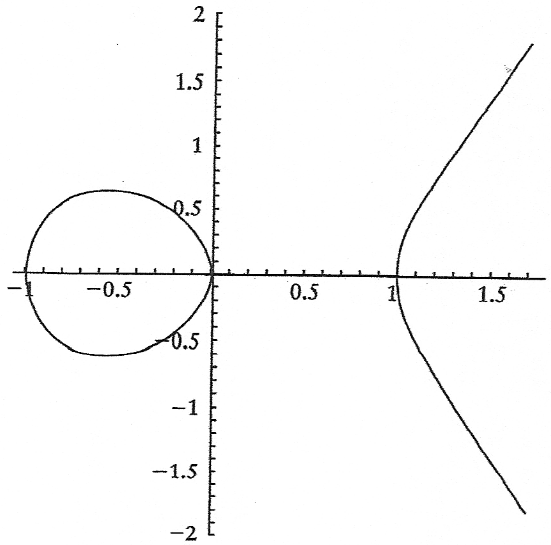

Figure 6.3. The elliptic curve $y^2 = x^3 - x$. Although it splits into two separate pieces, it is a single curve, determined by a single equation.

The two researchers approached the task by trying to find some way of "counting" the number of rational points on elliptic curves. Of course, since they were dealing with collections that could be infinite, the word "counting" has to be taken somewhat metaphorically.

One way to count a possibly infinite collection that sometimes works is to carry out a series of finite subcounts. This is what Birch and Swinnerton-Dyer did. To describe their method, we first have to break off and talk about finite arithmetic.

Counting by the Clock: Finite Arithmetic

We are all familiar with one situation where we count an endless (and hence potentially infinite) collection: the way we count minutes. There is (let's be optimistic) no last minute—time goes on forever. And yet we count minutes using just sixty numbers, 0 through 59. What we do, of course, is keep restarting the count. After we reach 59 minutes, we start again at 0. Another way to say this is that we treat 60 as if it were 0. Mathematicians would

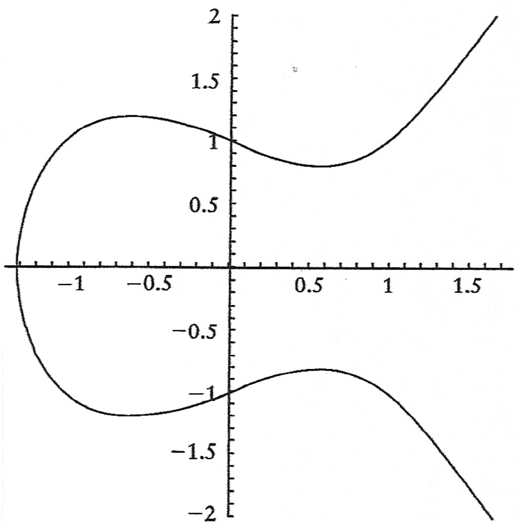

Figure 6.4. The elliptic curve $y^2 = x^3 - x + 1$. An example of an elliptic curve that does not split into two pieces.

say that we count minutes *modulo* 60. (The number 60 is the *modulus* for this counting.) Similarly, we count hours modulo 12 (or modulo 24).

For any positive whole number N, we can count modulo N. The numbers we use for this counting are 0, 1, 2, . . . , $N - 1$. After $N - 1$, we start again at 0.

We can then do arithmetic modulo N. To explain how, let's take the case $N = 7$. For this modulus, the counting numbers are 0, 1, 2, 3, 4, 5, 6. When we add any two numbers in this range, we discard 7 whenever it arises. For example, in arithmetic modulo 7,

$$2+3=5, \quad 3+4=0, \quad 4+5=2, \quad 6+6=5$$

Of course, this looks strange, and could be confusing, so mathematicians don't write it this way. Instead, they express the above additions like this:

$$2+3 \equiv 5 \pmod{7}$$

elliptic curve

er 60 is the
urs modulo

modulo N.
$\ldots, N-1$.

in how, let's
ing numbers
nbers in this
ple, in arith-

$6 = 5$

ng, so mathe-
ess the above

$$3+4 \equiv 0 \pmod 7$$
$$4+5 \equiv 2 \pmod 7$$
$$6+6 \equiv 5 \pmod 7$$

They call such expressions *congruences*. The first of the above four congruences is read "two plus three is congruent to five modulo seven." Notice that there is nothing special about 7 here. You could do the same thing with any other number.

Multiplication modulo 7 is defined similarly: You multiply the two numbers in the usual way and discard any multiples of 7. Thus

$$2 \times 3 \equiv 6 \pmod 7$$
$$3 \times 4 \equiv 5 \pmod 7$$
$$4 \times 5 \equiv 6 \pmod 7$$
$$6 \times 6 \equiv 1 \pmod 7$$

Similarly for any other modulus.

Since subtraction is the opposite of addition, you can always subtract in finite arithmetic. For example,

$$5-3 \equiv 2 \pmod 7$$
$$3-5 \equiv 5 \pmod 7$$
$$4-5 \equiv 6 \pmod 7$$
$$1-6 \equiv 2 \pmod 7$$

(To check these, simply add to both sides—modulo 7—the second term on the left.) The same is true for any modulus.

How about division? In the case where the modulus is 7, you can always divide. For example,

$$5 \div 3 \equiv 4 \pmod 7$$
$$3 \div 5 \equiv 2 \pmod 7$$

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

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

(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 mod
modulo p

For ex
and the pr

with all p
$y = 0, 1, 2$
(2, 1), (3,
equation,
The id
counting p
the equati

then (u m

where u m
generally,
leads to a
original ec
correspon
the origin
correspon
are infinit
expect tha
tions. (Th
shall see p
from the t
the curve,