $a^2 + x^2 = (a+z)^2$ and $(1/2)ax = ny^2$, so

$$x^2 = 2az + z^2, \quad ax = 2ny^2.$$

Since $z \neq 0$, we can solve for a in the first equation, so a is determined by x, y, and z. Multiplying the first equation by x and the second by $2z$, $x^3 = 2axz + xz^2 = 4ny^2z + xz^2$. Thus

$$4ny^2z = x^3 - xz^2.$$

Set $X = x$, $Y = 2ny$, and $Z = z/n$ to find $Y^2Z = X^3 - n^2XZ^2$, which is the homogeneous form of $Y^2 = X^3 - n^2X$.

Tracing this correspondence out explicitly from the start, if we begin with $[a,b,c,d]$ on C where $d \neq 0$ (the standard affine part of C), its image $[X,Z,Y]$ in $\mathbf{P}^2(\mathbf{R})$ is

$$\left[b, \frac{c-a}{n}, 2nd\right] = [nb, c-a, 2n^2d] = \left[\frac{nb}{c-a}, 1, \frac{2n^2d}{c-a}\right].$$

Since $d \neq 0$ implies $a \neq c$, using inhomogeneous coordinates with middle coordinate 1 in $\mathbf{P}^2(\mathbf{R})$ the point (a,b,c) goes to $(nb/(c-a), 2n^2/(c-a))$, which is the transformation in Theorem 4.1.

As an exercise in these techniques, consider the problem of classifying triangles with a given area $n > 0$ and a given angle θ. (Taking $\theta = \pi/2$ is the congruent number problem.) Let a, b, c be the side lengths of the triangle, with c the length of the edge opposite the angle θ. The equations in (A.1) are replaced by

$$a^2 + b^2 - 2ab\cos\theta = c^2, \quad \frac{1}{2}ab\sin\theta = n. \tag{A.5}$$

(If there is a solution with rational a, b, c, and n then $\cos\theta$ and $\sin\theta$ must be rational.) Show the solutions (a,b,c) of (A.5) are in one-to-one correspondence with the solutions (x,y) of the equation

$$\begin{aligned} y^2 &= x^3 + \frac{2n\cos\theta}{\sin\theta}x^2 - n^2x \\ &= x\left(x + n\frac{\cos\theta+1}{\sin\theta}\right)\left(x + n\frac{\cos\theta-1}{\sin\theta}\right), \end{aligned}$$

with $y \neq 0$. The correspondence should specialize to that in Theorem 4.1 when $\theta = \pi/2$.

Appendix B. Other Diophantine Equations

In Table 5, the first two columns show how to convert the sides (a,b,c) of a rational right triangle with area 1 into a positive rational solution of the equation $y^2 = x^4 - 1$ and conversely. (These correspondences are *not* inverses, but they do show a positive rational solution in the first column leads to a positive rational solution in the second column, and conversely.) The last two columns give a (bijective) correspondence between rational right triangles with area 2 and positive rational solutions of $y^2 = x^4 + 1$. So showing 1 and 2 are not congruent numbers is the same as showing the equations $y^2 = x^4 \pm 1$ don't have solutions in positive rational numbers.

A positive rational solution (x,y) to $y^2 = x^4 \pm 1$ can be turned into a positive integral solution (u,v,w) of $w^2 = u^4 \pm v^4$ by clearing a common denominator, and we can go in

[5]The cross term $t = c - a$ in the algebraic method is precisely z, so now we get a geometric interpretation of this cross term as a coordinate in a projection map to a plane.

$a^2+b^2=c^2$, $\frac{1}{2}ab=1$	$y^2=x^4-1$	$a^2+b^2=c^2$, $\frac{1}{2}ab=2$	$y^2=x^4+1$
$x=c/2$	$a=y/x$	$x=a/2$	$a=2x$
$y=\lvert a^2-b^2\rvert/4$	$b=2x/y$	$y=ac/4$	$b=2/x$
	$c=(x^4+1)/xy$		$c=2y/x$

TABLE 5. Correspondences between rational right triangles with area 1 and $y^2=x^4\pm 1$.

reverse by dividing by v^4. That 1 and 2 are not congruent is therefore the same as the equations $w^2=u^4\pm v^4$ having no positive integer solutions. The reader is referred to [1, pp. 252–256] for a proof by descent that $w^2=u^4\pm v^4$ has no positive integer solutions.

That the congruent number property for 1 and 2 is equivalent to the solvability of a single equation in positive rational numbers ($y^2=x^4-1$ for 1 and $y^2=x^4+1$ for 2) generalizes: n is congruent if and only if $y^2=x^4-n^2$ has a positive rational solution and if and only if $y^2=x^4+4n^2$ has a positive rational solution. See Table 6, where the first two columns turn rational right triangles with area n into positive rational solutions of $y^2=x^4-n^2$ and conversely, and the last two columns do the same with $y^2=x^4+4n^2$. As in Table 5, the correspondences in the first two columns of Table 6 are not inverses of each other, but the correspondences in the last two columns are inverses. (When $n=2$ the equation in Table 6 is $y^2=x^4+16$ rather than $y^2=x^4+1$ as in Table 5. We can easily pass from the former to the latter by replacing y with $4y$ and x with $2x$.) The equivalence of n being congruent with $y^2=x^4-n^2$ having a positive rational solution is due to Lucas (1877).

$a^2+b^2=c^2$, $\frac{1}{2}ab=n$	$y^2=x^4-n^2$	$a^2+b^2=c^2$, $\frac{1}{2}ab=n$	$y^2=x^4+4n^2$
$x=c/2$	$a=y/x$	$x=a$	$a=x$
$y=\lvert a^2-b^2\rvert/4$	$b=2nx/y$	$y=ac$	$b=2n/x$
	$c=(x^4+n^2)/xy$		$c=y/x$

TABLE 6. More correspondences between rational right triangles and Diophantine equations.

We pulled the equations $y^2=x^4-n^2$ and $y^2=x^4+4n^2$ out of nowhere. How could they be discovered? The arithmetic progression viewpoint on congruent numbers (Theorem 3.1) leads to one of them. If n is congruent, there are rational squares r^2, s^2, and t^2 with $s^2-r^2=n$ and $t^2-s^2=n$. Then $r^2=s^2-n$ and $t^2=s^2+n$, so multiplication gives $(rt)^2=s^4-n^2$ and we've solved $y^2=x^4-n^2$ in positive rational numbers.

Remark B.1. For $t\neq 0$, solutions to $y^2=x^4+t$ and to $Y^2=X^3-4tX$ are in a one-to-one correspondence, by $(x,y)\mapsto(2t/(y-x^2),4tx/(y-x^2))$ and $(X,Y)\mapsto(Y/2X,(Y^2+8tX)/4X^2)$. In particular, solutions to $y^2=x^4-n^2$ correspond to solutions to $Y^2=X^3+(2n)^2X$, which is *not* the equation $Y^2=X^3-(2n)^2X$ and thus isn't related to whether or not $2n$ is a congruent number. Explicit examples show the lack of a general connection between n and $2n$ being congruent: 5 is congruent but 10 is not, while 3 is not congruent but 6 is.

References

[1] D. M. Burton, "Elementary Number Theory," 6th ed., McGraw-Hill, New York, 2007.

[2] W. A. Coppel, "Number Theory: An Introduction to Mathematics. Part B," Springer-Verlag, New York, 2006.

[3] L. E. Dickson, "History of the Theory of Numbers," Vol. II, Chelsea, New York, 1952.

[4] A. Genocchi, "Sopra Tre Scritti Inediti di Leonardo Pisano Pubblicati da Baldassarre Boncompagni: Note Analitiche," Tipografia delle Belle Arti, Rome, 1855. URL https://archive.org/details/sopratrescritti00genogoog/mode/2up.

[5] B. Hemenway, On Recognizing Congruent Primes, M. Sc. Thesis, Simon Fraser University, 2006. URL https://summit.sfu.ca/item/6418.

[6] G. Henniart, Congruent Numbers, Elliptic Curves, and Modular Forms, translation by F. Lemmermeyer. URL http://www.fen.bilkent.edu.tr/~franz/publ/guy.pdf.

[7] N. Koblitz, "Introduction to Elliptic Curves and Modular Forms," 2nd ed., Springer–Verlag, New York, 1993.

[8] A. Knapp, "Elliptic Curves," Princeton Univ. Press, Princeton, 1992.

[9] N. M. Stephens, Congruence properties of congruent numbers, *Bull. London Math. Soc.* **7** (1975), 182–184.

[10] J. Tunnell, A Classical Diophantine Problem and Modular Forms of Weight 3/2, *Invent. Math.* **72** (1983), 323–334.

[11] E. Turrière, Le Problème de Jean de Palerme et de Léonard de Pise, *L'Enseignement Math.* **17** (1915), 315–324. URL https://www.e-periodica.ch/digbib/view?pid=ens-001%3A1915%3A17#478.

[12] A. Weil, "Number Theory; an Approach through History from Hammurapi to Legendre," Birkhauser, Boston, 1984.