tions modulo $p$; i.e., $N_p$ is the number of pairs $(x, y)$ of integers modulo $p$ such that

$$y^2 \equiv x^3 + ax + b \pmod{p}$$

For example, suppose we take the elliptic curve $y^2 = x^3 - x$ and the prime $p = 5$. Then, by testing the congruence

$$y^2 \equiv x^3 - x \pmod{5}$$

with all possible pairs of values $(x, y)$ for $x = 0, 1, 2, 3, 4$ and $y = 0, 1, 2, 3, 4$, we find that the solutions are $(0, 0)$, $(1, 0)$, $(4, 0)$, $(2, 1)$, $(3, 2)$, $(3, 3)$, $(2, 4)$. There are 7 of these. Hence, for this equation, $N_5 = 7$.

The idea behind looking at the finite, mod $p$, versions of the counting problem is this: If $(u, v)$ is a whole-number solution to the equation

$$y^2 = x^3 + ax + b$$

then $(u \bmod p, v \bmod p)$ solves the congruence

$$y^2 \equiv x^3 + ax + b \pmod{p}$$

where $u \bmod p$ is the remainder on dividing $u$ by $p$, etc. More generally, because division modulo a prime modulus always leads to a whole-number answer, any rational solution to the original equation gives rise to a whole-number solution to the corresponding congruence. Thus, if there is a rational point on the original elliptic curve, then for every prime number $p$, the corresponding mod $p$ congruence has a solution. If in fact there are infinitely many rational points on the elliptic curve, we can expect that for many primes $p$ the congruence has many solutions. (This last observation gains significance because, as we shall see presently, in the case of an elliptic curve that arises from the triangle area problem, if there is one rational point on the curve, then there are infinitely many.)

There is no obvious reason why the converse would be true: that the existence of many solutions to the mod $p$ congruences for lots of primes $p$ implies that the original equation definitely has a rational solution, let alone infinitely many. But it would surely seem a likely possibility—or so Birch and Swinnerton-Dyer assumed. More precisely, they based their conjecture on the assumption that the existence of *lots* of solutions to the congruences for *lots* of primes would imply that the original equation does indeed have infinitely many rational solutions.

The question then was, how do you find out whether there are lots of solutions to lots of those congruences?

Now, if you have reached this point, you will have a general idea of what the Birch and Swinnerton-Dyer conjecture is about, and how it relates to a classic geometry problem about right triangles. You should feel pretty good about having gotten this far. Unfortunately, the going is going to get quite a bit harder from this point on. Don't feel bad if you find yourself getting lost. Most readers will. Like many parts of modern advanced mathematics, the level of abstraction is simply too great for the nonexpert to make much headway. Although I have been a professional mathematician for over thirty years, number theory is not my area of expertise, and it took me considerable effort, spread over several weeks, aided by discussions with experts that I knew, before I understood the problem sufficiently to write this chapter. I would not even attempt to try to solve it.

If you still want to continue, let's pick up the thread again. (When you feel you cannot proceed any further, simply give up and start the next chapter—where, I have to be honest, you are likely to make even less progress than you have here.)

To determine whether there are lots of solutions to lots of those mod $p$ congruences, Birch and Swinnerton-Dyer computed the "density functions"

$$\prod_{p \leq M,\ p \text{ prime}} \frac{p}{N_p}$$

(where $N_p$ is as above) for larger and larger values of $M$.

[If you are not fa
the $\sum$ notation to
chapter for an exp
The next step
graphs of the valu
try to find some
formula to look a

taken over *all* pri
to give a finite a
Swinnerton-Dyer
would have provi
nite product, and
alyze their comput
uct cannot be gu
the strategy of lo
a good one, and i
Since that other
one above, howe
would have gone
and then describ
made in order to
If the origina
points, then for
have a large num
many primes the
the infinite prod
Birch and Swinne
work the other w
it is zero, then m
does in fact have
perhaps the ellip
points if and onl

[If you are not familiar with the $\prod$ notation used above, or with the $\sum$ notation to be used momentarily, see the appendix to this chapter for an explanation.]

The next step was to examine the data they got—primarily graphs of the values of $\prod_{p\leq M} \frac{p}{N_p}$ for increasing values of $M$—and try to find some formula that described the data. The obvious formula to look at first was the infinite product

$$\prod_{p} \frac{p}{N_p}$$

taken over *all* primes. If this infinite product were guaranteed to give a finite answer, the values of $\prod_{p\leq M} \frac{p}{N_p}$ that Birch and Swinnerton-Dyer computed for larger and larger values of $M$ would have provided a sequence of approximations to that infinite product, and they could have used the infinite product to analyze their computational data. Unfortunately, the infinite product cannot be guaranteed to give a finite answer. Nevertheless, the strategy of looking for a formula that captured the data was a good one, and it turned out that a related formula does work. Since that other infinite product is more complicated than the one above, however, what I'll do is outline the way the analysis would have gone had the infinite product above given an answer, and then describe the changes that Birch and Swinnerton-Dyer made in order to get an argument that worked.

If the original elliptic curve has infinitely many rational points, then for many primes $p$ the mod $p$ congruence should have a large number of solutions, which means that for infinitely many primes the ratio $\frac{p}{N_p}$ should be (much) less than 1, and hence the infinite product should work out to be 0. The conjecture Birch and Swinnerton-Dyer made was that this argument would work the other way round: If we calculate $\prod_p \frac{p}{N_p}$ and find that it is zero, then maybe that will tell us that the elliptic equation does in fact have infinitely many rational points. In other words, perhaps the elliptic curve will have an infinite number of rational points if and only if

$$\prod_p \frac{p}{N_p} = 0$$

But how do you work out this infinite product? Well, we've met an infinite product of fractions taken over all the primes before, in Chapter 1. Euler showed that for any real number $s > 1$, the infinite product

$$\prod_{p \text{ prime}} \frac{1}{1-(1/p^s)}$$

is equal to the infinite sum

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$$

Riemann (and others) then went on to show that the function $\zeta(s)$ could be extended to give an answer for any complex number $s$, and that the extended function could be studied using methods of calculus. Dirichlet showed that the same kind of process would work for a more general class of "zeta functions," called L-functions. (See the appendix to Chapter 1.)

Suppose you could do the same kind of thing for the Euler-like infinite product

$$\prod_p \frac{p}{N_p}$$

That is, suppose you could show that there is a function $L(E,s)$ that gives an answer for any complex number $s$ and that can be studied using methods of calculus, such that

$$L(E,1) = \prod_p \frac{p}{N_p}$$

(The $E$ is included in the notation for $L$ because the numbers $N_p$ depend on $E$.) Then, by calculating $L(E,1)$, you could get some information about the number of rational points on the elliptic

curve. In fa
everything y
puter runs,
infinite num
This, in
ture. But n
exactly as I
of carrying
you need t
$\prod_p \frac{p}{N_p}$. (For
uct does no
whether the
swer for all
cial case of
resolved un
proved it en
to 1994, it v
Dyer conjec
was a funct
there was su
$s$, in particu
such a funct
the conjectu
namely, that
only if $L(E,$
In the re
tail—and a
outlined.

## *Why Ellip*

Much of the
arise all over

3. Strictly spea
missing pieces
Diamond, and

Well, we've
ll the primes
real number

the function
mplex num-
udied using
kind of pro-
functions,"

or the Euler-

ction $L(E, s)$
d that can be

numbers $N_p$
uld get some
n the elliptic

curve. In fact, said Birch and Swinnerton-Dyer, you might get everything you wanted. Based on the evidence from their computer runs, they suggested that the elliptic curve will have an infinite number of rational points if and only if $L(E, 1) = 0$.

This, in essence, is the Birch and Swinnerton-Dyer conjecture. But note that modifier "in essence." If you try to do it exactly as I've described it, it won't work. To have any hope of carrying out a Dirichlet-like argument to get an "L-function," you need to take a slightly more complicated product than $\prod_p \frac{p}{N_p}$. (For one thing, as I mentioned, this simple infinite product does not give a finite answer.) Then there's the question of whether there really is a suitable L-function (that gives an answer for all complex numbers $s$). That turns out to be a special case of the Tanayama–Shimura conjecture, which was not resolved until 1994, when Andrew Wiles and Richard Taylor proved it en route to the solution of Fermat's last theorem.[3] Prior to 1994, it was not even certain that the Birch and Swinnerton-Dyer conjecture really made sense. No one knew whether there was a function $L(E, s)$; more precisely, no one knew whether there was such a function that gave an answer for all numbers $s$, in particular for the key value $s = 1$. Now that we know such a function does indeed exist, the big question is whether the conjecture Birch and Swinnerton-Dyer made about it is true, namely, that there are infinitely many rational points on $E$ if and only if $L(E, 1) = 0$.

In the remainder of this chapter I'll provide a bit more detail—and a bit more precision—about the argument I've just outlined.

## *Why Elliptic Curves Are Important: The Group Structure*

Much of the interest in elliptic curves, and the reason why they arise all over the place in modern mathematics, is bound up with

[3] Strictly speaking, Wiles and Taylor proved only part of the conjecture. The missing pieces were supplied in 1999 by Christophe Breuil, Brian Conrad, Fred Diamond, and Richard Taylor.