# 16. Diophantine problems and elliptic curves

## 16.1 Congruent numbers

Already Fermat knew that there is no right triangle with integer side lengths whose area is a perfect square (Corollary 10.7). In other words, there is no right triangle whose side lengths are rational numbers, and the area is equal to $1$. On the other hand, it is clear that there is such a triangle with the area equal to $6$. That is the triangle with sides $(3, 4, 5)$. It is not as obvious, but it was already known to Fibonacci that there is such a triangle with the area equal to $5$. That is the triangle with sides $(3/2, 20/3, 41/6)$. These examples bring us to the following definition.

**Definition 16.1.** *We say that a positive integer $n$ is a* congruent number *if it is equal to the area of a right triangle whose side lengths are rational numbers.*

We already saw that $5$ and $6$ are congruent numbers. The number $7$ is also congruent because it is equal to the area of the triangle with sides $(24/5, 35/12, 337/60)$. On the other hand, it is known that the numbers $1$, $2$, $3$, $4$, $8$, $9$ and $10$ are not congruent.

We come to the question, for a given positive integer $n$, how can we determine whether it is congruent or not. We will see that this question is connected with elliptic curves.

**Proposition 16.1.** *A positive integer $n$ is a congruent number if and only if there is a rational number $x$ such that $x$, $x - n$ and $x + n$ are the squares of rational numbers.*

*Proof:* Let rational numbers $a$, $b$, $c$ be the lengths of the legs and the hypotenuse of a right triangle with the area $ab/2 = n$. Let $x = c^2/4$. Then

$x - n = (a-b)^2/4$ and $x + n = (a+b)^2/4$. Hence, $x - n$, $x$ and $x + n$ are squares of rational numbers.

Conversely, if $x-n$, $x$, $x+n$ are squares of rational numbers, say $x = u^2$, $x - n = v^2$, $x + n = w^2$, then by putting $a = w + v$, $b = w - v$, $c = 2u$, we obtain a right triangle with side lengths $(a, b, c)$ and the area $ab/2 = n$, so $n$ is a congruent number. □

If the numbers $x - n$, $x$, $x + n$ are squares of rational numbers, then, of course, their product is the square of a rational number. We conclude that if $n$ is a congruent number, then on the elliptic curve

$$E_n : \quad y^2 = x^3 - n^2 x$$

there is, apart from the points of order 2: $(0,0)$, $(n,0)$ and $(-n,0)$, at least one additional rational point. The question arises, whether the converse of this statement holds. Let $P = (x, y)$, $y \neq 0$, be a rational point on a curve $E_n$. Then we know that the product of numbers $x - n$, $x$ and $x + n$ is the square of a rational number. However, this does not mean that each of those numbers is also the square of a rational number. From Theorem 15.9, we know that this stronger requirement is satisfied for the point $2P$. We can also check that directly. Indeed,

$$\begin{aligned}
x(2P) &= \left(\frac{3x^2 - n^2}{2y}\right)^2 - 2x = \frac{x^4 + 2n^2x^2 + n^4}{4y^2} = \left(\frac{x^2 + n^2}{2y}\right)^2, \\
x(2P) + n &= \left(\frac{x^2 + 2nx - n^2}{2y}\right)^2, \\
x(2P) - n &= \left(\frac{x^2 - 2nx - n^2}{2y}\right)^2.
\end{aligned}$$

Hence, we proved the following characterization of congruent numbers.

**Proposition 16.2.** *A positive integer $n$ is a congruent number if and only if the elliptic curve $E_n$ has at least one rational point $P = (x, y)$ with $y \neq 0$.*

It can be shown that, apart from the points of order 2, the curve $E_n$ does not have any other point of finite order (see [241, Chapter 5], [251, Chapter 1], [319, Chapter 24.1]). Therefore, the number $n$ is congruent if and only if the rank of $E_n$ is positive.

The result which came closest to answering the question how, for a given positive integer $n$, to determine whether it is congruent, is Tunnell's theorem from the paper [402], in whose proof many deep concepts and results connected to elliptic curves are used.

**Theorem 16.3** (Tunnell, 1983). *Let $n$ be a square-free positive integer and let $d = 1$ if $n$ is odd, and $d = 2$ if $n$ is even. If $n$ is a congruent number, then the number of integer solutions $(x, y, z)$ of the equation*

$$x^2 + 2dy^2 + 8z^2 = n/d$$

*is twice the number of the integer solutions of the equation*

$$x^2 + 2dy^2 + 32z^2 = n/d.$$

*Under the assumption that the Birch-Swinnerton-Dyer conjecture holds, the converse of this statement is also true.*

**Example 16.1.** Let $n = 3$. The equations $x^2 + 2y^2 + 8z^2 = 3$ and $x^2 + 2y^2 + 32z^2 = 3$ each have $4$ solutions: $(1, 1, 0)$, $(1, -1, 0)$, $(-1, 1, 0)$, $(-1, -1, 0)$, so from Tunnell's theorem, it follows that the number 3 is not congruent.

**Example 16.2.** Let $n = 34$. The equation $x^2 + 4y^2 + 8z^2 = 17$ has $8$ solutions: $(1, 2, 0)$, $(1, -2, 0)$, $(-1, 2, 0)$, $(-1, -2, 0)$, $(3, 0, 1)$, $(3, 0, -1)$, $(-3, 0, 1)$, $(-3, 0, -1)$, while the equation $x^2 + 4y^2 + 32z^2 = 17$ has $4$ solutions: $(1, 2, 0)$, $(1, -2, 0)$, $(-1, 2, 0)$, $(-1, -2, 0)$. Therefore, from the converse of Tunnell's theorem, we expect that the number $34$ is congruent. Let us make sure of that by finding a right triangle with rational side lengths whose area is equal to $34$. We start with the elliptic curve $y^2 = x^3 - 34^2 x$. There is the rational point $P = (-2, 48)$ on it. Let us denote by $x$ the first coordinate of the point $2P$. We calculate: $x = (145/12)^2$, $x - n = (127/12)^2$, $x + n = (161/12)^2$ and from the proof of Proposition 16.1, we find the side lengths of the right triangle: $a = 24$, $b = 17/6$, $c = 145/6$.

The number $n = 34$ from the previous example is the smallest positive integer such that $\text{rank}(E_n(\mathbb{Q})) = 2$. There are positive integers for which $\text{rank}(E_n(\mathbb{Q})) = 3, 4, 5, 6, 7$ (see [137]), but it is not known whether there is a positive integer $n$ such that $\text{rank}(E_n(\mathbb{Q})) \geq 8$.

## 16.2 Mordell's equation

In 1923, Mordell proved that a Diophantine equation of the form

$$y^2 = x^3 + ax^2 + bx + c,$$

where the cubic polynomial on the right-hand side of the equation does not have multiple roots, has only finitely many integer solutions. In other