Chapter 4
What integers are areas of right triangles?

In this chapter we study the set of integers that are the area of a right triangle with integer sides. We define a *congruent number* to be a natural number which is the area of a right triangle with rational sides. After verifying some easy properties of congruent numbers, we prove a theorem of Fermat (Theorem 4.4) that asserts no square is a congruent number. Later in the chapter, we explain the connection between congruent numbers and cubic equations. In the Notes, we review the history of congruent numbers and state a celebrated theorem of Tunnell.

4.1 Congruent numbers

If a, b, c are the three sides of an integral right triangle, with c the hypotenuse, since at least one of a, b is even then the area $ab/2$, is a natural number.

Question 4.1. Is there a criterion to decide whether a natural number n is the area of some integral right triangle?

It will become apparent very quickly that this is a difficult problem. In fact at the time of this writing, there is still no complete characterization of the set of areas of integral right triangles. It is, however, possible to obtain some information using elementary methods. We start with a definition.

Definition 4.2 (Congruent number). A natural number which is the area of a right triangle with rational sides is called a *congruent number*. We denote the set of all congruent numbers by $\mathscr{S}$.

Let's take a moment and clarify the connection between Question 4.1 and Definition 4.2. It is clear that if we have integral right triangles T and T' with side lengths a, b, c and $\lambda a, \lambda b, \lambda c$, respectively, with $\lambda \in \mathbb{N}$, then the area of T' is λ^2 times the area of T. This means if n is the area of some integral right triangle, then if $\lambda \in \mathbb{N}$, $\lambda^2 n \in \mathscr{S}$. This suggests that one should not be too concerned with the

R. Takloo-Bighash, *A Pythagorean Introduction to Number Theory*,
Undergraduate Texts in Mathematics, https://doi.org/10.1007/978-3-030-02604-2_4

square factors that show up in areas of integral right triangles. There is a bit of trouble here: Suppose we have a natural number n which is the area of some integral right triangle with side lengths a, b, c, and suppose n has a square factor u^2, $u \in \mathbb{N}$, so that $n = u^2 \cdot m$ with $m \in \mathbb{N}$. As tempted as we might be to scale down the triangle by a factor of u to get an integral triangle with side lengths $a/u, b/u, c/u$, sometimes these latter quotients are not integers. For example, the right triangle with side lengths (8, 15, 17) has area $60 = 2^2 \cdot 15$, but the triangle with half the size, with area 15, has side lengths (4, 15/2, 17/2) which are *rational*, and not integral.

We define a function *sqf*, *the square-free part of* n, by defining its value for a natural number n to be the smallest natural number m such that $n = m \cdot k^2$ for some natural number k. For example, $sqf(6) = 6$, $sqf(12) = 3$, and $sqf(9) = 1$. The following lemma is easy to prove.

Lemma 4.3. *For $n \in \mathbb{N}$, $n \in \mathscr{S}$ if and only if $sqf(n) \in \mathscr{S}$.*

The lemma shows that in order to determine the elements of the set $\mathscr{S}$ we just need to determine its square free elements. An important point to note is that a square-free element of $\mathscr{S}$ is not necessarily the area of a right triangle with integral sides. For example, the right triangle with sides (8, 15, 17) has area 60, so $60 \in \mathscr{S}$. We have $sqf(60) = 15$, so $15 \in \mathscr{S}$. However, as we see in Exercise 4.7, there are no integral right triangles with area 15.

We saw in Theorem 3.4 that if a, b, c are the three sides of a primitive right triangle, with c the hypotenuse, then there are co-prime integers x, y of different parity such that

$$\{a, b, c\} = \{x^2 - y^2, 2xy, x^2 + y^2\}.$$

The area S of this triangle is then equal to

$$S = \frac{1}{2}ab = xy(x^2 - y^2).$$

For this reason, one way to produce congruent numbers is to define a function

$$f(x, y) = sqf(xy(x^2 - y^2))$$

with domain being the set of pairs of integers (x, y), $\gcd(x, y) = 1$, $x > y$, and x, y of different parity. Then a natural number is a congruent number if its square free part is $f(x, y)$ for some (x, y) as above. For example, the values of $f(x, 1)$ for x larger than 1 and even are as follows: 6, 15, 210, 14, 110, ...

It is very hard to know which numbers appear as values of f. In fact, even when we know a number is a congruent number, it is not clear how one should go about finding the pair (x, y) such that $f(x, y)$ is equal to that number. For example, as noted in [70], 53 is a congruent number, but the first time it appears as $f(x, y)$ is when

$$x = 1873180325, \quad y = 1158313156.$$

In fact,

$$xy(x^2 - y^2) = 53 \times 297855654284978790^2.$$

4.2 Small numbers

In general it is fairly difficult to determine with bare hands if a natural number is congruent. We will see in a moment that 1 is not congruent. Lemma 4.3 then shows that no perfect square is congruent. We will see in Exercise 4.9 that 2 and 3 are not congruent. The smallest congruent number is 5: 5 is the area of the right triangle with rational sides $20/3, 3/2, 41/6$. We already saw that 6 is a congruent number as it is the area of the right triangle with side lengths 3, 4, 5. As already stated at this point despite all the progress made in the last few hundred years there are still many basic questions about congruent number which we do not know how to answer; see, however, the Notes to this chapter where we state a theorem of Tunnell and explain some recent progress.

The following theorem goes back to Fermat. The proof of this theorem, like the proof of Theorem 3.10, uses *infinite descent*.

Theorem 4.4 (Fermat). $1 \notin S$.

Proof. By Lemma 4.3 we need to show that there are no right triangles with rational sides whose area is the square of a natural number. Suppose we have a right triangle with rational sides a, b, c, with a, b the legs and c the hypotenuse, and suppose that the area $ab/2$ is a perfect square t^2. Let $\lambda \in \mathbb{N}$ be the common denominator between a, b, c. If we scale the triangle by λ, we obtain a new triangle with integral sides $a\lambda, b\lambda, c\lambda$, and area $\lambda^2 t^2$ which is still a perfect square. So we may assume, without loss of generality, that $a, b, c \in \mathbb{N}$. If $\gcd(a, b) = \delta$, then we write $a = a'\delta$, $b = b'\delta$ with $(a', b') = 1$. Clearly, $\delta \mid c$ and we can write $c = c'\delta$. Then $t^2 = ab/2 = a'b'\delta^2/2$. This implies that $a'b'/2 = t'^2$ for some integer t'. Consequently, we have a right triangle with side lengths a', b', c' such that $\gcd(a', b', c') = 1$ and whose area is a perfect square. So, we may without loss of generality assume that our original numbers a, b, c are coprime. We have

$$\begin{cases} c^2 = a^2 + b^2, \\ ab = 2t^2. \end{cases}$$

Observe that one of the a, b is even, so we may assume that $a = 2k$ is even. So we have

$$kb = t^2.$$

Since $\gcd(a, b) = 1$, we have $\gcd(k, b) = 1$. Since the product of k and b is a perfect square, by Proposition 2.21 each of k, b individually is a perfect square, i.e., $k = m^2$ and $b = n^2$, for some natural numbers m, n. Going back to a, b, we have $a = 2m^2$, $b = n^2$. Now the Pythagorean Equation becomes

$$4m^4 + n^4 = c^2. \tag{4.1}$$

This equation resembles Equation (3.6) which was studied in the proof of Theorem 3.10, and, in fact we use the method of infinite descent that was used in the proof of Theorem 3.10 to show every solution to Equation (4.1) satisfies $mn = 0$.

As in the proof of Theorem 3.10, suppose we have a solution of (4.1) such that c is the smallest possible. We use Theorem 3.4 to write

$$\begin{cases} 2m^2 = 2uv, \\ n^2 = u^2 - v^2, \\ c = u^2 + v^2, \end{cases}$$

for coprime integers u, v with different parities. Since $m^2 = uv$ and $\gcd(u, v) = 1$, Proposition 2.21 implies that $u = r^2$, $v = s^2$ for natural numbers r, s. If on the other hand we write the middle equation as a Pythagorean Equation $n^2 + v^2 = u^2$, we see that u is odd and v is even, and also that there are coprime integers x, y of different parity such that

$$\begin{cases} n = x^2 - y^2, \\ v = 2xy, \\ u = x^2 + y^2. \end{cases}$$

Suppose x is even, $x = 2\alpha$. Then we write the middle equation as $s^2 = 4\alpha y$. Since s is even, we write $\alpha y = (s/2)^2$. Again, we conclude that $\alpha = \beta^2$, $y = \gamma^2$ for integers β, γ. With these substitutions, the equation $u = x^2 + y^2$ becomes

$$4\beta^4 + \gamma^4 = r^2,$$

i.e., the numbers β, γ, r are another set of solutions of Equation (4.1). It is clear that $r < c$, and this is a contradiction. □

4.3 Connection to cubic equations

The problem of determining congruent numbers is intimately related to the study of rational solutions to the cubic equations considered in §3.3.

Theorem 4.5. *Let $n \in \mathbb{N}$ be fixed. There is a one-to-one correspondence between the following sets:*

$$V_1 = \{(a, b, c) \in \mathbb{Q}^3 \mid a^2 + b^2 = c^2, ab/2 = n\}$$

and

$$V_2 = \{(x, y) \in \mathbb{Q}^2 \mid y^2 = x^3 - n^2 x, xy \neq 0\}.$$

The correspondence is given by

$$f_1 : V_1 \to V_2,$$
$$(a, b, c) \mapsto \left(\frac{nb}{c-a}, \frac{2n^2}{c-a} \right),$$

and

$$f_2 : V_2 \to V_1,$$
$$(x, y) \mapsto \left(\frac{x^2 - n^2}{y}, \frac{2nx}{y}, \frac{x^2 + n^2}{y} \right).$$

The proof of this theorem is straightforward, and not too tedious, Exercise 4.10. Tunnell in the introduction of [105] attributes this construction to Don Zagier. The wonderful paper [70] has a fun appendix where it is explained how one might have found the above correspondence. One important point to note is that the correspondence described in the theorem is valid over every field, not just $\mathbb{Q}$. Furthermore, it gives a bijection between pairs of positive rational numbers (x, y), and positive rational numbers a, b, c described in the theorem, see Exercise 4.11.

The equation $y^2 = x^3 - n^2 x$ has very few solutions with $xy = 0$. In fact, by the easy Exercise 4.12, the only solutions of $y^2 = x^3 - n^2 x$ with $xy = 0$ are $(0, 0)$ and $(\pm n, 0)$. We call these solutions the *trivial solutions*. Hence we have the following corollary:

Corollary 4.6 (Stephens [97]). *A natural number n is a congruent number if and only if the equation $y^2 = x^3 - n^2 x$ has some non-trivial solution.*

We now consider an explicit example. The paper [70] contains many numerical examples of this nature.

Example 4.7. We start with the Pythagorean triple (5, 12, 13). The area of the triangle with these side lengths is $5 \times 12/2 = 30$. In this case, Theorem 4.5 says that the pair

$$(x, y) = \left(\frac{30 \times 12}{13 - 5}, \frac{2 \times 30^2}{13 - 5} \right) = (45, 225)$$

is a solution of the equation $y^2 = x^3 - 30^2 x$. Now we proceed as in Example 3.9. Implicit differentiation gives

$$y' = \frac{3x^2 - 30^2}{2y},$$

and consequently the slope of the tangent line at the point (45, 225) is

$$m = \frac{23}{2}.$$

A computation shows that the equation of the tangent line is

$$y = \frac{23}{2}x - \frac{585}{2}.$$

The points of intersection of this line with the curve $y^2 = x^3 - 30^2 x$ must satisfy the system

$$\begin{cases} y^2 = x^3 - 30^2 x, \\ y = \frac{23}{2}x - \frac{585}{2}. \end{cases}$$

Inserting y from the second equation into the first equation gives

$$\left(\frac{23}{2}x - \frac{585}{2}\right)^2 = x^3 - 30^2 x,$$

and this implies

$$x^3 - \left(\frac{23}{2}\right)^2 x^2 + Ax + B = 0$$

with numbers A, B the exact value of which is of no significant importance. Since we obtained this equation using a tangent line, two of the solutions are $x = 45$. The third solution must then satisfy

$$45 + 45 + x = \left(\frac{23}{2}\right)^2.$$

This gives $x = 169/4$, and we obtain the point

$$(x, y) = \left(\frac{169}{4}, \frac{1547}{8}\right)$$

on the curve $y^2 = x^3 - 30^2 x$. Now we apply the bijection f_2 from Theorem 4.5 to this pair to obtain a right triangle with rational sides whose area is 30. Explicitly, we have

$$\begin{aligned}(a, b, c) &= \left(\frac{(\frac{169}{4})^2 - 30^2}{\frac{1547}{8}}, \frac{2 \times 30 \times \frac{169}{4}}{\frac{1547}{8}}, \frac{(\frac{169}{4})^2 + 30^2}{\frac{1547}{8}}\right) \\ &= \left(\frac{119}{26}, \frac{1560}{119}, \frac{42961}{3094}\right).\end{aligned}$$

A quick computation shows that this triple in fact satisfies the Pythagorean Equation, and that

$$\frac{1}{2} \times \frac{119}{26} \times \frac{1560}{119} = 30.$$

We have obtained a new triangle with area 30.

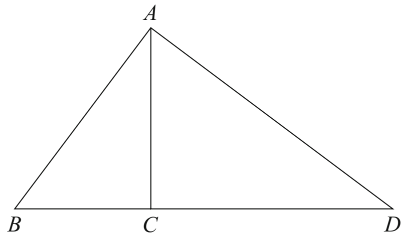

Fig. 4.1 The diagram for Problem 4.6

Exercises

4.1 Determine all right triangles with integral sides such that the perimeter and the area are equal.
4.2 Show that two right triangles with equal hypotenuse and area are congruent.
4.3 Show that for every $n \in \mathbb{N}$, there are n distinct integral right triangles with the same area.
4.4 A *Heronian triangle* is a triangle with rational sides whose area is a rational number. Show that triangles with side lengths (13, 14, 15) and (65, 119, 180) are Heronian.
4.5 Show that there are infinitely many isosceles Heronian triangles.
4.6 Let ABC and ACD be right triangles with rational sides which share a side AC as in Figure 4.1. Show that the triangle ABD is Heronian. Conversely, suppose ABD is a Heronian triangle with $\angle BAD$ the largest angle of the triangle. Draw the altitude AC and show that the triangles ABC and ACD are right triangles with rational sides.
4.7 Show $15 \notin \mathscr{S}$.
4.8 Show that a square-free natural number n is a congruent number if and only if there is a rational number x such that $x^2 - n$ and $x^2 + n$ are squares of rational numbers.
4.9 Show that 2 and 3 are not congruent numbers.
4.10 Prove Theorem 4.5 by direct computation.
4.11 Show that in Theorem 4.5, for $n \in \mathbb{N}$, x, y are positive rational numbers, if and only if a, b, c are positive rational numbers.
4.12 Show that the only solutions of $y^2 = x^3 - n^2x$ with $xy = 0$ are $(0, 0)$ and $(\pm n, 0)$.
4.13 Find three rational right triangles with area 6.
4.14 (✠) Find fifty congruent numbers.
4.15 (✠) Find ten rational right triangles with area 30.
4.16 (✠) Use Tunnell's Theorem 4.8 from the Notes to find all congruent numbers less than 100.

Notes

The history of congruent numbers

Like many other concepts in elementary number theory, the standard reference for the history of congruent numbers is Dickson's classic book [16], especially Chapter XVI. The definition that Dickson uses is different from ours. He defines a congruence number to be a natural number n if there is a rational number x such that $x^2 - n$ and $x^2 + n$ are squares of rational numbers; that this definition is equivalent to our definition is Exercise 4.8. Let us mention here that if S is the area of the right triangle with sides a, b, c, with c the hypotenuse, then

$$c^2 \pm 4S = c^2 \pm 2ab = a^2 + b^2 \pm 2ab = (a \pm b)^2.$$

This means, we have a three term arithmetic progression

$$\left(\frac{c}{2}\right)^2 - S, \quad \left(\frac{c}{2}\right)^2, \quad \left(\frac{c}{2}\right)^2 + S$$

consisting of rational squares. This is perhaps the reason for the name *congruent*. Dickson mentions that in tenth century an Iranian mathematician and this author's fellow townsman Mohammad Ben Hossein Karaji (953–1029) stated that the problem of determining congruent numbers was the "principal object of the theory of rational right triangles." Dickson [16, Ch. XVI] is a wonderful review of work by various mathematicians on the problem of characterizing congruent numbers over the millennium up to its publication. For a modern treatment of this subject we refer the reader to [30, Ch. 1].

Tunnell's theorem

The theory of rational points on cubic curves, the *theory of elliptic curves*, is a rich active area of research with connections to many parts of modern mathematics [47]. In the last three decades many results about congruent numbers have been obtained that use methods and techniques involving elliptic curves. It appears that Stephens's very short paper [97] was the first paper that made the connection to elliptic curves explicit. Tunnell's paper [105] pushed the theory far. Among other results, Tunnell proved the following surprising theorem:

Theorem 4.8 (Tunnell). *Define a formal power series in the variable q by*

$$g = q \prod_{n=1}^{\infty} (1 - q^{8n})(1 - q^{16n}),$$

and for each $t \in \mathbb{N}$ set $\theta_t = \sum_{n \in \mathbb{Z}} q^{tn^2}$. Define integers $a(n)$ and $b(n)$ via the identities

$$g\theta_2 = \sum_{n=1}^{\infty} a(n)q^n,$$

and

$$g\theta_4 = \sum_{n=1}^{\infty} b(n)q^n.$$

Then, we have

- *If* $a(n) \neq 0$*, then* n *is not a congruent number;*
- *If* $b(n) \neq 0$*, then* $2n$ *is not a congruent number.*

Conjecturally, both statements in the theorem should be *if and only if*. The coefficients $a(n)$, $b(n)$ are computable in terms of the number of solutions in integers of equations of the form

$$Ax^2 + By^2 + Cz^2 = n$$

for $A, B, C \in \mathbb{N}$. (We advise the reader to do this as an exercise!) Tunnell recovers a number of previously known results from his numerical criterion. For example, he shows a prime p of the form $8k + 3$ is not congruent, as for such primes $a(p) \equiv 2 \bmod 4$, or that if p, q are primes of the form $8k + 5$, then $2pq$ is not congruent. It is an easy exercise to derive Theorem 4.4 from Theorem 4.8.

At least conjecturally one expects the existence of many congruent numbers. For example, we have the following conjecture which is a consequence of the Birch and Swinnerton-Dyer Conjecutre [47, Conjecture 16.5]:

Conjecture 4.9 ([59, 60]). Every positive integer congruent to 5, 6, or 7 modulo 8 is a congruent number.

Recently some impressive results have been obtained in this direction [101, 102]. Smith [95] has proved that at least 55.9% of positive square free integers $n \equiv 5, 6, 7 \bmod 8$ are congruent numbers. In contrast, Smith [96] has proved that congruent numbers are rare among natural numbers $n \equiv 1, 2, 3 \bmod 8$.