13

The Birch and Swinnerton-Dyer Conjecture

This chapter is about a conjecture that Birch and Swinnerton-Dyer made in the 1960s on the ranks of elliptic curves.

First we discuss the congruent number problem, which is an ancient problem that goes back over one thousand years, and see how it is connected with the Birch and Swinnerton-Dyer conjecture.

13.1 The Congruent Number Problem

Definition 13.1.1 (Congruent Number). A nonzero rational number n is called 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

$$n = \frac{ab}{2} \qquad \text{and} \qquad a^2 + b^2 = c^2$$

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

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 congruent numbers up to 50:

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

Every congruence class modulo 8 except 3 is represented in this list, which suggests that if $n \equiv 3 \pmod 8$ then n is not a congruent number. This is true for $n \leq 218$, but $n = 219$ is a congruent number congruent to 3 mod 8. Something very subtle is going on.

This is another example which hints at the subtlety of congruent numbers. The number 157 is a congruent number, and Zagier showed that the *simplest* rational right triangle with area 157 has side lengths

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

This solution would take a long time to find by a brute force search.

The terminology "congruent" arises from the fact that if n is a congruent number, then there exists a rational number A such that $n - A$, A, and $n + A$ are all rational numbers. Thus n is the common congruence between the rational numbers.

Proposition 13.1.2. *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*

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

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 following open problem has motivated much of the work in the theory of congruent numbers.

Open Problem 13.1.3. *Give an algorithm which, given n, outputs whether or not n is a congruent number.*

As we will see, this problem is closely related to a problem about elliptic curves.

13.1.1 Congruent Numbers and Elliptic Curves

The following proposition establishes a link between elliptic curves and the congruent number problem. This link connects the congruent number problem with the Birch and Swinnerton-Dyer conjecture.

Proposition 13.1.4. *Let n be a nonzero rational number. There is a bijection between the sets*

$$A = \left\{(x, y, z) \in \mathbb{Q}^3 : \frac{xy}{2} = n, x^2 + y^2 = z^2\right\}$$

and

$$B = \left\{(r, s) \in \mathbb{Q}^2 : s^2 = r^3 - n^2 r, \text{ with } s \neq 0\right\}$$

given by the maps

$$f(x, y, z) = \left(-\frac{ny}{x+z}, 2n^2 x + z\right)$$

and

$$g(r, s) = \left(\frac{n^2 - r^2}{s}, -\frac{2rn}{s}, \frac{n^2 + r^2}{s}\right).$$

Proof. This proposition can be proved using nothing more than lots of elementary algebraic manipulation. By substitution, verify that f and g are well defined, then check that $f(g(r, s)) = (r, s)$. Finally, let K be the field of fractions of $\mathbb{Q}(n, y)[z]/(z^2 - (y^2 + (2n/y)^2))$. If $(x, y, z) \in A$ then $(x, y, z) = (2n/y, y, z)$ and we find, working in K, that $g(f(2n/y, y, z)) = (2n/y, y, z)$.

We illustrate how to verify that the maps are mutually inverse bijections using MAGMA, though one could of course do this by hand. Input the following:

```
R<n,y> := FieldOfFractions(PolynomialRing(Rationals(),2));
S<z>   := PolynomialRing(R);
T<z>   := quo<S | z^2 - (y^2 + (2*n/y)^2)>;
K<z>   := FieldOfFractions(T);
U<r,s> := FieldOfFractions(PolynomialRing(Rationals(),2));
function f(w)
   x,y,z := Explode(w);
   return [-n*y/(x+z), 2*n^2/(x+z)];
end function;
function g(w)
   r,s := Explode(w);
   return [(n^2-r^2)/s, -2*r*n/s, (n^2+r^2)/s];
end function;
```

Then

```
> g(f([2*n/y,y,z]));
[2*n/y, y, z]
> f(g([r,s]));
[n, y]
```

It says (n, y) instead of (r, s) because n and y were the names we first assigned for printing the variables of *the* polynomial ring in two variables (in MAGMA there is only one such ring). □

Corollary 13.1.5. *The nonzero rational number n is a congruent number if and only if the elliptic curve E_n defined by $y^2 = x^3 - n^2x$ has a solution with $y \neq 0$.*

Proof. The number n is a congruent number if and only if the set A from Proposition 13.1.4 is nonempty. By the proposition A is nonempty if and only if B is nonempty, which proves the corollary. □

Example 13.1.6. Let $n = 5$. Then E_n is defined by $y^2 = x^3 - 25x$, and we find by a brute force search the solution $(-4, -6)$. Then

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

Multiplying through by -1 yields the side lengths of a rational right triangle with area 5.

Example 13.1.7. 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 $y \neq 0$.

Recall that if A is an abelian group, then the *torsion subgroup* A_{tor} of A is the subgroup of elements of A with finite order.

Proposition 13.1.8. *The torsion subgroup of $E_n(\mathbb{Q})$ has order* 4.

This proposition can be proved by considering natural reduction maps from $E_n(\mathbb{Q})$ to the group of points on the elliptic curve over $\mathbb{F}_p$ defined by $y^2 = x^3 - n^2x$ for many p. For details, see e.g., [?, §9] (Neil Koblitz's book "Introduction to Elliptic Curves and Modular Forms").

Recall that the *rank* of an elliptic curve E over $\mathbb{Q}$ is the positive integer r such that $E(\mathbb{Q})/E(\mathbb{Q})_{\mathrm{tor}} \approx \mathbb{Z}^r$. Combining the above corollary and proposition proves the following theorem.

Theorem 13.1.9. *A nonzero rational number n is a congruent number if and only if $E_n(\mathbb{Q})$ has rank ≥ 1.*

The following corollary is not at all obvious from the definition of a congruent number, but it follows immediately from the theorem.

Corollary 13.1.10. *If n is a congruent number, then there are infinitely many right triangles with area $\pm n$.*

In the next section we will associate to any elliptic curve E over $\mathbb{Q}$ a holomorphic function $L(E, s)$ on $\mathbb{C}$. The Birch and Swinnerton-Dyer conjecture predicts that E has positive rank if and only if $L(E, 1) = 0$. Using "half integral weight modular forms" and a deep theorem of Waldspurger, Jerrold Tunnel gave a simple criterion for whether or not $L(E_n, 1) = 0$. Thus a proof of the Birch and Swinnerton-Dyer conjecture would also solve Problem 13.1.3.

Theorem 13.1.11 (Tunnel). *If n is an even squarefree integer then $L(E_n, 1) = 0$ if and only if*

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

If n is odd and squarefree then $L(E_n, 1) = 0$ if and only if

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

Example 13.1.12. When $n = 6$, we get

$$\#\emptyset = \#\emptyset,$$

and when $n = 1$, we get

$$\#\{(0,1,0)\} \neq \#\emptyset.$$

Partial results are known towards the assertion that $E_n(\mathbb{Q})$ is infinite if and only if $L(E_n, 1) = 0$. The implication "$E_n(\mathbb{Q})$ has positive rank implies that $L(E_n, 1) = 0$" was proved by John Coates and Andrew Wiles. The other implication "$L(E_n, 1) = 0$ implies that $E_n(\mathbb{Q})$ has positive rank" is still unknown today. It was proved in the special case when $L'(E_n, 1) \neq 0$ by Dick Gross and Don Zagier.