Chapter 11

The Integers

In this chapter we begin to study the most basic, and also perhaps the most fascinating, number system of all — the integers. Our first aim will be to investigate factorization properties of integers. We know already that every integer greater than 1 has a prime factorization (Proposition 8.1). This was quite easy to prove using Strong Induction. A somewhat more delicate question is whether the prime factorization of an integer is always *unique* — in other words, whether, given an integer n, one can write it as a product of primes in only one way. The answer is yes; and this is such an important result that it has acquired the grandiose title of "The Fundamental Theorem of Arithmetic." We shall prove it in the next chapter, and try there to show why it is such an important result by giving some examples of its use. In this chapter we lay the groundwork for this.

We begin with a familiar definition.

DEFINITION *Let $a, b \in \mathbb{Z}$. We say a* divides *b (or a is a factor of b) if $b = ac$ for some integer c. When a divides b, we write $a|b$.*

Usually, of course, given two integers a, b at random, it is unlikely that a will divide b. But we can "divide a into b" and get a quotient and a remainder:

PROPOSITION 11.1
Let a be a positive integer. Then for any $b \in \mathbb{Z}$, there are integers q, r such that

$$b = qa + r \quad \text{and} \quad 0 \leq r < a \ .$$

The integer q is called the quotient, and r is the remainder. For example, if $a = 17, b = 183$ then the equation in Proposition 11.1 is $183 = 10 \cdot 17 + 13$, the quotient is 10 and the remainder 13.

PROOF Consider the rational number $\frac{b}{a}$. There is an integer q such