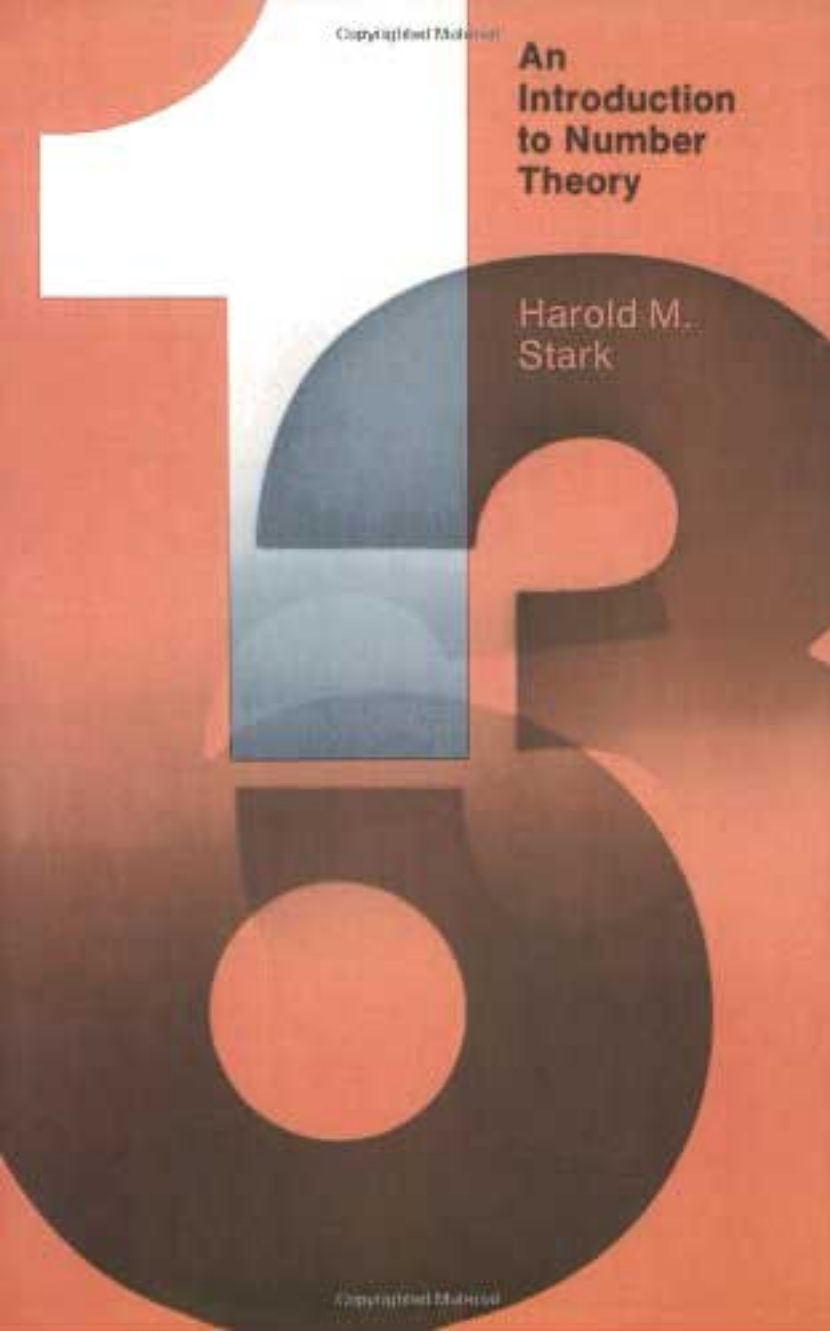
An Introduction to Number Theory

Harold M. Stark



An Introduction to Number Theory

Harold M. Stark

The MIT Press
Cambridge, Massachusetts, and London, England

Tenth printing, 1998

First MIT Press paperback edition, 1987

Original edition published by Markham Publishing Company, 1970

Printed and bound in the United States of America by Edwards Brothers.

Library of Congress Cataloging in Publication Data

Stark, Harold M 1939–
An introduction to number theory.

Originally published by Markham Pub. Co., Chicago.
Bibliography: p.
Includes index.
1. Numbers, Theory of. I. Title.
QA241.S72 1978 512'.7 78-2744
ISBN 0–262–69060–8

Contents

Chapter 1

AN INTRODUCTION TO NUMBER THEORY

1.1. An Introduction to Number Theory

The theory of numbers is concerned with properties of numbers, particularly properties of the integers, $0, \pm 1, \pm 2, \pm 3, \ldots$. It may be asked: What properties can numbers have? After all, they may be added, subtracted, multiplied, and divided; what else is there? It is the purpose of this section to illustrate some of the answers to this question. Many of the results indicated here will be proved in later chapters, but proofs of some are too advanced and cannot be included here.

One main subdivision of elementary number theory deals with multiplicative properties of integers. Fundamental to questions in this area is the notion of divisibility.

Definition. If a and b are integers, $a \neq 0$, and if there is an integer c such that $b = ac$, then we say that a **divides** b, and we write $a|b$. If a does not divide b, then we write $a \nmid b$.

Thus, although $\frac{7}{5} = 1.4$, the quotient is not an integer and thus $5 \nmid 7$. Other examples are

$$2|18, \quad 1|42, \quad 3|(-6), \quad -7|49, \quad 9 \nmid 80, \quad -6 \nmid 31.$$

Certain positive integers, such as 1, 2, 3, 13, and 10 006 721,[1] have the property that the only positive integers that divide them are themselves and 1. These numbers were called the prime numbers by the ancients, but more and more it has become advantageous to exclude 1 from this list, and thus the modern definition of a prime number is

[1] The usual commas that separate thousands and millions are too confusing. It is customary not to use them.

Definition. An integer greater than one whose only positive divisors are itself and one is called a **prime number**. An integer greater than one which is not a prime number is said to be **composite**.

All sorts of questions immediately spring to mind. How many primes are there? The answer is infinitely many. This means that there is no last prime. Or, alternatively, it can be thought of as meaning that there are more than 1 million primes, more than 1 billion primes, more than 1 trillion primes, in fact, more primes than any number that you care to name. This fact was known by Euclid over 2000 years ago, and his proof will be given shortly. What is the nth prime? For any given n, this question can always be answered in a finite amount of time. For example, the 664 999th prime is 10 006 721.[2] But in the sense of giving a formula which yields the nth prime for all n, this has never been done. Is there a formula which at least gives only primes? No one has ever found one. Centuries ago, it was believed that if n is an integer, then

$$n^2 + n + 41$$

is always a prime number. It is for $n = 0, 1, 2, 3, \ldots, 39$, but it fails to be for $n = 40$ and it fails obviously for $n = 41$ (there is a factor of 41 in both cases). We will see in Chapter 3 that no polynomial can give only primes. Fermat (1601–1665) conjectured that the numbers

$$F_n = 2^{2^n} + 1$$

are primes for all integers $n \geq 0$. He checked this for $n = 0, 1, 2, 3, 4$ and found that the corresponding F_n's, 3, 5, 17, 257, and 65 537, are indeed primes. Since

$$F_5 = 4\,294\,967\,297,$$

Fermat did not attempt to verify his conjecture any further. Fermat undoubtedly had good reasons for believing his conjecture, nevertheless, he was wrong. Euler (1707–1783) found in 1732 that $641 | F_5$ and hence F_5 is composite. Since then it has been discovered that several additional F_n's are composite. In fact, no F_n with $n > 4$ has yet been proved to be a prime.

How many primes are there less than a given integer n? Legendre (1752–

[2] I fear that this was done the hard way. All the primes from 2 to 10 006 721 were listed by D. N. Lehmer in 1914—before the days of computers (see the bibliography at the end of the book). There were 664 999 of them. Why did he stop here rather than at the next prime? Lehmer defined 1 to be a prime also, and thus, in his terminology, he stopped at the 665 000th prime. His goal was to list all primes from 1 to 10 000 000; at 5000 primes per page, he reached the last prime under 10 000 000 on page 133 and then simply completed the page.

1833) and, after him, Gauss (1777–1855) conjectured that the answer is approximately

$$\frac{n}{1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n}}.$$

The fact that the ratio of this number to the number of primes less than n gets nearer and nearer 1 as n gets larger is known as the **prime number theorem**. It was first proved in 1896 by Hadamard (1865–1963) and de la Vallée Poussin (1866–1962), and even today its proof is far from simple.

How can we tell whether or not a given integer is a prime? There is no general method, although it is sometimes possible to find a small factor of the given number by trial and error and hence show that it is composite. For example, is

$$32\,589\,158\,477\,190\,044\,731$$

a prime number? How would you tell? There are some general methods for answering this question theoretically, but they are completely unsuited for practical computations. For example, we will show in Chapter 3 that a number n is a prime if and only if

$$n \mid [(n-1)! + 1].$$

For example, $5 \mid (4! + 1)$ and hence is a prime, while $6 \nmid (5! + 1)$ and hence is not a prime. This is an interesting property of primes, but it is totally useless for verifying that the 20-digit number above is or is not a prime.

Another main category in number theory is given by additive questions. The most familiar question of this type to the reader is the problem of writing a perfect square as the sum of two perfect squares. Because of the Pythagorean theorem, this problem is equivalent to the problem of finding right triangles with integral sides. The reader has probably seen the 3,4,5 and 5,12,13 right triangles. With the exception of these triangles and triangles similar to them [such as twice the 3,4,5 triangle (6,8,10) or five times the 5,12,13 triangle (25,60,65)], the reader may not have seen others. But there are others. Both the 3,4,5 triangle and the 5,12,13 triangles have the hypotenuse being one unit longer than one of the sides. If the sides are a and b and the hypotenuse is $b + 1$, then by the Pythagorean theorem

$$a^2 + b^2 = (b+1)^2$$

or

$$a^2 = (b + 1)^2 - b^2 \tag{1}$$
$$= b^2 + 2b + 1 - b^2$$
$$= 2b + 1.$$

Since $2b + 1$ is an odd number, that is, since $2 \nmid (2b + 1)$ (since $b + \frac{1}{2}$ is not an integer), we see that a^2 is an odd number and so we put

$$a = 2n + 1. \tag{2}$$

Then we see from (1) that

$$b = \frac{a^2 - 1}{2} \tag{3}$$
$$= \frac{(2n + 1)^2 - 1}{2}$$
$$= \frac{4n^2 + 4n + 1 - 1}{2}$$
$$= 2n^2 + 2n.$$

In equations (2) and (3), we have a and b in terms of n. Thus, we expect that

$$(2n + 1), \quad (2n^2 + 2n), \quad (2n^2 + 2n + 1)$$

is a Pythagorean triplet; that is, $2n + 1$ and $2n^2 + 2n$ are the sides of a right triangle and $2n^2 + 2n + 1$ is the hypotenuse. This may be easily checked by merely verifying that

$$(2n + 1)^2 + (2n^2 + 2n)^2 = (2n^2 + 2n + 1)^2$$

for all n. When $n = 1$ and $n = 2$, we get the 3,4,5 triangles and the 5,12,13 triangles. When $n = 3$, $n = 4$, and $n = 5$, we get the triangles

$$7,24,25; \quad 9,40,41; \quad 11,60,61.$$

We may continue plugging in different values of n as long as we desire. As the 8,15,17 triangle shows, this method does not give all right triangles with integral sides, but it does go far beyond the old standards 3,4,5 and 5,12,13. The problem of finding all right triangles with integral sides boils down to finding all solutions to the equation

$$x^2 + y^2 = z^2$$

in positive integers. Such an equation is called a **Diophantine equation** in honor of the Greek mathematician Diophantus (4th century A.D.?), who

first investigated the problem of finding integral solutions to equations, particularly the cases with more unknowns than equations. In Chapter 5 we will study some of the simpler methods of solving such equations, but we will also run into them in other chapters.

Fermat generalized the Pythagorean equation by looking at the equation

$$x^n + y^n = z^n, \tag{4}$$

where n is an integer greater than or equal to 3. In the margin of his copy of the works of Diophantus, Fermat stated that he had a truly wondrous proof of the fact that, unlike the case of $n = 2$, when $n \geq 3$, equation (4) has no solutions where x, y, and z are all nonzero integers. Unfortunately, Fermat continued, the margin was not big enough to hold the proof. This result has come to be known as **Fermat's last theorem**, or **Fermat's great theorem** (as opposed to Fermat's lesser theorem, which we find in Chapter 3). It is unfortunate that Fermat left no hints as to his method of proof because no one has been able to prove his theorem since! In fact, it is one of the two or three most famous unsolved mathematical problems today.[3] The question naturally arises: Did Fermat really have a proof of his theorem? There are those who argue that Fermat did have a proof of his theorem and note that the wisdom of the ancients far exceeded that of the mere mortal man of today. Then there are the more cynical who believe that Fermat must have made one of the mistakes that many after him have made. This question is as much fun to argue as any philosophic or theologic question, and, like them, there are no facts to contradict one's arguments.

As another example of an additive question, we have Goldbach's conjecture made in 1742 that every even integer greater than 2 is the sum of two primes. For example,

$$4 = 2 + 2, \quad 6 = 3 + 3, \quad 8 = 5 + 3, \quad 20 = 13 + 7, \quad 100 = 83 + 17.$$

This conjecture has been verified by Pipping for all even numbers less than 100 000, but no one has been able to prove it.

In this book, we will prove many seemingly obvious theorems. Perhaps a word is in order on why we bother. There are two reasons why something is obvious: First, it may sound very reasonable and, second, it may have been

[3] Before the reader attempts to solve this problem, he should finish reading the book. If he still insists on solving the problem after that, I request that he not send his solution to me, as I am not qualified to judge the correctness of so difficult a work. The reader should be warned that thousands of people have submitted solutions to this problem and none has been anywhere near correct. An announcement by an amateur that he has solved the problem is greeted with the same skepticism as an announcement by a sailor that he has seen a sea serpent.

verified so often by personal experience that it no longer seems questionable (it is hard to doubt something that has worked a million times in a row). How obvious should something be before we accept it as true? A few examples may help answer this question.

Let us investigate the conjecture that any odd number which is not divisible by either 3 or 5 is a prime. The odd numbers less than 20 which are not divisible by 3 or 5 are 7, 11, 13, 17, and 19, all primes. The odd numbers between 20 and 40 not divisible by 3 or 5 are 23, 29, 31, and 37, also all primes. Perhaps we should believe the conjecture and try to prove it. But wait! In the next set of 20, we get the numbers 41, 43, 47, 49, 53, and 59, and $49 = 7 \cdot 7$ is not a prime. Thus the conjecture is false and having seen a counterexample, it is easy to construct others. The remaining counterexamples less than 100 are $77 = 7 \cdot 11$ and $91 = 7 \cdot 13$. Perhaps, then, we should not accept something as true until it has been verified past 100.

Twenty-five centuries ago, the Chinese gave what they believed was an infallible rule for determining primality. Their rule stated that n is a prime if and only if

$$n|(2^n - 2).$$

For example, $2^7 - 2 = 126 = 7 \cdot 18$ and 7 is a prime, while $2^{10} - 2 = 1022$, which is not divisible by the composite number 10. It is doubtful that the Chinese had any reason to believe their rule other than the fact that it seemed to work. Owing to the complexity of the number $2^n - 2$ when n is large, it is hard to believe that the Chinese verified their rule for very many n. And yet the Chinese rule was believed to be true for more than 23 centuries, and it has been verified for all n up to 300. Further, Fermat showed that the Chinese were correct when n is a prime. But in spite of all this, the Chinese were wrong. It can be shown that their rule fails for $n = 341 = 11 \cdot 31$. I would not advise checking this statement, since $2^{341} - 2$ has 103 digits. Besides, results of Fermat, Euler, and Gauss, presented in Chapter 3, will make it trivial that

$$341|(2^{341} - 2).$$

Let us examine another conjecture. By the number of prime factors of an integer n, we mean the number of factors (whether distinct from each other or not) when n is written as a product of primes. For example, $12 = 2 \cdot 2 \cdot 3$ has three prime factors by this definition, and $16 = 2 \cdot 2 \cdot 2 \cdot 2$ has four. We shall say that 1 has zero prime factors and that a prime has one. Let O_n be the number of positive integers less than or equal to n which have an odd number of prime factors and let E_n be the number of positive integers less than or equal to n which have an even number of prime factors. For example, $O_{12} = 7$ (the numbers being 2, 3, 5, 7, 8, 11, and 12) and $E_{12} = 5$ (the numbers

being 1, 4, 6, 9, and 10). A product of two primes is clearly greater than either of its prime factors. A product of four primes has smaller divisors which are products of three primes, and so on. Thus, in some sense, the numbers which are products of an odd number of primes come earlier in the sequence of positive integers than the numbers which are products of an even number of primes. This leads us to suspect that there are at least as many numbers less than n with an odd number of prime factors as there are numbers with an even number of prime factors. In other words, we have the conjecture that

$$O_n \geq E_n.$$

This is known as the *Polya conjecture*, after G. Polya (1887–), who in 1919 conjectured that if $n \geq 2$, then $O_n \geq E_n$ ($O_1 = 0$ and $E_1 = 1$, but after this, we come to the primes before we come to the product of two primes). The Polya conjecture sounds reasonable without even experimentally verifying it. But since the Polya conjecture had many important consequences in advanced number theory, it was checked experimentally and it was found to be true for the first million positive integers. Is it any wonder, then, that the majority of mathematicians were confident that the Polya conjecture would eventually be proved? But they were wrong. In 1958, Haselgrove showed that there are infinitely many n for which

$$O_n < E_n.$$

The smallest known counterexample to Polya's conjecture was found by R. S. Lehman in 1962, and it is

$$n = 906\,180\,359,$$

at which

$$O_n = E_n - 1.$$

Perhaps the word "obvious" is beginning to lose its meaning, but to make sure, we give one last example. We see that $x = 1, y = 0$ satisfies the Diophantine equation

$$x^2 - 1141y^2 = 1. \tag{5}$$

We might ask, does equation (5) have any solution in positive integers? We see from (5) that

$$x = \sqrt{1141y^2 + 1}.$$

Thus the question is: Is $1141y^2 + 1$ ever a perfect square? This may be checked experimentally. It turns out that the answer is no for all positive y less than 1 million. In view of the previous example, perhaps we should experiment further. The answer is still no for all y less than 1 trillion (1 million

million, or 10^{12}). We go overboard and check all y up to 1 trillion trillion (10^{24}). Again the answer is, no. No one in his right mind would really believe that there could be a positive y such that $\sqrt{1141y^2 + 1}$ is an integer if there is no such y less than 1 trillion trillion. But there is. In fact, there are infinitely many of them, the smallest among them having 26 digits. If you still do not believe this, we will prove in Chapter 7 that there are infinitely many such y and give a method whereby you may start from scratch and find the smallest positive value of y in less than an hour (with a desk calculator).

In later chapters, we will discuss two widely believed conjectures of Euler, both of which have been shown to be false within the last ten years. Thus it is that the mathematician refuses to accept a statement as true, no matter how plausible it is, until it is proved. In this vein, it is interesting to note that we have used an obvious result in two of the examples above. How do we know that every factorization of n into primes has the same number of prime factors? How do we know that if two primes greater than 5 are multiplied, the result will not be divisible by 3 or 5? Maybe it has never occurred to you to ask these questions, but the chances are that your beliefs are based on experience with rather small numbers. In view of the previous examples, we will prove these rather obvious statements in Chapter 2 as part of a general theorem on factorization. In Chapter 8, we will reexamine these "obvious" concepts from a more advanced standpoint.

There are other questions that may be asked about numbers that are neither multiplicative nor additive in character. For example, consider the number $\pi = 3.14159\ldots$. Pause at this point and think of a fraction which you associate with π. I suspect that you have thought of the number twenty-two sevenths. Assuming this to be true, let us ask why you associate this particular fraction with π. The first answer is that you were taught it in school. But why did your teachers pick $\frac{22}{7}$? Presumably, the answer is that $\frac{22}{7}$ is close to π and it is easier to work with $\frac{22}{7}$ than $3.14159\ldots$. But why sevenths? If it is ease of operation that we desire, $\frac{31}{10}$ is close to π and by far easier to use. Were your teachers being sadistic in making you always divide by 7 rather than by 10, or is $\frac{22}{7}$ somehow a better representative of π than $\frac{31}{10}$? The answer is that $\frac{22}{7}$ is a far better approximation to π than $\frac{31}{10}$. In fact, in a sense to be explained in Chapter 7, $\frac{22}{7}$ is one of the best approximations to π by fractions.

How close can we expect a fraction with denominator q to come to a given real number α? We can partially answer this question here. We consider all the fractions with denominator q:

$$\ldots, \frac{-5}{q}, \frac{-4}{q}, \frac{-3}{q}, \frac{-2}{q}, \frac{-1}{q}, \frac{0}{q}, \frac{1}{q}, \frac{2}{q}, \frac{3}{q}, \frac{4}{q}, \frac{5}{q}, \ldots.$$

Either α is one of these fractions or α lies between two consecutive fractions. In either case, there are two consecutive numerators n and $n + 1$ such that

$$\frac{n}{q} \leq \alpha \leq \frac{n+1}{q}.$$

Now the following theorem becomes reasonable.

Theorem 1.1. Given a real number α and a positive integer q, there is an integer p such that

$$\left|\alpha - \frac{p}{q}\right| \leq \frac{1}{2q}.$$

Proof. As noted above, there is an integer n such that

$$\frac{n}{q} \leq \alpha \leq \frac{n+1}{q}.$$

Therefore, either

$$\frac{n}{q} \leq \alpha \leq \frac{n}{q} + \frac{1}{2q}\left(= \frac{n+1}{q} - \frac{1}{2q}\right)$$

or

$$\frac{n+1}{q} - \frac{1}{2q} \leq \alpha \leq \frac{n+1}{q}.$$

In the first case, α is within $1/2q$ of n/q and we take $p = n$; in the second case, α is within $1/2q$ of $(n + 1)/q$ and we take $p = n + 1$. ▲[4]

Theorem 1.1 is the best that we can do for an arbitrary denominator. For example, with denominator $q = 2$, we can come no closer to $\frac{3}{4}$ than the $1/2q$ of the theorem. With the denominator $q = 10$, we come slightly closer to π ($|\pi - \frac{31}{10}| = .04159\ldots$) than the $\frac{1}{20} = .05$ guaranteed by the theorem. On the other hand, with the denominator $q = 7$, we come considerably closer to π than the $\frac{1}{14} = .0714\ldots$ of the theorem, since

$$|\pi - \tfrac{22}{7}| = .0012\ldots.$$

In other words, $\frac{22}{7}$ is roughly $.0714\ldots/.0012\ldots \approx 60$ times closer to π than what is guaranteed by Theorem 1.1. Thus it appears that for certain exceptional denominators, we can find far better fractional approximations to real

[4] We use the symbol ▲ to signify that we have reached the end of a proof.

numbers than what is guaranteed by Theorem 1.1. Let us illustrate the difference between the ordinary denominator and the exceptional denominator. The closest approximation to π with denominator 117 is given by the fraction 368/117 (it barely satisfies Theorem 1.1). The closest approximation to π with denominator 113 is given by the fraction 355/113. Suppose we wish to compute the circumference of the earth from its diameter. If we use 368/117 in place of π, we will make an error of about $29\frac{1}{2}$ miles, while if we use 355/113 in place of π, we will make an error of only $11\frac{1}{2}$ feet! In Chapter 7 we will learn how to find the exceptional fractional approximations to a real number.

Let us completely change the subject. In 1693, De la Loubère gave a rule for inserting the numbers $1, 2, \ldots, n^2$ into an $n \times n$ square (n odd) so that the sums of the numbers of any two rows or columns are the same (this square array is commonly called a magic square). We illustrate the Loubère method in Figure 1.1 with a 5×5 square. Place 1 anywhere in the square and then move diagonally upward to the right, inserting the numbers 2, 3, and 4 as you go. We pretend that the 5×5 squares on the boundary of our square are copies of the original. Thus when 4 is put in the lower-right-hand corner of the square above, we should also put 4 in the lower-right-hand corner of the original square. We always move diagonally upward when possible.

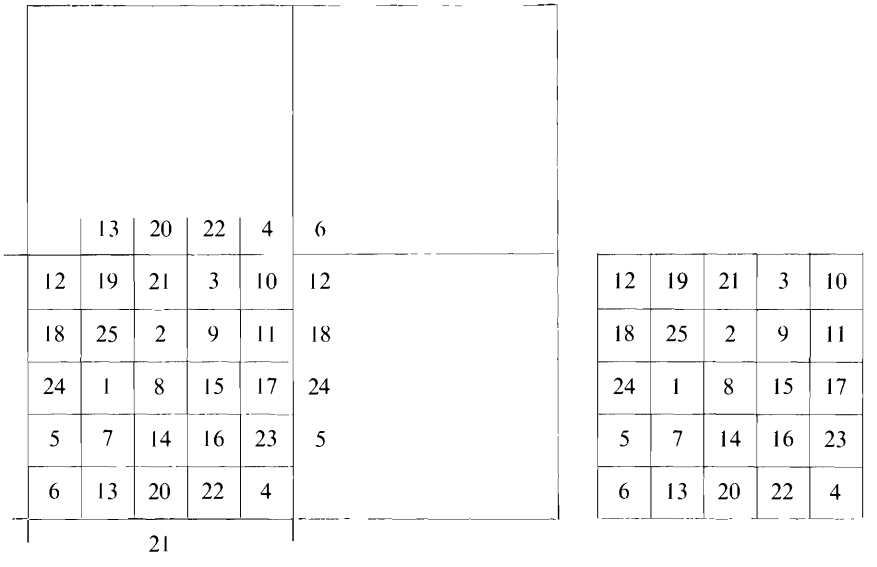


Figure 1.1. The constructive process and the finished square. The numbers in any row or column add up to 65.

When we are blocked by a previous entry, as in going from 5 to 6 or from 10 to 11, we drop down one square instead and then continue diagonally upward from there. In Chapter 4 we will apply the theory of Chapter 3 to show that the Loubère method does what it claims to do for all odd n. In the meantime, the reader may enjoy trying it out for other odd n.

1.2. Some Elementary Properties of Divisibility

In this section we derive some of the most used properties of divisibility that do not depend on the factorization of a number into primes. Throughout the rest of the book, unless otherwise mentioned, the small Roman letters $a, b, c, \ldots$ (with the possible exception of x, y, z) will stand for integers. The letter p, except in Chapter 7, will be reserved for primes. Small Greek letters $\alpha, \beta, \gamma, \ldots$ will stand for real numbers, except in Chapter 8, where they may be complex as well.

Number theory could be deduced from a small set of axioms but we shall not take this approach here. There are in particular two basic facts about integers that we shall use throughout the book. The first states that any nonempty set of positive integers contains a smallest member. Known as the **well-ordering principle**, this property of integers will be used implicitly time and again (for example, it is used in the paragraphs immediately before and after the statement of Theorem 1.5). The second fact is known as the **division algorithm** (logically, it is a consequence of the well-ordering principle). It states that if a and b are positive integers, then there are unique integers q and r such that

$$a = bq + r, \qquad 0 \leq r < b.$$

It is called an algorithm because the ordinary method of long division of a by b produces the quotient q and remainder r.

Theorem 1.2. If a, b, d, r, s are integers, $d \neq 0$, and $d|a, d|b$, then $d|(ra + sb)$. It follows that $d|(a + b), d|(a - b), d|ra$.

Proof. By definition, there are integers e and f such that

$$a = de, \qquad b = df.$$

Thus

$$\begin{aligned} ra + sb &= rde + sdf \\ &= d(re + sf), \end{aligned}$$

where $re + sf$ is also an integer. Therefore, $d|(ra + sb)$. The special cases have $r = s = 1$, $r = 1$ and $s = -1$, $b = a$ and $s = 0$, respectively. ▲

Theorem 1.3. If a, b, c are integers, $a \neq 0$, $b \neq 0$ and $a|b$, $b|c$, then $a|c$.

Proof. By definition, there are integers d and e such that

$$b = ad, \qquad c = be.$$

Therefore,

$$c = ade = a(de)$$

and hence $a|c$. ▲

Theorem 1.4. If a, b, and k are integers, $a \neq 0$, $k \neq 0$, then $a|b$ if and only if $ak|bk$.

Proof. If $a|b$, then there is an integer c such that

$$b = ac.$$

Therefore,

$$bk = (ak)c$$

and hence $ak|bk$. Conversely, if $ak|bk$, then there is an integer c such that

$$bk = (ak)c.$$

Thus, since $k \neq 0$,

$$b = ac$$

and hence $a|b$. ▲

As an example of the application of Theorem 1.3, let n be an integer greater than 1 and let m be the smallest divisor of n which is greater than 1 (this is n itself if n is a prime). Then m is a prime. For if m were composite, we would have an integer k, smaller than m but greater than 1, which divides m. Thus by Theorem 1.3, $k|n$, since $k|m$ and $m|n$. Thus k is a divisor of n which is greater than 1 and smaller than the smallest such divisor, m. This is a contradiction and hence m is a prime. By the way, it follows from this that every positive integer greater than 1 has a prime divisor.

Theorem 1.5. If n is an integer greater than 1, then either n is a prime or n is a finite product of primes.

Proof. If the theorem is false, then there are composite numbers which are not representable as a product of a finite number of primes. Let N be the smallest such number. Thus if $1 < n < N$, the theorem is true for n. Let p be a prime divisor of N. Since N is composite,

$$1 < \frac{N}{p} < N.$$

But this means that the theorem is true for N/p and hence there are primes $p_1, p_2, \ldots, p_k$ such that

$$\frac{N}{p} = p_1 p_2 \cdots p_k.$$

Therefore,

$$N = p p_1 p_2 \cdots p_k$$

is a product of a finite number of primes also. This is a contradiction and thus the theorem is true for all n. ▲

Let us illustrate Theorem 1.2 by giving Euclid's proof of a classic result.

Theorem 1.6. There are infinitely many primes.

Proof. Suppose to the contrary that there are only k primes, $p_1, p_2, \ldots, p_k$ and that all other integers greater than 1 are composite. Let

$$n = p_1 p_2 \cdots p_k + 1$$

and let p be a prime divisor of n (it is possible that $p = n$). Then p is one of the numbers $p_1, p_2, \ldots, p_k$ and hence $p|(p_1 p_2 \cdots p_k)$. Since $p|n$, Theorem 1.2 tells us that

$$p|(n - p_1 p_2 \cdots p_k).$$

But

$$n - p_1 p_2 \cdots p_k = 1$$

and $p \nmid 1$ since $p > 1$. This is a contradiction and hence there are infinitely many primes. ▲

In the examples

$$3 = 2 + 1, \quad 7 = 2 \cdot 3 + 1, \quad 31 = 2 \cdot 3 \cdot 5 + 1,$$

1 plus the product of the first k primes is a prime ($k = 1, 2, 3$). The obvious conjecture that this always occurs is false. The first counterexample is

$$2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 + 1 = 30\,031 = 59 \cdot 509,$$

which is composite.

EXERCISES

1. Show that if $a \neq 0$, then $a|0$ and $a|a$.
2. Show that if $d \neq 0$, $d|a$, then $d|(-a)$ and $-d|a$.
3. What properties of integers do you use to show that if $n > 1$, then $n \nmid 1$?
4. Show that if $a|b$ and $b|a$, then either $a = b$ or $a = -b$.
5. List all the divisors of 12.
6. List all the numbers which divide both 24 and 36 (compare your answer with your answer to the previous problem).

MISCELLANEOUS EXERCISES

1. Show that if n is composite, then there exists a prime $p \leq \sqrt{n}$ such that $p|n$. (*Hint:* Consider what happens when two numbers greater than $\sqrt{n}$ are multiplied.)
2. Use the idea of problem 1 to test the numbers 91, 103, and 343 as to whether they are prime or composite.
3. Write down the numbers from 1 to 40. Starting with $2 \cdot 2$, cross out every second number: 4, 6, 8, 10, ... Starting with $2 \cdot 3$, cross out every third number: 6, 9, 12, 15, ... Starting with $2 \cdot 5$, cross out every fifth number: 10, 15, 20, ... Use the result of problem 1 to show that the numbers that are not crossed out (except for 1) are exactly the set of primes less than 40.
4. Generalize the result of problem 3 to show how you would find all primes less than or equal to a given integer n. Show that in using this method, it is not necessary to know the primes less than $\sqrt{n}$ beforehand, since after the multiples of the jth prime have been crossed out, the next number remaining after the jth prime is the $(j + 1)$st prime. This method is known as the *Sieve of Eratosthenes*, and its generalizations have been used to construct the modern tables of primes. (For example, the 168 primes less than 1000 will produce all the primes less than 1 000 000.)
5. We will constantly be talking about the smallest (or first) integer of a set of positive integers. Show that there is no such thing as the smallest (or first) positive rational number.

6. Starting with 1 in the lower-left-hand corner, construct the 3×3 and 4×4 squares given by the Loubère method. Verify that all rows and columns have the sum 15 in the 3×3 square and that all the columns of the 4×4 square have the sum 34 but that the rows add up to 32 and 36.
7. Show that if $p \nmid n$ for all primes $p \leq \sqrt[3]{n}$, then n is either a prime or a product of two primes.
8. Let p and q be two consecutive odd members of the sequence of primes $2, 3, 5, 7, 11, \ldots$. Show that every factorization of $p + q$ into primes involves at least three (not necessarily distinct) primes. As an example, $7 + 11 = 2 \cdot 3 \cdot 3$.
9. Note that

   $$\underline{15}^2 = \underline{225}, \underline{35}^2 = \underline{1225}, \underline{85}^2 = \underline{7225}, \underline{105}^2 = \underline{11025}$$

   (the underlined portions are for emphasis only). Find a rule for squaring an integer ending in 5 and prove that it works.
10. Note that

$$\frac{1}{7} = \frac{7}{49} \approx \frac{7}{50} = \frac{.7}{5}.$$

$$\begin{array}{r|l} 5 & .7\,1\,4\,2\,8\,5\,7\ldots \\ \hline & 5 \\ \hline & 2\,1 \\ & 2\,0 \\ \hline & \quad 1\,4 \\ & \quad 1\,0 \\ \hline & \quad\quad 4\,2 \\ & \quad\quad 4\,0 \\ \hline & \quad\quad\quad 2\,8 \\ & \quad\quad\quad 2\,5 \\ \hline & \quad\quad\quad\quad 3\,5 \\ & \quad\quad\quad\quad 3\,5 \\ \hline & \quad\quad\quad\quad\quad\quad 7 \end{array} \qquad \text{(repeats)}$$

The modification of the usual division process for .7/5 shown above gives $\frac{7}{49}$ exactly. Use this illustration as a guide to find a simplified method for evaluating the decimal expansion of a/b when $0 < a < b$ and b ends in the digit 9. Illustrate your method with $\frac{1}{19}$ and prove that your method always works.

Chapter 2

THE EUCLIDEAN ALGORITHM AND UNIQUE FACTORIZATION

2.1. The Euclidean Algorithm

Consider the set of all common divisors of the two integers a and b. If $a = b = 0$, then the set of common divisors of a and b is the set of all nonzero integers. If not both a and b are 0, then there are only a finite number of common divisors of a and b, one of which is always 1, and thus there will be a greatest member of this set and it will be positive.

Definition. Let a and b be integers, not both zero. Let d be the largest number in the set of common divisors of a and b. Then we call d the **greatest common divisor** of a and b and we write

$$d = (a,b).$$

For example,

$$(6,4) = 2, \quad (3,5) = 1, \quad (-9,3) = 3, \quad (-6,-4) = 2, \quad (4,0) = 4, \quad (5,5) = 5.$$

Since any divisor of an integer n is also a divisor of $-n$, we see that if a and b are not both zero,

$$(a,b) = (|a|,|b|).$$

Hence we will restrict ourselves at first to finding the greatest common divisor of positive integers.

Let us illustrate the general process by an example. Let

$$d = (54,21).$$

By Theorem 1.2, d also divides

$$12 = 54 - 2 \cdot 21$$

and thus is a common divisor of 12 and 21. By Theorem 1.2, d divides

$$9 = 21 - 12,$$

and therefore d is a common divisor of 9 and 12. By Theorem 1.2 again, d divides

$$3 = 12 - 9.$$

Since $3|9$, we stop at this point. Now that we know that $d|3$, we know that $d \leq 3$. We turn these equations around and using Theorem 1.2 again each time see that 3 divides

$$12 = 3 + 9,$$

and then 3 divides

$$21 = 9 + 12,$$

and then 3 divides

$$54 = 12 + 2 \cdot 21.$$

Thus $3|21$, $3|54$, and $(21, 54) = d \leq 3$. Therefore,

$$(21,54) = 3.$$

We find also that we may use the above equations to write 3 as a linear combination of 21 and 54. Using each equation successively we get

$$\begin{aligned} 12 &= 54 - 2 \cdot 21, \\ 9 &= 21 - 12 = 21 - (54 - 2 \cdot 21) = 3 \cdot 21 - 54, \\ 3 &= 12 - 9 = (54 - 2 \cdot 21) - (3 \cdot 21 - 54) = 2 \cdot 54 - 5 \cdot 21. \end{aligned}$$

Everything done above is perfectly general. Let d_{-2} and d_{-1} be positive integers. The ordinary division algorithm for

$$\frac{d_{-2}}{d_{-1}}$$

gives a quotient a_0 and remainder d_0 such that

$$d_{-2} = a_0 d_{-1} + d_0, \qquad 0 \leq d_0 < d_{-1}.$$

If d_0 is 0 we stop; otherwise the division algorithm for

$$\frac{d_{-1}}{d_0}$$

gives a quotient a_1 and remainder d_1 such that

$$d_{-1} = a_1 d_0 + d_1, \qquad 0 \le d_1 < d_0.$$

If $d_1 \neq 0$, we continue onward, getting, successively,

$$\begin{aligned} d_0 &= a_2 d_1 + d_2, && 0 \le d_2 < d_1, \\ d_1 &= a_3 d_2 + d_3, && 0 \le d_3 < d_2, \\ &\vdots \\ d_{k-2} &= a_k d_{k-1} + d_k, && 0 \le d_k < d_{k-1}, \end{aligned}$$

where it is assumed that $d_j \neq 0$ if $j < k$. Since

$$d_{-1} > d_0 > d_1 > d_2 > d_3 > \cdots > d_{k-1} > d_k \ge 0,$$

it is clear that, sooner or later, some d_j will equal zero and, in fact, since each d_j is at least one smaller than the d_j before it, we will come to a $d_j = 0$ with $j < d_{-1}$. (Actually, it will happen much sooner than $j = d_{-1} - 1$; we are concerned here only with the fact that it does happen.) If $d_{k+1} = 0$, then

$$d_{k-1} = a_{k+1} d_k.$$

Thus, we may put these equations together as

$$\begin{aligned} d_{-2} &= a_0 d_{-1} + d_0, && 0 < d_0 < d_{-1} \\ d_{-1} &= a_1 d_0 + d_1, && 0 < d_1 < d_0, \\ &\vdots \\ d_{k-2} &= a_k d_{k-1} + d_k, && 0 < d_k < d_{k-1}, \\ d_{k-1} &= a_{k+1} d_k. \end{aligned} \tag{1}$$

Theorem 2.1. If d_{-2} and d_{-1} are positive integers and d_k is found from the process of equations (1), then

$$(d_{-2}, d_{-1}) = d_k.$$

Further, we may find integers r and s in a systematic way from equations (1) such that

$$r d_{-2} + s d_{-1} = d_k.$$

Proof. Let $d = (d_{-2}, d_{-1})$. When we put (1) in the form

$$\begin{aligned} d_0 &= d_{-2} - a_0 d_{-1}, \\ d_1 &= d_{-1} - a_1 d_0, \\ d_2 &= d_0 - a_2 d_1, \\ &\vdots \\ d_k &= d_{k-2} - a_k d_{k-1}, \end{aligned}$$

we see from Theorem 1.2 that $d|d_0$, and then $d|d_1, d|d_2, \ldots, d|d_k$. Therefore,

$$d \leq d_k. \tag{2}$$

On the other hand, by starting at the last of equations (1) and working up, we see from Theorem 1.2 that in succession,

$$d_k|d_{k-1}, d_k|d_{k-2}, \ldots, d_k|d_2, d_k|d_1, d_k|d_0, d_k|d_{-1}, d_k|d_{-2}.$$

Thus d_k is a common divisor of d_{-1} and d_{-2} and, therefore, by the definition of the greatest common divisor,

$$d_k \leq d.$$

This, combined with equation (2), says that

$$d_k = d,$$

as desired.

It is most convenient to give an inductive proof of the last part of the theorem. The main idea is that if we can express d_{j-2} and d_{j-1} as combinations of d_{-2} and d_{-1}, then we may use the equation

$$d_j = d_{j-2} - a_j d_{j-1}$$

to express d_j as a combination of d_{-2} and d_{-1} also. The actual induction is somewhat awkward since d_{j-2} and d_{j-1} are involved in getting the result for d_j. We may put things in the usual form for induction by complicating our induction hypothesis. Let S_n be the statement: There are integers r_{n-2}, s_{n-2}, r_{n-1}, and s_{n-1} such that

$$\begin{aligned} d_{n-2} &= r_{n-2} d_{-2} + s_{n-2} d_{-1}, \\ d_{n-1} &= r_{n-1} d_{-2} + s_{n-1} d_{-1}. \end{aligned}$$

Our goal is to prove that S_{k+1} is true since the second part of S_{k+1} says that there are integers r_k and s_k such that

$$d_k = r_k d_{-2} + s_k d_{-1}.$$

First, we note that

$$d_{-2} = 1 \cdot d_{-2} + 0 \cdot d_{-1},$$
$$d_{-1} = 0 \cdot d_{-2} + 1 \cdot d_{-1},$$

and thus S_0 is true. We now prove that if $0 \leq n \leq k$ and S_n is true, then S_{n+1} is true. Suppose that S_n is true so that there are integers r_{n-2}, s_{n-2}, r_{n-1}, and s_{n-1} such that

$$\begin{aligned} d_{n-2} &= r_{n-2}d_{-2} + s_{n-2}d_{-1}, \\ d_{n-1} &= r_{n-1}d_{-2} + s_{n-1}d_{-1}. \end{aligned} \tag{3}$$

We see from (1) that

$$d_n = d_{n-2} - a_n d_{n-1},$$

and if we substitute (3) into this, we get

$$\begin{aligned} d_n &= (r_{n-2}d_{-2} + s_{n-2}d_{-1}) - a_n(r_{n-1}d_{-2} + s_{n-1}d_{-1}) \\ &= (r_{n-2} - a_n r_{n-1})d_{-2} + (s_{n-2} - a_n s_{n-1})d_{-1} \\ &= r_n d_{-2} + s_n d_{-1}, \end{aligned}$$

where we have put

$$r_n = r_{n-2} - a_n r_{n-1},$$
$$s_n = s_{n-2} - a_n s_{n-1}.$$

Thus we have integers r_{n-1}, s_{n-1}, r_n, and s_n such that

$$d_{n-1} = r_{n-1}d_{-2} + s_{n-1}d_{-1},$$
$$d_n = r_n d_{-2} + s_n d_{-1},$$

which is the statement S_{n+1}. Thus S_{n+1} follows from S_n. Since S_0 is true, S_1 follows from S_0, and then S_2 follows from S_1, S_3 from S_2, ..., until finally S_{k+1} follows from S_k. ▲

Definition. The use of equations (1) for finding the greatest common divisor is called the **Euclidean algorithm**.

Euclid, of course, did not use algebraic manipulations but rather stated the whole process geometrically. We will say more about this in Chapter 7. In actual practice, when we wish to write d_k in terms of d_{-2} and d_{-1}, it is advantageous to proceed from the bottom of equations (1) rather than from the top.

As another example of the Euclidean algorithm, let us calculate (53, 77) and express it as a linear combination of 53 and 77. We see that

$$\begin{aligned} 77 &= 1 \cdot 53 + 24, \\ 53 &= 2 \cdot 24 + 5, \\ 24 &= 4 \cdot 5 + 4, \\ 5 &= 1 \cdot 4 + 1, \\ 4 &= 4 \cdot 1, \end{aligned}$$

and thus

$$(53,77) = 1.$$

Working backward we see that

$$\begin{aligned} 1 &= 5 - 1 \cdot 4 \\ &= 5 - 1 \cdot (24 - 4 \cdot 5) = 5 \cdot 5 - 1 \cdot 24 \\ &= 5 \cdot (53 - 2 \cdot 24) - 1 \cdot 24 = 5 \cdot 53 - 11 \cdot 24 \\ &= 5 \cdot 53 - 11 \cdot (77 - 1 \cdot 53) = 16 \cdot 53 - 11 \cdot 77. \end{aligned}$$

In the example above, 53 and 77 have 1 as their greatest common divisor and hence they have no common factors other than 1 and -1. Such a fact is sufficiently important to give it a name.

Definition. Let a and b be integers, not both zero. If

$$(a,b) = 1,$$

then we say that a and b are **relatively prime**.

Another way of putting this is to say that a and b are relatively prime if and only if 1 and -1 are their only common divisors.

The result on linear combinations will be very useful both here and later, and thus we will extend it to all integers and not just positive integers.

Theorem 2.2. Let a and b be integers, not both zero. Then there exist integers r and s such that

$$ar + bs = (a,b).$$

Proof. We take the cases of neither a and b are zero and one of a and b is zero separately. Suppose that $b = 0$. Then

$$(a,0) = (|a|, 0) = |a|$$

and

$$a(\pm 1) + 0(0) = |a|,$$

where the $+1$ is used if $a > 0$ and -1 is used if $a < 0$. In like manner, if $a = 0$, then

$$0(0) + b(\pm 1) = |b| = (0, b),$$

where the $+1$ is used if $b > 0$ and -1 is used if $b < 0$.

We may now restrict our attention to the case that neither a nor b is zero and, in this case, both $|a|$ and $|b|$ are positive. By Theorem 2.1, there are integers r and s such that

$$r|a| + s|b| = (|a|, |b|) = (a, b).$$

Since

$$a = \pm|a|, \qquad b = \pm|b|,$$

we see that

$$(\pm r)a + (\pm s)b = (a, b),$$

for an appropriate choice of signs. ▲

As an example, we saw earlier that

$$2 \cdot 54 + (-5) \cdot 21 = 3 = (54, 21)$$

and thus

$$(-2) \cdot (-54) + (-5) \cdot 21 = 3 = (-54, 21),$$
$$2 \cdot 54 + 5 \cdot (-21) = 3 = (54, -21),$$
$$(-2) \cdot (-54) + 5 \cdot (-21) = 3 = (-54, -21).$$

One result of Theorem 2.2 is the following.

Theorem 2.3. Let $d = (a,b)$. Then n is a common divisor of a and b if and only if $n|d$.

Proof. If $n|d$, then since $d|a$ and $d|b$, Theorem 1.3 says that $n|a$ and $n|b$, and hence any divisor of d is a divisor of a and b. Conversely, if $n|a$ and $n|b$, then

by Theorem 1.2, n divides

$$ar + bs = d,$$

where r and s are the integers given by Theorem 2.2. Thus a common divisor of a and b is also a divisor of d. ▲

This result is a much more useful property of the greatest common divisor than its definition as the largest of the common divisors. We will now assemble several of the other most used properties of greatest common divisors.

Theorem 2.4. Let $(a,b) = d$ and let k be an arbitrary integer. Then

(a) $(a, b + ka) = (a, b)$.

(b) $(ak,bk) = |k|(a,b) \qquad (k \neq 0)$.

(c) $\left(\frac{a}{d}, \frac{b}{d}\right) = 1$.

Proof. If $n|a$, $n|b$, then by Theorem 1.2, $n|(b + ka)$. Thus any divisor of a and b is a divisor of a and $b + ka$. Conversely, if $n|a$, $n|(b + ka)$, then $n|[(b + ka) - ka]$, and thus n is a common divisor of a and b. Hence the set of divisors of a and b is also the set of divisors of a and $b + ka$, and therefore the greatest member of this set is the greatest common divisor of a and $b + ka$ as well as the greatest common divisor of a and b. This proves (a). Let

$$(ak, bk) = n,$$

and, for the moment, let k be positive. Since $d|a$, $d|b$, we see that $dk|ak$, $dk|bk$ and thus, by Theorem 2.3,

$$dk|n.$$

Thus there is a positive integer m such that

$$(ak, bk) = dkm. \tag{4}$$

As a result,

$$dmk|ak, \qquad dmk|bk.$$

It follows from Theorem 1.4 that

$$dm|a, \qquad dm|b,$$

then from Theorem 2.3 that

$$dm|d \cdot 1,$$

and finally from Theorem 1.4 again that

$$m|1.$$

Thus $m = \pm 1$ and since $m > 0$, $m = 1$. Equation (4) is thus

$$(ak,bk) = dk = k(a,b) = |k|(a,b),$$

which proves (b) when $k > 0$. Now if $k < 0$, then $-k = |k| > 0$, and therefore

$$(ak,bk) = (-ak,-bk) = (a|k|,b|k|) = |k|(a,b),$$

and thus (b) is true. Last, since $d > 0$, it follows from (b) that

$$d = (a,b) = \left(d \cdot \frac{a}{d}, d \cdot \frac{b}{d}\right) = d\left(\frac{a}{d}, \frac{b}{d}\right),$$

which yields, after dividing both sides by d,

$$1 = \left(\frac{a}{d}, \frac{b}{d}\right). \qquad \blacktriangle$$

We may also define the greatest common divisor of more than two integers. We will use this concept for three integers in Chapter 5, and so we present here the necessary details and leave further results to the problems.

Definition. If a, b, and c are integers, not all zero, and d is the largest of the common divisors of a, b, and c, then we say that d is the **greatest common divisor** of a, b, and c and we write

$$d = (a,b,c).$$

Since $1|a$, $1|b$, $1|c$, we see that (a,b,c) is positive. As an example,

$$(4,8,10) = 2.$$

Theorem 2.5. If $(a,b,c) = d$, then

$$\left(\frac{a}{d}, \frac{b}{d}, \frac{c}{d}\right) = 1.$$

Proof. Let

$$\left(\frac{a}{d}, \frac{b}{d}, \frac{c}{d}\right) = n$$

so that $n \geq 1$. Thus

$$n \left| \frac{a}{d}, \quad n \right| \frac{b}{d}, \quad n \left| \frac{c}{d} \right.$$

and, by Theorem 1.4,

$$dn|a, \quad dn|b, \quad dn|c.$$

Hence dn is a common divisor of a, b, and c and hence is less than or equal to the greatest common divisor of a, b, and c:

$$dn \leq d.$$

We divide this by d and find that

$$n \leq 1.$$

Hence $n = 1$. ▲

We note that it is possible to have

$$(a,b,c) = 1$$

even though no two of the numbers a, b, and c are relatively prime. For example,

$$(6,10,15) = 1$$

even though

$$(6,10) = 2, \qquad (6,15) = 3, \qquad (10,15) = 5.$$

Definition. Let $a_1, a_2, \ldots, a_n$ be nonzero integers. We say that these numbers are **pairwise relatively prime** if the greatest common divisor of each pair of these integers is 1.

For example, the integers 4, 15, and 77 are pairwise relatively prime since

$$(4,15) = (4,77) = (15,77) = 1,$$

while the integers 4, 15, 77, and 91 are not pairwise relatively prime since

$$(77,91) = 7.$$

EXERCISES

1. Show that if a, b, c are pairwise relatively prime, then

$$(a,b,c) = 1.$$

2. Use the Euclidean algorithm to find the greatest common divisor of (a) 77 and 91, (b) 182 and 442, and (c) 2311 and 3701.
3. Express (17,37) as a linear combination of 17 and 37.
4. Express (399,703) as a linear combination of 399 and 703.
5. Find integers r and s such that $547r + 632s = 1$.
6. Find integers r and s such that $398r + 600s = 2$.
*7. Find integers r and s such that $922r + 2163s = 7$.
*8. Are there integers r and s such that $1841r + 3647s = 1$? Why?
9. Show that if there is no prime p such that $p|a$, $p|b$, then

$$(a, b) = 1.$$

10. In the proof of Theorem 2.1, why did we restrict the proof that S_n implies S_{n+1} to $0 \leq n \leq k$?
11. Are the integers 101, 209, 283, and 341 pairwise relatively prime?
12. Show that if p is a prime and a an integer, then either $(a,p) = 1$ or $(a,p) = p$.
13. Use Theorem 2.4(c) to show that a fraction m/n can always be reduced to lowest terms.
14. Let $\alpha_j = d_{j-2}/d_{j-1}$. Show that the Euclidean algorithm of equation (1) takes the form

$$\alpha_0 = a_0 + \frac{1}{\alpha_1}, \qquad a_0 < \alpha_0 < a_0 + 1,$$

$$\alpha_1 = a_1 + \frac{1}{\alpha_2}, \qquad a_1 < \alpha_1 < a_1 + 1,$$

$$\alpha_k = a_k + \frac{1}{\alpha_{k+1}}, \qquad a_k < \alpha_k < a_k + 1,$$

$$\alpha_{k+1} = a_{k+1}.$$

2.2. The Fundamental Theorem of Arithmetic

The fundamental theorem of arithmetic, otherwise known as the unique factorization theorem, states that if you and I independently write an integer greater than 1 as a product of primes, we will get the same result except for the order in which the primes are written in the two products. This theorem will be used constantly throughout the rest of the book and well deserves its name. There are times that the following milder-sounding theorems will suffice in the applications; they are not really milder since they will be used to prove the fundamental theorem later in this section.

Theorem 2.6. If $(n,a) = 1$ and $n|ab$, then $n|b$.

Proof. Since $(n,a) = 1$, by Theorem 2.2, there are integers r and s such that

$$nr + as = 1.$$

Thus

$$nrb + abs = b.$$

Since $n|n$ and $n|ab$, $n|[n(rb) + (ab)s]$, which is to say $n|b$. ▲

Theorem 2.7. If $(a,m,n) = 1$ (note that this is true whenever two of the numbers a, m, n are relatively prime), then

$$(a,mn) = (a,m) \cdot (a,n).$$

In particular, if $(a,m) = (a,n) = 1$, then $(a,mn) = 1$.

Proof. Let

$$d = (a,mn), \qquad d_1 = (a,m), \qquad d_2 = (a,n).$$

We then wish to show that $d = d_1 d_2$. By Theorem 2.2, there are integers r, s, t, and u such that

$$ar + ms = d_1, \qquad at + nu = d_2.$$

Therefore,

$$(ar + ms)(at + nu) = d_1 d_2;$$

that is,

$$a(art + rnu + mst) + mn(su) = d_1 d_2.$$

It follows from the definition of d and Theorem 1.2 that $d|d_1 d_2$. Hence

$$d \leq d_1 d_2. \tag{5}$$

In order to prove the opposite inequality, we need to prove that

$$(d_1,d_2) = 1.$$

This is done as follows. Let $(d_1,d_2) = e \geq 1$. Then $e|d_1, e|d_2$ and thus by the definition of d_1 and d_2 and by Theorem 2.3, $e|a$, $e|m$, $e|n$. Thus e is a common divisor of a, m, n, and if $e > 1$, this contradicts the fact that $(a, m, n) = 1$. Hence $e = 1$, as desired. But now, note that $d_1|a$, $d_1|m$ (by definition) and thus, by Theorem 2.3, $d_1|d$. In like manner, $d_2|a$, $d_2|n$, and thus $d_2|d$. But this

may be written $d_2|d_1 \cdot (d/d_1)$. Since $(d_2,d_1) = 1$, it follows from Theorem 2.6 that $d_2|(d/d_1)$, and then it follows from Theorem 1.4 that $d_1d_2|d$. Therefore,

$$d_1d_2 \leq d,$$

and comparing this with (5) we see that $d = d_1d_2$. ▲

The next theorem is usually proved by using Theorem 2.6, but it is somewhat simpler to use Theorem 2.7.

Theorem 2.8. If p is a prime and $p|(a_1a_2 \cdots a_k)$, then for some j, $1 \leq j \leq k$, $p|a_j$. As a special case, if $p|a^k$, then $p|a$.

Proof. We note that the only positive divisors of p are 1 and p. If a is an arbitrary integer, then since $(a,p)|p$, we see that $(a,p) = 1$ or $(a,p) = p$. In the second case $p|a$. Thus if a is an integer such that $p \nmid a$, then

$$(p,a) = 1.$$

Now suppose that p divides none of the numbers $a_1, a_2, \ldots, a_k$. Then

$$(p,a_1) = 1, (p,a_2) = 1, \ldots, (p,a_k) = 1.$$

By Theorem 2.7,

$$(p,a_1a_2) = 1.$$

By Theorem 2.7, again,

$$(p,a_1a_2a_3) = 1.$$

After the $(k-1)$st application of Theorem 2.7, we find that

$$(p,a_1a_2 \cdots a_k) = 1.$$

But this contradicts the fact that $p > 1$ is a common divisor of p and $a_1a_2 \cdots a_k$. Hence p divides one of the numbers $a_1, a_2, \ldots, a_k$, as desired. ▲

Theorem 2.9. (The Fundamental Theorem of Arithmetic, or the Unique Factorization Theorem for Positive Integers). Suppose that $n > 1$ and

$$n = p_1p_2p_3 \cdots p_r = q_1q_2 \cdots q_s,$$

where $p_1, p_2, \ldots, p_r, q_1, q_2, \ldots, q_s$ are primes. Then $r = s$ and the two factorizations of n are the same apart from the order of the factors.

Proof. Suppose that the theorem is false. Then the theorem is false for certain values of n, and we will let N be the smallest of these. Thus we shall assume that the theorem is true for all integers n between 1 and N but that

the theorem is false for $n = N$. We will show that this leads to a contradiction. Suppose that

$$N = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s,$$

where $p_1, p_2, \ldots, p_r, q_1, q_2, \ldots, q_s$ are primes.

The theorem is clearly true for primes and thus N must be composite and hence $r \geq 2$, $s \geq 2$. Since the order of the factors is not important, we may assume that they have been written so that

$$\begin{aligned} p_r &\geq p_j, \qquad 1 \leq j \leq r-1. \\ q_s &\geq q_j, \qquad 1 \leq j \leq s-1. \end{aligned} \tag{6}$$

We will first show that $p_r = q_s$. If this is false, then either $p_r > q_s$ or $q_s > p_r$. We will show here that $p_r > q_s$ is false; the proof that $q_s > p_r$ is false is identical and in fact may be given from our proof by interchanging the letters p and q and interchanging r and s. If $p_r > q_s$, then, by (6),

$$p_r > q_j, \qquad 1 \leq j \leq s.$$

Therefore, $p_r \nmid q_j$ for any of the q_j's. But by Theorem 2.8, this is a contradiction, since

$$p_r | (q_1 q_2 \cdots q_s),$$

the product being N. Thus the inequality $p_r > q_s$ is false and, in like manner, $q_s > p_r$ is false. Hence

$$p_r = q_s,$$

and therefore

$$\frac{N}{p_r} = p_1 p_2 \cdots p_{r-1} = q_1 q_2 \cdots q_{s-1}. \tag{7}$$

Since $r \geq 2$, $s \geq 2$, there is at least one prime in each of the factorizations of N/p_r in (7) and thus

$$1 < \frac{N}{p_r} < N.$$

As a result, the theorem holds for $n = N/p_r$ and therefore

$$r - 1 = s - 1,$$

and the factorization $q_1 q_2 \cdots q_{s-1}$ of N/p_r is the same factorization as $p_1 p_2 \cdots p_{r-1}$ except possibly for the order of the factors. It follows that $r = s$ and the two factorizations of N as $p_1 p_2 \cdots p_r$ and $q_1 q_2 \cdots q_r$ are the same

except possibly for the order of the factors. Thus the theorem is true for N and this contradicts the definition of N. Thus the theorem is true for all $n > 1$. ▲

As the example

$$2 = 1 \cdot 2 = 1 \cdot 1 \cdot 2 \cdot 1 \cdot 1 \cdot 1$$

shows, the fundamental theorem would be false if 1 were a prime. This is one reason why 1 is not considered a prime. As we see from the examples,

$$18 = 2 \cdot 3 \cdot 3, \qquad 36 = 2 \cdot 2 \cdot 3 \cdot 3, \qquad 64 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2,$$

it frequently happens that certain primes occur more than once in the factorization of a composite number. In such cases, it is customary to use exponents,

$$18 = 2 \cdot 3^2, \qquad 36 = 2^2 \cdot 3^2, \qquad 64 = 2^6,$$

and in general we will write

$$n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}.$$

When n is written this way, we will always assume that the numbers $p_1, p_2, \ldots, p_k$ are distinct primes and, unless otherwise stated, that $a_1 > 0$, $a_2 > 0, \ldots, a_k > 0$. The unique factorization theorem in this form says that if

$$n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k} = q_1^{b_1} q_2^{b_2} \cdots q_m^{b_m}$$

(where the q_j are also primes and the b_j are positive), then $k = m$ and, in some order, the primes $p_1, p_2, \ldots, p_k$ and $q_1, q_2, \ldots, q_m$ are the same with the corresponding exponents being equal also. The following result is an immediate corollary of either Theorem 2.8 or 2.9, but it is one which will be used time and again.

Theorem 2.10. Suppose that the factorization of n into primes is given as

$$n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$$

and that p is a prime such that $p|n$. Then for some j in the range $1 \leq j \leq k$, $p = p_j$.

Proof. By Theorem 2.8, $p|p_j$ for some j. Since $p > 1$ and the only positive divisors of p_j are 1 and p_j, it must be that $p = p_j$. ▲

We may easily find the greatest common divisor of two (or more) integers if we know their factorizations into primes. For example, from the factorizations

$$2600 = 2 \cdot 2 \cdot 2 \cdot 5 \cdot 5 \cdot 13$$

$$10\,140 = 2 \cdot 2 \cdot 3 \cdot 5 \cdot 13 \cdot 13,$$

it is easy to see that

$$(2600, 10\,140) = 2 \cdot 2 \cdot 5 \cdot 13 = 260,$$

particularly if we write the above factorizations as

$$2600 = (2 \cdot 2 \cdot 5 \cdot 13) \cdot 2 \cdot 5,$$

$$10\,140 = (2 \cdot 2 \cdot 5 \cdot 13) \cdot 3 \cdot 13.$$

This process is perfectly general; its only disadvantage for large numbers is that you must know how they factor into primes.

Theorem 2.11. Suppose that

$$n = p_1 p_2 \cdots p_k q_1 q_2 \cdots q_i,$$

$$m = p_1 p_2 \cdots p_k r_1 r_2 \cdots r_j,$$

where $p_1, p_2, \ldots, p_k, q_1, q_2, \ldots, q_i, r_1, r_2, \ldots, r_j$ are primes such that none of the q's are equal to any of the r's. (If $k = 0$, we interpret the product $p_1 p_2 \cdots p_k$ as 1 and similarly for $i = 0$ and $j = 0$.) Then

$$(n,m) = p_1 p_2 \cdots p_k.$$

Proof. Let

$$d = p_1 p_2 \cdots p_k.$$

Then $d|n$, $d|m$ and hence by Theorem 2.3, $d|(n,m)$. Thus there is a positive integer a such that

$$(n,m) = da.$$

Therefore,

$$da|dq_1 q_2 \cdots q_i, \qquad da|dr_1 r_2 \cdots r_j$$

and hence, by Theorem 1.4,

$$a|q_1 q_2 \cdots q_i, \qquad a|r_1 r_2 \cdots r_j.$$

Our goal is to prove that $a = 1$. If $a > 1$, then there is a prime p which divides a, and it must also divide $q_1 q_2 \cdots q_i$ and $r_1 r_2 \cdots r_j$. By Theorem 2.10, p is one of the q_m's and is also one of the r_m's. Thus the primes $q_1, \ldots, q_i$ have a prime in common with the primes $r_1, \ldots, r_j$, which is contrary to the hypothesis of the theorem. Hence $a = 1$ and therefore

$$(n,m) = d. \qquad \blacktriangle$$

EXERCISES

In problems 1–6, find the greatest common divisor of m and n by means of Theorem 2.11 and check your result by using the Euclidean algorithm. You may assume that the factorizations given of m and n are factorizations into primes.

1. $m = 143 = 11 \cdot 13$, $n = 187 = 11 \cdot 17$.
2. $m = 231 = 3 \cdot 7 \cdot 11$, $n = 561 = 3 \cdot 11 \cdot 17$.
3. $m = 588 = 2 \cdot 2 \cdot 3 \cdot 7 \cdot 7$, $n = 7546 = 2 \cdot 7 \cdot 7 \cdot 7 \cdot 11$.
4. $m = 119\,790 = 2 \cdot 3 \cdot 3 \cdot 5 \cdot 11 \cdot 11 \cdot 11$, $n = 42\,900 = 2 \cdot 2 \cdot 3 \cdot 5 \cdot 5 \cdot 11 \cdot 13$.
5. $m = 830\,407 = 823 \cdot 1009$, $n = 919\,199 = 911 \cdot 1009$.
6. $m = 9797 = 97 \cdot 101$, $n = 14\,507 = 89 \cdot 163$.
7. What can you conclude about the four numbers 1 456 813, 1 468 823, 1 476 221, and 1 488 391 given that $1\,456\,813 \cdot 1\,488\,391 = 1\,468\,823 \cdot 1\,476\,221$? Justify your conclusions.
8. Suppose that

$$n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}, \qquad m = p_1^{b_1} p_2^{b_2} \cdots p_k^{b_k}.$$

   (Any two positive integers may be written this way with the same primes if we allow zero exponents.) If $\min\{a,b\}$ means the smaller of a and b (or their common value if they are equal), show that

$$(n,m) = p_1^{\min\{a_1,b_1\}} p_2^{\min\{a_2,b_2\}} \cdots p_k^{\min\{a_k,b_k\}}.$$

9. Suppose that

$$n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}, \qquad m = p_1^{b_1} p_2^{b_2} \cdots p_k^{b_k},$$

   where zero exponents are allowed. Prove that $n|m$ if and only if

$$a_1 \le b_1, a_2 \le b_2, \ldots, a_k \le b_k.$$

*10. Show that Theorem 2.6 can be proved from Theorem 2.9 without use of the material of Section 2.1.
11. Show that Theorem 2.8 can be proved from Theorem 2.9.
12. Show that $\log_{10} 2$ is irrational. (*Hint:* Let $\log_{10} 2 = n/m$ and show that $2^m = 10^n$.)

13. Show that if p is a prime and $p|a^n$, then $p^n|a^n$.
14. How many zeros are there at the end of 100!?
15. Give an example of four positive integers such that any three of them have a common divisor greater than 1, although only ± 1 divide all four of them.

2.3. Applications of the Fundamental Theorem

This is actually a misleading section heading since it is usually Theorems 2.6, 2.7, and 2.8 that are used in applications rather than Theorem 2.9. But as none of these theorems could be true without unique factorization, the section heading accurately describes the fact that the results in this section depend on the unique factorization property of the positive integers. Our first application will be an application of the fundamental theorem itself. Although it seems very mild, Theorem 2.12 will be of great importance in Chapter 5.

Theorem 2.12. Suppose that a and b are relatively prime positive integers and

$$ab = c^n.$$

Then there are positive integers d and e such that

$$a = d^n, \qquad b = e^n.$$

Proof. If $a = 1$, then we may let $d = 1$, $e = c$; if $b = 1$, then we may let $d = c$, $e = 1$. Thus we may restrict our attention to the case that $a > 1, b > 1$. Since $(a,b) = 1$, the prime factors of a and b are distinct. Thus we may set

$$a = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}, \qquad b = p_{r+1}^{a_{r+1}} \cdots p_{r+s}^{a_{r+s}},$$

where $p_1, p_2, \ldots, p_{r+s}$ are distinct primes, $r \geq 1$, $s \geq 1$. Suppose that the prime decomposition of c is given by

$$c = q_1^{b_1} q_2^{b_2} \cdots q_k^{b_k}.$$

Then

$$p_1^{a_1} p_2^{a_2} \cdots p_{r+s}^{a_{r+s}} = q_1^{nb_1} q_2^{nb_2} \cdots q_k^{nb_k}.$$

By Theorem 2.9, $k = r + s$, the primes q_j are the same as the primes p_j (except for order), and the corresponding exponents are the same. Thus we may renumber the q's so that

$$q_j = p_j, \qquad 1 \leq j \leq r + s$$

and then

$$a_j = nb_j, \qquad 1 \leq j \leq r + s.$$

Hence

$$a = (p_1^{b_1} p_2^{b_2} \cdots p_r^{b_r})^n,$$

$$b = (p_{r+1}^{b_{r+1}} p_{r+2}^{b_{r+2}} \cdots p_{r+s}^{b_{r+s}})^n. \qquad \blacktriangle$$

The reader may have learned that $\sqrt{2}$ is irrational. This is a special case of the converse of a far more general result,

Theorem 2.13. Suppose that a and n are positive integers and $\sqrt[n]{a}$ is rational. Then $\sqrt[n]{a}$ is an integer.

Proof. Since $\sqrt[n]{a}$ is rational (and positive), there are positive integers r and s such that

$$\sqrt[n]{a} = \frac{r}{s}.$$

We may even assume that $(r,s) = 1$, since we may otherwise divide the numerator and denominator by (r,s). We will show that $s = 1$. If $s > 1$, then there is a prime p which divides s and then p divides

$$as^n = r^n.$$

By Theorem 2.8, p also divides r, and this contradicts the fact that $(r,s) = 1$. Hence $s = 1$ and therefore

$$\sqrt[n]{a} = r,$$

an integer. $\blacktriangle$

As an example of this theorem, since $1 < \sqrt{2} < 2$, $\sqrt{2}$ is not an integer and hence not rational. As another example, since

$$2^3 < 10 < 3^3,$$

it follows that

$$2 < \sqrt[3]{10} < 3,$$

and thus $\sqrt[3]{10}$ is not an integer. Therefore, $\sqrt[3]{10}$ is irrational.

The next application is actually only a preliminary result which is necessary in the proof of Theorem 2.15 in the next section (such a result is sometimes called a lemma).

Theorem 2.14. Suppose that m and n are relatively prime positive integers. If d is positive and $d|mn$, then there are unique positive integers d_1 and d_2 such that

$$d = d_1 d_2, \qquad d_1|m, \quad d_2|n.$$

Conversely, if $d_1|m$ and $d_2|n$, then $d_1 d_2|mn$.

Proof. Suppose that $d|mn$. We first show that there exists at least one such pair of integers d_1, d_2. Let

$$d_1 = (d,m), \qquad d_2 = (d,n). \tag{8}$$

Since $d|mn$, we see that $(d,mn) = d$. Further, since $(m,n) = 1$, we may apply Theorem 2.7 to get

$$d = (d,mn) = (d,m) \cdot (d,n) = d_1 d_2.$$

By definition, $d_1|m$, $d_2|n$, and thus d_1 and d_2 have the desired properties. Now suppose that d'_1 and d'_2 are positive integers with the properties that

$$d = d'_1 d'_2, \qquad d'_1|m, \quad d'_2|n.$$

Then we see from the definitions of d_1 and d_2 as greatest common divisors in (8) that

$$d'_1 \leq d_1, \qquad d'_2 \leq d_2 \tag{9}$$

and therefore

$$d'_1 d'_2 \leq d_1 d_2 = d. \tag{10}$$

The only way that equality may hold in (10) is that equality holds in both of (9) and hence

$$d'_1 = d_1, \qquad d'_2 = d_2.$$

This proves that the representation of d in the form of the theorem is unique. The converse follows from the definition of divisibility. ▲

EXERCISES

1. Prove that $\sqrt[3]{3}$ is irrational.
2. Prove that $\sqrt[5]{5}$ is irrational.
3. Prove that if $n \geq 2$, then $\sqrt[n]{n}$ is irrational. (*Hint*: Show that if $n \geq 2$, then $2^n > n$.)

*4. Verify that $\sqrt{2} + \sqrt{3}$ is a root of the equation

$$x^4 - 10x^2 + 1 = 0.$$

Use the methods in the proof of Theorem 2.13 to show that the only possible rational roots of this equation are $x = 1$ and $x = -1$, neither of which are roots. Conclude that the roots of this equation are all irrational.

5. The following numbers were once offered as a counterexample to Theorem 2.14: $m = 2^2 \cdot 3 \cdot 5$, $n = 7 \cdot 11$, $d = 11$ (the claim being that, as may be seen from the factorizations, there is no value of d_1 that will do). Is this really a counterexample?

2.4. Multiplicative Functions

Before we actually give a definition of multiplicative functions, we will present two examples.

Definition. Let n be a positive integer. We let $\boldsymbol{d(n)}$ be the number of positive integers which divide n (including 1 and n itself). We let $\boldsymbol{\sigma(n)}$ be the sum of the positive divisors of n (including 1 and n).

In Figure 2.1, we have evaluated $d(n)$ and $\sigma(n)$ for n in the range 1 to 20.

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
$d(n)$	1	2	2	3	2	4	2	4	3	4	2	6	2	4	4	5	2	6	2	6
$\sigma(n)$	1	3	4	7	6	12	8	15	13	18	12	28	14	24	24	31	18	39	20	42

Figure 2.1

It is clear that $d(n) = 2$ if and only if n is a prime and likewise $\sigma(n) = n + 1$ if and only if n is a prime. We should not expect a simple formula for either $d(n)$ or $\sigma(n)$, since then we could immediately decide from it whether or not a given integer is a prime. We will see shortly, however, that if we already know the factorization of n into primes, then there are simple formulas for $d(n)$ and $\sigma(n)$.

We see from the figure that there are times that $d(nm)$ [or $\sigma(mn)$] can be determined from $d(n)$ and $d(m)$ [or $\sigma(m)$ and $\sigma(n)$] by multiplication. For example,

$$d(2 \cdot 5) = 4 = d(2) \cdot d(5),$$

$$d(3 \cdot 4) = 6 = d(3) \cdot d(4),$$

$$\sigma(2 \cdot 9) = 39 = \sigma(2) \cdot \sigma(9),$$

$$\sigma(4 \cdot 5) = 42 = \sigma(4) \cdot \sigma(5).$$

On the other hand, this cannot always be done, as the following examples illustrate:

$$d(3 \cdot 6) = 6 \neq 8 = d(3) \cdot d(6),$$

$$\sigma(4 \cdot 4) = 31 \neq 49 = \sigma(4) \cdot \sigma(4).$$

In the above examples, we have had success in saying that

$$d(mn) = d(m) \cdot d(n),$$

$$\sigma(mn) = \sigma(m) \cdot \sigma(n),$$

in every case that $(m,n) = 1$. We will prove this to be true shortly. These examples motivate the following definition.

Definition. If the function $f(n)$ is defined for all positive integers n, then we say that $f(n)$ is **multiplicative** if for all pairs of relatively prime positive integers m and n,

$$f(mn) = f(m) \cdot f(n).$$

If this is true for all pairs of positive integers, relatively prime or not, then we say that $f(n)$ is **completely multiplicative**.

As the examples above show, the concept of completely multiplicative functions eliminates some functions of interest that the broader concept of multiplicative function is able to consider. Examples of completely multiplicative functions are $f(n) = n$ and the constant function, $f(n) = 1$. The usefulness of a multiplicative function is that if we know what it is at prime powers, then we know what it is for all positive integers by multiplication; for example, if $d(n)$ is multiplicative, then

$$d(126) = d(2 \cdot 3^2 \cdot 7) = d(2) \cdot d(3^2) \cdot d(7) = 2 \cdot 3 \cdot 2 = 12.$$

It is usually, but not always, easy to evaluate multiplicative functions at prime powers, and this leads to general formulas for all integers. The methods of showing that $d(n)$ and $\sigma(n)$ are multiplicative are virtually identical. As a result, we will prove a more general result which will be useful later and from which we may instantly show that $d(n)$ and $\sigma(n)$ are multiplicative.

It may be useful to review the summation notation before continuing. The reader is no doubt familiar with the notation

$$\sum_{n=a}^{b} f(n),$$

which is defined for $a \leq b$ as

$$\sum_{n=a}^{b} f(n) = f(a) + f(a+1) + f(a+2) + \cdots + f(b-1) + f(b).$$

It frequently happens that we do not wish to add $f(n)$ for all n in an interval, but that we wish to add $f(n)$ for all n restricted in a certain manner. In this case, the restriction is usually put under the summation sign. For example,

$$\sum_{\substack{n=1 \\ n \text{ even}}}^{6} f(n) = f(2) + f(4) + f(6),$$

$$\sum_{\substack{p=4 \\ p \text{ prime}}}^{9} f(p) = f(5) + f(7),$$

$$\sum_{\substack{n=1 \\ n \text{ a perfect square}}}^{17} f(n) = f(1) + f(4) + f(9) + f(16) = \sum_{m=1}^{4} f(m^2),$$

$$\sum_{\substack{n=1 \\ n \mid 60}}^{19} f(n) = f(1) + f(2) + f(3) + f(4) + f(5) + f(6) + f(10) + f(12) + f(15).$$

This last type of sum occurs particularly often in number theory. In such cases, it is usual to drop the range of summation and, if necessary, add a new restriction under the summation sign. For example, the last sum above may be written

$$\sum_{\substack{n \mid 60, \\ 1 \leq n \leq 19}} f(n).$$

It is always assumed in this notation that we are speaking of only the positive divisors of an integer. Thus the preceding sum may just as well be written

$$\sum_{\substack{n \mid 60 \\ n \leq 19}} f(n),$$

and this is always done by mathematicians. Other examples of this notation

are

$$\sum_{d|10} f(d) = f(1) + f(2) + f(5) + f(10),$$

$$\sum_{\substack{d|12,\\ d<12}} f(d) = f(1) + f(2) + f(3) + f(4) + f(6),$$

$$\sum_{d|10} f(d)g\left(\frac{10}{d}\right) = f(1)g(10) + f(2)g(5) + f(5)g(2) + f(10)g(1),$$

$$\sum_{\substack{d_1|10,\\ d_2|10,\\ d_1d_2=10}} f(d_1)g(d_2) = f(1)g(10) + f(2)g(5) + f(5)g(2) + f(10)g(1),$$

$$\sum_{\substack{d_1|3,\\ d_2|10}} f(d_1d_2) = f(1\cdot 1) + f(1\cdot 2) + f(1\cdot 5) + f(1\cdot 10) + f(3\cdot 1) + f(3\cdot 2) + f(3\cdot 5) + f(3\cdot 10),$$

$$\sum_{d|30} f(d) = f(1) + f(2) + f(5) + f(10) + f(3) + f(6) + f(15) + f(30).$$

Notice that the third and fourth sums are the same, as are the fifth and sixth.

We are going to prove that if $f(n)$ is multiplicative, then so is the function $g(n)$ defined by

$$g(n) = \sum_{d|n} f(d).$$

Let us first illustrate the proof with a numerical example. We will show that $g(30) = g(3)g(10)$.

$$\begin{aligned}
g(3)g(10) &= \sum_{d_1|3} f(d) \cdot \sum_{d_2|10} f(d_2) \\
&= [f(1) + f(3)] \cdot [f(1) + f(2) + f(5) + f(10)] \\
&= f(1)f(1) + f(1)f(2) + f(1)f(5) + f(1)f(10) \\
&\quad + f(3)f(1) + f(3)f(2) + f(3)f(5) + f(3)f(10) \\
&= f(1\cdot 1) + f(1\cdot 2) + f(1\cdot 5) + f(1\cdot 10) \\
&\quad + f(3\cdot 1) + f(3\cdot 2) + f(3\cdot 5) + f(3\cdot 10) \\
&= f(1) + f(2) + f(5) + f(10) + f(3) + f(6) + f(15) + f(30) \\
&= \sum_{d|30} f(30) \\
&= g(30).
\end{aligned}$$

In the summation notation, this string of equalities may be written

$$\begin{aligned} g(3)g(10) &= \sum_{d_1|3} f(d_1) \cdot \sum_{d_2|10} f(d_2) \\ &= \sum_{\substack{d_1|3 \\ d_2|10}} f(d_1)f(d_2) \\ &= \sum_{\substack{d_1|3 \\ d_2|10}} f(d_1d_2) \\ &= \sum_{d|30} f(d) \\ &= g(30). \end{aligned}$$

This is exactly what will be done in general.

Theorem 2.15. If $f(n)$ is multiplicative, and $g(n)$ is defined as

$$g(n) = \sum_{d|n} f(d),$$

then $g(n)$ is multiplicative.

Proof. Suppose that $n > 0$, $m > 0$, $(m,n) = 1$. Our goal is to show that

$$g(m)g(n) = g(mn).$$

We begin by finding $g(m)g(n)$,

$$\begin{aligned} g(m)g(n) &= \sum_{d_1|m} f(d_1) \sum_{d_2|n} f(d_2) \\ &= \sum_{\substack{d_1|m \\ d_2|n}} f(d_1)f(d_2). \end{aligned} \tag{11}$$

If $d_1|m$, $d_2|n$, and n and m have no common factors greater than 1, it follows that d_1 and d_2 have no common factors greater than 1, or, in other words, $(d_1,d_2) = 1$. Thus by the definition of multiplicative functions, if d_1 and d_2 are positive and $d_1|m$, $d_2|n$, then

$$f(d_1)f(d_2) = f(d_1d_2).$$

Thus the expression in (11) becomes

$$g(m)g(n) = \sum_{\substack{d_1|m \\ d_2|n}} f(d_1d_2). \tag{12}$$

By Theorem 2.14, the set of numbers d_1d_2, where d_1 and d_2 are positive divisors of m and n, is exactly the set of positive divisors of mn, and no

duplications occur. Therefore, we may put (12) in the form

$$\begin{aligned} g(m)g(n) &= \sum_{d|mn} f(d) \\ &= g(mn), \end{aligned}$$

and hence $g(n)$ is multiplicative. ▲

As immediate consequences of Theorem 2.15, we have

Theorem 2.16. The functions $d(n)$ and $\sigma(n)$ are multiplicative.

Proof. The function $f(n) = 1$ is multiplicative and

$$d(n) = \sum_{d|n} f(d),$$

since the sum on the right adds 1 as many times as there are positive divisors of n. By Theorem 2.15, $d(n)$ is multiplicative.

The function $f(n) = n$ is multiplicative and

$$\sigma(n) = \sum_{d|n} f(d).$$

Hence $\sigma(n)$ is also multiplicative. ▲

The facts that $d(n)$ and $\sigma(n)$ are multiplicative enable us to evaluate them in terms of the factorization of n into primes.

Theorem 2.17. If the factorization of n into primes is given by

$$n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k},$$

then

$$d(n) = (a_1 + 1)(a_2 + 1) \cdots (a_k + 1)$$

and

$$\begin{aligned} \sigma(n) &= (1 + p_1 + p_1^2 + \cdots + p_1^{a_1})(1 + p_2 + p_2^2 + \cdots + p_2^{a_2}) \cdots \\ &\quad \cdots (1 + p_k + p_k^2 + \cdots + p_k^{a_k}) \\ &= \frac{p_1^{a_1+1} - 1}{p_1 - 1} \frac{p_2^{a_2+1} - 1}{p_2 - 1} \cdots \frac{p_k^{a_k+1} - 1}{p_k - 1}. \end{aligned}$$

Proof. If p is a prime and $a \geq 1$, then the divisors of p^a are $1, p, p^2, \ldots, p^a$. Hence

$$d(p^a) = a + 1$$

and

$$\begin{aligned}\sigma(p^a) &= 1 + p + p^2 + \cdots + p^a \\ &= \frac{p^{a+1} - 1}{p - 1}.\end{aligned}$$

The last equality utilized the formula for the sum of a finite number of terms of a geometric progression (first term equals 1, and common ratio equals p). The result of the theorem now follows from the multiplicative properties of $d(n)$ and $\sigma(n)$ derived in Theorem 2.16. ▲

As an example, the factorization of 20 into primes is

$$20 = 2^2 \cdot 5^1$$

and hence

$$d(20) = (2 + 1)(1 + 1) = 6,$$

$$\sigma(20) = \left(\frac{2^3 - 1}{2 - 1}\right)\left(\frac{5^2 - 1}{5 - 1}\right) = \frac{7}{1} \cdot \frac{24}{4} = 42.$$

These results are of course the same as those listed in Figure 2.1.

The function $\sigma(n)$ has been an object of interest since before the time of Euclid. The ancients considered the function

$$\sigma(n) - n = \sum_{\substack{d|n \\ d<n}} d,$$

or, in words, the sum of the positive divisors of n other than n itself. This function is not multiplicative, as the example

$$\sigma(6) - 6 = 6 \neq 1 \cdot 1 = (\sigma(2) - 2) \cdot (\sigma(3) - 3)$$

shows. This is the reason that $\sigma(n)$ is usually investigated today rather than $\sigma(n) - n$. Certain integers n (such as $n = 6$) have the property that

$$\sigma(n) - n = n.$$

The ancients believed that such numbers had mystical properties and called them **perfect numbers**. A somewhat larger example than 6 of a perfect number is $2^{11212}(2^{11213} - 1)$,[1] which has 6751 digits. Euler knew the form of all even perfect numbers. He showed that an even perfect number must be of the following form (Euclid had shown such numbers to be perfect):

$$n = 2^{p-1}(2^p - 1),$$

[1] As this is being written, $2^{11213} - 1$ is the largest number that has been proved to be a prime.

where both p and $(2^p - 1)$ are primes. To this day, it is not known if there are infinitely many perfect numbers, nor is it known if there are any odd perfect numbers. It is known that there are no odd perfect numbers less than 10^{20}, but in view of the examples in Section 1.1, this should not be regarded as conclusive evidence that there are no odd perfect numbers.

EXERCISES

1. Verify that 6, 28, and 496 are perfect numbers.
2. The Greeks defined the numbers m and n to be **amicable** if

$$\sigma(m) - m = n, \qquad \sigma(n) - n = m.$$

   The amicable numbers 220 and 284 were known to Pythagoras. Verify that they are amicable.
3. Find $\sigma(n) - n$ for $n = 1184$ and $n = 1210$.
4. Find $\sigma(n) - n$ for $n = 12\,496 = 2^4 \cdot 11 \cdot 71$, $n = 14\,288 = 2^4 \cdot 19 \cdot 47$, $n = 15\,472 = 2^4 \cdot 967$, $n = 14\,536 = 2^3 \cdot 23 \cdot 79$, and $n = 14\,264 = 2^3 \cdot 1783$. These numbers were found by Poulet in 1918.
5. Prove that if $2^p - 1$ is a prime, then

$$n = 2^{p-1}(2^p - 1)$$

   is a perfect number.
6. Find an integer n less than or equal to 70 such that $d(n) = 12$.
7. Find an integer n such that

$$\sigma(n) = 546.$$

8. Let $\sigma_2(n)$ be the sum of the squares of the positive divisors of n. Show that $\sigma_2(n)$ is multiplicative and show that if

$$n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k},$$

   then

$$\sigma_2(n) = \frac{p_1^{2a_1+2} - 1}{p_1^2 - 1} \cdot \frac{p_2^{2a_2+2} - 1}{p_2^2 - 1} \cdots \frac{p_k^{2a_k+2} - 1}{p_k^2 - 1}$$

9.* Show that if n is a perfect square, then $\sigma(n) | \sigma_2(n)$ (see problem 8). Give an example of an integer n such that $\sigma(n) \nmid \sigma_2(n)$.

10.* We seem to have done more in problem 5 than Euler's result says that we can do since we did not require that p be a prime number. Prove that if $2^n - 1$ is a prime, then n is a prime. (*Hint:* If n is composite, show $2^n - 1$ may be factored.)

2.5. Linear Diophantine Equations

With this title, we could investigate 20 linear equations in 37 unknowns, but we will stick to one equation in two unknowns. Our aim is to either find all integers x and y which satisfy the equation

$$ax + by = c$$

(a, b, and c are integers) or show that there are none.

Theorem 2.18. Suppose that a and b are nonzero integers and $d = (a,b)$. If $d \nmid c$, then the equation

$$ax + by = c \tag{13}$$

has no integral solutions. If $d|c$, then the equation has infinitely many solutions. If $x = x_0$, $y = y_0$ is one integral solution to (13), then all integral solutions to (13) are given by

$$\begin{aligned} x &= x_0 + t\frac{b}{d}, \\ y &= y_0 - t\frac{a}{d}, \end{aligned} \tag{14}$$

where t is an integer.

Proof. Since $d|a$, $d|b$, it follows that $d|(ax + by)$ for all integers x and y. Thus if

$$ax + by = c,$$

then $d|c$. Hence (13) has no solutions if $d \nmid c$. Suppose now that $d|c$. Then there is an integer e such that

$$c = de.$$

By Theorem 2.2, there are integers r and s such that

$$ar + bs = d.$$

Hence

$$a(re) + b(se) = de = c$$

and (13) has an integral solution. If

$$ax_0 + by_0 = c, \tag{15}$$

then

$$a\left(x_0 + t\frac{b}{d}\right) + b\left(y_0 - t\frac{a}{d}\right) = ax_0 + by_0 = c,$$

and hence (13) has infinitely many solutions, among them being the infinitely many given in (14).

It remains to show that every solution of (13) can be put in the form of (14). Suppose that x and y are integers which satisfy (13). If we subtract (15) from (13), we get

$$a(x - x_0) + b(y - y_0) = 0$$

or

$$\frac{a}{d}(x - x_0) = -\frac{b}{d}(y - y_0). \tag{16}$$

Thus

$$\frac{b}{d}\Big|\frac{a}{d}(x - x_0), \qquad \text{but} \quad \left(\frac{b}{d}, \frac{a}{d}\right) = 1$$

by Theorem 2.4, and hence, by Theorem 2.6,

$$\frac{b}{d}\Big|(x - x_0).$$

Thus there is an integer t such that

$$x - x_0 = t\frac{b}{d}. \tag{17}$$

If we substitute this in (16), we get

$$\frac{a}{d} \cdot t\frac{b}{d} = -\frac{b}{d}(y - y_0)$$

and hence

$$y - y_0 = -t\frac{a}{d}.$$

From this and (17), we get

$$x = x_0 + t\frac{b}{d},$$

$$y = y_0 - t\frac{a}{d},$$

and thus every solution to (13) may be written in the form of (14). ▲

When a and b are small, it is frequently possible to find a solution to (13) by inspection. Otherwise the Euclidean algorithm gives us a systematic method of finding a particular solution to (13) (assuming that $d|c$). For example, suppose that we wish to solve the equation

$$12x + 25y = 331. \tag{18}$$

We first use the Euclidean algorithm to express (12,25) in terms of 12 and 25. Since

$$25 = 2 \cdot 12 + 1,$$

$$12 = 12 \cdot 1,$$

we see that $(12,25) = 1$ and

$$-2 \cdot 12 + 1 \cdot 25 = 1.$$

If we multiply this through by 331, we find

$$12(-662) + 25(331) = 331$$

and thus

$$x = -662, \qquad y = 331$$

is a particular solution to (18). The general solution to (18) is then given as

$$x = -662 + 25t, \qquad y = 331 - 12t. \tag{19}$$

It is interesting to note that (18) has a unique solution in nonnegative integers. If $x \geq 0$, then, by (19),

$$-662 + 25t \geq 0$$

$$25t \geq 662$$

$$t \geq \tfrac{662}{25} = 26 + \tfrac{12}{25}.$$

If $y \geq 0$, then by (19),

$$331 - 12t \geq 0$$

$$331 \geq 12t$$

$$27 + \tfrac{7}{12} = \tfrac{331}{12} \geq t.$$

Thus if $x \geq 0$ and $y \geq 0$, then

$$26 + \tfrac{12}{25} \leq t \leq 27 + \tfrac{7}{12},$$

and the only integer in this range is $t = 27$. If we put $t = 27$ into (19), then we get

$$x = 13, \qquad y = 7$$

as the only solution to (18) in nonnegative integers.

The fact that some Diophantine equations have unique solutions in positive integers leads to the possibility of being able to completely solve certain "word problems" without having as many equations available as unknowns. For example, consider the following problem: Jimmy bought a certain number of regular-size comic books at 12 cents apiece and a certain number of "giant"-size comic books at 25 cents apiece. If Jimmy spent \$3.31 altogether, how many comic books did he buy? If we let x be the number of regular size and y the number of giant-size comic books that Jimmy bought, then x and y are related by equation (18). Clearly, x and y are restricted to being nonnegative integers by the problem and thus, as was shown above, $x = 13$, $y = 7$. Therefore Jimmy bought 20 comic books altogether.

There is one last item that we will discuss here since it sometimes causes confusion. Since $x = 13$, $y = 7$ is a solution to (18), it follows from Theorem 2.18 that all solutions to (18) can be written in the form

$$\begin{aligned} x &= 13 + 25T, \\ y &= \ \ 7 - 12T. \end{aligned} \tag{20}$$

This seems to contradict what we derived in (19), but it does not. Equations (19) and (20) are connected by the relation

$$T = t - 27.$$

For example, the solution $x = 38$, $y = -5$ to (18) is given by $t = 28$ in (19) and $T = 1$ in (20). The form of the final answer depends on which particular solution is used in expressing it. There are infinitely many ways of writing the solution to (18). The reader should remember this if his answer to some of the exercises differs from the answer given at the back of the book.

EXERCISES

In problems 1–6, either find all integral solutions to the given equation or show that it has none.

1. $3x + 2y = 1$.
2. $3x - 2y = 1$.
3. $17x + 14y = 4$.
4. $33x - 12y = 9$.
5. $91x + 221y = 15$.
6. $401x + 503y = 20$.

In problems 7–10, find all solutions in positive integers to the given equation or show that there are none.

7. $23x - 7y = 1$.
8. $9x + 11y = 79$.
9. $39x + 47y = 4151$.
10. $5x + 6y = 50$. (You may check your answer by looking at the stars on an American flag.)
11. Harold and Betty find that their house is $\frac{39}{12}$ of a Harold length plus $\frac{59}{10}$ of a Betty length long. They find this hard to remember and would much prefer integral Harold and Betty lengths. Can this be done if Harold is 6 feet tall and Betty is 5 feet tall?
12. A grocer sells a 1-gallon container of milk for 79 cents and a $\frac{1}{2}$-gallon container of milk for 41 cents. At the end of the day he sold \$63.58 worth of milk. How many 1-gallon and $\frac{1}{2}$-gallon containers did he sell?

*13. A teacher has been designing a word problem for a number theory examination. Thus far he has decided on the following outline for his problem. A furniture dealer used to sell 49 black-and-white TV sets a week at \$70 apiece with a profit of 30 percent on each set. Since the advent of color TV, black-and-white TV sets became cheaper at the wholesale level, but the dealer has kept his price at \$70 a set and now he makes 40 percent on each set. However, in order to capture a greater share of the color-TV market, the dealer has reduced his profit on color-TV sets to 19 percent per set, which enables him to sell color-TV sets for only \$300 apiece. The dealer's total sales in TV sets last week was d dollars. How did his profits last week compare with the days before color TV?

The teacher desires to have the answer come out that the dealer made \$13 more with his present arrangements. What value of d should he use in his problem to get the desired answer? With this value of d, will the teacher's students get a unique answer?

MISCELLANEOUS EXERCISES

1. Show that $(a,b,c) = ((a,b),c)$ provided that a and b are not both 0.
2. Show that if m and n are positive, then

$$\frac{mn}{(m,n)}$$

is the least common multiple of m and n (that is, the smallest positive integer divisible by both m and n).

3. Show that if

$$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 = 0,$$

where $a_0, a_1, \ldots, a_n$ are integers and $x = r/s$ is rational, $(r,s) = 1$, then $s|a_n$ and $r|a_0$. (In applications, it must be remembered that r/s may be negative.) In particular, show that if $a_n = 1$ and x is rational, then x is an integer.

4. If $ax^2 + bx + c = 0$, then, as is well known,

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

Reconcile this with problem 3, which says that if x is rational, then the denominator of x divides a.

5. Suppose that b and c are integers and that

$$r = -b + \sqrt{b^2 - c}$$

is rational. Since r is a root of the equation

$$x^2 + 2bx + c = 0,$$

it follows from problem 3 that r is an integer and $r|c$. Prove this directly.

6. Prove that $(a^2,b^2) = (a,b)^2$.

7. Factor the numbers 1 456 813, 1 468 823, 1 476 221, and 1 488 391 into primes (and prove that you have primes when you are done), given only that none of these numbers have any prime factors less than 35 and

$$1\,456\,813 \cdot 1\,488\,391 = 1\,468\,823 \cdot 1\,476\,221.$$

8. Show that if there are integral solutions to the equation

$$ax + by + cz = e,$$

then $(a,b,c)|e$. Suppose that $(a,b,c)|e$. Show that there are integers w and z such that

$$(a,b)w + cz = e$$

(see problem 1). Then show that there are integers x and y such that

$$ax + by = (a,b)w.$$

(This same technique works for one equation in n unknowns. Solutions may be found—when they exist—by the analogous process of converting the equation to $n - 1$ successive equations in two unknowns.)

9. Use the method of problem 8 to find all the integral solutions of the equation

$$323x + 391y + 437z = 10473.$$

Your answer should have two integer variables in it. Find all positive solutions.

10. When Mr. Smith returned from Europe in 1966, he found that he had in his possession 35 British sixpence coins, 55 French ten-centime pieces, and 77 Greek drachmas. Mr. Smith converted each of these coins to its value in American money (rounded off to the nearest cent) and found that the total was worth \$5.86. How much was each coin worth in 1966 (to the nearest cent)? If the phrase "rounded off to the nearest cent" were dropped from the problem, would your answer above necessarily be near the correct coin values?
11. For $n > 0$, show that if $2^n + 1$ is a prime, then n is a power of 2.
12. We may use the unique factorization theorem to give another proof (due to Euler) that there are infinitely many primes. Assume that there are only finitely many primes, $p_1, p_2, \ldots, p_k$. Prove that

$$\left(\sum_{a_1=0}^{\infty} \frac{1}{p_1^{a_1}}\right)\left(\sum_{a_2=0}^{\infty} \frac{1}{p_2^{a_2}}\right)\cdots\left(\sum_{a_k=0}^{\infty} \frac{1}{p_k^{a_k}}\right)$$
$$= \left[\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_k}\right)\right]^{-1}.$$

The product of the finite number of series on the left will converge absolutely since each series is absolutely convergent. Show that the product of the series on the left is

$$\sum_{n=1}^{\infty} \frac{1}{n},$$

which diverges. Hence there are infinitely many primes.

13. Prove that n is a common divisor of a, b, and c if and only if n is a divisor of (a,b,c).

Chapter 3

CONGRUENCES

3.1. Introduction

We may thank Gauss for the exceedingly useful concept of congruences. Some of the results of this chapter were known earlier, but Gauss was the first to systematically develop the subject.

Definition. Let a and b be integers and n a positive integer. If $n|(a - b)$, then we say that a is **congruent** to b **modulo** n, and we write

$$a \equiv b(\text{mod } n).$$

We also write $a \not\equiv b(\text{mod } n)$ when we wish to say that a is not congruent to b modulo n. This is equivalent to saying that $n \not| (a - b)$.

Thus by the definition of divisibility, $a \equiv b(\text{mod } n)$ if and only if there exists k such that $a = b + kn$. For example,

$$\begin{aligned} 37 &\equiv \quad 25(\text{mod } 12), \\ -9 &\equiv \quad 31(\text{mod } 10), \\ 7216 &\equiv 29\,216(\text{mod } 1000), \\ 5 &\not\equiv \quad 7(\text{mod } 3). \end{aligned}$$

Congruences occur in everyday life. Ordinary clocks and wrist watches measure hours (mod 12). Days of the week measure days (mod 7). A car speedometer (technically an odometer) measures mileage (mod 100 000). A speedometer that reads 51 937 does not say (even if it has not been tampered with) that the car has driven 51 937 miles; the fact that this is the unanimous interpretation is a comment on today's low-quality production methods, which virtually ensure that no car will last 151 937 miles.

The congruence sign, $\equiv$, resembles an equal sign. This is particularly appropriate since congruences possess many of the properties of ordinary equality. As an illustration, suppose that a and b are positive integers and

$$a \equiv b(\text{mod } 1000).$$

This says that

$$1000|(a - b),$$

or, in other words, the last three digits of $(a - b)$ are zeros. Thus the last three digits of a and b must be the same. Conversely, if the last three digits of a and b are the same, then

$$1000|(a - b)$$

and hence

$$a \equiv b(\text{mod } 1000).$$

Therefore, two positive integers are congruent modulo 1000 if and only if their last three digits agree. If you think about it for a minute, you will realize that the last three digits of the sum and product of two positive integers depends only on the last three digits of the two integers. Thus, if a, b, c, and d are positive integers and

$$a \equiv b(\text{mod } 1000), \qquad c \equiv d(\text{mod } 1000),$$

then

$$a + c \equiv b + d(\text{mod } 1000), \qquad ac \equiv bd(\text{mod } 1000).$$

We will shortly prove these rules for all moduli n.

The above result on products modulo 1000 has an amusing application. A beginning mind reader asks a person to think of a number from 1 to 999, multiply it by 143, and state the last three digits of the answer. Once this is done, the mind reader promptly states the original number used and explains that being a beginner, he needed to make the person concentrate on his original number and hence the multiplication by 143. On the other hand, he did not want the audience to think that he was merely able to rapidly divide by 143, and hence he asked for only the last three digits of the answer.

The "mind reader" is of course no such thing. He simply takes the three-digit number given to him and multiplies by 7. The last three digits of the answer gives the original number. For instance, if 492 is the number thought of originally, then the last three digits of $492 \cdot 143$ $(= 70\,356)$ are 356. The product of 7 and 356 is 2492, the last three digits of which give the original number. The only remaining question is: Why does this work?

The trick is based on the fact that

$$7 \cdot 143 = 1001.$$

If x is any three-digit integer, then $1001x$ is simply two copies of x, for instance $1001 \cdot 492 = 492\,492$. The whole process of multiplying by 143, taking the last three digits and multiplying by 7, and taking the last three digits reduces to the process of multiplying by 1001 and taking the last three digits, thus getting the original number. In terms of congruences, we wish to find a three-, two-, or one-digit number, x. We are told only that a given number b consists of the last three digits of $143x$. Thus we are given the congruence

$$143x \equiv b \pmod{1000}.$$

Clearly,

$$7 \equiv 7 \pmod{1000};$$

we may multiply these congruences together and get

$$7 \cdot 143x \equiv 7b \pmod{1000},$$

or

$$1001x \equiv 7b \pmod{1000}.$$

Since

$$1001 \equiv 1 \pmod{1000}$$

and

$$x \equiv x \pmod{1000},$$

we see that

$$1001x \equiv x \pmod{1000}$$

and therefore

$$x \equiv 7b \pmod{1000}.$$

This says that the last three digits of $7b$ and the last three digits of x agree. Since x has at most three digits, the last three digits of $7b$ give x completely.

What the "mind-reading" trick really boils down to is solving the congruence equation

$$143x \equiv b \pmod{1000}$$

for x. We will look into such problems later in the chapter.

EXERCISES

1. True or false? $17 \equiv 2 \pmod 5$, $14 \equiv -6 \pmod{10}$, and $97 \equiv 5 \pmod{13}$.
2. Verify that $3 \cdot 5 \equiv 3 \cdot 13 \pmod 4$, $7 \cdot 18 \equiv 7(-2) \pmod{10}$, and $3 \cdot 4 \equiv 3 \cdot 14 \pmod 6$.
3. Which of the following are valid? $5 \equiv 13 \pmod 4$, $18 \equiv -2 \pmod{10}$, and $4 \equiv 14 \pmod 6$.

Problems 2 and 3 combined show that the assertion "If $ab \equiv ac \pmod n$, then $b \equiv c \pmod n$" is not always correct, even if $a \not\equiv 0$.

4. Find a if $a \equiv 97 \pmod 7$ and $1 \leq a \leq 7$.
5. Find a if $a \equiv 32 \pmod{19}$ and $52 \leq a \leq 70$.
6. Show that, modulo 1000, adding 999 to a number is the same as subtracting 1.
7. Prove that if $a \equiv b \pmod n$, then $a + c \equiv b + c \pmod n$.
8. Prove that if $a \equiv b \pmod n$, then $ac \equiv bc \pmod n$.
9. Why did we restrict a and b to be positive integers when we said that "$a \equiv b \pmod{1000}$ if and only if the last three digits of a and b are the same"?
10. At 5 P.M. (Eastern Standard Time), Dec. 7, 1967, how many hours had passed (mod 24) in New York City since the beginning of the century?
11. If n is positive, show that $n|a$ if and only if $a \equiv 0 \pmod n$.

3.2. Fundamental Properties of Congruences

Theorem 3.1. Let n be a positive integer. For all integers a,

$$a \equiv a \pmod n.$$

If $a \equiv b \pmod n$, then $b \equiv a \pmod n$. If $a \equiv b \pmod n$ and $b \equiv c \pmod n$, then $a \equiv c \pmod n$.

Proof. Since $n|0$, $a \equiv a \pmod n$ by definition. If $a \equiv b \pmod n$, then $n|(a - b)$. Thus n divides $(-1)(a - b) = (b - a)$ and therefore $b \equiv a \pmod n$. Finally, if $a \equiv b \pmod n$ and $b \equiv c \pmod n$, then $n|(a - b)$ and $n|(b - c)$. Therefore, n divides the number

$$(a - b) + (b - c) = a - c$$

and hence $a \equiv c \pmod n$. ▲

Theorem 3.1 is analogous to the corresponding result for equalities. It will be used in many ways usually without specific mention. For example, because of Theorem 3.1, we may write something like

$$a \equiv b \equiv c \equiv d \equiv e \equiv f \pmod n$$

and immediately infer that $a \equiv f \pmod{n}$. As another example, this theorem is the justification for the inference

$$\text{"}1001x \equiv 7b \pmod{1000} \text{ and } 1001x \equiv x \pmod{1000};$$
$$\text{therefore, } x \equiv 7b \pmod{1000},\text{"}$$

which was used in Section 3.1.

Theorem 3.2. If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then

$$a + c \equiv b + d \pmod{n}, \qquad a - c \equiv b - d \pmod{n}, \qquad ac \equiv bd \pmod{n}.$$

If $a \equiv b \pmod{n}$, then for all c,

$$a + c \equiv b + c \pmod{n}, \qquad a - c \equiv b - c \pmod{n}, \qquad ac \equiv bc \pmod{n}.$$

Proof. Since

$$(a + c) - (b + d) = (a - b) + (c - d),$$
$$(a - c) - (b - d) = (a - b) - (c - d),$$
$$ac - bd = c(a - b) + b(c - d),$$

the first part of the theorem follows from Theorem 1.2 and the definition of congruence. By Theorem 3.1, $c \equiv c \pmod{n}$ for all c, and thus the second part of the theorem is a special case of the first part. ▲

We illustrate Theorem 3.2 by solving the following word problem. The town of Anyplace, U.S.A., derives its principal income from fines paid by nonresidents cited for speeding while passing through town. Mr. Storer, who as a boy was cited for bicycling down Main Street at 100 miles an hour, finds to his horror that he must go to Anyplace every seven months on business starting in October. Thus it occurred that every seven months beginning in October, Mr. Storer received a speeding citation. The first citation came in October, the second in the following May, the third in December, and so on. Which were the first two citations in the series that were received in January?

We assign the numbers $1, 2, 3, \ldots, 12$ to the months January, February, March, ..., December, respectively. October is assigned the number 10 and January the number 1. Thus we wish to find x, where

$$10 + 7(x - 1) \equiv 1 \pmod{12}$$

(the expression on the left is not merely $10 + 7x$, since the first citation, rather than the zeroth, occurred in the tenth month of the year). Hence

$$7x \equiv -2 \pmod{12}. \tag{1}$$

If we subtract (1) from the obviously true congruence,

$$12x \equiv 0 (\text{mod } 12),$$

we get

$$5x \equiv 2 (\text{mod } 12). \tag{2}$$

Subtracting (2) from (1) gives

$$2x \equiv -4 \equiv 8 (\text{mod } 12). \tag{3}$$

Doubling (3) gives

$$4x \equiv 16 \equiv 4 (\text{mod } 12),$$

and if we subtract this from (2) we see that

$$x \equiv -2 \equiv 10 (\text{mod } 12).$$

Therefore,

$$x = 10 + 12k;$$

the first two positive values of x that result are $x = 10$ and 22. These values satisfy the original equation and hence the first two citations received by Mr. Storer in the month of January were the tenth and twenty-second of the series.

The reader has possibly noticed that we had the opportunity to divide both sides of (3) by 2. Such a division would have given us the incorrect result

$$x \equiv 4 (\text{mod } 12).$$

The conditions under which one can divide both sides of a congruence are given in the next theorem.

Theorem 3.3. If $(a,n) = 1$ and $ab \equiv ac (\text{mod } n)$, then $b \equiv c (\text{mod } n)$. More generally, if $(a,n) = d$ and $ab \equiv ac (\text{mod } n)$, then $b \equiv c (\text{mod } n/d)$.

Proof. Suppose that $(a,n) = d$ and $ab \equiv ac (\text{mod } n)$. Then there is an integer k such that

$$ab = ac + kn. \tag{4}$$

Let

$$a_1 = \frac{a}{d}, \qquad n_1 = \frac{n}{d};$$

these numbers are integers and

$$(a_1,n_1) = \left(\frac{a}{d},\frac{n}{d}\right) = 1.$$

We divide (4) by d and get

$$a_1(b - c) = kn_1 \tag{5}$$

and thus $a_1|kn_1$. Since $(a_1,n_1) = 1$, $a_1|k$ by Theorem 2.6. Thus there is an integer k_1 such that $k = a_1k_1$. It follows from (5) that

$$b - c = k_1n_1$$

or, in other words, $n_1|(b - c)$. Therefore, by definition,

$$b \equiv c(\text{mod } n_1). \qquad \blacktriangle$$

There is another very important fact about congruences that we shall prove here. We first prove that any integer is congruent modulo n to exactly one of the numbers $0, 1, 2, \ldots, n - 1$. We show this as follows. Given an integer a, the division algorithm says that we may write it in the form

$$a = qn + r, \qquad 0 \leq r < n.$$

Thus

$$a \equiv qn + r \equiv q \cdot 0 + r \equiv r(\text{mod } n)$$

and hence a is congruent, modulo n, to at least one of the numbers $0, 1, 2, \ldots, n - 1$. Suppose that r_1 and r_2 are two different integers in the range $0, 1, \ldots, n - 1$ and that

$$a \equiv r_1(\text{mod } n), \qquad a \equiv r_2(\text{mod } n).$$

We may as well assume that $r_1 > r_2$. We see that

$$r_1 \equiv r_2(\text{mod } n)$$

and hence

$$n|(r_1 - r_2).$$

But

$$0 < r_1 - r_2 \leq (n - 1) - (0) < n;$$

that is, $r_1 - r_2$ is a positive number less than n. As such, it cannot be divisible by n and therefore a cannot be congruent to two different numbers in the range 0 to $n - 1$. Thus each integer is congruent (mod n) to exactly one of

the numbers $0, 1, \ldots, n-1$, as stated. The numbers $0, 1, \ldots, n-1$ give one example of a complete system of residues (mod n).

Definition. A set of n integers, $a_1, a_2, \ldots, a_n$, is called a **complete system of residues** (or a **complete residue system**) (mod n) if every integer is congruent (mod n) to exactly one of the a_j's.

The reason for restricting the definition to n integers is that if the set $a_1, a_2, \ldots, a_r$ has the properties of the definition, then $n = r$. This is easy to show and is left to problems 17 and 18 at the end of the section. Note that for a complete residue system (a_j), if $j \neq k$, then $a_j \not\equiv a_k \pmod{n}$, as otherwise a_j would be congruent (mod n) to two members of the system: itself and a_k.

Theorem 3.4. Any set of n consecutive integers is a complete residue system (mod n).

Proof. We have already seen that the set $0, 1, 2, \ldots, n-1$ is a complete residue system (mod n). Let b be the first of n consecutive integers which are then given by $b, b+1, b+2, \ldots, b+n-1$. Given an integer a, there is, by the definition of a complete residue system, an integer j in the range $0 \leq j \leq n-1$ such that

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

Therefore,

$$a \equiv b + j \pmod{n}$$

and hence any integer is congruent to at least one of the numbers $b, b+1, \ldots, b+n-1$. Suppose that j_1 and j_2 are different integers in the range $0 \leq j \leq n-1$ and there is an integer a such that

$$a \equiv b + j_1 \pmod{n}, \qquad a \equiv b + j_2 \pmod{n}.$$

Then

$$a - b \equiv j_1 \pmod{n}, \qquad a - b \equiv j_2 \pmod{n}$$

and thus $a - b$ is congruent (mod n) to two distinct members of the complete residue system (mod n), $0, 1, 2, \ldots, n-1$, which is impossible. Hence every integer is congruent (mod n) to exactly one of the n integers $b, b+1, \ldots, b+n-1$; this set is therefore a complete system of residues (mod n). ▲

The most commonly used complete systems of residues (mod n) are the sets

$$0, 1, 2, \ldots, n-1;$$

$$1, 2, 3, \ldots, n;$$

and when n is odd,

$$-\frac{n-1}{2}, -\frac{n-1}{2}+1, \ldots, -1, 0, 1, \ldots, \frac{n-1}{2}-1, \frac{n-1}{2}.$$

This last set is often given (for odd n) as the set of all integers j with the property that

$$|j| < \frac{n}{2}$$

(for example, when $n = 5$, the numbers j such that $|j| < \frac{5}{2}$ are $-2, -1, 0, 1, 2$).

The fact that the numbers $0, 1, \ldots, n-1$ give a complete system of residues (mod n) says that any combination of sums, differences, and products of these numbers is congruent (mod n) to a unique integer of the system. This leads to the concept of arithmetic (mod n) or, as it is sometimes called, modular arithmetic. Figures 3.1 and 3.2 show the tables for addition and multiplication (mod 5) and (mod 6), respectively.

It follows from Theorem 3.2 that many of the usual laws of arithmetic are valid for arithmetic (mod n). For instance, the law

$$a(b + c) = ab + ac$$

a \ b	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$a + b$ (mod 5)

a \ b	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

ab (mod 5)

Figure 3.1. Arithmetic (mod 5).

a \ b	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

$a + b \pmod 6$

a \ b	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

$ab \pmod 6$

Figure 3.2. Arithmetic (mod 6).

becomes

$$a(b + c) \equiv ab + ac \pmod n. \tag{6}$$

The reason that this is not an utter triviality in arithmetic (mod n) is that the numbers $b + c$, ab, ac found by the arithmetic (mod n) tables are, as likely as not, different from the usual sums and products. Thus (6) becomes a statement of the fact that when $a(b + c)$ is reduced (mod n) in two different ways to the complete system of residues $0, 1, \ldots, n - 1$, the results are the same. For example, by Figure 3.1,

$$3(4 + 4) \equiv 3(3) \equiv 4 \pmod 5,$$

$$3 \cdot 4 + 3 \cdot 4 \equiv 2 + 2 \equiv 4 \pmod 5.$$

We may put arithmetic (mod n) to another use. For example, we see in Figure 3.1 that the numbers $0^2, 1^2, 2^2, 3^2$, and 4^2 are congruent (mod 5) to one of the numbers 0, 1, and 4. Since the numbers 0, 1, 2, 3, and 4 give a complete system of residues (mod 5), every integer squared is congruent to either 0, 1, or 4 (mod 5). Thus, although there are infinitely many perfect squares, none of them leave the remainder 2 or 3 when divided by 5![1] It is not uncommon to find people who think that five verifications surely proves the theorem. Here it has actually happened.

The next theorem has many applications. We give a few of the more interesting applications immediately after its proof.

[1] This is not to be interpreted as five factorial (there would then be a period following the exclamation mark).

Theorem 3.5. Let $f(x)$ be a polynomial with integral coefficients. If $a \equiv b(\text{mod } n)$, then

$$f(a) \equiv f(b)(\text{mod } n).$$

Proof. Let

$$f(x) = a_k x^k + a_{k-1}x^{k-1} + \cdots + a_1 x + a_0,$$

where $a_0, a_1, \ldots, a_k$ are integers. Then by Theorem 3.2,

$$a_k a^k + a_{k-1}a^{k-1} + \cdots + a_0 \equiv a_k b^k + a_{k-1}b^{k-1} + \cdots + a_0(\text{mod } n);$$

that is,

$$f(a) \equiv f(b)(\text{mod } n). \qquad \blacktriangle$$

As our first application of Theorem 3.5, we show that there is no polynomial $f(x)$ with integral coefficients and degree ≥ 1 such that $f(a)$ is a prime for all integers a. Let

$$f(x) = a_k x^k + a_{k-1}x^{k-1} + \cdots + a_0,$$

where $a_0, a_1, \ldots, a_k$ are integers and $a_k \neq 0$. If $a_k > 0$, then $f(x) \to +\infty$ as $x \to +\infty$, while if $a_k < 0$, then $f(x) \to -\infty$ as $x \to +\infty$. Since the word prime has been defined to mean positive, we let $a_k > 0$. The same proof would show that if $a_k < 0$, we do not always get negative primes. Since $f(x) \to \infty$ as $x \to \infty$, we can take the integer a sufficiently large to ensure that

$$n = f(a) > 1.$$

Just because we have used the letter n does not mean that n is not a prime. Let j be so large that

$$f(a + jn) > n;$$

this is again possible since $f(x) \to \infty$ as $x \to \infty$. But

$$a + jn \equiv a(\text{mod } n)$$

and hence, by Theorem 3.5,

$$f(a + jn) \equiv f(a) \equiv n \equiv 0(\text{mod } n).$$

Thus

$$n \mid f(a + jn),$$

and since

$$1 < n < f(a + jn),$$

$f(a + jn)$ is not a prime.

As another illustration, we show that every positive integer is congruent to the sum of its digits (mod 9). Let $n > 0$ have the decimal representation

$$n = a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + \cdots + a_1 \cdot 10 + a_0,$$

where for all j, $0 \leq a_j \leq 9$; the numbers $a_0, \ldots, a_k$ are thus the digits of the number n. Let

$$f(x) = a_k x^k + a_{k-1} x^{k-1} + \cdots + a_1 x + a_0.$$

Theorem 3.5 says that

$$f(10) \equiv f(1) (\text{mod } 9);$$

that is,

$$n \equiv a_k + a_{k-1} + \cdots + a_0 (\text{mod } 9),$$

which was to be shown. For example,

$$\begin{aligned} 139\,854\,872 &\equiv 1 + 3 + 9 + 8 + 5 + 4 + 8 + 7 + 2 \\ &\equiv 47 \equiv 4 + 7 \equiv 11 \equiv 1 + 1 \equiv 2 (\text{mod } 9). \end{aligned}$$

Usually one does not actually sum the digits of n as we did above, but rather one sums them (mod 9). In particular, one may neglect any 9's that show up or any combination of numbers that add up to 9. In the above calculation, for example, one may ignore the 9, the 8 and 1, the 5 and 4, the 7 and 2; only the digits 3 and 8 are left, their sum is 11 which is congruent to 2(mod 9). It is because we may ignore 9's that this result goes by the name "casting out nines."

The process of casting out nines serves as a partial check on the arithmetic operations of addition, subtraction, and multiplication. For example, if we wished to check the claim that

$$147^2 = 21\,509$$

we would cast out the nines in 147 and 21 509:

$$147 \equiv 1 + 4 + 7 \equiv 3 (\text{mod } 9),$$

$$147^2 \equiv 3^2 \equiv 0 (\text{mod } 9),$$

but

$$21\,509 \equiv 2 + 1 + 5 + 0 + 9 \equiv 8 (\text{mod } 9).$$

Therefore, $147^2 \neq 21\,509$. The method is not foolproof; casting out nines would not have disproved the absurd claim that $147^2 = 18$. In fact, one out of every nine integers is congruent to $147^2 (\text{mod } 9)$. Thus, speaking very loosely, casting out nines will find 8 of 9 errors.

As a last illustration of Theorem 3.5, we present a process that is sometimes called "casting out elevens." Let the decimal representation of a positive integer n be

$$n = a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + \cdots + a_1 \cdot 10 + a_0,$$

where the numbers $a_0, \ldots, a_k$ are the digits of n and are in the range 0 to 9. Let

$$f(x) = a_k x^k + a_{k-1} x^{k-1} + \cdots + a_1 x + a_0.$$

Then

$$f(10) \equiv f(-1) (\text{mod } 11);$$

that is,

$$n \equiv (-1)^k a_k + (-1)^{k-1} a_{k-1} + \cdots + a_4 - a_3 + a_2 - a_1 + a_0 (\text{mod } 11).$$

In words, we add the units, hundreds, ten thousands, ..., digits of n and subtract from this the sum of the tens, thousands, hundred thousands, ..., digits of n. The result is congruent to $n (\text{mod } 11)$. For example,

$$37\,147\,289 \equiv (9 + 2 + 4 + 7) - (8 + 7 + 1 + 3) \equiv 3 (\text{mod } 11).$$

The casting-out-elevens process also serves as a partial check on the arithmetic operations of addition, subtraction, and multiplication. For example, in the supposed equality

$$147^2 = 21\,509,$$

we find that

$$147 \equiv 7 - 4 + 1 \equiv 4 (\text{mod } 11),$$

$$147^2 \equiv 4^2 \equiv 16 \equiv 6 - 1 \equiv 5 (\text{mod } 11),$$

while

$$21\,509 \equiv (9 + 5 + 2) - (0 + 1) \equiv 4 (\text{mod } 11).$$

Thus

$$147^2 \neq 21\,509.$$

Here again the method of casting out elevens is not foolproof, but, loosely speaking, it will discover 10 of 11 errors.

EXERCISES

1. Show that if $a \equiv b (\text{mod } n)$ and $d | n$, then $a \equiv b (\text{mod } d)$.
2. Show that if $a \equiv b (\text{mod } n)$ and $c > 0$, then $ac \equiv bc (\text{mod } nc)$.

3. Use Figure 3.2 to calculate $4 \cdot (2 \cdot 5)$ and $(4 \cdot 2) \cdot 5 \pmod 6$.
4. Construct the tables for addition and multiplication (mod 7) corresponding to Figures 3.1 and 3.2.
5. Show that a perfect square is congruent to either 0 or 1 (mod 4).
6. Show that a perfect square is congruent to either 0, 1, or 4 (mod 8).
7. Show that for all n, $n^3 \equiv n \pmod 3$.
8. Show that if $5 \nmid n$, then $n^4 \equiv 1 \pmod 5$.
9. We did not prove that if $a \equiv b \pmod n$, then $c^a \equiv c^b \pmod n$. Let $c = 2$, $n = 7$, $a = 2$, $b = 9$, and show that for these values, $c^a \not\equiv c^b \pmod n$, thus disproving such a result.
10. Show that the prime numbers split up into the three classes: 2, those primes congruent to 1(mod 4), and those primes $\equiv 3 \pmod 4$.
11. Show that every prime number is in one of the six classes: 2, 3, $p \equiv 1 \pmod{12}$, $p \equiv 5 \pmod{12}$, $p \equiv 7 \pmod{12}$, and $p \equiv 11 \pmod{12}$.
12. In 1825 Gauss gave the following construction for writing a prime congruent to 1(mod 4) as the sum of two squares: Let $p = 4k + 1$ be a prime number. Determine x (this is uniquely possible by Theorem 3.4) so that

$$x \equiv \frac{(2k)!}{2(k!)^2} \pmod p, \qquad |x| < \frac{p}{2}.$$

Now determine y so that

$$y \equiv x \cdot (2k)! \pmod p, \qquad |y| < \frac{p}{2}.$$

Gauss showed that $x^2 + y^2 = p$. Verify Gauss's result for $p = 5$ and $p = 13$.
13. Find all the possible values of the sum of two squares (mod 4). Use your result to show that 4 926 834 923 is not the sum of two squares.
14. There is reason to believe (but it has never been proved) that there are infinitely many primes which are the sum of the squares of three different prime numbers (the smallest example is $83 = 3^2 + 5^2 + 7^2$). Let $p = p_1^2 + p_2^2 + p_3^2$, where p, p_1, p_2, and p_3 are primes. Use congruences (mod 3) to show that one of the three primes p_1, p_2, and p_3 is, in fact, 3.
15. Suppose that $m \geq 0$. Show that $17 \mid (3 \cdot 5^{2m+1} + 2^{3m+1})$. [*Hint:* Use congruences (mod 17). A further hint is given in the answers at the back of the book.]
16. Suppose that $m \geq 0$. Show that $49 \mid (5 \cdot 3^{4m+2} + 53 \cdot 2^{5m})$.
17. Given m integers where $m > n$, show that two of these integers must be congruent (mod n). (*Hint:* Any integer is congruent to one of the numbers

$0, 1, \ldots, n-1$; show that two of the m integers are congruent to the same thing and hence to each other.)

18. Given m integers where $m < n$, show that there is an integer in the range $0, 1, \ldots, n-1$ which is congruent to none of the given integers.
19. Show that if n is a positive integer with two or more digits, then the sum of the digits of n is less than n. This shows that the process of casting out nines ultimately leads to a single digit.
20. Show that an integer is divisible by 9 if and only if the process of casting out nines leads ultimately to 0 or 9.
21. Show that an integer is divisible by 3 if and only if the process of casting out nines leads ultimately to 0, 3, 6, or 9.
22. Show that an integer is divisible by 11 if and only if the process of casting out elevens leads ultimately to 0.
23. Let $n = a_2 \cdot 10^2 + a_1 \cdot 10 + a_0$. Show that $n \equiv a_0 + 3a_1 + 2a_2 \pmod 7$ and use this result to find criteria for divisibility of a three (or less)-digit number by 7.
24. It is a fact that $23\,538 \equiv 38 + 35 + 02 \equiv 75 \pmod{99}$. Prove the result that this suggests. The result could well be called "casting out ninety nines." [*Hint:* In the case of 23 538, the relevant polynomial is $f(x) = 2x^2 + 35x + 38$ with $f(100) \equiv f(1) \pmod{99}$.]
25. Show that a number is divisible by 11 if and only if the casting-out-ninety-nines method of the previous problem ultimately gives either 0 or a two-digit number with both digits equal.
26. It is a fact that $4\,176\,204\,105 \equiv 105 - 204 + 176 - 4 \equiv 73 \pmod{1001}$. Prove the result that this suggests; we shall call it "casting out one thousand and ones."
27. Suppose that the method of casting out one thousand and ones of the previous problem ultimately reduces n to the three (or less)-digit number m. Prove that $7|n$ if and only if $7|m$. Prove that $11|n$ if and only if $11|m$. Finally, show that $13|n$ if and only if $13|m$. It may be useful to know that $1001 = 7 \cdot 11 \cdot 13$.
28. In the proof that a polynomial of degree greater than or equal to one never gives only primes, where did we use the fact that the degree is greater than or equal to one? [We had better have used it someplace; the result is not true for polynomials of degree zero, for example, $f(x) = 3$.]
29. Show that for infinitely many n, $43|(n^2 + n + 41)$.
30. What is involved in checking an arithmetic operation (mod 10)?
31. Show that if $a_1, \ldots, a_n$ have the property that no two of them are congruent (mod n), then they form a complete residue system (mod n).
32. Find $(a,26)$ given that $a^{10} \equiv 10 \pmod{26}$.

33. Show that if $n^2 + 2$ and $n^2 - 2$ are both primes, then $3|n$.
34. The polynomial $x^2 + 1$ cannot be factored. Does this contradict the fact that not all numbers of the form $n^2 + 1$ are primes?
35. Under the present calendar system, every fourth year is a leap year. There are three exceptions to this rule every 400 years. If a year number is divisible by 100, then it is a leap year if and only if it is divisible by 400. Thus 1800, 1900, 2100 are not leap years, but 2000 is a leap year. The beginning of the twentieth century, January 1, 1900, was a Monday. Show that although Sunday begins every week, it will never begin a a century.
36. Show that anybody born between 1901 and 2071 will celebrate his twenty-eighth birthday on the same day of the week as the day he was born.

3.3. Linear Congruence Equations

An equation of the form

$$a_1x_1 + a_2x_2 + \cdots + a_kx_k \equiv b(\text{mod } n), \tag{7}$$

with unknowns $x_1, \ldots, x_k$, is a linear congruence equation in k variables. A solution to this equation is a set of *integers* which satisfies the equation. The definition of congruence shows that equation (7) is equivalent to the Diophantine equation

$$a_1x_1 + a_2x_2 + \cdots + a_kx_k - nx_{k+1} = b \tag{8}$$

with $k + 1$ unknowns. Equation (8) either has no solutions or it has infinitely many. Thus the same is true of (7). In the case that $k = 1$, we know exactly how to find the solutions to (8) (when they exist) and hence (7). In dealing with (7), we wish to know how many solutions there are (mod n). By this we mean that two different solutions of (7) are the same (mod n) if the different values of x_j are congruent (mod n) for all j. Thus we say that the solution $x = 1$, $y = 2$, $z = 3$ to

$$x + y + z \equiv -1(\text{mod } 7)$$

is the same (mod 7) as the solution $x = 8$, $y = -5$, $z = 17$ but different (mod 7) from the solution $x = 1$, $y = 3$, $z = 2$. In particular, when there is only one solution to (7) (mod n), we say that the solution is unique (mod n).

Theorem 3.6. The equation

$$ax \equiv b(\text{mod } n) \tag{9}$$

has solutions if and only if $d|b$, where $d = (a,n)$. If $d|b$, then the solution is unique (mod n/d). If $(a,n) = 1$, then (9) always has a solution and it is unique (mod n).

Proof. If $x = x_0$ is a solution to (9), then there is an integer y_0 such that

$$ax_0 = b + ny_0;$$

that is, the equation

$$ax - ny = b \tag{10}$$

has a solution. If $x = x_0$, $y = y_0$ is a solution to (10), then

$$ax_0 \equiv ax_0 - ny_0 \equiv b(\text{mod } n),$$

and thus (9) has a solution. Therefore, (9) has solutions if and only if (10) has solutions and further, any solution for x in (10) gives a solution for x in (9). By Theorem 2.18, (10) has solutions if and only if $d|b$. Thus (9) has solutions if and only if $d|b$. Suppose that $d|b$, so that (10) has a solution. Let $x = x_0$, $y = y_0$ be a solution to (10). By Theorem 2.18, every solution of (10) is then of the form

$$x = x_0 + t\frac{n}{d}, \qquad y = y_0 + t\frac{a}{d},$$

where t is an integer. Thus every solution to (9) is of the form

$$x = x_0 + t\frac{n}{d}.$$

Since

$$x_0 + t\frac{n}{d} \equiv x_0 \left(\text{mod } \frac{n}{d}\right),$$

we see that all solutions to (9) are congruent to $x_0(\text{mod } n/d)$ and hence the solution to (9) is unique (mod n/d). The last statement of the theorem follows from the first two. ▲

We developed a systematic process in Chapter 2 for solving (10) and as a result (9). Usually, one can shortcut the Euclidean algorithm by taking advantage of situations as they arise. If in (9), $d = (a,n) > 1$, then it is best to divide everything through by d using Theorem 3.3. We are then left with an equation of the same type as (9) but with $(a,n) = 1$. We give several illustrations. The equation

$$14x \equiv 13(\text{mod } 21)$$

has no solutions since $(14,21) = 7$ and $7 \nmid 13$. We now solve the equation

$$9x \equiv 15 \pmod{21}. \tag{11}$$

Here $(9,21) = 3$ and $3|15$. Thus the equation will have a unique solution (mod 7). We first divide everything by 3, by Theorem 3.3,

$$3x \equiv 5 \pmod{7}.$$

Therefore,

$$3x \equiv 5 + 7 \equiv 12 \pmod{7}$$

and since $(3,7) = 1$, Theorem 3.3 says that

$$x \equiv 4 \pmod{7}. \tag{12}$$

The original equation was (mod 21); we may wish to know the solutions (mod 21) also. This is easily done. In any complete residue system (mod 7), there is a unique solution to (11) and it can be found from (12). Thus in the set 0, 1, 2, 3, 4, 5, 6, $x = 4$ is the unique solution to (11); in the set 7, 8, 9, 10, 11, 12, 13, $x = 11$ is the unique solution to (11); and in the set 14, 15, 16, 17, 18, 19, 20, $x = 18$ is the unique solution to (11). These three sets combined give a complete residue system (mod 21). Thus there are 3 solutions to (11) (mod 21). They are

$$x \equiv 4, 11, 18 \pmod{21}. \tag{13}$$

Equations (12) and (13) are two ways of saying the same thing. In like manner, the equations

$$x \equiv 7 \pmod{8}, \qquad x \equiv 7, 15, 23, 31, 39 \pmod{40}$$

are equivalent. In general, the congruence

$$x \equiv a \pmod{n}$$

has the m solutions (mod mn) given by

$$x \equiv a, a + n, a + 2n, \ldots, a + (m - 1)n \pmod{mn}.$$

Let us illustrate the systematic and nonsystematic ways of solving the equation

$$8x \equiv 7 \pmod{13}. \tag{14}$$

The systematic method involves using the Euclidean algorithm to find (8, 13). All x satisfy

$$13x \equiv 13 \pmod{13}.$$

Subtracting (14) from this gives

$$5x \equiv 6 \pmod{13}. \tag{15}$$

Subtracting this from (14) gives

$$3x \equiv 1 \pmod{13}. \tag{16}$$

Subtracting this from (15) gives

$$2x \equiv 5 \pmod{13}.$$

Subtracting this from (16) gives

$$x \equiv -4 \equiv 9 \pmod{13}.$$

We already know that (14) has a unique solution (mod 13); this must be it. In contrast to the systematic method, the nonsystematic methods usually take advantage of the possibility of dividing both sides by common factors. When the coefficient of x is small, it is usually possible to arrange for a common factor by inspection. This is what we did in deriving (12). As another example, (14) may be written

$$8x \equiv 7 + 13 \equiv 20 \pmod{13}$$

and, since $(4,13) = 1$,

$$2x \equiv 5 \equiv 5 + 13 \equiv 18 \pmod{13}$$

and thus, since $(2,13) = 1$,

$$x \equiv 9 \pmod{13}.$$

The unexpected may naturally occur when one proceeds in a nonsystematic manner. The following example is particularly instructive. Since $(7,39) = 1$, the equation

$$7x \equiv 22 \pmod{39} \tag{17}$$

has a unique solution (mod 39). Subtracting equation (17) five times from

$$39x \equiv 0 \pmod{39}$$

gives

$$4x \equiv -110 \equiv -110 + 3 \cdot 39 \equiv 7 \pmod{39}.$$

We subtract this from (17) and get

$$3x \equiv 15 \pmod{39}. \tag{18}$$

Here we have the opportunity to divide both sides by 3. But since $(3,39) = 3$,

Theorem 3.3 says that the result is *not necessarily*

$$x \equiv 5 (\text{mod } 39)$$

but only

$$x \equiv 5 (\text{mod } 13).$$

This is equivalent to

$$x \equiv 5, 18, 31 (\text{mod } 39). \tag{19}$$

We seem to be claiming that (17) has three solutions (mod 39) instead of a unique solution as guaranteed by Theorem 3.6. Of course, this is not true. We have merely shown that if x is a solution to (17), then x satisfies (19) also. Thus two of the "solutions" in (19) will be extraneous solutions that will not satisfy (17); the other will be our desired solution. In this instance,

$$x \equiv 31 (\text{mod } 39)$$

is the correct solution; the obvious $x \equiv 5 (\text{mod } 39)$ is not a solution and neither is $x \equiv 18 (\text{mod } 39)$.

What has happened above is not that unusual in mathematics. It is very easy to get extraneous solutions to equations. For example, we may solve the equation

$$\sqrt{x + \sqrt{x - 2}} = 2 \tag{20}$$

by successive squarings:

$$\begin{aligned} x + \sqrt{x - 2} &= 4, \\ \sqrt{x - 2} &= 4 - x, \\ x - 2 &= 16 - 8x + x^2, \\ x^2 - 9x + 18 &= 0, \\ (x - 3)(x - 6) &= 0, \\ x &= 3, 6. \end{aligned} \tag{21}$$

Again, we have not shown that $x = 3$ and $x = 6$ are solutions to (20) but only that if x is a solution to (20), then $x = 3$ or $x = 6$. In fact, $x = 3$ is a solution to (20) while $x = 6$ leads to $\sqrt{8} = 2$, which is absurd. Thus $x = 6$ is an extraneous solution to (20) (which is a kind way of saying that it is not a solution at all). One should always check one's answer with the original problem. There are times when it is legal (but not advisable) to sidestep the

checking procedure. Sometimes an existence theorem (such as Theorem 3.6) will tell you that a certain equation has a unique solution; then if you find only one possibility, you know that you have indeed found the unique solution—assuming you made no arithmetic mistakes.

We will now discuss the subject of several equations in one unknown. Sometimes they are inconsistent, as in the two equations

$$x \equiv 2 (\text{mod } 4), \qquad x \equiv 1 (\text{mod } 6).$$

The first equation requires x to be even while the second requires x to be odd, and thus there is no common solution to both equations. Another way we can see the inconsistency of the two equations is to look at them both (mod 2) [a congruence (mod mn) is also a valid congruence (mod n)]. Then we see that a common solution satisfies both

$$x \equiv 2 (\text{mod } 2), \qquad x \equiv 1 (\text{mod } 2),$$

which is false since $2 \not\equiv 1 (\text{mod } 2)$.

There are other times when two such equations do have a common solution. For example, consider the equations

$$\begin{aligned} x &\equiv 2 (\text{mod } 4), \\ x &\equiv 3 (\text{mod } 5). \end{aligned} \tag{22}$$

which have the common solution $x = -2$. Let us find all the solutions of (22). The first equation is satisfied by x if and only if

$$x = 2 + 4t,$$

where t is an integer. We put this in the second equation and get

$$\begin{aligned} 2 + 4t &\equiv 3 (\text{mod } 5), \\ -t \equiv 4t &\equiv 1 (\text{mod } 5), \\ t &\equiv -1 \equiv 4 (\text{mod } 5). \end{aligned} \tag{23}$$

Equation (23) has a unique solution (mod 5), this is the only possibility and hence is the unique solution to (23). Thus t is a solution to (23) if and only if t can be written

$$t = 4 + 5k,$$

where k is an integer. Thus x satisfies both of equations (22) if and only if there is an integer k such that

$$x = 4(4 + 5k) + 2 = 20k + 18.$$

[It is easily seen that this really is a solution to both of equations (22).] The

common solution to equations (22) is unique (mod 20). The situation in (22) is perfectly general.

Theorem 3.7. If $(m,n) = 1$, then the equations

$$\begin{aligned} x &\equiv a(\text{mod } m), \\ x &\equiv b(\text{mod } n) \end{aligned} \tag{24}$$

have a unique common solution (mod mn).

Proof. An integer x satisfies the first equation if and only if there is an integer t such that

$$x = a + mt. \tag{25}$$

This satisfies the second equation if and only if

$$mt \equiv b - a(\text{mod } n). \tag{26}$$

Since $(m,n) = 1$, this last equation has a unique solution (mod n), say,

$$t \equiv c(\text{mod } n).$$

Thus t satisfies (26) if and only if there is an integer k such that

$$t = c + nk.$$

We put this in (25) and find that x is a common solution to equations (24) if and only if

$$\begin{aligned} x &= a + m(c + nk) \\ &= (a + mc) + mnk. \end{aligned}$$

Hence equations (24) have common solutions, $a + mc$ is one, and all solutions are congruent to $a + mc(\text{mod } mn)$. Thus the common solutions to (24) are unique (mod mn). ▲

Theorem 3.7 is a special case of a more general result which was known to to the ancient Chinese.

Theorem 3.8 (Chinese Remainder Theorem[2]). Let $m_1, \ldots, m_k$ be positive integers which are relatively prime in pairs. Then the k equations

$$\begin{aligned} x &\equiv a_1(\text{mod } m_1) \\ &\vdots \\ x &\equiv a_k(\text{mod } m_k) \end{aligned} \tag{27}$$

have a unique solution (mod $m_1 m_2 \cdots m_k$).

[2] More rarely known as the Formosa Theorem.

Proof. We use Theorem 3.7 $(k-1)$ times. By Theorem 3.7, the first two equations have a unique solution (mod m_1m_2); let this solution be given by

$$x \equiv b_2 (\text{mod } m_1m_2). \tag{28}$$

The third equation is

$$x \equiv a_3 (\text{mod } m_3). \tag{29}$$

By hypothesis,

$$(m_1, m_3) = (m_2, m_3) = 1$$

and therefore, by Theorem 2.7,

$$(m_1m_2, m_3) = 1.$$

We can now apply Theorem 3.7 to (28) and (29). There is a unique solution to (28) and (29) (mod $m_1m_2m_3$); in other words, there is a unique solution to the first three equations of (27). Let that unique solution be

$$x \equiv b_3 (\text{mod } m_1m_2m_3). \tag{30}$$

Consider the fourth equation of (27),

$$x \equiv a_4 (\text{mod } m_4). \tag{31}$$

Since

$$(m_1, m_4) = (m_2, m_4) = (m_3, m_4) = 1,$$

we see that

$$(m_1m_2m_3, m_4) = 1.$$

Thus there is a unique solution to (30) and (31) (mod $m_1m_2m_3m_4$) and it is the unique solution to the first four equations of (27). We continue in this manner. After $(k-1)$ applications of Theorem 3.7, we will arrive at the fact that there is a unique solution (mod $m_1m_2 \cdots m_k$) to

$$x \equiv b_{k-1} (\text{mod } m_1m_2 \cdots m_{k-1})$$

and

$$x \equiv a_k (\text{mod } m_k);$$

this solution also provides the unique solution (mod $m_1m_2 \cdots m_k$) to the k equations in (27). ▲

If for each j, we restrict a_j to the range from 0 to $m_j - 1$, then the existence part of the Chinese remainder theorem may be put in the form; if $m_1, \ldots, m_k$ are pairwise relatively prime, then there exists an integer x such that for each

$j (j = 1, 2, \ldots, k)$, x leaves the remainder a_j when divided by m_j. This explains the name of the theorem. (It also explains how a theorem about congruences could be known before congruences were invented; we have merely put an old theorem in modern form.)

The reader is no doubt wondering why we restricted our attention in Theorems 3.7 and 3.8 to equations having the coefficient of x equal to one. Consider the set of equations

$$a_1 x \equiv b_1 (\text{mod } n_1), \ldots, a_k x \equiv b_k (\text{mod } n_k). \tag{32}$$

If there is a common solution, then each equation is individually solvable. This means that $d_i | b_i$, where $d_i = (a_i, n_i)$, and this is true for $i = 1, 2, \ldots, k$. We know what the solutions to the individual equations of (32) look like,

$$x \equiv c_1 (\text{mod } m_1), \ldots, x \equiv c_k (\text{mod } m_k)$$

where the m_i are given by the formulas

$$m_1 = \frac{n_1}{d_1}, \ldots, m_k = \frac{n_k}{d_k}.$$

Thus if for all i, $d_i | b_i$ and if the numbers $m_1, \ldots, m_k$ are relatively prime in pairs, then equations (32) have a unique common solution (mod $m_1 m_2 \cdots m_k$). Thus Theorem 3.8 is sufficient for the theoretical purpose of proving that under certain conditions, (32) has a unique solution (mod $m_1 m_2 \cdots m_k$). When actually solving a specific problem, it is a complete waste of time to first solve each of (32) individually and then find the common solution. It takes only half the work to simply solve the first equation of (32), put the solution of the first equation into the second equation of (32) and solve, put the common solution of the first two equations in the third, and so on.

We now touch briefly on the subject of linear congruence equations with more than one unknown. We will content ourselves with examining the simplest case of two equations and two unknowns; the result, however, will be very useful in Chapter 4.

Theorem 3.9. Suppose $(cf - de, n) = 1$. Then the equations

$$\begin{aligned} cx + ey &\equiv a (\text{mod } n), \\ dx + fy &\equiv b (\text{mod } n) \end{aligned} \tag{33}$$

have a unique common solution for x and y(mod n).

Proof. Let us suppose that there is a solution to (33) and attempt to find it. We multiply the first equation by f, the second equation by e, and subtract;

the result is

$$(cf - de)x \equiv af - be \pmod{n}. \tag{34}$$

We multiply the first equation by d, the second equation by c, and subtract the first from the second; the result is

$$(cf - de)y \equiv bc - ad \pmod{n}. \tag{35}$$

Since $(cf - de, n) = 1$, Theorem 3.6 says that there is a unique $x \pmod{n}$ satisfying (34) and a unique $y \pmod{n}$ satisfying (35). Hence if there is a solution to (33), it is unique (mod n).

Unfortunately, the fact that (34) and (35) have solutions does not mean that the original equations (33) have solutions. It is clear how we should proceed, however. We take the solutions to (34) and (35) and show that they do satisfy (33). There is a slight hitch in this. We cannot just divide both sides of (34) and (35) by $(cf - de)$, because we have not defined congruences for rational numbers.[3] But we can find an integer which does the same job (mod n) as $1/(cf - de)$. Since $(cf - de, n) = 1$, Theorem 3.6 says that there is an integer z such that

$$z(cf - de) \equiv 1 \pmod{n}. \tag{36}$$

We use the integer z to solve (34) and (35). If x and y satisfy (34) and (35), then

$$\begin{aligned} x &\equiv z(cf - de)x \equiv z(af - be) \pmod{n}, \\ y &\equiv z(cf - de)y \equiv z(bc - ad) \pmod{n}. \end{aligned} \tag{37}$$

Now we can verify that (33) does have solutions. Let x, y, and z be given by (36) and (37). Then

$$\begin{aligned} cx + ey &\equiv cz(af - be) + ez(bc - ad) \pmod{n} \\ &\equiv czaf - ezad \pmod{n} \\ &\equiv az(cf - de) \pmod{n} \\ &\equiv a \pmod{n} \end{aligned}$$

and

$$\begin{aligned} dx + fy &\equiv dz(af - be) + fz(bc - ad) \pmod{n} \\ &\equiv -dzbe + fzbc \pmod{n} \\ &\equiv bz(cf - de) \pmod{n} \\ &\equiv b \pmod{n}. \end{aligned}$$

[3] It may be useful to remind the reader that the solutions to two equations in two unknowns with integral coefficients are usually not integers but only rational numbers. Here we are looking for integers which satisfy the equations (mod n).

Thus there are integral solutions to (33); we have already shown that they must be unique (mod n). ▲

EXERCISES

In problems 1–13, either find all integral solutions (all common integral solutions, if more than one equation) or show that there are none.

1. Solve: $5x \equiv 1 \pmod 7$.
2. Solve: $14x \equiv 5 \pmod{45}$.
3. Solve: $14x \equiv 35 \pmod{87}$.
4. Solve: $3x \equiv 2 \pmod{78}$.
5. Solve: $6x \equiv 10 \pmod{14}$.
6. Solve: $9x \equiv 21 \pmod{12}$.
7. Solve: $x \equiv 2 \pmod 3$, $x \equiv 3 \pmod 4$.
8. Solve: $x \equiv 7 \pmod 9$, $x \equiv 13 \pmod{23}$, $x \equiv 1 \pmod 2$.
9. Solve: $2x \equiv 3 \pmod 5$, $4x \equiv 3 \pmod 7$.
10. Solve: $6x \equiv 8 \pmod{10}$, $15x \equiv 30 \pmod{55}$.
11. Solve: $5x + 4y \equiv 6 \pmod 7$, $3x - 2y \equiv 6 \pmod 7$.
12. Solve: $2x + 7y \equiv 8 \pmod{13}$, $5x + 10y \equiv 7 \pmod{13}$.
13. Solve: $x + 2y + 3z \equiv 1 \pmod{11}$, $x + 5y + 6z \equiv 3 \pmod{11}$, $x + 4y + 7z \equiv 5 \pmod{11}$.
14. Find all solutions (mod 7): $3x + 4y \equiv 1 \pmod 7$.
15. Find all solutions (mod 8): $3x + 7y \equiv 2 \pmod 8$.
*16. Show that if $(a,n) = (b,n) = 1$, then the equation

$$ax + by \equiv c \pmod n$$

has exactly n different solutions (mod n).

17. Find all solutions (mod 6): $2x + 3y \equiv 1 \pmod 6$.
18. Find all common solutions (mod 12) (or show that there are none) to

$$4x + y \equiv 6 \pmod{12}, \qquad x + 4y \equiv 2 \pmod{12}.$$

19. Find all common solutions (mod 12) (or show that there are none) to

$$4x + y \equiv 6 \pmod{12}, \qquad x + 4y \equiv 9 \pmod{12}.$$

20. Find all positive integers less than 1000 which leave the remainder 1 when divided by 2, 3, 5, and 7.
21. A multiplication has been performed incorrectly, but the answer is correct (mod 9), (mod 10), and (mod 11). What is the closest that the incorrect result can possibly be to the correct result?
22. The following multiplication was correct, but unfortunately the printer inserted an x in place of a digit in the answer

$$172\,195 \cdot 572\,167 = 98\,524\,2x6\,565.$$

Determine x without redoing the multiplication.

23. Show that an integer is divisible by 4 if and only if the number left when all digits other than the last two are eliminated is divisible by 4. Use this rule to find conditions for divisibility by 12.
24. Show that every integer satisfies at least one of the following six congruences: $x \equiv 0 \pmod 2$, $x \equiv 0 \pmod 3$, $x \equiv 1 \pmod 4$, $x \equiv 1 \pmod 6$, $x \equiv 3 \pmod 8$, and $x \equiv 11 \pmod{12}$.
25. Prove Theorem 3.8 by induction.

3.4. Reduced Residue Systems and Euler's ϕ Function

We see from Theorem 3.6 that the equation

$$ax \equiv 1 \pmod n$$

is solvable (in integers) if and only if $(a,n) = 1$. The numbers that are relatively prime to n have other interesting congruence properties. In this section we single these numbers out for special attention.

Definition. Let S be a complete residue system (mod n). The set S' consisting of those members of S which are relatively prime to n is called a **reduced residue system** (mod n).

If $b \equiv a \pmod n$, then we may write b in the form $b = a + kn$. By Theorem 2.4,

$$(b,n) = (a + kn,n) = (a,n).$$

Thus if $a \equiv b \pmod n$, then a is relatively prime to n if and only if b is relatively prime to n.

Theorem 3.10. Let S' be a reduced residue system (mod n). If $(a,n) = 1$, then a is congruent (mod n) to a unique member of S'. If S'' is another reduced residue system (mod n), then S' and S'' have exactly the same number of members and, in fact, if $a_1, \ldots, a_k$ are the members of S', then the members of S'' can be listed in such an order, say $b_1, \ldots, b_k$, that $a_1 \equiv b_1, \ldots, a_k \equiv b_k \pmod n$ [that is, (mod n), S'' is simply a rearrangement of S'].

Proof. Let S be a complete residue system containing S'. By the definition of S, there is a unique integer b in S such that

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

Since $(a,n) = 1$, $(b,n) = 1$ also. Therefore, by definition, b is in S'. Since b is

unique in S, it is certainly unique in S'. This takes care of the first part of the theorem.

It follows from the first part of the theorem that each element of S'' is congruent to a unique member of S'. No two members of a complete residue system (mod n) are congruent (mod n). Therefore, no two members of S'' are congruent (mod n) to the same member of S', and since different members of S'' are congruent (mod n) to different members of S', we see that S' has at least as many members as S''. But everything done thus far is equally valid with S' and S'' interchanged. Thus S'' has at least as many members as S'. This combined with the previous statement says that S'' and S' have exactly the same number of members. Let k be the number of integers in each set. The last part of the theorem is now clear: Since different members of S'' are congruent (mod n) to different members of S' and since each has k members, the sets S' and S'' are the same (mod n) except for the order of the elements. ▲

Definition. For $n \geq 1$, let $\phi(n)$ denote the number of integers in a reduced residue system (mod n). [By Theorem 3.10, $\phi(n)$ does not depend on which reduced residue system (mod n) is chosen.] This function of n is called **Euler's ϕ function.** (It is also sometimes called **Euler's totient function.**)

It is interesting to note that although the function was invented by Euler, the present notation was given by Gauss. The following theorem is often used as the definition of $\phi(n)$.

Theorem 3.11. If $n \geq 1$, then the number of positive integers which are less than or equal to n and relatively prime to n is $\phi(n)$.

Proof. The numbers $1, 2, \ldots, n$ form a complete residue system (mod n). Thus the positive integers which are less than or equal to n and relatively prime to n form a reduced residue system (mod n). Their number is thus $\phi(n)$. ▲

A few examples are shown in Figure 3.3 (we take as our complete residue system (mod n), the numbers $1, 2, 3, \ldots, n$). Since $(n,n) = n$, we see that n is in a reduced residue system (mod n) if and only if $n = 1$. Thus for $n > 1$, $\phi(n)$ is the number of positive integers which are less than n and relatively prime to n. Every positive integer less than a prime p is relatively prime to p and hence

$$\phi(p) = p - 1.$$

n	1	2	3	4	5	6	7	8	9	10
A reduced residue system mod (n)	1	1	1, 2	1, 3	1, 2, 3, 4	1, 5	1, 2, 3, 4, 5, 6	1, 3, 5, 7	1, 2, 4, 5, 7, 8	1, 3, 7, 9
$\phi(n)$	1	1	2	2	4	2	6	4	6	4

Figure 3.3

The next theorem gives another simple property of numbers relatively prime to n.

Theorem 3.12. Suppose $(a,n) = 1$. If the numbers $a_1, \ldots, a_n$ form a complete residue system (mod n), then for all b the numbers $aa_1 + b, \ldots, aa_n + b$ also form a complete residue system (mod n). If the numbers $a_1, \ldots, a_{\phi(n)}$ form a reduced residue system (mod n), then so do the numbers $aa_1, \ldots, aa_{\phi(n)}$.

Proof. Since $(a,n) = 1$, by Theorem 3.6, there is an integer c such that

$$ac \equiv 1 \pmod{n}.$$

Suppose that $a_1, \ldots, a_n$ gives a complete residue system (mod n). If d is an integer, then there is a (unique) k such that

$$c(d - b) \equiv a_k \pmod{n}.$$

But then

$$d - b \equiv ac(d - b) \equiv aa_k \pmod{n} \qquad \text{or} \qquad d \equiv aa_k + b \pmod{n}.$$

If

$$d \equiv aa_j + b \pmod{n} \qquad \text{and} \qquad d \equiv aa_k + b \pmod{n},$$

then

$$c(d - b) \equiv aca_j \equiv a_j \pmod{n}, \qquad c(d - b) \equiv aca_k \equiv a_k \pmod{n},$$

which is false if $j \neq k$. Thus every integer is congruent to exactly one of the n integers $aa_1 + b, \ldots, aa_n + b$, and thus this set is a complete system of residues (mod n). If $a_1, \ldots, a_{\phi(n)}$ form a reduced residue system (mod n), then they are distinct elements of a complete residue system, and thus by the first part of the theorem with $b = 0$, $aa_1, \ldots, aa_{\phi(n)}$ are distinct elements of a complete residue system (mod n). A reduced residue system has exactly $\phi(n)$ elements; therefore, we need only show that each of the numbers

$aa_1, \ldots, aa_{\phi(n)}$ is relatively prime to n and we will have found all $\phi(n)$ elements of a reduced residue system (mod n). Since $(a_k,n) = 1$ for all k and $(a,n) = 1$, we see from Theorem 2.7 that $(aa_k,n) = 1$ for all k, $k = 1, \ldots, \phi(n)$. ▲

The preceding theorem has a remarkable consequence.

Theorem 3.13 (Euler's Theorem; also known as the Euler–Fermat Theorem). If $(a,n) = 1$, then $a^{\phi(n)} \equiv 1 (\text{mod } n)$.

Proof. Let $a_1, \ldots, a_{\phi(n)}$ be a reduced residue system (mod n). Then the numbers $aa_1, \ldots, aa_{\phi(n)}$ are also a reduced residue system (mod n). By Theorem 3.10, the numbers $aa_1, \ldots, aa_{\phi(n)}$ are just a rearrangement (mod n) of the numbers $a_1, \ldots, a_{\phi(n)}$, and thus the products of all the numbers in the two systems are the same (mod n):

$$(aa_1)(aa_2)\cdots(aa_{\phi(n)}) \equiv a_1 a_2 \cdots a_{\phi(n)} (\text{mod } n). \tag{38}$$

Since each a_k is relatively prime to n, it may be canceled from both sides of (38). When we do this for each k, we are left with

$$a^{\phi(n)} \equiv 1 (\text{mod } n). \quad ▲$$

Theorem 3.14 (Fermat's Theorem; also known as the Little Fermat Theorem). Suppose p is a prime. Then for all a,

$$a^p \equiv a (\text{mod } p).$$

If $p \nmid a$, then

$$a^{p-1} \equiv 1 (\text{mod } p).$$

Proof. When $p|a$, both sides of the first congruence are congruent to 0(mod p) and hence congruent. When $p \nmid a$, then the first congruence is a times the second, and thus it suffices to prove that the second congruence is valid. Since p is a prime, $p \nmid a$ is equivalent to $(a,p) = 1$. This combined with the fact that $\phi(p) = p - 1$ makes this theorem a corollary of the previous theorem. ▲

Historically, Fermat's theorem was stated in 1640, and it was generalized by Euler in 1760 to the form that if $(a,n) = 1$, then $n|(a^{\phi(n)} - 1)$. A special case of Fermat's theorem is that if p is a prime, then

$$p|(2^p - 2).$$

The ancient Chinese knew this fact and also believed that the converse is

true. The converse states that if $n > 1$ and

$$n|(2^n - 2),$$

then n is a prime. It is probable that the Chinese observed this experimentally and never thought of proving their conjecture. In any event, they were wrong. For example,

$$341|(2^{341} - 2),$$

even though $341 = 11 \cdot 31$. The theory of congruences makes it possible to check this without having to find 2^{341} (a number of 103 digits). Since 11 is a prime, Fermat's theorem says that

$$2^{10} \equiv 1 (\text{mod } 11).$$

Therefore,

$$2^{341} \equiv 2(2^{10})^{34} \equiv 2(1)^{34} \equiv 2 (\text{mod } 11)$$

and hence

$$11|(2^{341} - 2).$$

Also,

$$2^5 \equiv 32 \equiv 1 (\text{mod } 31)$$

and therefore

$$2^{341} \equiv 2(2^5)^{68} \equiv 2(1)^{68} \equiv 2 (\text{mod } 31)$$

and therefore

$$31|(2^{341} - 2).$$

Since 11 and 31 are relatively prime, their product divides $(2^{341} - 2)$; that is,

$$341|(2^{341} - 2).$$

Thus the ancient Chinese were wrong. In honor of their mistake, we say today that a composite integer n such that

$$n|(2^n - 2)$$

is a **pseudoprime.** The first two pseudoprimes are $341 = 11 \cdot 31$ and $561 = 3 \cdot 11 \cdot 17$. There are infinitely many pseudoprimes. In fact, there are infinitely many even pseudoprimes, but they are harder to find. The first known example of an even pseudoprime is

$$161\,038 = 2 \cdot 73 \cdot 1103,$$

which was found in 1950 by D. H. Lehmer.

EXERCISES

1. Find a reduced residue system (mod 20) and give $\phi(20)$.
2. Find a reduced residue system (mod 30) and give $\phi(30)$.
3. Give two examples to show that when 2 is added to every member of a reduced residue system (mod n), the result may or may not be a reduced residue system (mod n).
4. Show that $561 = 3 \cdot 11 \cdot 17$ is a pseudoprime.
5. Show that, in fact, for all integers a, $a^{561} \equiv a \pmod{561}$.
6. Show that $3^3 \equiv -4 \pmod{31}$ and use this to show that $3^{10} \equiv -6 \pmod{31}$. Use this result and Euler's theorem to show that

$$3^{341} \not\equiv 3 \pmod{31}$$

and therefore

$$3^{341} \not\equiv 3 \pmod{341}.$$

7. Find a composite number n such that $n|(3^n - 3)$. (*Hint:* There is such a number less than 10.)
8. Show that if $(a,561) = 1$, then $a^{80} \equiv 1 \pmod{561}$. [*Note:* Do not try to find $\phi(561)$, as it is greater than 300.]
9. Show that if p is a prime, a is an integer, and k is a nonnegative integer, then

$$a^{1+k(p-1)} \equiv a \pmod{p}.$$

10. Show that if n is odd and a is an integer,

$$a^n \equiv a \pmod{3}.$$

3.5. More on Euler's ϕ Function

We see that if we are going to apply Euler's theorem in a particular problem, then we must be able to calculate $\phi(n)$ from n. If n is small, it is fairly easy to find all the numbers less than or equal to n which are relatively prime to n, and then we immediately have $\phi(n)$. But what if we wish something like $\phi(1776)$? In this section we develop a formula for $\phi(n)$ in terms of the prime factorization of n. The key to this result will be a proof of the fact that $\phi(n)$ is multiplicative.

We first illustrate the proof that $\phi(n)$ is multiplicative by showing that $\phi(30) = \phi(5) \cdot \phi(6)$. We first write the numbers from 1 to 30 in a rectangular array as in Figure 3.4. We note that a number is relatively prime to 30 if and only if it is relatively prime to both 5 and 6. Thus $n(1 \leq n \leq 30)$ is relatively prime to 30 if and only if it is one of $\phi(5)$ numbers in $\phi(6)$ columns

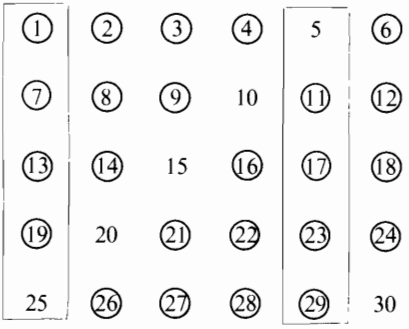


Figure 3.4. Numbers relatively prime to 6 are in the large vertical rectangles, numbers relatively prime to 5 are in circles. Numbers relatively prime to 30 are in both the large vertical rectangles and circles. The numbers from 1 to 30 that are relatively prime to 6 are in the first and fifth columns [$\phi(6)$ columns in all] and each column contains exactly four [which equals $\phi(5)$] numbers relatively prime to 5.

(the first and fifth). There are $\phi(5) \cdot \phi(6)$ such numbers and thus $\phi(30) = \phi(5)\phi(6)$. The situation here is perfectly general and leads to a proof that $\phi(n)$ is multiplicative.

Theorem 3.15. $\phi(n)$ is multiplicative.

Proof. Suppose m and n are positive integers with $(m,n) = 1$. We put the first mn positive integers in a rectangular array with m columns and n rows as in Figure 3.5. The numbers in the jth column are $m \cdot 0 + j$, $m \cdot 1 + j$, $m \cdot 2 + j, \ldots, m(n-1) + j$. By Theorem 2.4,

$$(ma + j, m) = (j,m),$$

$$\begin{array}{cccc} 1 & 2 & \cdots & m \\ m+1 & m+2 & \cdots & m+m \\ 2m+1 & 2m+2 & \cdots & 2m+m \\ \vdots & \vdots & \cdots & \vdots \\ (n-1)m+1 & (n-1)m+2 & \cdots & (n-1)m+m \end{array}$$

Figure 3.5

and thus either every element of the jth column is relatively prime to m or no element of the jth column is relatively prime to m. Therefore, exactly $\phi(m)$ columns contain numbers relatively prime to m and every entry in these $\phi(m)$ columns is relatively prime to m.

Since $(m,n) = 1$, by Theorem 3.12 the n numbers in the jth column form a complete residue system (mod n). Thus by definition, the jth column contains exactly $\phi(n)$ numbers relatively prime to n. Hence in each of the $\phi(m)$ columns containing the numbers relatively prime to m, there are $\phi(n)$ numbers relatively prime to n, and these are the only numbers relatively prime to both m and n. That is, there are exactly $\phi(m)\phi(n)$ numbers in the array of Figure 3.5 that are relatively prime to both m and n. But an integer is relatively prime to mn if and only if it is relatively prime to both m and n. Therefore,

$$\phi(mn) = \phi(m)\phi(n). \qquad \blacktriangle$$

After Theorem 3.15, we can evaluate $\phi(n)$ if we can find $\phi(p^a)$, where p is a prime. This is an easy task and the result is

Theorem 3.16. Let the prime factorization of n be

$$n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}.$$

Then

$$\phi(n) = n(1 - 1/p_1)(1 - 1/p_2)\cdots(1 - 1/p_k).$$

Proof. We begin by finding $\phi(p^a)$, where p is a prime and $a \geq 1$. A number is relatively prime to p^a unless it is divisible by p. The numbers from 1 to p^a which are divisible by p are $1 \cdot p, 2 \cdot p, \ldots, p^{a-1} \cdot p$. Thus exactly p^{a-1} positive integers less than or equal to p^a are divisible by p, and therefore there are exactly $p^a - p^{a-1}$ positive integers less than or equal to p^a which are not divisible by p. Hence

$$\phi(p^a) = p^a - p^{a-1} = p^a(1 - 1/p).$$

But now, by Theorem 3.15,

$$\begin{aligned}
\phi(n) &= \phi(p_1^{a_1})\phi(p_2^{a_2})\cdots\phi(p_k^{a_k}) \\
&= p_1^{a_1}\left(1 - \frac{1}{p_1}\right)p_2^{a_2}\left(1 - \frac{1}{p_2}\right)\cdots p_k^{a_k}\left(1 - \frac{1}{p_k}\right) \\
&= p_1^{a_1}p_2^{a_2}\cdots p_k^{a_k}\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_k}\right) \\
&= n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_k}\right). \qquad \blacktriangle
\end{aligned}$$

As an example, let us answer the question that started all this, and find $\phi(1776)$. We need to factor 1776 first; fortunately, we see that there is a factor of 2 and 3 (casting out nines reduces 1776 to 3) to get us started. We then find without much trouble that

$$1776 = 2^4 \cdot 3 \cdot 37.$$

Thus

$$\begin{aligned}\phi(1776) &= 1776(1 - \tfrac{1}{2})(1 - \tfrac{1}{3})(1 - \tfrac{1}{37}) \\ &= 2^4 \cdot 3 \cdot 37 \cdot \tfrac{1}{2} \cdot \tfrac{2}{3} \cdot \tfrac{36}{37} \\ &= 2^4 \cdot 36 \\ &= 576.\end{aligned}$$

This is considerably simpler than examining the first 1776 positive integers to see which have factors of 2, 3, and 37 and which do not.

There are other methods of deriving the crucial Theorem 3.15. Two of them are given in the miscellaneous exercises. We have now been able to evaluate three different functions from the knowledge that they are multiplicative [$d(n)$, $\sigma(n)$, and $\phi(n)$]. In the next theorem, we again make use of the knowledge that a function is multiplicative in order to find it.

Theorem 3.17. If $n \geq 1$, then

$$\sum_{d|n} \phi(d) = n.$$

Proof. Let

$$f(n) = \sum_{d|n} \phi(d).$$

Since $\phi(n)$ is multiplicative, Theorem 2.15 says that $f(n)$ is also multiplicative. Thus we first wish to find $f(p^a)$, where p is a prime and $a \geq 1$. Here we have

$$\begin{aligned}f(p^a) &= \sum_{d|p^a} \phi(d) \\ &= \phi(1) + \phi(p) + \phi(p^2) + \cdots + \phi(p^a) \\ &= 1 + p\left(1 - \frac{1}{p}\right) + p^2\left(1 - \frac{1}{p}\right) + \cdots + p^a\left(1 - \frac{1}{p}\right) \\ &= 1 + (p - 1) + (p^2 - p) + (p^3 - p^2) + \cdots + (p^a - p^{a-1}) \\ &= p^a,\end{aligned}$$

with all the other terms canceling each other. Therefore, if n factors as

$$n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k},$$

then

$$\begin{aligned} f(n) &= f(p_1^{a_1}) f(p_2^{a_2}) \cdots f(p_k^{a_k}) \\ &= p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k} \\ &= n. \qquad \blacktriangle \end{aligned}$$

EXERCISES

1. Find $\phi(n)$ for $n = 20, 60, 63, 341$, and 561.
2. Show that if n is odd, $\phi(2n) = \phi(n)$.
3. Show that if n is even, $\phi(2n) = 2\phi(n)$.
4. What goes wrong with the proof of Theorem 3.15 if $(n, m) > 1$?
5. Does Theorem 3.16 give $\phi(1)$?
6. Verify Theorem 3.17 for $n = 30$.
7. Let x be the smallest positive integer such that $2^x \equiv 1 (\text{mod } 63)$. Find x and verify that $x | \phi(63)$.

*8. Repeat problem 7 with 63 replaced by 105.

*9. Find the last three digits of 7^{9999}.

3.6. Polynomial Congruences

Definition. Let $f(x)$ and $g(x)$ be polynomials with integral coefficients. If the coefficients of each power of x are congruent (mod n), then we say that $f(x)$ and $g(x)$ are **congruent as polynomials** (mod n) and we write

$$f(x) \equiv g(x) (\text{poly mod } n).$$

For example

$$\begin{aligned} 5x^2 - 6x + 3 &\equiv x^2 + 2x - 1 (\text{poly mod } 4), \\ x^3 + 4x^2 - 2x + 1 &\equiv 3x^4 + 4x^3 + x^2 - 8x + 22 (\text{poly mod } 3), \\ x^3 - 1 &\equiv (x - 1)^3 (\text{poly mod } 3), \\ x^2 + 2x + 1 &\not\equiv 6x^2 + 3x + 6 (\text{poly mod } 5), \\ x^5 &\not\equiv x (\text{poly mod } 5). \end{aligned}$$

Missing powers of x are assumed to have the coefficient 0. Thus in the second example, we may assume that the polynomial on the left is

$$0x^4 + x^3 + 4x^2 - 2x + 1$$

and in the third example the polynomial on the left is

$$x^3 + 0x^2 + 0x - 1.$$

The fifth example is extremely instructive. The polynomials x^5 and x are not congruent as polynomials (mod 5) since the coefficients of x are incongruent (mod 5). This is true in spite of the fact that by Fermat's theorem (3.14)

$$x^5 \equiv x(\text{mod } 5)$$

for all integers x. Thus it may happen that two polynomials may be incongruent as polynomials (mod n) and still be congruent (mod n) for all integral values of the variable. This is a situation which does not occur with equalities. Two polynomials $f(x)$ and $g(x)$ are the same if and only if $f(x) = g(x)$ for all integers x. Thus when we write $f(x) = g(x)$, it does not matter whether we think of the equality as saying f and g are the same polynomials or f and g give the same values for all values of x; the two concepts are the same.

This is our reason for distinguishing between $f(x)$ and $g(x)$ being congruent as polynomials (mod n) and just being congruent (mod n). When we write

$$f(x) \equiv g(x)(\text{mod } n) \tag{39}$$

we simply mean that (39) is true for all integral values of x. There is yet a second meaning of (39) and that is the meaning of solving an equation. This is a situation that occurs with equalities. For instance,

$$(x + 1)^2 = x^2 + 2x + 1$$

is an identity, true for all values of x, while

$$(x + 1)^2 = 2x^2 + 2x$$

is true only for certain values of x which can be found by solving the equation. The reader should be able to distinguish between the two meanings of (39), particularly since they will usually be accompanied by a phrase such as "for all integers, x," or "solve."[4]

The following result, although trivial, is sufficiently fundamental to be called a theorem.

[4] It should be noted that the notation

$$f(x) \equiv g(x)(\text{poly mod } n)$$

is unique with this book and is presented as a public service to help minimize confusion. Other books and articles customarily use (39) for this purpose also and leave it to the reader to figure out which meaning is being used. (The kind author will attach a phrase such as "congruent as polynomials," but he is under no compulsion to do so and usually does not.)

Theorem 3.18. If

$$f(x) \equiv g(x)(\text{poly mod } n)$$

then for all integers x,

$$f(x) \equiv g(x)(\text{mod } n).$$

Proof. The result follows from the definition of

$$f(x) \equiv g(x)(\text{poly mod } n)$$

and Theorem 3.2 (the theorem on sums and products of congruent numbers being congruent). ▲

As the example

$$x^5 \equiv x(\text{mod } 5)$$

shows, the converse of Theorem 3.18 is not necessarily true. Thus the statement

$$f(x) \equiv g(x)(\text{poly mod } n)$$

contains more information than the statement

$$f(x) \equiv g(x)(\text{mod } n).$$

Let us give an example of how much more information the first statement can carry. It is easy to show that if p is a prime, then

$$x^p - x \equiv x(x+1)(x+2)\cdots(x+p-1)(\text{mod } p) \tag{40}$$

for all integers x. By Fermat's theorem (3.14), the left side of (40) is congruent to $0(\text{mod } p)$ for all integers x. Since the numbers $1, 2, \ldots, p$ form a complete residue system (mod p), given an integer x, there is an integer j in the range from 1 to p such that

$$x \equiv j(\text{mod } p).$$

But then the factor $[x + (p - j)]$ in the right side of (40) is congruent to 0:

$$x + p - j \equiv j + p - j \equiv 0(\text{mod } p),$$

and thus the right side of (40) is congruent to $0(\text{mod } p)$ for all integers x. This proves the relation (40). Equation (40) is not very useful as it stands, but it so happens that (40) is also true as a congruence of polynomials; that is,

$$x^p - x \equiv x(x+1)(x+2)\cdots(x+p-1)(\text{poly mod } p). \tag{41}$$

We will prove this later in this section. If we accept this as true, then the

coefficients on each side of (41) are congruent (mod p). [This is precisely the difference between (40) and (41).] If we equate the coefficient of x on both sides of (41), we get

$$-1 \equiv (p-1)!(\text{mod } p). \tag{42}$$

Thus from (40) we get nothing, but (41) is full of information [and (42) is just the result of equating one coefficient of (41)]. As examples of (42),

$$2|(1!+1), \quad 5|(4!+1), \quad 7|(6!+1), \quad 101|(100!+1).$$

The reader can verify the first three of these easily enough, but the fourth might take a few days (100! has 158 digits).

By Fermat's theorem, the congruence

$$x^p - x \equiv 0(\text{mod } p)$$

has the roots $0, -1, -2, \ldots, -(p-1)$ (among others). With ordinary equality, roots lead to factors and thus, by analogy, (41) seems quite reasonable. This is, in fact, how we will eventually derive (41). In the meantime, we prove several preliminary theorems on polynomial congruences familiar to the reader as equalities.

Theorem 3.19. If

$$f_1(x) \equiv f_2(x)(\text{poly mod } n),$$
$$g_1(x) \equiv g_2(x)(\text{poly mod } n),$$

then

$$f_1(x) + g_1(x) \equiv f_2(x) + g_2(x)(\text{poly mod } n),$$
$$f_1(x)g_1(x) \equiv f_2(x)g_2(x)(\text{poly mod } n).$$

Proof. Coefficients of sums and products of polynomials are determined as combinations of sums and products of the coefficients of the original polynomials. Therefore, changing the coefficients of the original polynomials to congruent numbers (mod n) changes the coefficients of the answer to congruent numbers (mod n). ▲

Theorem 3.20. If $f(x)$ is a polynomial with integral coefficients and $f(a) \equiv 0(\text{mod } n)$, then there is a polynomial $g(x)$ with integral coefficients such that

$$f(x) \equiv (x-a)g(x)(\text{poly mod } n).$$

Proof. Let us divide $f(x)$ by $(x - a)$. The result is a quotient $g(x)$ with integral coefficients and a remainder b:

$$f(x) = (x - a)g(x) + b.$$

Therefore,

$$f(a) = (a - a)g(a) + b = b$$

and hence

$$b \equiv f(a) \equiv 0 (\text{mod } n).$$

Therefore,

$$f(x) \equiv f(x) - b \equiv (x - a)g(x) (\text{poly mod } n). \qquad \blacktriangle$$

For example, let $f(x) = x^2 + x + 1$. Then

$$f(1) \equiv 0 (\text{mod } 3).$$

When we divide $f(x)$ by $x - 1$, we get the result

$$\begin{array}{r} x + 2 \\ x - 1 \overline{)\, x^2 + x + 1} \\ \underline{x^2 - x} \\ 2x + 1 \\ \underline{2x - 2} \\ 3 \end{array}$$

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

(The reader acquainted with synthetic division may perform the calculations quicker and easier.) Hence

$$x^2 + x + 1 \equiv (x - 1)(x + 2) (\text{poly mod } 3).$$

Since

$$x + 2 \equiv x - 1 (\text{poly mod } 3),$$

this may be written

$$x^2 + x + 1 \equiv (x - 1)^2 (\text{poly mod } 3).$$

If we were told that

$$f(x) = (x - a)g(x),$$

$$f(b) = 0, \qquad b \neq a,$$

then we would deduce that

$$(b - a)g(b) = 0, \qquad b - a \neq 0$$

and hence

$$g(b) = 0.$$

From this we see that there is a factor of $x - b$ in $g(x)$ and this gives factors of $(x - a)(x - b)$ in $f(x)$. This is the process used in showing that successive roots of the equation

$$f(x) = 0$$

correspond to successive factors of f. We wish to imitate this process for congruences, but we immediately find that there are difficulties. Consider the example

$$x^2 - 1 \equiv 0 (\text{mod } 8). \tag{43}$$

Since

$$x \equiv 1 (\text{mod } 8)$$

is a solution, there is a factor of $(x - 1)$ in $x^2 - 1$:

$$x^2 - 1 \equiv (x - 1)(x + 1) (\text{poly mod } 8) \tag{44}$$

But now

$$x \equiv 3 (\text{mod } 8)$$

is another solution to (43), in spite of the fact that $x + 1$ does not have a factor of $x - 3 (\text{mod } 8)$. If we substitute $x = 3$ into (44), we find the trouble,

$$0 \equiv 2 \cdot 4 (\text{mod } 8).$$

The proof above that two roots of an equation correspond to two factors depends on the fact that if the product of two numbers is zero, then one of the numbers is zero. This does not always happen for congruences, as is seen above. Arithmetic (mod n) does not behave sufficiently like ordinary arithmetic to enable us to show that two distinct roots of a congruence equation correspond to two distinct factors of the polynomial.[5]

[5] The question at issue is whether the polynomial can have both factors simultaneously. For example, $x^2 - 1$ does have a factor of $(x - 1)$ (mod 8), and it also has a factor of $(x - 3) (\text{mod } 8)$:

$$x^2 - 1 \equiv (x - 3)(x + 3) (\text{poly mod } 8),$$

but $x^2 - 1$ does not have both $(x - 1)$ and $(x - 3)$ as factors simultaneously.

There is an instance that the "product of two numbers is zero implies one of them is zero" theorem carries over to congruences. If p is a prime and

$$a_1 a_2 \cdots a_k \equiv 0 (\text{mod } p),$$

then for some j,

$$a_j \equiv 0 (\text{mod } p).$$

This follows immediately from the definition of congruence and Theorem 2.8. Thus when we have a polynomial congruence (mod p), there is hope that we can proceed as with equalities. This is, in fact, true, and for the rest of this section we will restrict ourselves to prime moduli.

Theorem 3.21. If $f(x)$ is a polynomial with integral coefficients and if $a_1, a_2, \ldots, a_k$ are pairwise incongruent integers (mod p) (where p is a prime) which are solutions of the congruence equation

$$f(x) \equiv 0 (\text{mod } p),$$

then there is a polynomial $g(x)$ with integral coefficients such that

$$f(x) \equiv (x - a_1)(x - a_2) \cdots (x - a_k) g(x) (\text{poly mod } p).$$

Proof. By Theorem 3.20, there is a polynomial $g_1(x)$ with integral coefficients such that

$$f(x) \equiv (x - a_1) g_1(x) (\text{poly mod } p).$$

We now proceed to give a proof by induction. Suppose that there is a polynomial $g_j(x)$ with integral coefficients such that

$$f(x) \equiv (x - a_1)(x - a_2) \cdots (x - a_j) g_j(x) (\text{poly mod } p). \tag{45}$$

(As we have just seen, this is true for $j = 1$.) Then

$$0 \equiv f(a_{j+1}) \equiv (a_{j+1} - a_1)(a_{j+1} - a_2) \cdots (a_{j+1} - a_j) g_j(a_{j+1}) (\text{mod } p).$$

By hypothesis, none of the numbers $a_{j+1} - a_1, a_{j+1} - a_2, \ldots, a_{j+1} - a_j$ is congruent to 0(mod p) and therefore

$$g_j(a_{j+1}) \equiv 0 (\text{mod } p).$$

Thus, by Theorem 3.20, there is a polynomial $g_{j+1}(x)$ with integral coefficients such that

$$g_j(x) \equiv (x - a_{j+1}) g_{j+1}(x) (\text{poly mod } p).$$

By Theorem 3.19, we may insert this into (45) and get

$$f(x) \equiv (x - a_1)(x - a_2) \cdots (x - a_{j+1}) g_{j+1}(x) (\text{poly mod } p).$$

This completes the inductive step. Since (45) is possible for $j = 1$, it is possible for $j = 2$ and then $j = 3, \ldots$, and finally, $j = k$. ▲

Thus far, we have said nothing about the degree of a polynomial. It will be necessary to use this concept in the near future.

Definition. Let $f(x) = a_k x^k + a_{k-1}x^{k-1} + \cdots + a_1 x + a_0$ be a polynomial with integral coefficients. We define the **degree (mod *n*)** of $f(x)$ to be the largest number d such that

$$a_d \not\equiv 0 (\text{mod } n).$$

If $d < k$ this means that

$$a_{d+1} \equiv a_{d+2} \equiv \cdots \equiv a_k \equiv 0 (\text{mod } n).$$

It is possible that every coefficient of $f(x)$ is congruent to $0 (\text{mod } n)$, and then we say that the degree (mod n) of f is **undefined.**

Thus the degree (mod n) of a polynomial $f(x)$ is undefined if and only if

$$f(x) \equiv 0 (\text{poly mod } n).$$

For example, if

$$f(x) = 30x^4 - 60x^3 + 12x^2 - 6x + 3,$$

then

$$\begin{aligned}
&\text{the degree (mod 12) of } f(x) = 4,\\
&\text{the degree (mod 7) of } f(x) = 4,\\
&\text{the degree (mod 5) of } f(x) = 2,\\
&\text{the degree (mod 6) of } f(x) = 0,\\
&\text{the degree (mod 3) of } f(x) \quad \text{is undefined.}
\end{aligned}$$

Theorem 3.22. Let p be a prime and let $f(x)$ be a polynomial with integral coefficients and let the degree (mod p) of $f(x)$ be defined and equal to n. Then the equation

$$f(x) \equiv 0 (\text{mod } p) \tag{46}$$

has at most n distinct roots (mod p).

Proof. Suppose the integers $a_1, a_2, \ldots, a_{n+1}$ are pairwise incongruent (mod p) and are also solutions to (46). By Theorem 3.21, there is a polynomial

$g(x)$ with integral coefficients such that

$$f(x) \equiv (x - a_1)(x - a_2)\cdots(x - a_{n+1})g(x)(\text{poly mod } p). \tag{47}$$

It is clear from the definition of degree (mod p) that two polynomials, which are congruent as polynomials (mod p), have the same degree (mod p). Thus, since the degree (mod p) of $f(x)$ is n, the degree (mod p) of the right side of (47) is defined and equal to n. If the degree (mod p) of g is not defined, then

$$g(x) \equiv 0(\text{poly mod } p),$$

and it follows from (47) that

$$f(x) \equiv 0(\text{poly mod } p).$$

This is false, since it would imply that the degree (mod p) of $f(x)$ is undefined, whereas it is part of the hypothesis that the degree (mod p) of f is defined. Thus the degree (mod p) of $g(x)$ is also defined. Let k be the degree (mod p) of $g(x)$. By the definition of degree (mod p),

$$k \geq 0.$$

Let b_j be the coefficient of x^j in $g(x)$. Thus

$$b_k \not\equiv 0(\text{mod } p).$$

It is possible that there are powers of x higher than the kth in $g(x)$, but all their coefficients are congruent to 0(mod p) by the definition of k. Therefore,

$$g(x) \equiv b_k x^k + b_{k-1}x^{k-1} + \cdots + b_0(\text{poly mod } p)$$

and thus

$$(x - a_1)(x - a_2)\cdots(x - a_{n+1})g(x) \equiv (x - a_1)(x - a_2)\cdots \cdots(x - a_{n+1})(b_k x^k + \cdots + b_0)(\text{poly mod } p). \tag{48}$$

Hence the right side of (48) also has n as its degree (mod p). But this is absurd, since the coefficient of x^{n+1+k} on the right side is

$$b_k \not\equiv 0(\text{mod } p).$$

This contradicts our supposition that (46) can have $n + 1$ distinct roots (mod p). It follows that (46) cannot have more than $n + 1$ distinct roots (mod p) and hence must have at most n distinct roots (mod p). ▲

As the example

$$x^2 - 1 \equiv 0(\text{mod } 8)$$

[with distinct roots (mod 8) of 1, 3, 5, 7] shows, the restriction to primes in Theorem 3.22 cannot be eliminated.

Theorem 3.23. Let p be a prime, $f(x)$ be a polynomial with integral coefficients and degree (mod p) defined and equal to n. Suppose that b is the coefficient of x^n in $f(x)$ and suppose that the n integers $a_1, a_2, \ldots, a_n$ are distinct (mod p) solutions to the equation

$$f(x) \equiv 0 (\text{mod } p).$$

Then

$$f(x) \equiv b(x - a_1)(x - a_2) \cdots (x - a_n) (\text{poly mod } p).$$

Proof. We could prove this substantially the same as we proved Theorem 3.22. But instead, we will illustrate a typical application of Theorem 3.22 in this proof. Let

$$g(x) = b(x - a_1)(x - a_2) \cdots (x - a_n),$$

$$h(x) = f(x) - g(x).$$

We will use Theorem 3.22 to show that

$$h(x) \equiv 0 (\text{poly mod } p),$$

and this is obviously equivalent to the result of the theorem. Clearly $g(a_j) = 0$ for each a_j and by hypothesis $f(a_j) \equiv 0 (\text{mod } p)$ for each a_j. Therefore, the distinct (mod p) integers $a_1, a_2, \ldots, a_n$ are solutions to the congruence equation

$$h(x) \equiv 0 (\text{mod } p).$$

Thus by Theorem 3.22, either the degree (mod p) of $h(x)$ is defined and greater than or equal to n or the degree (mod p) of $h(x)$ is undefined. But $g(x)$ has no terms involving powers of x higher than the nth power and hence, if $k > n$, the coefficient of x^k in $h(x)$ is the same as the coefficient of x^k in $f(x)$, which is congruent to 0(mod p) by the definition of n. Also, by the definition of b, the coefficient of x^n in $h(x)$ is 0. Hence the degree (mod p) of $h(x)$ cannot possibly be defined and greater than or equal to n. Thus, by Theorem 3.22, the congruence

$$h(x) \equiv 0 (\text{mod } p)$$

has too many solutions to allow the degree (mod p) of $h(x)$ to be defined. Therefore, the degree (mod p) of $h(x)$ is not defined and therefore

$$h(x) \equiv 0 (\text{poly mod } p). \qquad \blacktriangle$$

We illustrate the application of Theorem 3.23 by proving the result in (42). It is more convenient to derive this from the factorization of $x^{p-1} - 1$ than from (41).

Theorem 3.24 (Wilson's Theorem). If p is a prime, then

$$(p-1)! \equiv -1 (\text{mod } p).$$

Proof. By Fermat's theorem (3.14), the $p-1$ pairwise incongruent (mod p) numbers $-1, -2, -3, \ldots, -(p-1)$ satisfy the congruence

$$x^{p-1} - 1 \equiv 0 (\text{mod } p).$$

Clearly the degree (mod p) of $x^{p-1} - 1$ is $p-1$ and the coefficient of x^{p-1} in $x^{p-1} - 1$ is 1. Therefore, by Theorem 3.23,

$$x^{p-1} - 1 \equiv (x+1)(x+2)\cdots(x+p-1) (\text{poly mod } p). \tag{49}$$

Hence the constant terms (the coefficient of x^0) on both sides are congruent,

$$-1 \equiv 1 \cdot 2 \cdot 3 \cdots (p-1) (\text{mod } p). \qquad \blacktriangle$$

EXERCISES

1. Factor $x^2 - 3x - 3$ into linear factors (poly mod 5).
2. Factor $2x^2 - 3x - 2$ into linear factors (poly mod 7).
3. Factor $x^2 + 1$ into linear factors (poly mod 13).
4. Factor $x^2 + 1$ into linear factors (poly mod 17).
5. Factor $x^3 + x^2 + 4x + 1$ into linear factors (poly mod 7).
6. Factor $x^3 + 4x^2 + 3x + 6$ into linear factors (poly mod 7).
7. Is it allowable to divide both sides of (40) by x and then substitute $x = 0$ in the resulting congruence to prove Theorem 3.24? Explain.
8. Use the fact that

$$p - j \equiv -j (\text{mod } p)$$

to show that if p is an odd prime, $p = 2k + 1$, then

$$(p-1)! \equiv (-1)^k \left[\left(\frac{p-1}{2} \right)! \right]^2 (\text{mod } p).$$

9. Use the result of problem 8 to show that if p is a prime, $p \equiv 1 (\text{mod } 4)$, then $[(p-1)/2]!$ is a solution to the congruence equation

$$x^2 + 1 \equiv 0 (\text{mod } p).$$

10. If $n > 4$ is a composite number, show that $n | (n-1)!$ Conclude that

$$(n-1)! \not\equiv -1 (\text{mod } n).$$

(This shows that Wilson's theorem can be used as a proof of primality. It is unfortunately not practical for large numbers.)

11. What is the result when the coefficients of x^{p-2} are equated on both sides of (49)? Is your result valid for $p = 2$? Explain.

*12. What is the result when the coefficients of x^{p-3} are equated on both sides of (49)? Separate the cases of $p = 2$, $p = 3$, $p > 3$. Prove the result for $p > 3$ without the use of polynomials. The formulas

$$\sum_{j=1}^{n} j = \frac{n(n+1)}{2}, \qquad \sum_{j=1}^{n} j^2 = \frac{n(n+1)(2n+1)}{6}, \qquad \sum_{j=1}^{n} j^3 = \left[\frac{n(n+1)}{2}\right]^2$$

may be helpful.

13. Find all distinct solutions (mod 5) or show there are none:

$$x^2 + x + 3 \equiv 0 \pmod 5.$$

14. Find all distinct solutions (mod 5) or show there are none:

$$x^2 + 2x + 3 \equiv 0 \pmod 5.$$

15. Find all distinct solutions (mod 15) or show there are none:

$$x^2 \equiv 4 \pmod{15}.$$

16. Find all distinct solutions (mod 8) or show there are none:

$$x^2 + x + 4 \equiv 0 \pmod 8.$$

17. Find all distinct solutions (mod 11) or show there are none:

$$x^3 + 2x^2 + 5x + 6 \equiv 0 \pmod{11}.$$

*18. Use the coefficient of x on both sides of (49) to prove that if $p \geq 3$, then $p|a$, where

$$\frac{a}{b} = 1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{p-1}.$$

19. Use the congruence equation $x^2 - 1 \equiv 0 \pmod p$ to show that if $(a,p) = 1$, then

$$a^{(p-1)/2} \equiv \pm 1 \pmod p.$$

3.7. Primitive Roots

We have seen that if $(a,n) = 1$, then

$$a^{\phi(n)} \equiv 1 \pmod n.$$

In this section we investigate the twin problems of finding the smallest positive power such that a to that power is congruent to $1 \pmod n$ and finding those a for which this power is actually $\phi(n)$.

Definition. Suppose that $(a,n) = 1$. We define the **order** of $a(\text{mod } n)$ to be the smallest positive integer, call it b, such that

$$a^b \equiv 1(\text{mod } n)$$

and we write

$$b = \text{ord}_n(a).$$

For example, $\text{ord}_{13}(5) = 4$, since

$$5^1 \equiv 5(\text{mod } 13), \qquad 5^2 \equiv 25 \equiv -1(\text{mod } 13),$$

$$5^3 \equiv -5(\text{mod } 13), \qquad 5^4 \equiv -25 \equiv 1(\text{mod } 13).$$

Thanks to Euler's theorem (3.13), if $(a,n) = 1$, we are guaranteed that there is a power to which a can be raised to be congruent to $1(\text{mod } n)$ and thus there really is such a thing as $\text{ord}_n(a)$. It also follows from Euler's theorem that if $(a,n) = 1$,

$$\text{ord}_n(a) \leq \phi(n).$$

On the other hand, if $(a,n) > 1$, then the equation

$$ax \equiv 1(\text{mod } n) \tag{50}$$

has no solutions, by Theorem 3.6. Thus for $b \geq 1$,

$$a^b \equiv 1(\text{mod } n)$$

is impossible, since it would provide the solution $x = a^{b-1}$ to (50). Thus if $(a,n) > 1$, it is impossible to define the order of $a(\text{mod } n)$.

Definition. If $(a,n) = 1$ and $\text{ord}_n(a) = \phi(n)$, then we say that a is a **primitive root** of n.

Unfortunately, the analogous situation in equalities is worded differently: If $\alpha^k = 1$, but $\alpha^m \neq 1$ for $0 < m < k$, then it is said that α is a **primitive *k*th root of unity.** By analogy, if $\text{ord}_n(a) = \phi(n)$, then

$$a^{\phi(n)} \equiv 1(\text{mod } n), \qquad \text{but } a^m \not\equiv 1(\text{mod } n) \qquad \text{for } 0 < m < \phi(n),$$

and at the very least we would expect something like "a is a primitive root of unity (mod n)." But this is never said. As an example, 3 is a primitive root of 10, since $\phi(10) = 4$ and

$$3^1 \equiv 3(\text{mod } 10), \qquad 3^2 \equiv 9 \equiv -1(\text{mod } 10),$$

$$3^3 \equiv -3(\text{mod } 10), \qquad 3^4 \equiv -9 \equiv 1(\text{mod } 10).$$

As another example, there are no primitive roots of 8, since $\phi(8) = 4$ and a reduced residue system is given by the numbers 1, 3, 5, and 7 with

$$1^1 \equiv 1 (\text{mod } 8), \qquad 3^2 \equiv 1 (\text{mod } 8),$$

$$5^2 \equiv 1 (\text{mod } 8), \qquad 7^2 \equiv 1 (\text{mod } 8).$$

We will shortly show that there are primitive roots mod p if p is a prime. In the meantime, we prove a result that will help us limit the possible values of $\text{ord}_n(a)$.

Theorem 3.25. If $b > 0$, $c > 0$, $d = (b,c)$, and

$$a^b \equiv 1 (\text{mod } n), \qquad a^c \equiv 1 (\text{mod } n),$$

then

$$a^d \equiv 1 (\text{mod } n).$$

Proof. By Theorem 2.2, there are integers r and s such that

$$d = br - cs.$$

This means that for all integers t,

$$d = b(r + ct) - c(s + bt),$$

and since if we take t sufficiently large, both $r + ct$ and $s + bt$ will be positive, we may as well assume that $r > 0$, $s > 0$. But then

$$a^d \equiv 1^s a^d \equiv (a^c)^s a^d \equiv a^{cs+d} \equiv a^{br} \equiv (a^b)^r \equiv 1^r \equiv 1 (\text{mod } n). \qquad \blacktriangle$$

We worried about making r and s positive because otherwise the multiplications in the last step would be divisions and we have not even defined $a/b (\text{mod } n)$, let alone prove any results about it. As an example of the last theorem, we show that $x \equiv 1 (\text{mod } 29)$ is the only solution to the congruence

$$x^{13} \equiv 1 (\text{mod } 29). \tag{51}$$

Suppose $x = a$ is a solution to (51). Then $(a,29) = 1$. If follows from Fermat's theorem (3.14) that

$$a^{28} \equiv 1 (\text{mod } 29).$$

But since $(13,28) = 1$, Theorem 3.25 says that

$$a^1 \equiv 1 (\text{mod } 29)$$

also. [It is easily seen that this is a solution to (51).] As another example of Theorem 3.25 at work, we have the result,

Theorem 3.26. If $(a,n) = 1$ and for some $b > 0$,

$$a^b \equiv 1 (\text{mod } n),$$

then $\text{ord}_n(a) | b$. In particular, $\text{ord}_n(a) | \phi(n)$. Conversely, if $\text{ord}_n(a) | b$, then

$$a^b \equiv 1 (\text{mod } n).$$

Proof. Let

$$d = (\text{ord}_n(a), b).$$

Then

$$d \leq \text{ord}_n(a) \tag{52}$$

and also, by Theorem 3.25,

$$a^d \equiv 1 \ (\text{mod } n).$$

But by the definition of $\text{ord}_n(a)$, this means that

$$d \geq \text{ord}_n(a).$$

This, combined with (52), says that

$$\text{ord}_n(a) = d.$$

By the definition of d, $d | b$, and hence $\text{ord}_n(a) | b$. Conversely, if $\text{ord}_n(a) | b$, then for some k,

$$b = k \cdot \text{ord}_n(a)$$

and hence

$$a^b \equiv [a^{\text{ord}_n(a)}]^k \equiv 1 (\text{mod } p). \qquad \blacktriangle$$

Theorem 3.26 lightens the labor when we attempt to find $\text{ord}_n(a)$, since it is now only necessary to check the divisors of $\phi(n)$. As an example, let us find $\text{ord}_{23}(2)$. Since $\phi(23) = 22$, we see that $\text{ord}_{23}(2)$ is one of the four divisors of 22 : 1, 2, 11, 22. The numbers 1 and 2 are obvious failures. [In fact, $\text{ord}_n(a) = 1$ if and only if $a \equiv 1 (\text{mod } n)$.] Thus we need only look at $2^{11} (\text{mod } 23)$. If we make no mistakes, we will come up with $2^{11} \equiv \pm 1 (\text{mod } 23)$ (see problem 19 of Section 3.6), but this remark is meant to serve only as a check. The useful thing is that we do not have to look at each power of 2 in getting up to 2^{11}.

$$2^2 \equiv 4 (\text{mod } 23),$$

$$2^4 \equiv 4^2 \equiv 16 \equiv -7 (\text{mod } 23),$$

$$2^8 \equiv (-7)^2 \equiv 49 \equiv 3 (\text{mod } 23),$$

$$2^{10} \equiv 2^8 \cdot 2^2 \equiv 3 \cdot 4 \equiv 12 (\text{mod } 23),$$

$$2^{11} \equiv 2^{10} \cdot 2 \equiv 12 \cdot 2 \equiv 1 (\text{mod } 23).$$

Thus $\text{ord}_{23}(2) = 11$.

At this point we will restrict ourselves to prime moduli. As the example of $n = 8$ showed, not all n have primitive roots. The next theorem will aid us in showing that all primes have primitive roots.

Theorem 3.27. If p is a prime and $d|(p-1)$, then the congruence equation

$$x^d \equiv 1 (\text{mod } p)$$

has exactly d distinct solutions.

Proof. We already know that the equation

$$x^{p-1} - 1 \equiv 0 (\text{mod } p)$$

has exactly $p-1$ distinct solutions (mod p) (this is Fermat's theorem, 3.14). Since $d|(p-1)$, let $kd = p-1$. Then

$$\begin{aligned} x^{p-1} - 1 &= x^{kd} - 1 \\ &= (x^d - 1)[x^{d(k-1)} + x^{d(k-2)} + x^{d(k-3)} + \cdots + x^d + 1]. \end{aligned}$$

Therefore, there are $(p-1)$ distinct solutions to the congruence

$$(x^d - 1)[x^{d(k-1)} + x^{d(k-2)} + \cdots + x^d + 1] \equiv 0 (\text{mod } p), \tag{53}$$

and since p is a prime, every solution to (53) is a solution of at least one of the two congruences

$$x^d - 1 \equiv 0 (\text{mod } p), \tag{54}$$

$$x^{d(k-1)} + x^{d(k-2)} + \cdots + x^d + 1 \equiv 0 (\text{mod } p). \tag{55}$$

By Theorem 3.22, (55) has at most $d(k-1)$ distinct solutions (mod p). Since there are $p-1$ distinct numbers (mod p) that satisfy at least one of (54) and (55), and at most $d(k-1)$ of them satisfy (55), at least $(p-1) - d(k-1)$ distinct integers (mod p) satisfy (54); that is, (54) has at least

$$(p-1) - d(k-1) = [(p-1) - dk] + d = d$$

distinct solutions (mod p). By Theorem 3.22, (54) can have no more than d solutions and thus has exactly d solutions. ▲

Theorem 3.28. Let p be a prime and let $d|(p-1)$. Then there are exactly $\phi(d)$ distinct integers (mod p) whose order (mod p) is d. In particular, there are exactly $\phi(p-1)$ primitive roots of p.

Proof. Since any solution of the equation

$$x^d \equiv 1 (\text{mod } p)$$

must be relatively prime to p [recall that the definition of order (mod p) had this condition], we need only show that there are $\phi(d)$ solutions to this equation that do not satisfy similar equations with smaller d. We will give a proof by contradiction (which in this case is a means of avoiding a proof by induction). Let us suppose that the theorem is false. Then there is a smallest d for which the theorem is false and we will let n be that smallest value. Thus if $d < n$ and $d|(p-1)$, there are exactly $\phi(d)$ distinct numbers (mod p) whose order is d. Let us look at the solutions to

$$x^n \equiv 1 (\text{mod } p). \tag{56}$$

By Theorem 3.26, $x = a$ is a solution of (56) if and only if $\text{ord}_p(a)|n$. Thus the number of solutions to (56) with order (mod p) less than n is

$$\begin{aligned} &\sum_{\substack{d|n \\ d<n}} (\text{number of distinct integers (mod } p) \text{ whose order (mod } p) \text{ is } d) \\ &\quad = \sum_{\substack{d|n \\ d<n}} \phi(d) \\ &\quad\quad \sum_{d|n} \phi(d) - \phi(n) \\ &\quad = n - \phi(n), \end{aligned}$$

by Theorem 3.17. Thus the number of solutions of (56) with order (mod p) equal to n is

$$n - [n - \phi(n)] = \phi(n).$$

This contradicts the definition of n, thereby proving the theorem. ▲

Shown in Table 2 at the end of the book are the smallest primitive roots of each $p < 500$. As we noted earlier, there are no primitive roots of 8. To satisfy the reader's curiosity, an integer n has primitive roots if and only if n is one of the five categories

$$n = 1, \qquad n = 2, \qquad n = 4, \qquad n = p^k, \qquad n = 2p^k,$$

where p is an odd prime and k is a positive integer. Thus 7^{47}, $2 \cdot 101^2$, and 10 have primitive roots (the last was verified earlier) while 8, 16, 15, and 20 do not. This result is left to miscellaneous exercises 3–7 at the end of the chapter. The result that there are $\phi(p-1)$ primitive roots of p is sometimes written: There are $\phi(\phi(p))$ primitive roots of p. This is the more general form, since it can be shown that if there is a primitive root of n, then there are exactly

$\phi(\phi(n))$ primitive roots of n which are distinct (mod n) (problem 11 at the end of the section).

We conclude the chapter with two applications of the above theorems. Another application to decimal expansions of rational numbers will be given in Chapter 6. As our first example, we investigate the question as to when the equation

$$x^2 + 1 \equiv 0 (\text{mod } p)$$

has solutions. This is the equation for equality that resulted in the invention of complex numbers. Here the situation is different, as there are sometimes already integral solutions to the congruence equation.

Theorem 3.29. Let p be a prime. The equation

$$x^2 \equiv -1 (\text{mod } p) \tag{57}$$

has solutions if $p = 2$ or if $p \equiv 1 (\text{mod } 4)$ but does not have any solutions if $p \equiv 3 (\text{mod } 4)$.

Proof. When $p = 2$, $x = 1$ is a solution. Suppose that $p \equiv 1 (\text{mod } 4)$. Then $4 | (p - 1)$. By Theorem 3.28, there is an integer a such that

$$\text{ord}_p(a) = 4.$$

In particular,

$$(a^2 - 1)(a^2 + 1) \equiv a^4 - 1 \equiv 0 (\text{mod } p)$$

and hence either

$$a^2 - 1 \equiv 0 (\text{mod } p)$$

or

$$a^2 + 1 \equiv 0 (\text{mod } p).$$

The first case cannot happen since $\text{ord}_p(a) = 4$ and therefore

$$a^2 + 1 \equiv 0 (\text{mod } p).$$

Hence a is a solution to (57).

Suppose that $p \equiv 3 (\text{mod } 4)$. Then

$$2 | (p - 1), \qquad \text{but } 4 \nmid (p - 1)$$

and hence

$$(p - 1, 4) = 2 \tag{58}$$

Suppose that

$$a^2 \equiv -1 \pmod{p}. \tag{59}$$

Then

$$a^4 \equiv (a^2)^2 \equiv (-1)^2 \equiv 1 \pmod{p} \tag{60}$$

[it follows that $(a,p) = 1$] and by Fermat's theorem (3.14),

$$a^{p-1} \equiv 1 \pmod{p} \tag{61}$$

also. Hence, by (58), (60), (61) and Theorem 3.25,

$$a^2 \equiv 1 \pmod{p}. \tag{62}$$

It follows from (59) and (62) that

$$1 \equiv -1 \pmod{p}$$

and hence

$$2 \equiv 0 \pmod{p}.$$

This is impossible, since it says that an odd prime divides 2. Therefore, (59) is untenable and hence (57) has no solutions when $p \equiv 3 \pmod{4}$. ▲

The next theorem is a simple corollary of Theorem 3.29, but it will be used in Chapters 5 and 8.

Theorem 3.30. If p is a prime $\equiv 3 \pmod{4}$ and a and b are integers such that

$$a^2 + b^2 \equiv 0 \pmod{p},$$

then

$$a \equiv b \equiv 0 \pmod{p}.$$

Proof. We first show that $b \equiv 0 \pmod{p}$. If $b \not\equiv 0 \pmod{p}$, then there exists an integer c such that

$$bc \equiv 1 \pmod{p},$$

and then

$$(ac)^2 \equiv a^2c^2 \equiv -b^2c^2 \equiv -(bc)^2 \equiv -1 \pmod{p}.$$

But this is impossible by Theorem 3.29. Therefore,

$$b \equiv 0 \pmod{p}$$

and hence

$$a^2 \equiv a^2 + 0^2 \equiv a^2 + b^2 \equiv 0 (\text{mod } p)$$

so that $p|a^2$, and thus $p|a$; that is,

$$a \equiv 0 (\text{mod } p). \qquad \blacktriangle$$

We turn now to a completely different area. Gauss showed that if α is a primitive kth root of unity (that is, $\alpha^k = 1$ but $\alpha^m \neq 1$ if $0 < m < k$), then

$$\left(\sum_{j=0}^{k-1} \alpha^{j^2}\right)^2 = \begin{cases} k & \text{if } k \equiv 1 (\text{mod } 4), \\ 0 & \text{if } k \equiv 2 (\text{mod } 4), \\ -k & \text{if } k \equiv 3 (\text{mod } 4), \\ 2k\alpha^{k/4} & \text{if } k \equiv 4 (\text{mod } 4). \end{cases}$$

This is difficult to check in particular cases because of the nature of α (a complex number with irrational real and imaginary parts when $k > 12$). Owing to the great similarities between the theory of congruences and equalities, we might suspect that a similar result is true for congruences. We have noted one major difference between arithmetic (mod n) and equalities: If n is composite, then 0 is congruent (mod n) to the product of two nonzero (mod n) integers. This made a great difference when we dealt with polynomial equations (mod n). Since Gauss's result certainly deals with polynomial equations, it seems best to investigate Gauss's result for congruences (mod p), where p is a prime. The analogue of a primitive kth root of unity is an integer whose order (mod p) is k. Thus we may conjecture that if p is a prime and

$$\text{ord}_p(a) = k,$$

then

$$\left(\sum_{j=0}^{k-1} a^{j^2}\right)^2 \equiv \begin{cases} k (\text{mod } p) & \text{if } k \equiv 1 (\text{mod } 4), \\ 0 (\text{mod } p) & \text{if } k \equiv 2 (\text{mod } 4), \\ -k (\text{mod } p) & \text{if } k \equiv 3 (\text{mod } 4), \\ 2ka^{k/4} (\text{mod } p) & \text{if } k \equiv 4 (\text{mod } 4). \end{cases} \tag{63}$$

Let us check this conjecture for $k = 3$. We cannot choose any prime that comes to mind; by Theorem 3.26,

$$\text{ord}_p(a) | (p - 1),$$

in this case, $3|(p - 1)$. If $3|(p - 1)$, then by Theorem 3.28, there will be integers whose order (mod p) is 3. Let us pick $p = 13$ for our example. The next question is: Can we find a number whose order (mod 13) is 3 without

proceeding by trial and error? The answer is yes, if there is a table of primitive roots available. We see from Table two at the end of the book that 2 is a primitive root of 13. Thus

$$2^{12} \equiv 1 (\text{mod } 13), \qquad \text{but} \quad 2^n \not\equiv 1 (\text{mod } 13) \qquad \text{for} \quad 1 \leq n \leq 11.$$

It follows that

$$(2^4)^3 \equiv 1 (\text{mod } 13), \qquad \text{but} \quad (2^4)^m \not\equiv 1 (\text{mod } 13) \qquad \text{for} \quad m = 1, 2.$$

Thus by definition,

$$\text{ord}_{13}(16) = 3.$$

For our calculations, it will be best to replace 16 by the congruent number 3(mod 13) and thus we let $a = 3$. Then

$$\begin{aligned} \left(\sum_{j=0}^{2} 3^{j^2} \right)^2 &\equiv (3^0 + 3^1 + 3^4)^2 \ (\text{mod } 13) \\ &\equiv (1 + 3 + 3^3 \cdot 3)^2 (\text{mod } 13) \\ &\equiv (1 + 3 + 3)^2 \qquad (\text{mod } 13) \\ &\equiv 7^2 \qquad (\text{mod } 13) \\ &\equiv 49 - 4 \cdot 13 \qquad (\text{mod } 13) \\ &\equiv -3 \qquad (\text{mod } 13), \end{aligned}$$

as predicted by (63).

This example is instructive for two reasons. First it has illustrated several of the theorems of this chapter at work in a numerical example. Second, the conjecture itself (assuming it is true) is likely to have a proof that parallels the proof of Gauss's result for equalities. Here, as in much of this chapter, we have taken proofs from results on equalities and adapted them to congruences. In other circumstances, we might have to readapt these proofs once again. This illustrates the great advantage of the modern axiomatic method. Starting from a certain set of axioms [in this case, the so-called field axioms, satisfied by the rational numbers, the real numbers, the complex numbers, congruences (mod p), and other systems] one derives certain theorems. The resulting theorems are then true for everything that satisfies the axioms, which results in a great saving of needless duplication of proofs.

EXERCISES

1. Did this section prove the conjecture in (63) for $k = 3$?
2. How many distinct solutions (mod 102) are there to the equation

$$x^{85} \equiv 1 (\text{mod } 102)?$$

3. Suppose that $(a,n) = 1$. Prove that

$$a^b \equiv a^c \pmod{n}$$

if and only if

$$b \equiv c \pmod{\operatorname{ord}_n(a)}.$$

4. Show that if $(a,15) = 1$, then

$$a^{\phi(15)/2} \equiv 1 \pmod{15}$$

and hence 15 has no primitive roots. [*Hint:* Examine the congruence (mod 3) and (mod 5).]
5. Show that 21 has no primitive roots (see problem 4).
6. Show that 35 has no primitive roots (see problem 4).
7. Show that if g is a primitive root of n, then the numbers

$$g, g^2, g^3, \ldots, g^{\phi(n)}$$

form a reduced residue system (mod n).
8. Show that if p is a prime, $p \equiv 1 \pmod 4$ and g is a primitive root of p, then $g^{(p-1)/4}$ is a solution to the equation

$$x^2 \equiv -1 \pmod{p}.$$

9. There are four solutions to the equation

$$x^2 + 1 \equiv 0 \pmod{65}.$$

Find them by solving this equation (mod 5) and (mod 13) and then using the Chinese remainder theorem.
10. Given that 3 is a primitive root of 31, show that 3^5, 3^{10}, 3^{15}, 3^{20}, 3^{25}, and 3^{30} are the six distinct roots of the equation

$$x^6 \equiv 1 \pmod{31}.$$

Since

$$x^6 - 1 = (x^3 - 1)(x^3 + 1) = (x - 1)(x^2 + x + 1)(x + 1)(x^2 - x + 1),$$

the six numbers above satisfy the equation

$$(x - 1)(x^2 + x + 1)(x + 1)(x^2 - x + 1) \equiv 0 \pmod{31}.$$

Which solution goes with which factor? (Do this without substituting the solutions into the factors, if possible.)
11. Show that if n has a primitive root, then n has exactly $\phi(\phi(n))$ primitive roots. (*Hint:* Use the result of problem 7 and decide which powers of g give the primitive roots of n.)

12. Find all solutions to the equation

$$x^{10} \equiv 1 (\text{mod } 14).$$

13. Verify the conjecture in (63) for $k = 5$ and whatever values of p and a that you find convenient.
14. Repeat problem 13 with $k = 6$.
15. Repeat problem 13 with $k = 7$.
16. Repeat problem 13 with $k = 8$.

MISCELLANEOUS EXERCISES

1. Show that if p and q are different odd primes, and if $(a,pq) = 1$, then

$$a^{\phi(pq)/2} \equiv 1 (\text{mod } pq).$$

2. Show that if $n > 2$, then $2|\phi(n)$.
3. Use the ideas in problems 1 and 2 to show that if $n = ab$, where $a > 2$, $b > 2$, $(a,b) = 1$, then n has no primitive roots. Show that the only numbers which can possibly have primitive roots are those of the form 1, 2, 4, p^k, and $2p^k$, where p is an odd prime.
4. Suppose p is an odd prime, k and g are positive integers. Use the binomial theorem to show that

$$(g + p)^{\phi(p^k)} \equiv g^{\phi(p^k)} - p^k g^{\phi(p^k)-1} (\text{mod } p^{k+1}).$$

   This result is false if $p = 2$ (try $g = 1$, $k = 2$). Where does your proof use the fact that p is odd?
5. Show that if p is an odd prime and n is a positive integer then there is a primitive root of p^n. [*Hint:* Suppose g is a primitive root of p^k. Use problem 4 to show that either g or $g + p$ (or both) is a primitive root of p^{k+1}.]
6. Show that if p is an odd prime, $n > 0$, then there is a primitive root of $2p^n$. [*Hint:* Let g be a primitive root of p^n (such a number exists by problem 5). Show that either g or $g + p^n$ is a primitive root of $2p^n$.]
7. Show that if g is a primitive root of p^2, then g is a primitive root of p^n for all $n \geq 2$. [*Hint:* By problem 5, there are primitive roots of p^n and problem 11, page 107, there are exactly $\phi(\phi(p^n))$ such primitive roots. Investigate how these are related to the $\phi(\phi(p^2))$ primitive roots of p^2.]
8. The Fermat numbers are defined as

$$F_n = 2^{2^n} + 1.$$

   Raise the congruence

$$2^{2^n} \equiv -1 (\text{mod } F_n)$$

to the (2^{2^n-n})th power and use your result to show that every F_n is either a prime or a pseudoprime. The Polish astronomer Banachiewicz has conjectured that Fermat knew this fact and that this is one of the reasons Fermat conjectured that every F_n is prime after having verified only that F_0, F_1, F_2, F_3, and F_4 are primes (recall that in Fermat's time, the Chinese conjecture that there is no such thing as a pseudoprime was still believed). Thus when Euler showed in 1732 that F_5 was not a prime, he had actually produced a pseudoprime 87 years before the first announced example of one.

9. Let

$$F_n = 2^{2^n} + 1$$

and suppose that $p|F_n$, where p is a prime (possibly F_n itself). Show that

$$2^{2^{n+1}} \equiv 1 (\text{mod } p)$$

so that $\text{ord}_p(2)|2^{n+1}$. Use this to show that

$$\text{ord}_p(2) = 2^{n+1}$$

[first show that $\text{ord}_p(2)$ is a power of 2]. Since $\text{ord}_p(2)|(p-1)$, show that there is an integer k such that

$$p = k \cdot 2^{n+1} + 1.$$

In the next two problems, we will see that if $n > 1$, then k is even.

10. Suppose $p = 8m + 1$ is a prime. Show that

$$2^{4m} \cdot (4m)! = 2 \cdot 4 \cdot 6 \cdots 4m[p - (4m-1)][p - (4m-3)] \cdots [p-1]$$

and use this to show that

$$\begin{aligned} 2 \cdot 4 \cdot 6 \cdots 8m &\equiv 2 \cdot 4 \cdot 6 \cdots 4m[-(4m-1)][-(4m-3)] \cdots [-1] (\text{mod } p) \\ &\equiv (-1)^{2m} 2 \cdot 4 \cdot 6 \cdots 4m(4m-1)(4m-3) \cdots (1) (\text{mod } p) \\ &\equiv (4m)! (\text{mod } p). \end{aligned}$$

Use this to prove that

$$2^{(p-1)/2} \equiv 1 (\text{mod } p).$$

11. Use the results of problems 9 and 10 to show that if $n > 1$ and p is a prime divisor of F_n, then

$$\text{ord}_p(2) \left| \left(\frac{p-1}{2} \right) \right.$$

and thus there is an integer t such that

$$p = t \cdot 2^{n+2} + 1.$$

As an example, if $n = 5$, then any prime divisor of F_5 must be of the form

$$p = 128t + 1.$$

When $t = 5$, we get the prime $p = 641$, which does divide F_5:

$$F_5 = 641 \cdot 6\,700\,417.$$

This was done in 1732 by Euler, who, in addition, announced that 6 700 417 was a prime so that F_5 could be factored no further. If p is a prime divisor of 6 700 417, show that there is an integer t such that

$$p = 128t + 1.$$

Given that $(128 \cdot 21 + 1)^2 > 6\,700\,417$, show that if 6 700 417 is composite, then it is divisible by a prime among one of the twenty numbers

$$128t + 1, \qquad 1 \leq t \leq 20.$$

The primes in this list are $257(t = 2)$, $641(t = 5)$, $769(t = 6)$, $1153(t = 9)$, and $1409(t = 11)$, none of which divide 6 700 417. Thus 6 700 417 is a prime.

12. Show that every integer of the form

$$4 \cdot 14^k + 1, \qquad k \geq 1$$

is composite. (*Hint:* Show that there is a factor of 3 when k is odd and a factor of 5 when k is even.)

13. Show that every integer of the form

$$521 \cdot 12^k + 1, \qquad k \geq 1$$

is composite. [*Hint:* Show that there is a factor of 13 when k is odd, a factor of 5 when $k \equiv 2 (\text{mod } 4)$, and a factor of 29 when $4|k$.]

14. Show that every integer of the form $a \cdot 2^k + 1$, where $k \geq 1$ and

$$a = 2\,935\,363\,331\,541\,925\,531,$$

is composite. You may assume that

$$a \equiv 1 (\text{mod } F_0F_1F_2F_3F_4p_1), \qquad a \equiv -1 (\text{mod } p_2),$$

where

$$p_1 = 6\,700\,417, \qquad p_2 = 641,$$

and

$$p_1 p_2 = F_5.$$

[*Hint:* Consider separately the cases $k \equiv 1 (\text{mod } 2)$, $k \equiv 2 (\text{mod } 4)$, $k \equiv 4 (\text{mod } 8)$, $k \equiv 8 (\text{mod } 16)$, $k \equiv 16 (\text{mod } 32)$, $k \equiv 32 (\text{mod } 64)$, and $k \equiv 64 (\text{mod } 64)$.] This result was first proved in 1960 by Sierpinski, who compared it with the unsolved problem of whether or not there are infinitely many primes of the form $1 \cdot 2^k + 1$ (when $k = 2^n$ we have F_n). Sierpinski also noted that if $1 \leq a \leq 100$, then there is at least one prime of the form $a \cdot 2^k + 1$.

15. The Mersenne numbers, M_m, defined by

$$M_m = 2^m - 1$$

have been well known since 1644 when Mersenne made an incorrect conjecture on the primality (or lack of primality) of all M_m with $m \leq 257$. Show that if m is a prime, then M_m is either a prime or a pseudoprime. Show further that if m is a pseudoprime, then M_m is a pseudoprime. Conclude that there are infinitely many pseudoprimes. The number $M_{11} = 23 \cdot 89$ is a pseudoprime and thus there was a number well known to Fermat available as an example of a pseudoprime 175 years before the first announced example of one.

16. Suppose p is a prime $\equiv 1 (\text{mod } 8)$. Use the result of problem 10 to show that 2 is congruent (mod p) to an even power of a primitive root of p and hence show that the equation

$$x^2 \equiv 2 (\text{mod } p)$$

has solutions.

17. Suppose that p is a prime and $(a,p) = 1$. Show that the equation

$$x^2 \equiv a (\text{mod } p)$$

has solutions if

$$a^{(p-1)/2} \equiv 1 (\text{mod } p)$$

and does not have solutions if

$$a^{(p-1)/2} \equiv -1 (\text{mod } p).$$

18. Determine whether or not 945 827 is a prime, given that

$$a \equiv 149\,762 (\text{mod } 945\,827),$$

where a is the product of all the primes less than 1000.

19. Show that if p is a prime and $\operatorname{ord}_p(a) = 3$, then

$$\left(\sum_{j=0}^{2} a^{j^2}\right)^2 \equiv -3 (\operatorname{mod} p).$$

20. Show that if p is a prime and $\operatorname{ord}_p(a) = 4$, then

$$\left(\sum_{j=0}^{3} a^{j^2}\right)^2 \equiv 8a (\operatorname{mod} p).$$

21. Show that if p is a prime and $\operatorname{ord}_p(a) = 6$, then

$$\sum_{j=0}^{5} a^{j^2} \equiv 0 (\operatorname{mod} p).$$

22. Show that for all integers a and b,

$$ab(a^2 - b^2)(a^2 + b^2)$$

is divisible by 30. When showing that 2, 3, or 5 divides this number, do not break the problem up into cases (such as, for example, case 1 : one of a and b even ; case 2 : both of a and b odd).

23. Show that

$$\lim_{k \to \infty} \frac{n^{k+1}}{\sigma(n^k)} = \phi(n)$$

and use this equation to prove that $\phi(n)$ is multiplicative. (Of course, the way we have done things in this chapter, this equation could not be derived without the knowledge that $\phi(n)$ is multiplicative.)

24. The Möbius function is defined as

$$\mu(n) = \begin{cases} 1 & \text{if } n = 1, \\ (-1)^k & \text{if } n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}, \quad a_1 = a_2 = \cdots = a_k = 1, \\ 0 & \text{if } n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}, \quad \text{some } a_j \geq 2. \end{cases}$$

Show that $\mu(n)$ is multiplicative and that

$$\sum_{d|n} \mu(d) = \begin{cases} 1 & \text{if } n = 1, \\ 0 & \text{if } n > 1. \end{cases}$$

25. Since $d|(j, n)$ if and only if $d|j$ and $d|n$, use the result of problem 24 to show that

$$\phi(n) = \sum_{j=1}^{n} \sum_{\substack{d|j \\ d|n}} \mu(d) = \sum_{d|n} \sum_{\substack{j=1 \\ d|j}}^{n} \mu(d) = \sum_{d|n} \frac{n}{d} \mu(d) = n \sum_{d|n} \frac{\mu(d)}{d}$$

and use this to show that $\phi(n)$ is multiplicative. Show also that this result gives $\phi(p^a)$ when p is a prime and $a \geq 1$.

26. There is a general connection between Theorem 3.17 and the result of problem 25, which is known as the Möbius inversion formula. Use the result of problem 24 to show that

$$f(n) = \sum_{d|n} g(d)$$

for all n if and only if

$$g(n) = \sum_{d|n} f(n/d)\mu(d)$$

for all n.

27. After problem 26, the result of problem 25 follows immediately from Theorem 3.17. Prove Theorem 3.17 directly by showing that

$$n = \sum_{d|n} \sum_{\substack{j=1 \\ (j,n)=d}}^{n} 1 = \sum_{d|n} \phi(n/d).$$

28. From a given date we may calculate how many days have passed (or will pass) between then and today. This number of days (mod 7) will tell us the day of the week of the given date (assuming we know what day it is). This principle allows us to determine the day of the week of any date in history. Let the days of the week be represented by the numbers 0, 1, 2, 3, 4, 5, 6 (Sunday being 0 and Saturday being 6). Suppose that the 0th of a given month and year (that is, the last day of the previous month) falls on the weekday M. Show that the dth day of the month falls on the day w of the week given by

$$w \equiv M + d \pmod 7.$$

We can find M from the weekday Y which represents the 0th day of the year (that is, the last day of the previous year). Unfortunately, for March and later months, M will depend not only on Y but also on whether or not the year involved is a leap year. Most perpetual calendars get around this problem by defining the beginning of the year to be March 1. Thus in calculating the day of the week of February 28, 1970, we would use the year 1969 in our calculations. From this point on, we assume that January and February belong to the year containing the previous December. Thus Y is the day of the week of March 0 [that is, February 28 or 29, according as to whether the year before (ending in February) is a normal or a leap year].

Day	w
Sunday	0
Monday	1
Tuesday	2
Wednesday	3
Thursday	4
Friday	5
Saturday	6

Month	m
March	0
April	3
May	5
June	1
July	3
August	6
September	2
October	4
November	0
December	2
January	5
February	1

Show that

$$M \equiv Y + m(\text{mod } 7),$$

where m is given in the accompanying table (30 days hath September, April, June, and so on). Let y be the last two digits in the year (for example, in January 1900, $y = 99$; in April 1914, $y = 14$). Let c be the weekday of March 0th of the first year of the century containing the date in question. Show that, (mod 7), a normal year has one day and a leap year two days and hence prove that

$$Y \equiv c + y + \left[\frac{y}{4}\right](\text{mod } 7),$$

where $[y/4]$ indicates that any remainder in $y/4$ ($\frac{1}{4}, \frac{2}{4}, \frac{3}{4}$) is thrown out (it is useful to note that the right-hand side usually increases by 1, but every fourth y, starting with 4, the right-hand side increases by 2). Combining all the equations, we have

$$w \equiv m + d + y + \left[\frac{y}{4}\right] + c(\text{mod } 7).$$

For example, on January 19, 1944, we have

$$\begin{aligned} w &\equiv 5 + 19 + 43 + [\tfrac{43}{4}] + c(\text{mod } 7) \\ &\equiv c(\text{mod } 7), \end{aligned}$$

and assuming that in 1900, $c = 3$, we see that January 19, 1944 is a Wednesday. Use today's date and day to show that in 1900, $c = 3$.

Century	c	
1500	3	
1600	2	
1700	0	
1800	5	periodic
1900	3	
2000	2	
2100	0	
2200	5	

Since March 0, 1900 ($w = c = 3$) was the same day as February 28, 1900 ($m = 1, d = 28, y = 99$), show that in 1800, $c = 5$. Verify the values given of c in 1500, 1600, 1700, 2000, 2100, and 2200 (1600 and 2000 are the only leap years among these; a year divisible by 100 is a leap year only when it is divisible by 400).

29. Our present calendar, the Gregorian calendar, was introduced by Pope Gregory XIII in 1582 to correct a slight error in the Julian calendar (introduced by Julius Caesar in 46 B.C.) which was gradually accumulating into a significant error. The Julian calendar is the same as the Gregorian calendar, except that every year (such as 1900) divisible by 100 is a leap year. Thus the Julian calendar has three extra days every four centuries. In 1582, the Julian calendar was in error by 10 days; thus October 5, 1582 (Julian calendar) was converted to October 15, 1582 (Gregorian calendar). In the notation of the previous problem, show that the Julian calendar c of 1500 is $c = 6$. Show that in the Julian calendar, c decreases by one

Century	c	
1300	1	
1400	0	
1500	6	
1600	5	
1700	4	periodic
1800	3	
1900	2	
2000	1	

(mod 7) each century. The Gregorian calendar was adopted in 1582 by France and Spain, but England and her American colonies waited until 1752 to adopt it and Russia did not adopt it until after the revolution in 1917.

30. On what days of the week did the following events occur (see problems 28 and 29)?

August 6, 258 (A.D.)	(Julian calendar). The martyrdom of Pope Sixtus II.
August 6, 1637	(Julian calendar). Ben Jonson, dramatist, died.
August 6, 1644	Louise de la Valliere, mistress of Louis XIV, born.
August 6, 1660	Diego Velasquez, Spanish painter, died.
August 6, 1759	Eugene Aram, English scholar and murderer, hanged.
August 6, 1811	Peter Barlow readies for print his book, *An Elementary Investigation of the Theory of Numbers with Its Applications to the Indeterminant and Diophantine Analysis, the Analytical and Geometrical Division of the Circle and Several Other Curious Algebraical and Arithmetical Problems*, containing a proof of Fermat's last theorem which depends on an incorrect corollary on page 20.
August 6, 1848	*H.M.S. Daedalus* sights a sea serpent.
August 6, 1890	First successful operation of an electric chair, State Prison, Auburn, New York.
August 6, 1930	Judge Crater, justice on the New York Supreme Court, disappears.
August 6, 1939	The author's birthday.
August 6, 1945	The first wartime use of an atomic bomb, Hiroshima.
August 6, 1966	The President's daughter's marriage on an inauspicious day.

31. Show that if $f(x)$ is a polynomial with integral coefficients and

$$f(a) \equiv f'(a) \equiv f''(a) \equiv \cdots \equiv f^{(r)}(a) \equiv 0 (\text{mod } n),$$

$$(r!, n) = 1,$$

then there is a polynomial $g(x)$ with integral coefficients and degree (mod n) equaling the degree (mod n) of $f(x)$ minus $(r + 1)$ such that

$$f(x) \equiv (x - a)^{r+1} g(x) (\text{poly mod } n).$$

Apply this result with $a = 3$ to the polynomial equation

$$x^4 + 6x^3 + 2x^2 + 4x + 2 \equiv 0 (\text{mod } 11).$$

32. Suppose that $(r!,n) = 1$ and let the numbers $a_0, a_1, \ldots, a_r$ be defined by the equations

$$(j!)a_j \equiv 1 (\text{mod } n), \qquad j = 0, 1, \ldots, r.$$

Suppose that $f(x)$ is a polynomial with integral coefficients and degree (mod n) equal to r. Show that if a is an integer, then

$$f(x) \equiv \sum_{j=0}^{r} a_j f^{(j)}(a)(x - a)^j (\text{poly mod } n).$$

There are times that this problem overlaps problem 31. Apply the result here with $a = 3$ to the polynomial of problem 31.