CHAPTER 2 NUMBERS OF VARIOUS SORTS

In Chapter 1 we used the word "number" very loosely, despite our concern with the basic properties of numbers. It will now be necessary to distinguish carefully various kinds of numbers.

The simplest numbers are the "counting numbers"

$$1, 2, 3, \ldots .$$

The fundamental significance of this collection of numbers is emphasized by its symbol $\mathbf{N}$ (for **natural numbers**). A brief glance at P1–P12 will show that our basic properties of "numbers" do not apply to $\mathbf{N}$—for example, P2 and P3 do not make sense for $\mathbf{N}$. From this point of view the system $\mathbf{N}$ has many deficiencies. Nevertheless, $\mathbf{N}$ is sufficiently important to deserve several comments before we consider larger collections of numbers.

The most basic property of $\mathbf{N}$ is the principle of "mathematical induction." Suppose $P(x)$ means that the property P holds for the number x. Then the principle of mathematical induction states that $P(x)$ is true for all natural numbers x provided that

(1) $P(1)$ is true.
(2) Whenever $P(k)$ is true, $P(k+1)$ is true.

Note that condition (2) merely asserts the truth of $P(k+1)$ under the assumption that $P(k)$ is true; this suffices to ensure the truth of $P(x)$ for all x, if condition (1) also holds. In fact, if $P(1)$ is true, then it follows that $P(2)$ is true (by using (2) in the special case $k = 1$). Now, since $P(2)$ is true it follows that $P(3)$ is true (using (2) in the special case $k = 2$). It is clear that each number will eventually be reached by a series of steps of this sort, so that $P(k)$ is true for all numbers k.

A favorite illustration of the reasoning behind mathematical induction envisions an infinite line of people,

$$\text{person number } 1, \text{ person number } 2, \text{ person number } 3, \ldots .$$

If each person has been instructed to tell any secret he hears to the person behind him (the one with the next largest number) and a secret is told to person number 1, then clearly every person will eventually learn the secret. If $P(x)$ is the assertion that person number x will learn the secret, then the instructions given (to tell all secrets learned to the next person) assures that condition (2) is true, and telling the secret to person number 1 makes (1) true. The following example is a less facetious use of mathematical induction. There is a useful and striking formula which expresses the sum of the first n numbers in a simple way:

$$1 + \cdots + n = \frac{n(n+1)}{2}.$$

To prove this formula, note first that it is clearly true for $n = 1$. Now *assume* that for some natural number k we have

$$1 + \cdots + k = \frac{k(k+1)}{2}.$$

Then

$$\begin{aligned} 1 + \cdots + k + (k+1) &= \frac{k(k+1)}{2} + k + 1 \\ &= \frac{k(k+1) + 2k + 2}{2} \\ &= \frac{k^2 + 3k + 2}{2} \\ &= \frac{(k+1)(k+2)}{2}, \end{aligned}$$

so the formula is also true for $k + 1$. By the principle of induction this proves the formula for all natural numbers n. This particular example illustrates a phenomenon that frequently occurs, especially in connection with formulas like the one just proved. Although the proof by induction is often quite straightforward, the method by which the formula was discovered remains a mystery. Problems 5 and 6 indicate how some formulas of this type may be derived.

The principle of mathematical induction may be formulated in an equivalent way without speaking of "properties" of a number, a term which is sufficiently vague to be eschewed in a mathematical discussion. A more precise formulation states that if A is any collection (or "set"—a synonymous mathematical term) of natural numbers and

(1) 1 is in A,
(2) $k + 1$ is in A whenever k is in A,

then A is the set of all natural numbers. It should be clear that this formulation adequately replaces the less formal one given previously—we just consider the set A of natural numbers x which satisfy $P(x)$. For example, suppose A is the set of natural numbers n for which it is true that

$$1 + \cdots + n = \frac{n(n+1)}{2}.$$

Our previous proof of this formula showed that A contains 1, and that $k + 1$ is in A, if k is. It follows that A is the set of all natural numbers, i.e., that the formula holds for all natural numbers n.

There is yet another rigorous formulation of the principle of mathematical induction, which looks quite different. If A is any collection of natural numbers, it is tempting to say that A must have a smallest member. Actually, this statement can fail to be true in a rather subtle way. A particularly important set of natural numbers is the collection A that contains no natural numbers at all, the "empty collection" or "null set,"* denoted by $\emptyset$. The null set $\emptyset$ is a collection of natural numbers that has no smallest member—in fact, it has no members at all. This is the only possible exception, however; if A is a nonnull set of natural numbers, then A has a least member. This "intuitively obvious" statement, known as the "well-ordering principle," can be proved from the principle of induction as follows. Suppose that the set A has no least member. Let B be the set of natural numbers n such that $1, \dots, n$ are all *not* in A. Clearly 1 is in B (because if 1 were in A, then A would have 1 as smallest member). Moreover, if $1, \dots, k$ are not in A, surely $k+1$ is not in A (otherwise $k+1$ would be the smallest member of A), so $1, \dots, k+1$ are all not in A. This shows that if k is in B, then $k+1$ is in B. It follows that every number n is in B, i.e., the numbers $1, \dots, n$ are *not* in A for any natural number n. Thus $A = \emptyset$, which completes the proof.

It is also possible to prove the principle of induction from the well-ordering principle (Problem 10). Either principle may be considered as a basic assumption about the natural numbers.

There is still another form of induction which should be mentioned. It sometimes happens that in order to prove $P(k+1)$ we must assume not only $P(k)$, but also $P(l)$ for all natural numbers $l \leq k$. In this case we rely on the "principle of complete induction": If A is a set of natural numbers and

(1) 1 is in A,
(2) $k+1$ is in A if $1, \dots, k$ are in A,

then A is the set of all natural numbers.

Although the principle of complete induction may appear much stronger than the ordinary principle of induction, it is actually a consequence of that principle. The proof of this fact is left to the reader, with a hint (Problem 11). Applications will be found in Problems 7, 17, 20 and 22.

Closely related to proofs by induction are "recursive definitions." For example, the number $n!$ (read "n factorial") is defined as the product of all the natural numbers less than or equal to n:

$$n! = 1 \cdot 2 \cdot \ldots \cdot (n-1) \cdot n.$$

This can be expressed more precisely as follows:

(1) $1! = 1$
(2) $n! = n \cdot (n-1)!$.

This form of the definition exhibits the relationship between $n!$ and $(n-1)!$ in an

*Although it may not strike you as a collection, in the ordinary sense of the word, the null set arises quite naturally in many contexts. We frequently consider the set A, consisting of all x satisfying some property P; often we have no guarantee that P is satisfied by *any* number, so that A might be $\emptyset$—in fact often one proves that P is always false by showing that $A = \emptyset$.

explicit way that is ideally suited for proofs by induction. Problem 23 reviews a definition already familiar to you, which may be expressed more succinctly as a recursive definition; as this problem shows, the recursive definition is really necessary for a rigorous proof of some of the basic properties of the definition.

One definition which may not be familiar involves some convenient notation which we will constantly be using. Instead of writing

$$a_1 + \cdots + a_n,$$

we will usually employ the Greek letter Σ (capital sigma, for "sum") and write

$$\sum_{i=1}^{n} a_i.$$

In other words, $\sum_{i=1}^{n} a_i$ denotes the sum of the numbers obtained by letting $i = 1, 2, \ldots, n$. Thus

$$\sum_{i=1}^{n} i = 1 + 2 + \cdots + n = \frac{n(n+1)}{2}.$$

Notice that the letter i really has nothing to do with the number denoted by $\sum_{i=1}^{n} i$, and can be replaced by any convenient symbol (except n, of course!):

$$\sum_{j=1}^{n} j = \frac{n(n+1)}{2},$$

$$\sum_{j=1}^{i} j = \frac{i(i+1)}{2},$$

$$\sum_{n=1}^{j} n = \frac{j(j+1)}{2}.$$

To define $\sum_{i=1}^{n} a_i$ precisely really requires a recursive definition:

$$(1) \quad \sum_{i=1}^{1} a_i = a_1,$$

$$(2) \quad \sum_{i=1}^{n} a_i = \sum_{i=1}^{n-1} a_i + a_n.$$

But only purveyors of mathematical austerity would insist too strongly on such precision. In practice, all sorts of modifications of this symbolism are used, and no one ever considers it necessary to add any words of explanation. The symbol

$$\sum_{\substack{i=1 \\ i \neq 4}}^{n} a_i,$$

for example, is an obvious way of writing

$$a_1 + a_2 + a_3 + a_5 + a_6 + \cdots + a_n,$$

or more precisely,

$$\sum_{i=1}^{3} a_i + \sum_{i=5}^{n} a_i.$$

The deficiencies of the natural numbers which we discovered at the beginning of this chapter may be partially remedied by extending this system to the set of **integers**

$$\ldots, -2, -1, 0, 1, 2, \ldots.$$

This set is denoted by $\mathbf{Z}$ (from German "Zahl," number). Of properties P1–P12, only P7 fails for $\mathbf{Z}$.

A still larger system of numbers is obtained by taking quotients m/n of integers (with $n \neq 0$). These numbers are called **rational numbers**, and the set of all rational numbers is denoted by $\mathbf{Q}$ (for "quotients"). In this system of numbers all of P1–P12 are true. It is tempting to conclude that the "properties of numbers," which we studied in some detail in Chapter 1, refer to just one set of numbers, namely, $\mathbf{Q}$. There is, however, a still larger collection of numbers to which properties P1–P12 apply—the set of all **real numbers**, denoted by $\mathbf{R}$. The real numbers include not only the rational numbers, but other numbers as well (the **irrational numbers**) which can be represented by infinite decimals; π and $\sqrt{2}$ are both examples of irrational numbers. The proof that π is irrational is not easy—we shall devote all of Chapter 16 of Part III to a proof of this fact. The irrationality of $\sqrt{2}$, on the other hand, is quite simple, and was known to the Greeks. (Since the Pythagorean theorem shows that an isosceles right triangle, with sides of length 1, has a hypotenuse of length $\sqrt{2}$, it is not surprising that the Greeks should have investigated this question.) The proof depends on a few observations about the natural numbers. Every natural number n can be written either in the form $2k$ for some integer k, or else in the form $2k + 1$ for some integer k (this "obvious" fact has a simple proof by induction (Problem 8)). Those natural numbers of the form $2k$ are called **even**; those of the form $2k + 1$ are called **odd**. Note that even numbers have even squares, and odd numbers have odd squares:

$$\begin{aligned}(2k)^2 &= 4k^2 = 2 \cdot (2k^2),\\ (2k+1)^2 &= 4k^2 + 4k + 1 = 2 \cdot (2k^2 + 2k) + 1.\end{aligned}$$

In particular it follows that the converse must also hold: if n^2 is even, then n is even; if n^2 is odd, then n is odd. The proof that $\sqrt{2}$ is irrational is now quite simple. Suppose that $\sqrt{2}$ were rational; that is, suppose there were natural numbers p

and q such that

$$\left(\frac{p}{q}\right)^2 = 2.$$

We can assume that p and q have no common divisor (since all common divisors could be divided out to begin with). Now we have

$$p^2 = 2q^2.$$

This shows that p^2 is even, and consequently p must be even; that is, $p = 2k$ for some natural number k. Then

$$p^2 = 4k^2 = 2q^2,$$

so

$$2k^2 = q^2.$$

This shows that q^2 is even, and consequently that q is even. Thus both p and q are even, contradicting the fact that p and q have no common divisor. This contradiction completes the proof.

It is important to understand precisely what this proof shows. We have demonstrated that there is no rational number x such that $x^2 = 2$. This assertion is often expressed more briefly by saying that $\sqrt{2}$ is irrational. Note, however, that the use of the symbol $\sqrt{2}$ implies the existence of *some* number (necessarily irrational) whose square is 2. We have not proved that such a number exists and we can assert confidently that, at present, a proof is *impossible* for us. Any proof at this stage would have to be based on P1–P12 (the only properties of $\mathbf{R}$ we have mentioned); since P1–P12 are also true for $\mathbf{Q}$ the exact same argument would show that there is a rational number whose square is 2, and this we know is false. (Note that the reverse argument will not work—our proof that there is no rational number whose square is 2 cannot be used to show that there is no real number whose square is 2, because our proof used not only P1–P12 but also a special property of $\mathbf{Q}$, the fact that every number in $\mathbf{Q}$ can be written p/q for integers p and q.)

This particular deficiency in our list of properties of the real numbers could, of course, be corrected by adding a new property which asserts the existence of square roots of positive numbers. Resorting to such a measure is, however, neither aesthetically pleasing nor mathematically satisfactory; we would still not know that every number has an nth root if n is odd, and that every positive number has an nth root if n is even. Even if we assumed this, we could not prove the existence of a number x satisfying $x^5 + x + 1 = 0$ (even though there does happen to be one), since we do not know how to write the solution of the equation in terms of nth roots (in fact, it is known that the solution cannot be written in this form). And, of course, we certainly do not wish to assume that all equations have solutions, since this is false (no real number x satisfies $x^2 + 1 = 0$, for example). In fact, this direction of investigation is not a fruitful one. The most useful hints about the property distinguishing $\mathbf{R}$ from $\mathbf{Q}$, the most compelling evidence for the necessity of elucidating this property, do not come from the study of numbers alone. In order to study the properties of the real numbers in a more profound way, we must study more than the real numbers. At this point we must begin with the foundations of calculus, in particular the fundamental concept on which calculus is based—functions.

PROBLEMS

1. Prove the following formulas by induction.

(i) $1^2 + \cdots + n^2 = \dfrac{n(n+1)(2n+1)}{6}$.

(ii) $1^3 + \cdots + n^3 = (1 + \cdots + n)^2$.

2. Find a formula for

(i) $\displaystyle\sum_{i=1}^{n}(2i-1) = 1 + 3 + 5 + \cdots + (2n-1)$.

(ii) $\displaystyle\sum_{i=1}^{n}(2i-1)^2 = 1^2 + 3^2 + 5^2 + \cdots + (2n-1)^2$.

Hint: What do these expressions have to do with $1 + 2 + 3 + \cdots + 2n$ and $1^2 + 2^2 + 3^2 + \cdots + (2n)^2$?

3. If $0 \le k \le n$, the "binomial coefficient" $\dbinom{n}{k}$ is defined by

$$\binom{n}{k} = \frac{n!}{k!(n-k)!} = \frac{n(n-1)\cdots(n-k+1)}{k!}, \quad \text{if } k \neq 0, n$$

$$\binom{n}{0} = \binom{n}{n} = 1 \text{ (a special case of the first formula if we define } 0! = 1\text{)},$$

and for $k < 0$ or $k > n$ we just define the binomial coefficient to be 0.

(a) Prove that

$$\binom{n+1}{k} = \binom{n}{k-1} + \binom{n}{k}.$$

(The proof does not require an induction argument.)

This relation gives rise to the following configuration, known as "Pascal's triangle"—a number not on one of the sides is the sum of the two numbers above it; the binomial coefficient $\dbinom{n}{k}$ is the $(k+1)$st number in the $(n+1)$st row.

$$\begin{array}{ccccccccccc}
 & & & & & 1 & & & & & \\
 & & & & 1 & & 1 & & & & \\
 & & & 1 & & 2 & & 1 & & & \\
 & & 1 & & 3 & & 3 & & 1 & & \\
 & 1 & & 4 & & 6 & & 4 & & 1 & \\
1 & & 5 & & 10 & & 10 & & 5 & & 1
\end{array}$$

(b) Notice that all the numbers in Pascal's triangle are natural numbers. Use part (a) to prove by induction that $\binom{n}{k}$ is always a natural number. (Your entire proof by induction will, in a sense, be summed up in a glance by Pascal's triangle.)

(c) Give another proof that $\binom{n}{k}$ is a natural number by showing that $\binom{n}{k}$ is the number of sets of exactly k integers each chosen from $1, \dots, n$.

(d) Prove the "binomial theorem": If a and b are any numbers and n is a natural number, then

$$\begin{aligned}(a+b)^n &= a^n + \binom{n}{1}a^{n-1}b + \binom{n}{2}a^{n-2}b^2 + \cdots + \binom{n}{n-1}ab^{n-1} + b^n \\ &= \sum_{j=0}^{n}\binom{n}{j}a^{n-j}b^j.\end{aligned}$$

(e) Prove that

(i) $$\sum_{j=0}^{n}\binom{n}{j} = \binom{n}{0} + \cdots + \binom{n}{n} = 2^n.$$

(ii) $$\sum_{j=0}^{n}(-1)^j\binom{n}{j} = \binom{n}{0} - \binom{n}{1} + \cdots \pm \binom{n}{n} = 0.$$

(iii) $$\sum_{l \text{ odd}}\binom{n}{l} = \binom{n}{1} + \binom{n}{3} + \cdots = 2^{n-1}.$$

(iv) $$\sum_{l \text{ even}}\binom{n}{l} = \binom{n}{0} + \binom{n}{2} + \cdots = 2^{n-1}.$$

4. (a) Prove that

$$\sum_{k=0}^{l}\binom{n}{k}\binom{m}{l-k} = \binom{n+m}{l}.$$

Hint: Apply the binomial theorem to $(1+x)^n(1+x)^m$.

(b) Prove that

$$\sum_{k=0}^{n}\binom{n}{k}^2 = \binom{2n}{n}.$$

5. (a) Prove by induction on n that

$$1 + r + r^2 + \cdots + r^n = \frac{1 - r^{n+1}}{1 - r}$$

if $r \neq 1$ (if $r = 1$, evaluating the sum certainly presents no problem).

(b) Derive this result by setting $S = 1 + r + \cdots + r^n$, multiplying this equation by r, and solving the two equations for S.

6. The formula for $1^2 + \cdots + n^2$ may be derived as follows. We begin with the formula

$$(k + 1)^3 - k^3 = 3k^2 + 3k + 1.$$

Writing this formula for $k = 1, \ldots, n$ and adding, we obtain

$$\begin{aligned}
2^3 - 1^3 &= 3 \cdot 1^2 + 3 \cdot 1 + 1 \\
3^3 - 2^3 &= 3 \cdot 2^2 + 3 \cdot 2 + 1 \\
&\ \vdots \\
(n + 1)^3 - n^3 &= 3 \cdot n^2 + 3 \cdot n + 1 \\
\hline
(n + 1)^3 - 1 &= 3[1^2 + \cdots + n^2] + 3[1 + \cdots + n] + n.
\end{aligned}$$

Thus we can find $\sum_{k=1}^{n} k^2$ if we already know $\sum_{k=1}^{n} k$ (which could have been found in a similar way). Use this method to find

(i) $1^3 + \cdots + n^3$.

(ii) $1^4 + \cdots + n^4$.

(iii) $\dfrac{1}{1 \cdot 2} + \dfrac{1}{2 \cdot 3} + \cdots + \dfrac{1}{n(n + 1)}$.

(iv) $\dfrac{3}{1^2 \cdot 2^2} + \dfrac{5}{2^2 \cdot 3^2} + \cdots + \dfrac{2n + 1}{n^2(n + 1)^2}$.

***7.** Use the method of Problem 6 to show that $\sum_{i=1}^{n} k^p$ can always be written in the form

$$\frac{n^{p+1}}{p + 1} + An^p + Bn^{p-1} + Cn^{p-2} + \cdots.$$

(The first 10 such expressions are

$$\begin{aligned}
\sum_{k=1}^{n} k &= \tfrac{1}{2}n^2 + \tfrac{1}{2}n \\
\sum_{k=1}^{n} k^2 &= \tfrac{1}{3}n^3 + \tfrac{1}{2}n^2 + \tfrac{1}{6}n \\
\sum_{k=1}^{n} k^3 &= \tfrac{1}{4}n^4 + \tfrac{1}{2}n^3 + \tfrac{1}{4}n^2 \\
\sum_{k=1}^{n} k^4 &= \tfrac{1}{5}n^5 + \tfrac{1}{2}n^4 + \tfrac{1}{3}n^3 - \tfrac{1}{30}n \\
\sum_{k=1}^{n} k^5 &= \tfrac{1}{6}n^6 + \tfrac{1}{2}n^5 + \tfrac{5}{12}n^4 - \tfrac{1}{12}n^2 \\
\sum_{k=1}^{n} k^6 &= \tfrac{1}{7}n^7 + \tfrac{1}{2}n^6 + \tfrac{1}{2}n^5 - \tfrac{1}{6}n^3 + \tfrac{1}{42}n \\
\sum_{k=1}^{n} k^7 &= \tfrac{1}{8}n^8 + \tfrac{1}{2}n^7 + \tfrac{7}{12}n^6 - \tfrac{7}{24}n^4 + \tfrac{1}{12}n^2 \\
\sum_{k=1}^{n} k^8 &= \tfrac{1}{9}n^9 + \tfrac{1}{2}n^8 + \tfrac{2}{3}n^7 - \tfrac{7}{15}n^5 + \tfrac{2}{9}n^3 - \tfrac{1}{30}n \\
\sum_{k=1}^{n} k^9 &= \tfrac{1}{10}n^{10} + \tfrac{1}{2}n^9 + \tfrac{3}{4}n^8 - \tfrac{7}{10}n^6 + \tfrac{1}{2}n^4 - \tfrac{3}{20}n^2 \\
\sum_{k=1}^{n} k^{10} &= \tfrac{1}{11}n^{11} + \tfrac{1}{2}n^{10} + \tfrac{5}{6}n^9 - 1n^7 + 1n^5 - \tfrac{1}{2}n^3 + \tfrac{5}{66}n.
\end{aligned}$$

Notice that the coefficients in the second column are always $\frac{1}{2}$, and that after the third column the powers of n with nonzero coefficients decrease by 2 until n^2 or n is reached. The coefficients in all but the first two columns seem to be rather haphazard, but there actually is some sort of pattern; finding it may be regarded as a super-perspicacity test. See Problem 27-17 for the complete story.)

8. Prove that every natural number is either even or odd.

9. Prove that if a set A of natural numbers contains n_0 and contains $k+1$ whenever it contains k, then A contains all natural numbers $\geq n_0$.

10. Prove the principle of mathematical induction from the well-ordering principle.

11. Prove the principle of complete induction from the ordinary principle of induction. Hint: If A contains 1 and A contains $n+1$ whenever it contains $1, \dots, n$, consider the set B of all k such that $1, \dots, k$ are all in A.

12. (a) If a is rational and b is irrational, is $a+b$ necessarily irrational? What if a and b are both irrational?

(b) If a is rational and b is irrational, is ab necessarily irrational? (Careful!)
(c) Is there a number a such that a^2 is irrational, but a^4 is rational?
(d) Are there two irrational numbers whose sum and product are both rational?

13. (a) Prove that $\sqrt{3}$, $\sqrt{5}$, and $\sqrt{6}$ are irrational. Hint: To treat $\sqrt{3}$, for example, use the fact that every integer is of the form $3n$ or $3n+1$ or $3n+2$. Why doesn't this proof work for $\sqrt{4}$?
(b) Prove that $\sqrt[3]{2}$ and $\sqrt[3]{3}$ are irrational.

14. Prove that

(a) $\sqrt{2}+\sqrt{6}$ is irrational.
(b) $\sqrt{2}+\sqrt{3}$ is irrational.

15. (a) Prove that if $x = p+\sqrt{q}$ where p and q are rational, and m is a natural number, then $x^m = a + b\sqrt{q}$ for some rational a and b.
(b) Prove also that $(p-\sqrt{q}\,)^m = a - b\sqrt{q}$.

16. (a) Prove that if m and n are natural numbers and $m^2/n^2 < 2$, then $(m+2n)^2/(m+n)^2 > 2$; show, moreover, that

$$\frac{(m+2n)^2}{(m+n)^2} - 2 < 2 - \frac{m^2}{n^2}.$$

(b) Prove the same results with all inequality signs reversed.
(c) Prove that if $m/n < \sqrt{2}$, then there is another rational number m'/n' with $m/n < m'/n' < \sqrt{2}$.

***17.** It seems likely that $\sqrt{n}$ is irrational whenever the natural number n is not the square of another natural number. Although the method of Problem 13 may actually be used to treat any particular case, it is not clear in advance that it will always work, and a proof for the general case requires some extra information. A natural number p is called a **prime number** if it is impossible to write $p = ab$ for natural numbers a and b unless one of these is p, and the other 1; for convenience we also agree that 1 is *not* a prime number. The first few prime numbers are 2, 3, 5, 7, 11, 13, 17, 19. If $n > 1$ is not a prime, then $n = ab$, with a and b both $< n$; if either a or b is not a prime it can be factored similarly; continuing in this way proves that we can write n as a product of primes. For example, $28 = 4 \cdot 7 = 2 \cdot 2 \cdot 7$.

(a) Turn this argument into a rigorous proof by complete induction. (To be sure, any reasonable mathematician would accept the informal argument, but this is partly because it would be obvious to her how to state it rigorously.)

A fundamental theorem about integers, which we will not prove here, states that this factorization is unique, except for the order of the factors. Thus, for example, 28 can never be written as a product of primes one of which is 3, nor can it be written in a way that involves 2 only once (now you should appreciate why 1 is not allowed as a prime).

(b) Using this fact, prove that $\sqrt{n}$ is irrational unless $n = m^2$ for some natural number m.

(c) Prove more generally that $\sqrt[k]{n}$ is irrational unless $n = m^k$.

(d) No discussion of prime numbers should fail to allude to Euclid's beautiful proof that there are infinitely many of them. Prove that there cannot be only finitely many prime numbers $p_1, p_2, p_3, \dots, p_n$ by considering $p_1 \cdot p_2 \cdot \dots \cdot p_n + 1$.

***18.** (a) Prove that if x satisfies

$$x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0,$$

for some integers $a_{n-1}, \dots, a_0$, then x is irrational unless x is an integer. (Why is this a generalization of Problem 17?)

(b) Prove that $\sqrt{6} - \sqrt{2} - \sqrt{3}$ is irrational.

(c) Prove that $\sqrt{2} + \sqrt[3]{2}$ is irrational. Hint: Start by working out the first 6 powers of this number.

19. Prove Bernoulli's inequality: If $h > -1$, then

$$(1+h)^n \geq 1 + nh$$

for any natural number n. Why is this trivial if $h > 0$?

20. The Fibonacci sequence $a_1, a_2, a_3, \dots$ is defined as follows:

$$\begin{aligned} a_1 &= 1, \\ a_2 &= 1, \\ a_n &= a_{n-1} + a_{n-2} \qquad \text{for } n \geq 3. \end{aligned}$$

This sequence, which begins $1, 1, 2, 3, 5, 8, \dots$, was discovered by Fibonacci (circa 1175–1250), in connection with a problem about rabbits. Fibonacci assumed that an initial pair of rabbits gave birth to one new pair of rabbits per month, and that after two months each new pair behaved similarly. The number a_n of pairs born in the nth month is $a_{n-1} + a_{n-2}$, because a pair of rabbits is born for each pair born the previous month, and moreover each pair born two months ago now gives birth to another pair. The number of interesting results about this sequence is truly amazing—there is even a Fibonacci Association which publishes a journal, *The Fibonacci Quarterly*. Prove that

$$a_n = \frac{\left(\dfrac{1+\sqrt{5}}{2}\right)^n - \left(\dfrac{1-\sqrt{5}}{2}\right)^n}{\sqrt{5}}.$$

One way of deriving this astonishing formula is presented in Problem 24-16.

21. The Schwarz inequality (Problem 1-19) actually has a more general form:

$$\sum_{i=1}^{n} x_i y_i \le \sqrt{\sum_{i=1}^{n} x_i{}^2}\sqrt{\sum_{i=1}^{n} y_i{}^2}.$$

Give three proofs of this, analogous to the three proofs in Problem 1-19.

22. The result in Problem 1-7 has an important generalization: If $a_1, \dots, a_n \ge 0$, then the "arithmetic mean"

$$A_n = \frac{a_1 + \cdots + a_n}{n}$$

and "geometric mean"

$$G_n = \sqrt[n]{a_1 \dots a_n}$$

satisfy

$$G_n \le A_n.$$

(a) Suppose that $a_1 < A_n$. Then some a_i satisfies $a_i > A_n$; for convenience, say $a_2 > A_n$. Let $\bar{a}_1 = A_n$ and let $\bar{a}_2 = a_1 + a_2 - \bar{a}_1$. Show that

$$\bar{a}_1 \bar{a}_2 \ge a_1 a_2.$$

Why does repeating this process enough times eventually prove that $G_n \le A_n$? (This is another place where it is a good exercise to provide a formal proof by induction, as well as an informal reason.) When does equality hold in the formula $G_n \le A_n$?

The reasoning in this proof is related to another interesting proof.

(b) Using the fact that $G_n \le A_n$ when $n = 2$, prove, by induction on k, that $G_n \le A_n$ for $n = 2^k$.

(c) For a general n, let $2^m > n$. Apply part (b) to the 2^m numbers

$$a_1, \dots, a_n, \underbrace{A_n, \dots, A_n}_{2^m - n \text{ times}}$$

to prove that $G_n \le A_n$.

23. The following is a recursive definition of a^n:

$$\begin{aligned} a^1 &= a, \\ a^{n+1} &= a^n \cdot a. \end{aligned}$$

Prove, by induction, that

$$\begin{aligned} a^{n+m} &= a^n \cdot a^m, \\ (a^n)^m &= a^{nm}. \end{aligned}$$

(Don't try to be fancy: use either induction on n or induction on m, not both at once.)

24. Suppose we know properties P1 and P4 for the natural numbers, but that multiplication has never been mentioned. Then the following can be used as a recursive definition of multiplication:

$$1 \cdot b = b,$$
$$(a+1) \cdot b = a \cdot b + b.$$

Prove the following (in the order suggested!):

$a \cdot (b + c) = a \cdot b + a \cdot c$ (use induction on a),
$a \cdot 1 = a$,
$a \cdot b = b \cdot a$ (you just finished proving the case $b = 1$).

25. In this chapter we began with the natural numbers and gradually built up to the real numbers. A completely rigorous discussion of this process requires a little book in itself (see Part V). No one has ever figured out how to get to the real numbers without going through this process, but if we do accept the real numbers as given, then the natural numbers can be *defined* as the real numbers of the form 1, $1+1$, $1+1+1$, etc. The whole point of this problem is to show that there is a rigorous mathematical way of saying "etc."

(a) A set A of real numbers is called **inductive** if

(1) 1 is in A,
(2) $k+1$ is in A whenever k is in A.

Prove that

(i) **R** is inductive.
(ii) The set of positive real numbers is inductive.
(iii) The set of positive real numbers unequal to $\frac{1}{2}$ is inductive.
(iv) The set of positive real numbers unequal to 5 is not inductive.
(v) If A and B are inductive, then the set C of real numbers which are in both A and B is also inductive.

(b) A real number n will be called a **natural number** if n is in *every* inductive set.

(i) Prove that 1 is a natural number.
(ii) Prove that $k+1$ is a natural number if k is a natural number.

26. There is a puzzle consisting of three spindles, with n concentric rings of decreasing diameter stacked on the first (Figure 1). A ring at the top of a stack may be moved from one spindle to another spindle, provided that it is not placed on top of a smaller ring. For example, if the smallest ring is moved to spindle 2 and the next-smallest ring is moved to spindle 3, then the smallest ring may be moved to spindle 3 also, on top of the next-smallest. Prove that the entire stack of n rings can be moved onto spindle 3 in $2^n - 1$ moves, and that this cannot be done in fewer than $2^n - 1$ moves.

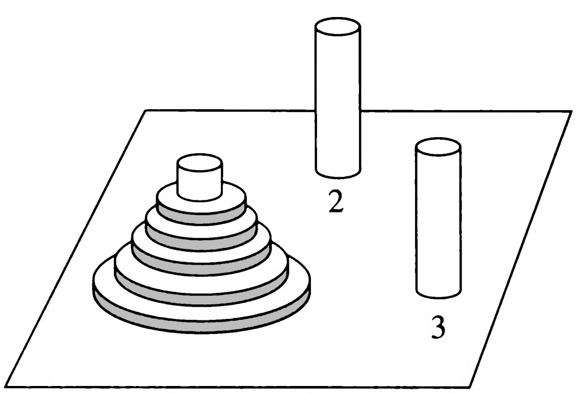

FIGURE 1

***27.** University B. once boasted 17 tenured professors of mathematics. Tradition prescribed that at their weekly luncheon meeting, faithfully attended by all 17, any members who had discovered an error in their published work should make an announcement of this fact, and promptly resign. Such an announcement had never actually been made, because no professor was aware of any errors in her or his work. This is not to say that no errors existed, however. In fact, over the years, in the work of every member of the department at least one error had been found, by some other member of the department. This error had been mentioned to all other members of the department, but the actual author of the error had been kept ignorant of the fact, to forestall any resignations.

One fateful year, the department was augmented by a visitor from another university, one Prof. X, who had come with hopes of being offered a permanent position at the end of the academic year. Naturally, he was apprised, by various members of the department, of the published errors which had been discovered. When the hoped-for appointment failed to materialize, Prof. X obtained his revenge at the last luncheon of the year. "I have enjoyed my visit here very much," he said, "but I feel that there is one thing that I have to tell you. At least one of you has published an incorrect result, which has been discovered by others in the department." What happened the next year?

****28.** After figuring out, or looking up, the answer to Problem 27, consider the following: Each member of the department already knew what Prof. X asserted, so how could his saying it change anything?

PART 2
FOUNDATIONS

The statement is so frequently made
that the differential calculus deals with
continuous magnitude, and yet
an explanation of this continuity is
nowhere given;
even the most rigorous expositions
of the differential calculus do not base
their proofs upon continuity but,
with more or less consciousness of the fact,
they either appeal to geometric notions
or those suggested by geometry,
or depend upon theorems which are never
established in a purely arithmetic manner.
Among these, for example,
belongs the above-mentioned theorem,
and a more careful investigation
convinced me that this theorem, or
any one equivalent to it, can be regarded
in some way as a sufficient basis
for infinitesimal analysis.
It then only remained to discover its true
origin in the elements of arithmetic
and thus at the same time
to secure a real definition of
the essence of continuity.
I succeeded Nov. 24, 1858, and
a few days afterward I communicated
the results
of my meditations to my dear friend
Durège with whom I had a long
and lively discussion.

RICHARD DEDEKIND