$$4 \div 5 \equiv 5 \pmod 7$$

$$1 \div 6 \equiv 6 \pmod 7$$

(To check these, simply multiply—modulo 7—both sides by the second term on the left.) In fact, division works whenever the modulus is a prime number. But for a composite modulus, it is not always possible to divide one number by another in finite arithmetic. (Of course, you can't always divide one whole number by another in ordinary arithmetic if you want the answer to be a whole number as well.)

Thus, modular arithmetic—as these finite versions of arithmetic are sometimes called—is just like regular arithmetic. If the modulus is prime, then the corresponding modular arithmetic even has the additional property that you can divide any number by another (and get a whole-number answer).

Modular arithmetic has proved useful on a number of occasions. One of those was in providing a way for Birch and Swinnerton-Dyer to count the rational points on an elliptic curve.

How to Count an Infinite Set

In order to count rational points on an elliptic curve, Birch and Swinnerton-Dyer decided to carry out analogous counts modulo p for various primes p. That is to say, instead of trying to count the possibly infinite number of rational solutions to an equation

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

they took different prime numbers p and counted the number of pairs (x, y) of integers modulo p such that

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

For any given prime p, this counting is finite, of course, and hence can actually be carried out. Let N_p be the number of solu-

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 mod p, v mod p) solves the congruence

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

where u mod 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"

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

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

[If you are not 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 $\prod_{p \le M} \frac{p}{N_p}$ 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 $\prod_{p \le M} \frac{p}{N_p}$ 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