FIGURE 6.5. Louis J. Mordell

6.5 Elliptic Curves Over the Rational Numbers

Let E be an elliptic curve defined over $\mathbf{Q}$. The following is a deep theorem about the group $E(\mathbf{Q})$.

Theorem 6.5.1 (Mordell). *The group $E(\mathbf{Q})$ is finitely generated. That is, there are points $P_1, \ldots, P_s \in E(\mathbf{Q})$ such that every element of $E(\mathbf{Q})$ is of the form $n_1P_1 + \cdots + n_sP_s$ for integers $n_1, \ldots n_s \in \mathbf{Z}$.*

Mordell's theorem implies that it makes sense to ask whether or not we can compute $E(\mathbf{Q})$, where by "compute" we mean find a finite set $P_1, \ldots, P_s$ of points on E that generate $E(\mathbf{Q})$ as an abelian group. There is a systematic approach to computing $E(\mathbf{Q})$ called "descent" (see e.g., [Cre97, Cre, Sil86]). It is widely believed that descent will always succeeds, but nobody has yet proved that it does. Proving that descent works for all curves is one of the central open problem in number theory, and is closely related to the Birch and Swinnerton-Dyer conjecture (one of the Clay Math Institute's million dollar prize problems). The crucial difficulty amounts to deciding whether or not certain explicitly given curves have any rational points on them or not (these are curves that have points over $\mathbf{R}$ and modulo n for all n).

The details of using descent to computing $E(\mathbf{Q})$ are beyond the scope of this book. In several places below we will simply assert that $E(\mathbf{Q})$ has a certain structure or is generated by certain elements. In each case, we computed $E(\mathbf{Q})$ using a computer implementation of this method.

6.5.1 The Torsion Subgroup of $E(\mathbf{Q})$ and the Rank

For any abelian group G, let G_{tor} be the subgroup of elements of finite order. If E is an elliptic curve over $\mathbf{Q}$, then $E(\mathbf{Q})_{\mathrm{tor}}$ is a subgroup of $E(\mathbf{Q})$, which must be finite because of Theorem 6.5.1 (see Exercise 6.6).

One can also prove that $E(\mathbf{Q})_{\mathrm{tor}}$ is finite by showing that there is a prime p and an injective reduction homomorphism $E(\mathbf{Q})_{\mathrm{tor}} \hookrightarrow E(\mathbf{Z}/p\mathbf{Z})$, then noting that $E(\mathbf{Z}/p\mathbf{Z})$ is finite. For example, if E is $y^2 = x^3 - 5x + 4$, then $E(\mathbf{Q})_{\mathrm{tor}} = \{\mathcal{O}, (1,0)\} \cong \mathbf{Z}/2\mathbf{Z}$.

The possibilities for $E(\mathbf{Q})_{\mathrm{tor}}$ are known.

Theorem 6.5.2 (Mazur, 1976). *Let E be an elliptic curve over $\mathbf{Q}$. Then $E(\mathbf{Q})_{\mathrm{tor}}$ is isomorphic to one of the following 15 groups:*

$$\begin{array}{rl} \mathbf{Z}/n\mathbf{Z} & \textit{for } n \leq 10 \textit{ or } n = 12, \\ \mathbf{Z}/2 \times \mathbf{Z}/2n & \textit{for } n \leq 4. \end{array}$$

The quotient $E(\mathbf{Q})/E(\mathbf{Q})_{\mathrm{tor}}$ is a finitely generated free abelian group, so it is isomorphism to $\mathbf{Z}^r$ for some integer r, called the *rank* of $E(\mathbf{Q})$. For example, using descent one finds that if E is $y^2 = x^3 - 5x + 4$, then $E(\mathbf{Q})/E(\mathbf{Q})_{\mathrm{tor}}$ is generated by the point $(0,2)$. Thus $E(\mathbf{Q}) \cong \mathbf{Z} \times (\mathbf{Z}/2\mathbf{Z})$.

The following is a folklore conjecture, not associated to any particular mathematician:

Conjecture 6.5.3. *There are elliptic curves over $\mathbf{Q}$ of arbitrarily large rank.*

The "world record" is the following curve, whose rank is at least 24:

$$\begin{aligned} y^2 + xy + y = x^3 &- 120039822036992245303534619191166796374x \\ &+ 504224992484910670010801799168082726759443756222911415116 \end{aligned}$$

It was discovered in January 2000 by Roland Martin and William McMillen of the National Security Agency.

6.5.2 The Congruent Number Problem

Definition 6.5.4 (Congruent Number). We call a nonzero rational number n a *congruent number* if $\pm n$ is the area of a right triangle with rational side lengths. Equivalently, n is a *congruent number* if the system of two equations

$$\begin{aligned} a^2 + b^2 &= c^2 \\ \frac{1}{2}ab &= n \end{aligned}$$

has a solution with $a, b, c \in \mathbf{Q}$.

For example, 6 is the area of the right triangle with side lengths 3, 4, and 5, so 6 is a congruent number. Less obvious is that 5 is also a congruent number; it is the area of the right triangle with side lengths 3/2, 20/3, and 41/6. It is nontrivial to prove that 1, 2, 3, and 4 are not congruent numbers. Here is a list of the integer congruent numbers up to 50:

$$5, 6, 7, 13, 14, 15, 20, 21, 22, 23, 24, 28, 29, 30, 31, 34, 37, 38, 39, 41, 45, 46, 47.$$

Every congruence class modulo 8 except 3 is represented in this list, which incorrectly suggests that if $n \equiv 3 \pmod 8$ then n is not a congruent number. Though no $n \leq 218$ with $n \equiv 3 \pmod 8$ is a congruent number, $n = 219$ is a congruent number congruent and $219 \equiv 3 \pmod 8$.

Deciding whether an integer n is a congruent number can be subtle since the simplest triangle with area n can be very complicated. For example, as Zagier pointed out, the number 157 is a congruent number, and the "simplest" rational right triangle with area 157 has side lengths

$$a = \frac{6803298487826435051217540}{411340519227716149383203} \text{ and } b = \frac{411340519227716149383203}{21666555693714761309610}.$$

This solution would be difficult to find by a brute force search.

We call congruent numbers "congruent" because of the following proposition, which asserts that any congruent number is the common "congruence" between three perfect squares.

Proposition 6.5.5. *Suppose n is the area of a right triangle with rational side lengths a, b, c, with $a \leq b < c$. Let $A = (c/2)^2$. Then*

$$A - n, \quad A, \quad \text{and } A + n$$

are all perfect squares of rational numbers.

Proof. We have

$$\begin{aligned} a^2 + b^2 &= c^2 \\ \frac{1}{2}ab &= n \end{aligned}$$

Add or subtract 4 times the second equation to the first to get

$$\begin{aligned} a^2 \pm 2ab + b^2 &= c^2 \pm 4n \\ (a \pm b)^2 &= c^2 \pm 4n \\ \left(\frac{a \pm b}{2}\right)^2 &= \left(\frac{c}{2}\right)^2 \pm n \\ &= A \pm n \end{aligned}$$

□

The main motivating open problem related to congruent numbers, is to give a systematic way to recognize them.

Open Problem 6.5.6. *Give an algorithm which, given n, outputs whether or not n is a congruent number.*

Fortunately, the vast theory developed about elliptic curves has something to say about the above problem. In order to understand this connection, we begin with an elementary algebraic proposition that establishes a link between elliptic curves and the congruent number problem.

Proposition 6.5.7 (Congruent numbers and elliptic curves). *Let n be a rational number. There is a bijection between*

$$A = \left\{(a,b,c) \in \mathbf{Q}^3 \;:\; \frac{ab}{2} = n,\; a^2+b^2=c^2\right\}$$

and

$$B = \left\{(x,y) \in \mathbf{Q}^2 \;:\; y^2 = x^3 - n^2x, \text{ with } y \neq 0\right\}$$

given explicitly by the maps

$$f(a,b,c) = \left(-\frac{nb}{a+c},\; 2n^2a + c\right)$$

and

$$g(x,y) = \left(\frac{n^2-x^2}{y},\; -\frac{2xn}{y},\; \frac{n^2+x^2}{y}\right).$$

The proof of this proposition is not deep, but involves substantial (elementary) algebra and we will not prove it in this book.

For $n \neq 0$, let E_n be the elliptic curve $y^2 = x^3 - n^2x$.

Proposition 6.5.8 (Congruent number criterion). *The rational number n is a congruent number if and only if there is a point $P = (x,y) \in E_n(\mathbf{Q})$ with $y \neq 0$.*

Proof. The number n is a congruent number if and only if the set A from Proposition 6.5.7 is nonempty. By the proposition A is nonempty if and only if B is nonempty. □

Example 6.5.9. Let $n = 5$. Then E_n is $y^2 = x^3 - 25x$, and we notice that $(-4,-6) \in E_n(\mathbf{Q})$. We next use the bijection of Proposition 6.5.7 to find the corresponding right traingle:

$$g(-4,-6) = \left(\frac{25-16}{-6}, -\frac{-40}{-6}, \frac{25+16}{-6}\right) = \left(-\frac{3}{2}, -\frac{20}{3}, -\frac{41}{6}\right).$$

Multiplying through by -1 yields the side lengths of a rational right triangle with area 5. *Are there any others?*

Observe that we can apply g to any point in $E_n(\mathbf{Q})$ with $y \neq 0$. Using the group law we find that $2(-4,-6) = (1681/144, 62279/1728)$, and

$$g(2(-4,-6)) = \left(-\frac{1519}{492}, -\frac{4920}{1519}, \frac{3344161}{747348}\right).$$

Example 6.5.10. Let $n = 1$, so E_1 is defined by $y^2 = x^3 - x$. Since 1 is not a congruent number, the elliptic curve E_1 has no point with $y \neq 0$. See Exercise 6.10.

Example 6.5.9 foreshadows the following theorem.

Theorem 6.5.11 (Infinitely Many Triangles). *If n is a congruent number, then there are infinitely many distinct right triangles with rational side lengths and area n.*

We will not prove this theorem, except to note that one proves it by showing that $E_n(\mathbf{Q})_{\text{tor}} = \{\mathcal{O}, (0,0), (n,0), (-n,0)\}$, so the elements of the set B in Proposition 6.5.7 all have infinite order, hence B is infinite so A is infinite.

Tunnell has proved that the Birch and Swinnerton-Dyer (alluded to above), implies the existence of an elementary way to decide whether or not an integer n is a congruent number. We state Tunnell's elementary way in the form of a conjecture.

Conjecture 6.5.12. *Let a, b, c denote integers. If n is an even square-free integer then n is a congruent number if and only if*

$$\#\left\{(a,b,c) \in \mathbf{Z}^3 : 4a^2 + b^2 + 8c^2 = \frac{n}{2} : c \text{ is even}\right\}$$

$$= \#\left\{(a,b,c) : 4a^2 + b^2 + 8c^2 = \frac{n}{2} : c \text{ is odd}\right\}.$$

If n is odd and square free then n is a congruent number if and only if

$$\#\left\{(a,b,c) : 2a^2 + b^2 + 8c^2 = n : c \text{ is even}\right\}$$

$$= \#\left\{(a,b,c) : 2a^2 + b^2 + 8c^2 = n : c \text{ is odd}\right\}.$$

Enough of the Birch and Swinnerton-Dyer conjecture is known to prove one direction of Conjecture 6.5.12. In particular, it is a very deep theorem that if we do not have equality of the displayed cardinalities, then n is not a congruent number. For example, when $n = 1$,

The even more difficult (and still open!) part of Conjecture 6.5.12 is the converse: If one has equality of the displayed cardinalities, prove that n is a congruent number. The difficulty in this direction, which appears to be very deep, is that we must somehow construct (or prove the existence of) elements of $E_n(\mathbf{Q})$. This has been accomplished in some cases do to groundbreaking work of Gross and Zagier ([GZ86]) but much work remains to be done.

The excellent book [Kob84] is about congruent numbers and Conjecture 6.5.12, and we encourage the reader to consult it. The Birch and Swinnerton-Dyer conjecture is a Clay Math Institute million dollar millennium prize problem (see [Cla, Wil00]).