6 CHAPTER Finite Arithmetic

6.1 Three Examples

This book began by stressing the role of infinity in mathematics, its presence in the concept of number, and the importance of learning to live with it. Since then, infinity has appeared in many situations, and we have seen many ways to approach and tame it. Still, it is remarkable how often we succeed. Even if the world of ideas is infinite, as Dedekind believed, there is no doubt that *proofs* are finite, so success with infinity depends on capturing its properties by finite methods. Induction is one such method, but there are others.

Several times we have proved results about all numbers by considering only a finite set, such as the set of remainders that can occur when an integer is divided by 2 or 4. Apparently, the infinitude of the set of integers is irrelevant in some problems, and a way to see the relevant part is to focus on remainders. If so, the arithmetic of remainders deserves further clarification and development.

In daily life, we know it can be meaningful and useful to do arithmetic with remainders. For example, we add 3 hours to 11 o'clock and get 2 o'clock, the remainder when $11 + 3$ is divided by 12. Addition *mod 12*, as this is called, is the ideal arithmetic for keeping the time of day and is no great mathematical challenge. The plot

J. Stillwell, *Numbers and Geometry*

thickens when we combine addition and multiplication on finite sets. The idea not only seems to work, it actually seems capable of producing serious results, which are hard to notice or understand in the infinite set of natural numbers.

Example 1. Even and odd.

In proving that $2n^2 \neq m^2$ for all integers m and n (Section 1.1) we used the facts that even × even = even and odd × odd = odd. These facts follow from facts about 0 and 1: that if two integers leave remainder 0 on division by 2 then so does their product, and if two integers leave remainder 1 on division by 2 then so does their product. Such facts, and others such as even+even = even and even+odd = odd, hint at an "arithmetic of even and odd" that reflects the behavior of 0 and 1 as remainders on division by 2.

Example 2. Sums of two squares.

In proving that a primitive Pythagorean triple (a, b, c) cannot have a and b both odd (Section 4.2, Exercises), we used the fact that a square leaves remainder 0 or 1 on division by 4. Because this implies that the sum of odd squares leaves remainder 2, the sum of odd squares cannot be a square. Again it looks like there is a finite arithmetic in the background here, this time an arithmetic of the remainders 0, 1, 2, 3 on division by 4.

Example 3. Rational points on $x^2 + y^2 = 3$.

In Section 4.4 we observed that these exist only if there are relatively prime integers a, b, and c such that $a^2 + b^2 = 3c^2$. We found that such integers do not exist by a similar appeal to remainders on division by 4: a and b are not both even, so at least one of them leaves remainder 1 on division by 4, and so does its square. Hence $a^2 + b^2$ leaves remainder 1 or 2, whereas $3c^2$ leaves remainder 0 or 3.

These examples seem to be telling us that it is useful to divide the integers into finitely many "classes" according to their remainders on division by n. Certain things are impossible in the integers merely because they are impossible in a suitably chosen set of remainders, so a fruitless infinite search through the integers may be avoided by looking instead through a finite set.

Exercises

Our ordinary base 10 system of numerals is quite convenient for finding remainders on division by 2, 4, 8, ... To find the remainder of any number on division by 2, take the remainder of its last digit; to find the remainder on division by 4, take the remainder of its last two digits, treating them as a two-digit number, and so on.

6.1.1. Show that the remainder on division by 8 can be found as the remainder of the last three digits, regarded as a three-digit number.

6.1.2. Explain why the last n digits suffice to find the remainder of any number on division by 2^n.

Another problem that can be settled by looking at remainders is Exercise 4.6.5*. A related problem is the following property of sums of three squares.

6.1.3. If x, y, and z are integers, show that $x^2 + y^2 + z^2$ leaves remainder 0, 1, 2, 3, 4, 5, or 6 on division by 8.

6.1.4. Deduce from Exercise 6.1.3 that a number of the form $8n + 7$, for any integer n, is not a sum of three squares.

Thus there are infinitely many natural numbers that are not sums of three squares. However, every natural number is a sum of four squares, by a famous theorem of Lagrange (1770). A few years later, Legendre found that the natural numbers that are not sums of three squares are those of the form $4^m(8n+7)$. Sums of two squares are also interesting, and we shall say more about them in this chapter and the next. The first thing to know about them is the following, which can be proved by considering remainders on division by 4.

6.1.5. Show that an integer of the form $4n+3$ is not a sum of two squares.

6.2 Arithmetic mod n

The arithmetic of remainders on division by n was first made precise by Gauss in his famous book the *Disquisitiones Arithmeticae* of 1801. Gauss based this arithmetic on the idea of *congruence mod n*, for which he introduced the notation

$$a \equiv b \pmod{n}.$$

This expression is read "a is congruent to b modulo (or simply mod) n" and it means that a and b leave the same remainder on division by n. Putting it more concisely, $a \equiv b \pmod{n}$ means that n divides $a - b$. The natural number n is called the *modulus*.

It is sometimes convenient to use the notation $a \bmod n$ for the remainder when a is divided by n. Then the congruence $a \equiv b$ (mod n) can be written as the ordinary equation $a \bmod n = b \bmod n$.

We are already familiar with the concept of congruence when the modulus $n = 2$. It is just another way to describe the even and odd numbers. The even numbers are those congruent to 0 (mod 2), and the odd numbers are those congruent to 1 (mod 2).

Numbers that are congruent mod n are interchangeable in some remainder calculations. For example, it is valid to say things like "odd + even = odd," "odd − even = odd," and "odd × even = even" because adding, subtracting, or multiplying *any* odd number and *any* even number gives a result with the same remainder on division by 2. The situation is similar with any modulus n in place of 2: numbers that are congruent mod n are *arithmetically equivalent* in the sense that they produce the same results in sums, differences, and products.

Arithmetic equivalence mod n. *If $a_1 \equiv a_2$ (mod n) and $b_1 \equiv b_2$ (mod n), then*

$$\begin{aligned} a_1 + b_1 &\equiv a_2 + b_2 \pmod{n} \\ a_1 - b_1 &\equiv a_2 - b_2 \pmod{n} \\ a_1 b_1 &\equiv a_2 b_2 \pmod{n}. \end{aligned}$$

Proof Because $c \equiv d$ (mod n) means n divides $c - d$, the two given congruences can be translated into statements about divisibility. Manipulating them slightly and translating back gives the three required congruences quite easily, especially the first two. The first goes like this:

$$\begin{aligned} & a_1 \equiv a_2 \pmod{n} \text{ and } b_1 \equiv b_2 \pmod{n} \\ \Rightarrow\quad & n \text{ divides } a_1 - a_2 \text{ and } n \text{ divides } b_1 - b_2 \end{aligned}$$