CHAPTER 3

PRIMES AND THEIR DISTRIBUTION

Mighty are numbers, joined with art resistless.
EURIPIDES

3.1 THE FUNDAMENTAL THEOREM OF ARITHMETIC

Essential to everything discussed herein—in fact, essential to every aspect of number theory—is the notion of a prime number. We have previously observed that any integer $a > 1$ is divisible by ± 1 and $\pm a$; if these exhaust the divisors of a, then it is said to be a prime number. In Definition 3.1 we state this somewhat differently.

> **Definition 3.1.** An integer $p > 1$ is called a *prime number*, or simply a *prime*, if its only positive divisors are 1 and p. An integer greater than 1 that is not a prime is termed *composite*.

Among the first ten positive integers, 2, 3, 5, 7 are primes and 4, 6, 8, 9, 10 are composite numbers. Note that the integer 2 is the only even prime, and according to our definition the integer 1 plays a special role, being neither prime nor composite.

In the rest of this book, the letters p and q will be reserved, so far as is possible, for primes.

Proposition 14 of Book IX of Euclid's *Elements* embodies the result that later became known as the Fundamental Theorem of Arithmetic, namely, that every integer greater than 1 can, except for the order of the factors, be represented as a product of primes in one and only one way. To quote the proposition itself: "If a number be the least that is measured by prime numbers, it will not be measured by any other

prime except those originally measuring it." Because every number $a > 1$ is either a prime or, by the Fundamental Theorem, can be broken down into unique prime factors and no further, the primes serve as the building blocks from which all other integers can be made. Accordingly, the prime numbers have intrigued mathematicians through the ages, and although a number of remarkable theorems relating to their distribution in the sequence of positive integers have been proved, even more remarkable is what remains unproved. The open questions can be counted among the outstanding unsolved problems in all of mathematics.

To begin on a simpler note, we observe that the prime 3 divides the integer 36, where 36 may be written as any one of the products

$$6 \cdot 6 = 9 \cdot 4 = 12 \cdot 3 = 18 \cdot 2$$

In each instance, 3 divides at least one of the factors involved in the product. This is typical of the general situation, the precise result being Theorem 3.1.

Theorem 3.1. If p is a prime and $p \mid ab$, then $p \mid a$ or $p \mid b$.

Proof. If $p \mid a$, then we need go no further, so let us assume that $p \nmid a$. Because the only positive divisors of p are 1 and p itself, this implies that $\gcd(p, a) = 1$. (In general, $\gcd(p, a) = p$ or $\gcd(p, a) = 1$ according as $p \mid a$ or $p \nmid a$.) Hence, citing Euclid's lemma, we get $p \mid b$.

This theorem easily extends to products of more than two terms.

Corollary 1. If p is a prime and $p \mid a_1 a_2 \cdots a_n$, then $p \mid a_k$ for some k, where $1 \leq k \leq n$.

Proof. We proceed by induction on n, the number of factors. When $n = 1$, the stated conclusion obviously holds; whereas when $n = 2$, the result is the content of Theorem 3.1. Suppose, as the induction hypothesis, that $n > 2$ and that whenever p divides a product of less than n factors, it divides at least one of the factors. Now let $p \mid a_1 a_2 \cdots a_n$. From Theorem 3.1, either $p \mid a_n$ or $p \mid a_1 a_2 \cdots a_{n-1}$. If $p \mid a_n$, then we are through. As regards the case where $p \mid a_1 a_2 \cdots a_{n-1}$, the induction hypothesis ensures that $p \mid a_k$ for some choice of k, with $1 \leq k \leq n - 1$. In any event, p divides one of the integers $a_1, a_2, \ldots, a_n$.

Corollary 2. If $p, q_1, q_2, \ldots, q_n$ are all primes and $p \mid q_1 q_2 \cdots q_n$, then $p = q_k$ for some k, where $1 \leq k \leq n$.

Proof. By virtue of Corollary 1, we know that $p \mid q_k$ for some k, with $1 \leq k \leq n$. Being a prime, q_k is not divisible by any positive integer other than 1 or q_k itself. Because $p > 1$, we are forced to conclude that $p = q_k$.

With this preparation out of the way, we arrive at one of the cornerstones of our development, the Fundamental Theorem of Arithmetic. As indicated earlier, this theorem asserts that every integer greater than 1 can be factored into primes in essentially one way; the linguistic ambiguity *essentially* means that $2 \cdot 3 \cdot 2$ is not considered as being a different factorization of 12 from $2 \cdot 2 \cdot 3$. We state this precisely in Theorem 3.2.

Theorem 3.2 Fundamental Theorem of Arithmetic. Every positive integer $n > 1$ can be expressed as a product of primes; this representation is unique, apart from the order in which the factors occur.

Proof. Either n is a prime or it is composite; in the former case, there is nothing more to prove. If n is composite, then there exists an integer d satisfying $d \mid n$ and $1 < d < n$. Among all such integers d, choose p_1 to be the smallest (this is possible by the Well-Ordering Principle). Then p_1 must be a prime number. Otherwise it too would have a divisor q with $1 < q < p_1$; but then $q \mid p_1$ and $p_1 \mid n$ imply that $q \mid n$, which contradicts the choice of p_1 as the smallest positive divisor, not equal to 1, of n.

We therefore may write $n = p_1 n_1$, where p_1 is prime and $1 < n_1 < n$. If n_1 happens to be a prime, then we have our representation. In the contrary case, the argument is repeated to produce a second prime number p_2 such that $n_1 = p_2 n_2$; that is,

$$n = p_1 p_2 n_2 \qquad 1 < n_2 < n_1$$

If n_2 is a prime, then it is not necessary to go further. Otherwise, write $n_2 = p_3 n_3$, with p_3 a prime:

$$n = p_1 p_2 p_3 n_3 \qquad 1 < n_3 < n_2$$

The decreasing sequence

$$n > n_1 > n_2 > \cdots > 1$$

cannot continue indefinitely, so that after a finite number of steps n_{k-1} is a prime, call it, p_k. This leads to the prime factorization

$$n = p_1 p_2 \cdots p_k$$

To establish the second part of the proof—the uniqueness of the prime factorization—let us suppose that the integer n can be represented as a product of primes in two ways; say,

$$n = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s \qquad r \leq s$$

where the p_i and q_j are all primes, written in increasing magnitude so that

$$p_1 \leq p_2 \leq \cdots \leq p_r \qquad q_1 \leq q_2 \leq \cdots \leq q_s$$

Because $p_1 \mid q_1 q_2 \cdots q_s$, Corollary 2 of Theorem 3.1 tells us that $p_1 = q_k$ for some k; but then $p_1 \geq q_1$. Similar reasoning gives $q_1 \geq p_1$, whence $p_1 = q_1$. We may cancel this common factor and obtain

$$p_2 p_3 \cdots p_r = q_2 q_3 \cdots q_s$$

Now repeat the process to get $p_2 = q_2$ and, in turn,

$$p_3 p_4 \cdots p_r = q_3 q_4 \cdots q_s$$

Continue in this fashion. If the inequality $r < s$ were to hold, we would eventually arrive at

$$1 = q_{r+1} q_{r+2} \cdots q_s$$

which is absurd, because each $q_j > 1$. Hence, $r = s$ and

$$p_1 = q_1 \qquad p_2 = q_2, \ldots, p_r = q_r$$

making the two factorizations of n identical. The proof is now complete.

Of course, several of the primes that appear in the factorization of a given positive integer may be repeated, as is the case with $360 = 2 \cdot 2 \cdot 2 \cdot 3 \cdot 3 \cdot 5$. By collecting like primes and replacing them by a single factor, we can rephrase Theorem 3.2 as a corollary.

Corollary. Any positive integer $n > 1$ can be written uniquely in a *canonical form*

$$n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$$

where, for $i = 1, 2, \ldots, r$, each k_i is a positive integer and each p_i is a prime, with $p_1 < p_2 < \cdots < p_r$.

To illustrate, the canonical form of the integer 360 is $360 = 2^3 \cdot 3^2 \cdot 5$. As further examples we cite

$$4725 = 3^3 \cdot 5^2 \cdot 7 \qquad \text{and} \qquad 17460 = 2^3 \cdot 3^2 \cdot 5 \cdot 7^2$$

Theorem 3.2 should not be taken lightly because number systems do exist in which the factorization into "primes" is not unique. Perhaps the most elemental example is the set E of all positive even integers. Let us agree to call an even integer an e-prime if it is not the product of two other even integers. Thus, 2, 6, 10, 14, ... all are e-primes, whereas 4, 8, 12, 16, ... are not. It is not difficult to see that the integer 60 can be factored into e-primes in two distinct ways; namely,

$$60 = 2 \cdot 30 = 6 \cdot 10$$

Part of the difficulty arises from the fact that Theorem 3.1 is lacking in the set E; that is, $6 \mid 2 \cdot 30$, but $6 \nmid 2$ and $6 \nmid 30$.

This is an opportune moment to insert a famous result of Pythagoras. Mathematics as a science began with Pythagoras (569–500 B.C.), and much of the content of Euclid's *Elements* is due to Pythagoras and his School. The Pythagoreans deserve the credit for being the first to classify numbers into odd and even, prime and composite.

Theorem 3.3 Pythagoras. The number $\sqrt{2}$ is irrational.

Proof. Suppose, to the contrary, that $\sqrt{2}$ is a rational number, say, $\sqrt{2} = a/b$, where a and b are both integers with $\gcd(a, b) = 1$. Squaring, we get $a^2 = 2b^2$, so that $b \mid a^2$. If $b > 1$, then the Fundamental Theorem of Arithmetic guarantees the existence of a prime p such that $p \mid b$. It follows that $p \mid a^2$ and, by Theorem 3.1, that $p \mid a$; hence, $\gcd(a, b) \geq p$. We therefore arrive at a contradiction, unless $b = 1$. But if this happens, then $a^2 = 2$, which is impossible (we assume that the reader is willing to grant that no integer can be multiplied by itself to give 2). Our supposition that $\sqrt{2}$ is a rational number is untenable, and so $\sqrt{2}$ must be irrational.

There is an interesting variation on the proof of Theorem 3.3. If $\sqrt{2} = a/b$ with $\gcd(a, b) = 1$, there must exist integers r and s satisfying $ar + bs = 1$. As a result,

$$\sqrt{2} = \sqrt{2}(ar + bs) = (\sqrt{2}a)r + (\sqrt{2}b)s = 2br + as$$

This representation of $\sqrt{2}$ leads us to conclude that $\sqrt{2}$ is an integer, an obvious impossibility.

PROBLEMS 3.1

1. It has been conjectured that there are infinitely many primes of the form $n^2 - 2$. Exhibit five such primes.
2. Give an example to show that the following conjecture is not true: Every positive integer can be written in the form $p + a^2$, where p is either a prime or 1, and $a \geq 0$.
3. Prove each of the assertions below:
   (a) Any prime of the form $3n + 1$ is also of the form $6m + 1$.
   (b) Each integer of the form $3n + 2$ has a prime factor of this form.
   (c) The only prime of the form $n^3 - 1$ is 7.
   [*Hint:* Write $n^3 - 1$ as $(n - 1)(n^2 + n + 1)$.]
   (d) The only prime p for which $3p + 1$ is a perfect square is $p = 5$.
   (e) The only prime of the form $n^2 - 4$ is 5.
4. If $p \geq 5$ is a prime number, show that $p^2 + 2$ is composite.
   [*Hint:* p takes one of the forms $6k + 1$ or $6k + 5$.]
5. (a) Given that p is a prime and $p \mid a^n$, prove that $p^n \mid a^n$.
   (b) If $\gcd(a, b) = p$, a prime, what are the possible values of $\gcd(a^2, b^2)$, $\gcd(a^2, b)$ and $\gcd(a^3, b^2)$?
6. Establish each of the following statements:
   (a) Every integer of the form $n^4 + 4$, with $n > 1$, is composite.
   [*Hint:* Write $n^4 + 4$ as a product of two quadratic factors.]
   (b) If $n > 4$ is composite, then n divides $(n - 1)!$.
   (c) Any integer of the form $8^n + 1$, where $n \geq 1$, is composite.
   [*Hint:* $2^n + 1 \mid 2^{3n} + 1$.]
   (d) Each integer $n > 11$ can be written as the sum of two composite numbers.
   [*Hint:* If n is even, say $n = 2k$, then $n - 6 = 2(k - 3)$; for n odd, consider the integer $n - 9$.]
7. Find all prime numbers that divide 50!.
8. If $p \geq q \geq 5$ and p and q are both primes, prove that $24 \mid p^2 - q^2$.
9. (a) An unanswered question is whether there are infinitely many primes that are 1 more than a power of 2, such as $5 = 2^2 + 1$. Find two more of these primes.
   (b) A more general conjecture is that there exist infinitely many primes of the form $n^2 + 1$; for example, $257 = 16^2 + 1$. Exhibit five more primes of this type.
10. If $p \neq 5$ is an odd prime, prove that either $p^2 - 1$ or $p^2 + 1$ is divisible by 10.
11. Another unproven conjecture is that there are an infinitude of primes that are 1 less than a power of 2, such as $3 = 2^2 - 1$.
   (a) Find four more of these primes.
   (b) If $p = 2^k - 1$ is prime, show that k is an odd integer, except when $k = 2$.
   [*Hint:* $3 \mid 4^n - 1$ for all $n \geq 1$.]
12. Find the prime factorization of the integers 1234, 10140, and 36000.
13. If $n > 1$ is an integer not of the form $6k + 3$, prove that $n^2 + 2^n$ is composite.
   [*Hint:* Show that either 2 or 3 divides $n^2 + 2^n$.]
14. It has been conjectured that every even integer can be written as the difference of two consecutive primes in infinitely many ways. For example,

$$6 = 29 - 23 = 137 - 131 = 599 - 593 = 1019 - 1013 = \cdots$$

   Express the integer 10 as the difference of two consecutive primes in 15 ways.
15. Prove that a positive integer $a > 1$ is a square if and only if in the canonical form of a all the exponents of the primes are even integers.

16. An integer is said to be *square-free* if it is not divisible by the square of any integer greater than 1. Prove the following:
   (a) An integer $n > 1$ is square-free if and only if n can be factored into a product of distinct primes.
   (b) Every integer $n > 1$ is the product of a square-free integer and a perfect square. [*Hint:* If $n = p_1^{k_1} p_2^{k_2} \cdots p_s^{k_s}$ is the canonical factorization of n, then write $k_i = 2q_i + r_i$ where $r_i = 0$ or 1 according as k_i is even or odd.]

17. Verify that any integer n can be expressed as $n = 2^k m$, where $k \geq 0$ and m is an odd integer.

18. Numerical evidence makes it plausible that there are infinitely many primes p such that $p + 50$ is also prime. List 15 of these primes.

19. A positive integer n is called *square-full*, or *powerful*, if $p^2 \mid n$ for every prime factor p of n (there are 992 square-full numbers less than 250,000). If n is square-full, show that it can be written in the form $n = a^2 b^3$, with a and b positive integers.

3.2 THE SIEVE OF ERATOSTHENES

Given a particular integer, how can we determine whether it is prime or composite and, in the latter case, how can we actually find a nontrivial divisor? The most obvious approach consists of successively dividing the integer in question by each of the numbers preceding it; if none of them (except 1) serves as a divisor, then the integer must be prime. Although this method is very simple to describe, it cannot be regarded as useful in practice. For even if one is undaunted by large calculations, the amount of time and work involved may be prohibitive.

There is a property of composite numbers that allows us to reduce materially the necessary computations—but still the process remains cumbersome. If an integer $a > 1$ is composite, then it may be written as $a = bc$, where $1 < b < a$ and $1 < c < a$. Assuming that $b \leq c$, we get $b^2 \leq bc = a$, and so $b \leq \sqrt{a}$. Because $b > 1$, Theorem 3.2 ensures that b has at least one prime factor p. Then $p \leq b \leq \sqrt{a}$; furthermore, because $p \mid b$ and $b \mid a$, it follows that $p \mid a$. The point is simply this: A composite number a will always possess a prime divisor p satisfying $p \leq \sqrt{a}$.

In testing the primality of a specific integer $a > 1$, it therefore suffices to divide a by those primes not exceeding $\sqrt{a}$ (presuming, of course, the availability of a list of primes up to $\sqrt{a}$). This may be clarified by considering the integer $a = 509$. Inasmuch as $22 < \sqrt{509} < 23$, we need only try out the primes that are not larger than 22 as possible divisors, namely, the primes 2, 3, 5, 7, 11, 13, 17, 19. Dividing 509 by each of these, in turn, we find that none serves as a divisor of 509. The conclusion is that 509 must be a prime number.

Example 3.1. The foregoing technique provides a practical means for determining the canonical form of an integer, say $a = 2093$. Because $45 < \sqrt{2093} < 46$, it is enough to examine the primes 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43. By trial, the first of these to divide 2093 is 7, and $2093 = 7 \cdot 299$. As regards the integer 299, the seven primes that are less than 18 (note that $17 < \sqrt{299} < 18$) are 2, 3, 5, 7, 11, 13, 17. The first prime divisor of 299 is 13 and, carrying out the required division, we obtain $299 = 13 \cdot 23$. But 23 is itself a prime, whence 2093 has exactly three prime factors, 7, 13, and 23:

$$2093 = 7 \cdot 13 \cdot 23$$

Another Greek mathematician whose work in number theory remains significant is Eratosthenes of Cyrene (276–194 B.C.). Although posterity remembers him mainly as the director of the world-famous library at Alexandria, Eratosthenes was gifted in all branches of learning, if not of first rank in any; in his own day, he was nicknamed "Beta" because, it was said, he stood at least second in every field. Perhaps the most impressive feat of Eratosthenes was the accurate measurement of the earth's circumference by a simple application of Euclidean geometry.

We have seen that if an integer $a > 1$ is not divisible by any prime $p \leq \sqrt{a}$, then a is of necessity a prime. Eratosthenes used this fact as the basis of a clever technique, called the *Sieve of Eratosthenes*, for finding all primes below a given integer n. The scheme calls for writing down the integers from 2 to n in their natural order and then systematically eliminating all the composite numbers by striking out all multiples $2p, 3p, 4p, 5p, \ldots$ of the primes $p \leq \sqrt{n}$. The integers that are left on the list—those that do not fall through the "sieve"—are primes.

To see an example of how this works, suppose that we wish to find all primes not exceeding 100. Consider the sequence of consecutive integers 2, 3, 4, . . . ,100. Recognizing that 2 is a prime, we begin by crossing out all even integers from our listing, except 2 itself. The first of the remaining integers is 3, which must be a prime. We keep 3, but strike out all higher multiples of 3, so that 9, 15, 21, . . . are now removed (the even multiples of 3 having been removed in the previous step). The smallest integer after 3 that has not yet been deleted is 5. It is not divisible by either 2 or 3—otherwise it would have been crossed out—hence, it is also a prime. All proper multiples of 5 being composite numbers, we next remove 10, 15, 20, . . . (some of these are, of course, already missing), while retaining 5 itself. The first surviving integer 7 is a prime, for it is not divisible by 2, 3, or 5, the only primes that precede it. After eliminating the proper multiples of 7, the largest prime less than $\sqrt{100} = 10$, all composite integers in the sequence 2, 3, 4, . . . ,100 have fallen through the sieve. The positive integers that remain, to wit, 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, are all of the primes less than 100.

The following table represents the result of the completed sieve. The multiples of 2 are crossed out by \; the multiples of 3 are crossed out by /; the multiples of 5 are crossed out by —; the multiples of 7 are crossed out by ~.

	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

By this point, an obvious question must have occurred to the reader. Is there a largest prime number, or do the primes go on forever? The answer is to be found in a remarkably simple proof given by Euclid in Book IX of his *Elements*. Euclid's argument is universally regarded as a model of mathematical elegance. Loosely

speaking, it goes like this: Given any finite list of prime numbers, one can always find a prime not on the list; hence, the number of primes is infinite. The actual details appear below.

Theorem 3.4 Euclid. There is an infinite number of primes.

Proof. Euclid's proof is by contradiction. Let $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, $p_4 = 7, \ldots$ be the primes in ascending order, and suppose that there is a last prime, called p_n. Now consider the positive integer

$$P = p_1 p_2 \cdots p_n + 1$$

Because $P > 1$, we may put Theorem 3.2 to work once again and conclude that P is divisible by some prime p. But $p_1, p_2, \ldots, p_n$ are the only prime numbers, so that p must be equal to one of $p_1, p_2, \ldots, p_n$. Combining the divisibility relation $p \mid p_1 p_2 \cdots p_n$ with $p \mid P$, we arrive at $p \mid P - p_1 p_2 \cdots p_n$ or, equivalently, $p \mid 1$. The only positive divisor of the integer 1 is 1 itself and, because $p > 1$, a contradiction arises. Thus, no finite list of primes is complete, whence the number of primes is infinite.

For a prime p, define $p^{\#}$ to be the product of all primes that are less than or equal to p. Numbers of the form $p^{\#} + 1$ might be termed *Euclidean numbers*, because they appear in Euclid's scheme for proving the infinitude of primes. It is interesting to note that in forming these integers, the first five, namely,

$$\begin{aligned} 2^{\#} + 1 &= 2 + 1 = 3 \\ 3^{\#} + 1 &= 2 \cdot 3 + 1 = 7 \\ 5^{\#} + 1 &= 2 \cdot 3 \cdot 5 + 1 = 31 \\ 7^{\#} + 1 &= 2 \cdot 3 \cdot 5 \cdot 7 + 1 = 211 \\ 11^{\#} + 1 &= 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 + 1 = 2311 \end{aligned}$$

are all prime numbers. However,

$$\begin{aligned} 13^{\#} + 1 &= 59 \cdot 509 \\ 17^{\#} + 1 &= 19 \cdot 97 \cdot 277 \\ 19^{\#} + 1 &= 347 \cdot 27953 \end{aligned}$$

are not prime. A question whose answer is not known is whether there are infinitely many primes p for which $p^{\#} + 1$ is also prime. For that matter, are there infinitely many composite $p^{\#} + 1$?

At present, 19 primes of the form $p^{\#} + 1$ have been identified. These correspond to the values $p = 2, 3, 5, 7, 11, 31, 379, 1019, 1021, 2657, 3229, 4547, 4787, 11549, 13649, 18523, 23801, 24029$, and 42209; the largest of these, a number consisting of 18241 digits, was discovered in 2000. The integer $p^{\#} + 1$ is composite for all other $p \leq 120000$.

Euclid's theorem is too important for us to be content with a single proof. Here is a variation in the reasoning: Form the infinite sequence of positive integers

$$\begin{aligned} n_1 &= 2 \\ n_2 &= n_1 + 1 \\ n_3 &= n_1 n_2 + 1 \\ n_4 &= n_1 n_2 n_3 + 1 \\ &\vdots \\ n_k &= n_1 n_2 \cdots n_{k-1} + 1 \\ &\vdots \end{aligned}$$

Because each $n_k > 1$, each of these integers is divisible by a prime. But no two n_k can have the same prime divisor. To see this, let $d = \gcd(n_i, n_k)$ and suppose that $i < k$. Then d divides n_i and, hence, must divide $n_1 n_2 \cdots n_{k-1}$. Because $d \mid n_k$, Theorem 2.2 (g) tells us that $d \mid n_k - n_1 n_2 \cdots n_{k-1}$ or $d \mid 1$. The implication is that $d = 1$, and so the integers $n_k (k = 1, 2, \ldots)$ are pairwise relatively prime. The point we wish to make is that there are as many distinct primes as there are integers n_k, namely, infinitely many of them.

Let p_n denote the nth of the prime numbers in their natural order. Euclid's proof shows that the expression $p_1 p_2 \cdots p_n + 1$ is divisible by at least one prime. If there are several such prime divisors, then p_{n+1} cannot exceed the smallest of these so that $p_{n+1} \leq p_1 p_2 \cdots p_n + 1$ for $n \geq 1$. Another way of saying the same thing is that

$$p_n \leq p_1 p_2 \cdots p_{n-1} + 1 \qquad n \geq 2$$

With a slight modification of Euclid's reasoning, this inequality can be improved to give

$$p_n \leq p_1 p_2 \cdots p_{n-1} - 1 \qquad n \geq 3$$

For instance, when $n = 5$, this tells us that

$$11 = p_5 \leq 2 \cdot 3 \cdot 5 \cdot 7 - 1 = 209$$

We can see that the estimate is rather extravagant. A sharper limitation on the size of p_n is given by *Bonse's inequality*, which states that

$$p_n^2 < p_1 p_2 \cdots p_{n-1} \qquad n \geq 5$$

This inequality yields $p_5^2 < 210$, or $p_5 \leq 14$. A somewhat better size-estimate for p_5 comes from the inequality

$$p_{2n} \leq p_2 p_3 \cdots p_n - 2 \qquad n \geq 3$$

Here, we obtain

$$p_5 < p_6 \leq p_2 p_3 - 2 = 3 \cdot 5 - 2 = 13$$

To approximate the size of p_n from these formulas, it is necessary to know the values of $p_1, p_2, \ldots, p_{n-1}$. For a bound in which the preceding primes do not enter the picture, we have the following theorem.

Theorem 3.5. If p_n is the nth prime number, then $p_n \leq 2^{2^{n-1}}$.

Proof. Let us proceed by induction on n, the asserted inequality being clearly true when $n = 1$. As the hypothesis of the induction, we assume that $n > 1$ and that the result holds for all integers up to n. Then

$$\begin{aligned} p_{n+1} &\leq p_1 p_2 \cdots p_n + 1 \\ &\leq 2 \cdot 2^2 \cdots 2^{2^{n-1}} + 1 = 2^{1+2+2^2+\cdots+2^{n-1}} + 1 \end{aligned}$$

Recalling the identity $1 + 2 + 2^2 + \cdots + 2^{n-1} = 2^n - 1$, we obtain

$$p_{n+1} \leq 2^{2^n - 1} + 1$$

However, $1 \leq 2^{2^n - 1}$ for all n; whence

$$\begin{aligned} p_{n+1} &\leq 2^{2^n - 1} + 2^{2^n - 1} \\ &= 2 \cdot 2^{2^n - 1} = 2^{2^n} \end{aligned}$$

completing the induction step, and the argument.

There is a corollary to Theorem 3.5 that is of interest.

Corollary. For $n \geq 1$, there are at least $n + 1$ primes less than 2^{2^n}.

Proof. From the theorem, we know that $p_1, p_2, \ldots, p_{n+1}$ are all less than 2^{2^n}.

We can do considerably better than is indicated by Theorem 3.5. In 1845, Joseph Bertrand conjectured that the prime numbers are well-distributed in the sense that between $n \geq 2$ and $2n$ there is at least one prime. He was unable to establish his conjecture, but verified it for all $n \leq 3{,}000{,}000$. (One way of achieving this is to consider a sequence of primes 3, 5, 7, 13, 23, 43, 83, 163, 317, 631, 1259, 2503, 5003, 9973, 19937, 39869, 79699, 159389, ... each of which is less than twice the preceding.) Because it takes some real effort to substantiate this famous conjecture, let us content ourselves with saying that the first proof was carried out by the Russian mathematician P. L. Tchebycheff in 1852. Granting the result, it is not difficult to show that

$$p_n < 2^n \qquad n \geq 2$$

and as a direct consequence, $p_{n+1} < 2p_n$ for $n \geq 2$. In particular,

$$11 = p_5 < 2 \cdot p_4 = 14$$

To see that $p_n < 2^n$, we argue by induction on n. Clearly, $p_2 = 3 < 2^2$, so that the inequality is true here. Now assume that the inequality holds for an integer n, whence $p_n < 2^n$. Invoking Bertrand's conjecture, there exists a prime number p satisfying $2^n < p < 2^{n+1}$; that is, $p_n < p$. This immediately leads to the conclusion that $p_{n+1} \leq p < 2^{n+1}$, which completes the induction and the proof.

Primes of special form have been of perennial interest. Among these, the repunit primes are outstanding in their simplicity. A *repunit* is an integer written (in decimal notation) as a string of 1's, such as 11, 111, or 1111. Each such integer must have the form $(10^n - 1)/9$. We use the symbol R_n to denote the repunit consisting of n consecutive 1's. A peculiar feature of these numbers is the apparent scarcity of primes among them. So far, only R_2, R_{19}, R_{23}, R_{317}, R_{1031}, R_{49081}, and R_{86453}

have been identified as primes (the last one in 2001). It is known that the only possible repunit primes R_n for all $n \leq 45000$ are the seven numbers just indicated. No conjecture has been made as to the existence of any others. For a repunit R_n to be prime, the subscript n must be a prime; that this is not a sufficient condition is shown by

$$R_5 = 11111 = 41 \cdot 271 \qquad R_7 = 1111111 = 239 \cdot 4649$$

PROBLEMS 3.2

1. Determine whether the integer 701 is prime by testing all primes $p \leq \sqrt{701}$ as possible divisors. Do the same for the integer 1009.
2. Employing the Sieve of Eratosthenes, obtain all the primes between 100 and 200.
3. Given that $p \nmid n$ for all primes $p \leq \sqrt[3]{n}$, show that $n > 1$ is either a prime or the product of two primes.
   [*Hint:* Assume to the contrary that n contains at least three prime factors.]
4. Establish the following facts:
   (a) $\sqrt{p}$ is irrational for any prime p.
   (b) If $a > 0$ and $\sqrt[n]{a}$ is rational, then $\sqrt[n]{a}$ must be an integer.
   (c) For $n \geq 2$, $\sqrt[n]{n}$ is irrational.
   [*Hint:* Use the fact that $2^n > n$.]
5. Show that any composite three-digit number must have a prime factor less than or equal to 31.
6. Fill in any missing details in this sketch of a proof of the infinitude of primes: Assume that there are only finitely many primes, say $p_1, p_2, \ldots, p_n$. Let A be the product of any r of these primes and put $B = p_1 p_2 \cdots p_n / A$. Then each p_k divides either A or B, but not both. Because $A + B > 1$, $A + B$ has a prime divisor different from any of the p_k, which is a contradiction.
7. Modify Euclid's proof that there are infinitely many primes by assuming the existence of a largest prime p and using the integer $N = p! + 1$ to arrive at a contradiction.
8. Give another proof of the infinitude of primes by assuming that there are only finitely many primes, say $p_1, p_2, \ldots, p_n$, and using the following integer to arrive at a contradiction:

$$N = p_2 p_3 \cdots p_n + p_1 p_3 \cdots p_n + \cdots + p_1 p_2 \cdots p_{n-1}$$

9. (a) Prove that if $n > 2$, then there exists a prime p satisfying $n < p < n!$.
   [*Hint:* If $n! - 1$ is not prime, then it has a prime divisor p; and $p \leq n$ implies $p \mid n!$, leading to a contradiction.]
   (b) For $n > 1$, show that every prime divisor of $n! + 1$ is an odd integer that is greater than n.
10. Let q_n be the smallest prime that is strictly greater than $P_n = p_1 p_2 \cdots p_n + 1$. It has been conjectured that the difference $q_n - (p_1 p_2 \cdots p_n)$ is always a prime. Confirm this for the first five values of n.
11. If p_n denotes the nth prime number, put $d_n = p_{n+1} - p_n$. An open question is whether the equation $d_n = d_{n+1}$ has infinitely many solutions. Give five solutions.
12. Assuming that p_n is the nth prime number, establish each of the following statements:
   (a) $p_n > 2n - 1$ for $n \geq 5$.
   (b) None of the integers $P_n = p_1 p_2 \cdots p_n + 1$ is a perfect square.
   [*Hint:* Each P_n is of the form $4k + 3$ for $n > 1$.]

(c) The sum

$$\frac{1}{p_1} + \frac{1}{p_2} + \cdots + \frac{1}{p_n}$$

is never an integer.

13. For the repunits R_n, verify the assertions below:

(a) If $n \mid m$, then $R_n \mid R_m$.

[*Hint:* If $m = kn$, consider the identity

$$x^m - 1 = (x^n - 1)(x^{(k-1)n} + x^{(k-2)n} + \cdots + x^n + 1).]$$

(b) If $d \mid R_n$ and $d \mid R_m$, then $d \mid R_{n+m}$.

[*Hint:* Show that $R_{m+n} = R_n 10^m + R_m$.]

(c) If $\gcd(n, m) = 1$, then $\gcd(R_n, R_m) = 1$.

14. Use the previous problem to obtain the prime factors of the repunit R_{10}.

3.3 THE GOLDBACH CONJECTURE

Although there is an infinitude of primes, their distribution within the positive integers is most mystifying. Repeatedly in their distribution we find hints or, as it were, shadows of a pattern; yet an actual pattern amenable to precise description remains elusive. The difference between consecutive primes can be small, as with the pairs 11 and 13, 17 and 19, or for that matter 1000000000061 and 1000000000063. At the same time there exist arbitrarily long intervals in the sequence of integers that are totally devoid of any primes.

It is an unanswered question whether there are infinitely many pairs of *twin primes*; that is, pairs of successive odd integers p and $p + 2$ that are both primes. Numerical evidence leads us to suspect an affirmative conclusion. Electronic computers have discovered 152892 pairs of twin primes less than 30000000 and 20 pairs between 10^{12} and $10^{12}+ 10000$, which hints at their growing scarcity as the positive integers increase in magnitude. Many examples of immense twins are known. The largest twins to date, each 51090 digits long,

$$33218925 \cdot 2^{169690} \pm 1$$

were discovered in 2002.

Consecutive primes cannot only be close together, but also can be far apart; that is, arbitrarily large gaps can occur between consecutive primes. Stated precisely: Given any positive integer n, there exist n consecutive integers, all of which are composite. To prove this, we simply need to consider the integers

$$(n + 1)! + 2, (n + 1)! + 3, \ldots, (n + 1)! + (n + 1)$$

where $(n + 1)! = (n + 1) \cdot n \cdots 3 \cdot 2 \cdot 1$. Clearly, there are n integers listed and they are consecutive. What is important is that each integer is composite. Indeed, $(n + 1)! + 2$ is divisible by 2, $(n + 1)! + 3$ is divisible by 3, and so on.

For instance, if a sequence of four consecutive composite integers is desired, then the previous argument produces 122, 123, 124, and 125:

$$5! + 2 = 122 = 2 \cdot 61$$
$$5! + 3 = 123 = 3 \cdot 41$$
$$5! + 4 = 124 = 4 \cdot 31$$
$$5! + 5 = 125 = 5 \cdot 25$$

Of course, we can find other sets of four consecutive composites, such as 24, 25, 26, 27 or 32, 33, 34, 35.

As this example suggests, our procedure for constructing gaps between two consecutive primes gives a gross overestimate of where they occur among the integers. The first occurrences of prime gaps of specific lengths, where all the intervening integers are composite, have been the subject of computer searches. For instance, there is a gap of length 778 (that is, $p_{n+1} - p_n = 778$) following the prime 42842283925351. No gap of this size exists between two smaller primes. The largest effectively calculated gap between consecutive prime numbers has length 1132, with a string of 1131 composites immediately after the prime

$$1693182318746371$$

Interestingly, computer researchers have not identified gaps of every possible width up to 1132. The smallest missing gap size is 796. The conjecture is that there is a prime gap (a string of $2k - 1$ consecutive composites between two primes) for every even integer $2k$.

This brings us to another unsolved problem concerning the primes, the Goldbach conjecture. In a letter to Leonhard Euler in the year 1742, Christian Goldbach hazarded the guess that every even integer is the sum of two numbers that are either primes or 1. A somewhat more general formulation is that every even integer greater than 4 can be written as a sum of two odd prime numbers. This is easy to confirm for the first few even integers:

$$\begin{aligned}
2 &= 1 + 1 \\
4 &= 2 + 2 = 1 + 3 \\
6 &= 3 + 3 = 1 + 5 \\
8 &= 3 + 5 = 1 + 7 \\
10 &= 3 + 7 = 5 + 5 \\
12 &= 5 + 7 = 1 + 11 \\
14 &= 3 + 11 = 7 + 7 = 1 + 13 \\
16 &= 3 + 13 = 5 + 11 \\
18 &= 5 + 13 = 7 + 11 = 1 + 17 \\
20 &= 3 + 17 = 7 + 13 = 1 + 19 \\
22 &= 3 + 19 = 5 + 17 = 11 + 11 \\
24 &= 5 + 19 = 7 + 17 = 11 + 13 = 1 + 23 \\
26 &= 3 + 23 = 7 + 19 = 13 + 13 \\
28 &= 5 + 23 = 11 + 17 \\
30 &= 7 + 23 = 11 + 19 = 13 + 17 = 1 + 29
\end{aligned}$$

Although it seems that Euler never tried to prove the result, upon writing to Goldbach at a later date, Euler countered with a conjecture of his own: Any even integer (≥ 6) of the form $4n + 2$ is a sum of two numbers each being either a prime of the form $4n + 1$ or 1.

The numerical data suggesting the truth of Goldbach's conjecture are overwhelming. It has been verified by computers for all even integers less than $4 \cdot 10^{14}$.

As the integers become larger, the number of different ways in which $2n$ can be expressed as the sum of two primes increases. For example, there are 219400 such representations for the even integer 100000000. Although this supports the feeling that Goldbach was correct in his conjecture, it is far from a mathematical proof, and all attempts to obtain a proof have been completely unsuccessful. One of the most famous number theorists of the last century, G. H. Hardy, in his address to the Mathematical Society of Copenhagen in 1921, stated that the Goldbach conjecture appeared "... probably as difficult as any of the unsolved problems in mathematics." It is currently known that every even integer is the sum of six or fewer primes.

We remark that if the conjecture of Goldbach is true, then each odd number larger than 7 must be the sum of three odd primes. To see this, take n to be an odd integer greater than 7, so that $n - 3$ is even and greater than 4; if $n - 3$ could be expressed as the sum of two odd primes, then n would be the sum of three.

The first real progress on the conjecture in nearly 200 years was made by Hardy and Littlewood in 1922. On the basis of a certain unproved hypothesis, the so-called generalized Riemann hypothesis, they showed that every sufficiently large odd number is the sum of three odd primes. In 1937, the Russian mathematician I. M. Vinogradov was able to remove the dependence on the generalized Riemann hypothesis, thereby giving an unconditional proof of this result; that is to say, he established that all odd integers greater than some effectively computable n_0 can be written as the sum of three odd primes.

$$n = p_1 + p_2 + p_3 \qquad (n \text{ odd}, n \text{ sufficiently large})$$

Vinogradov was unable to decide how large n_0 should be, but Borozdkin (1956) proved that $n_0 < 3^{3^{15}}$. In 2002, the bound on n_0 was reduced to 10^{1346}. It follows immediately that every even integer from some point on is the sum of either two or four primes. Thus, it is enough to answer the question for every odd integer n in the range $9 \leq n \leq n_0$, which, for a given integer, becomes a matter of tedious computation (unfortunately, n_0 is so large that this exceeds the capabilities of the most modern electronic computers).

Because of the strong evidence in favor of the famous Goldbach conjecture, we readily become convinced that it is true. Nevertheless, it might be false. Vinogradov showed that if $A(x)$ is the number of even integers $n \leq x$ that are not the sum of two primes, then

$$\lim_{x \to \infty} A(x)/x = 0$$

This allows us to say that "almost all" even integers satisfy the conjecture. As Edmund Landau so aptly put it, "The Goldbach conjecture is false for at most 0% of all even integers; this *at most* 0% does not exclude, of course, the possibility that there are infinitely many exceptions."

Having digressed somewhat, let us observe that according to the Division Algorithm, every positive integer can be written uniquely in one of the forms

$$4n \qquad 4n + 1 \qquad 4n + 2 \qquad 4n + 3$$

for some suitable $n \geq 0$. Clearly, the integers $4n$ and $4n + 2 = 2(2n + 1)$ are both even. Thus, all odd integers fall into two progressions: one containing integers of the form $4n + 1$, and the other containing integers of the form $4n + 3$.

The question arises as to how these two types of primes are distributed within the set of positive integers. Let us display the first few odd prime numbers in consecutive order, putting the $4n + 3$ primes in the top row and the $4n + 1$ primes under them:

3	7	11	19	23	31	43	47	59	67	71	79	83
5	13	17	29	37	41	53	61	73	89			

At this point, one might have the general impression that primes of the form $4n + 3$ are more abundant than are those of the form $4n + 1$. To obtain more precise information, we require the help of the function $\pi_{a,b}(x)$, which counts the number of primes of the form $p = an + b$ not exceeding x. Our small table, for instance, indicates that $\pi_{4,1}(89) = 10$ and $\pi_{4,3}(89) = 13$.

In a famous letter written in 1853, Tchebycheff remarked that $\pi_{4,1}(x) \leq \pi_{4,3}(x)$ for small values of x. He also implied that he had a proof that the inequality always held. In 1914, J. E. Littlewood showed that the inequality fails infinitely often, but his method gave no indication of the value of x for which this first happens. It turned out to be quite difficult to find. Not until 1957 did a computer search reveal that $x = 26861$ is the smallest prime for which $\pi_{4,1}(x) > \pi_{4,3}(x)$; here, $\pi_{4,1}(x) = 1473$ and $\pi_{4,3}(x) = 1472$. This is an isolated situation, because the next prime at which a reversal occurs is $x = 616{,}841$. Remarkably, $\pi_{4,1}(x) > \pi_{4,3}(x)$ for the 410 million successive integers x lying between 18540000000 and 18950000000.

The behavior of primes of the form $3n \pm 1$ provided more of a computational challenge: the inequality $\pi_{3,1}(x) \leq \pi_{3,2}(x)$ holds for all x until one reaches $x = 608981813029$.

This furnishes a pleasant opportunity for a repeat performance of Euclid's method for proving the existence of an infinitude of primes. A slight modification of his argument reveals that there is an infinite number of primes of the form $4n + 3$. We approach the proof through a simple lemma.

Lemma. The product of two or more integers of the form $4n + 1$ is of the same form.

Proof. It is sufficient to consider the product of just two integers. Let us take $k = 4n + 1$ and $k' = 4m + 1$. Multiplying these together, we obtain

$$\begin{aligned} kk' &= (4n + 1)(4m + 1) \\ &= 16nm + 4n + 4m + 1 = 4(4nm + n + m) + 1 \end{aligned}$$

which is of the desired form.

This paves the way for Theorem 3.6.

Theorem 3.6. There are an infinite number of primes of the form $4n + 3$.

Proof. In anticipation of a contradiction, let us assume that there exist only finitely many primes of the form $4n + 3$; call them $q_1, q_2, \ldots, q_s$. Consider the positive integer

$$N = 4q_1q_2 \cdots q_s - 1 = 4(q_1q_2 \cdots q_s - 1) + 3$$

and let $N = r_1r_2 \cdots r_t$ be its prime factorization. Because N is an odd integer, we have $r_k \neq 2$ for all k, so that each r_k is either of the form $4n + 1$ or $4n + 3$. By the lemma, the product of any number of primes of the form $4n + 1$ is again an integer of this type. For N to take the form $4n + 3$, as it clearly does, N must contain at least one prime factor r_i of the form $4n + 3$. But r_i cannot be found among the listing $q_1, q_2, \ldots, q_s$, for this would lead to the contradiction that $r_i \mid 1$. The only possible conclusion is that there are infinitely many primes of the form $4n + 3$.

Having just seen that there are infinitely many primes of the form $4n + 3$, we might reasonably ask: Is the number of primes of the form $4n + 1$ also infinite? This answer is likewise in the affirmative, but a demonstration must await the development of the necessary mathematical machinery. Both these results are special cases of a remarkable theorem by P. G. L. Dirichlet on primes in arithmetic progressions, established in 1837. The proof is much too difficult for inclusion here, so that we must content ourselves with the mere statement.

Theorem 3.7 Dirichlet. If a and b are relatively prime positive integers, then the arithmetic progression

$$a, a + b, a + 2b, a + 3b, \ldots$$

contains infinitely many primes.

Dirichlet's theorem tells us, for instance, that there are infinitely many prime numbers ending in 999, such as 1999, 100999, 1000999, ... for these appear in the arithmetic progression determined by $1000n + 999$, where $\gcd(1000, 999) = 1$.

There is no arithmetic progression $a, a + b, a + 2b, \ldots$ that consists solely of prime numbers. To see this, suppose that $a + nb = p$, where p is a prime. If we put $n_k = n + kp$ for $k = 1, 2, 3, \ldots$ then the n_kth term in the progression is

$$a + n_kb = a + (n + kp)b = (a + nb) + kpb = p + kpb$$

Because each term on the right-hand side is divisible by p, so is $a + n_kb$. In other words, the progression must contain infinitely many composite numbers.

It is an old, but still unsolved question of whether there exist arbitrarily long but finite arithmetic progressions consisting only of prime numbers (not necessarily consecutive primes). The longest progression found to date is composed of the 22 primes:

$$11410337850553 + 4609098694200n \qquad 0 \leq n \leq 21$$

The prime factorization of the common difference between the terms is

$$2^3 \cdot 3 \cdot 5^2 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \cdot 1033$$

which is divisible by 9699690, the product of the primes less than 22. This takes place according to Theorem 3.8.

Theorem 3.8. If all the $n > 2$ terms of the arithmetic progression

$$p, p + d, p + 2d, \ldots, p + (n - 1)d$$

are prime numbers, then the common difference d is divisible by every prime $q < n$.

Proof. Consider a prime number $q < n$ and assume to the contrary that $q \nmid d$. We claim that the first q terms of the progression

$$p, p + d, p + 2d, \ldots, p + (q - 1)d \tag{1}$$

will leave different remainders when divided by q. Otherwise there exist integers j and k, with $0 \leq j < k \leq q - 1$, such that the numbers $p + jd$ and $p + kd$ yield the same remainder upon division by q. Then q divides their difference $(k - j)d$. But $\gcd(q , d) = 1$, and so Euclid's lemma leads to $q \mid k - j$, which is nonsense in light of the inequality $k - j \leq q - 1$.

Because the q different remainders produced from Eq. (1) are drawn from the q integers $0, 1, \ldots, q - 1$, one of these remainders must be zero. This means that $q \mid p + td$ for some t satisfying $0 \leq t \leq q - 1$. Because of the inequality $q < n \leq p \leq p + td$, we are forced to conclude that $p + td$ is composite. (If p were less than n, one of the terms of the progression would be $p + pd = p(1 + d)$.) With this contradiction, the proof that $q \mid d$ is complete.

It has been conjectured that there exist arithmetic progressions of finite (but otherwise arbitrary) length, composed of consecutive prime numbers. Examples of such progressions consisting of three and four primes, respectively, are 47, 53, 59, and 251, 257, 263, 269.

Most recently a sequence of 10 consecutive primes was discovered in which each term exceeds its predecessor by just 210; the smallest of these primes has 93 digits. Finding an arithmetic progression consisting of 11 consecutive primes is likely to be out of reach for some time. Absent the restriction that the primes involved be consecutive, strings of 11-term arithmetic progressions are easily located. One such is

$$110437 + 13860n \qquad 0 \leq n \leq 10$$

In the interest of completeness, we might mention another famous problem that, so far, has resisted the most determined attack. For centuries, mathematicians have sought a simple formula that would yield every prime number or, failing this, a formula that would produce nothing but primes. At first glance, the request seems modest enough: Find a function $f(n)$ whose domain is, say, the nonnegative integers and whose range is some infinite subset of the set of all primes. It was widely believed years ago that the quadratic polynomial

$$f(n) = n^2 + n + 41$$

assumed only prime values. This was shown to be false by Euler, in 1772. As evidenced by the following table, the claim is a correct one for $n = 0, 1, 2, \ldots, 39$.

n	$f(n)$	n	$f(n)$	n	$f(n)$
0	41	14	251	28	853
1	43	15	281	29	911
2	47	16	313	30	971
3	53	17	347	31	1033
4	61	18	383	32	1097
5	71	19	421	33	1163
6	83	20	461	34	1231
7	97	21	503	35	1301
8	113	22	547	36	1373
9	131	23	593	37	1447
10	151	24	641	38	1523
11	173	25	691	39	1601
12	197	26	743		
13	223	27	797		

However, this provocative conjecture is shattered in the cases $n = 40$ and $n = 41$, where there is a factor of 41:

$$f(40) = 40 \cdot 41 + 41 = 41^2$$

and

$$f(41) = 41 \cdot 42 + 41 = 41 \cdot 43$$

The next value $f(42) = 1847$ turns out to be prime once again. In fact, for the first 100 integer values of n, the so-called Euler polynomial represents 86 primes. Although it starts off very well in the production of primes, there are other quadratics such as

$$g(n) = n^2 + n + 27941$$

that begin to best $f(n)$ as the values of n become larger. For example, $g(n)$ is prime for 286129 values of $0 \leq n \leq 10^6$, whereas its famous rival yields 261081 primes in this range.

It has been shown that no polynomial of the form $n^2 + n + q$, with q a prime, can do better than the Euler polynomial in giving primes for successive values of n. Indeed, until fairly recently no other quadratic polynomial of any kind was known to produce more than 40 successive prime values. The polynomial

$$h(n) = 103n^2 - 3945n + 34381$$

found in 1988, produces 43 distinct prime values for $n = 0, 1, 2, \ldots, 42$. The current record holder in this regard

$$k(n) = 36n^2 - 810n + 2753$$

does slightly better by giving a string of 45 prime values.

The failure of the previous functions to be prime-producing is no accident, for it is easy to prove that there is no nonconstant polynomial $f(n)$ with integral

coefficients that takes on just prime values for integral n. We assume that such a polynomial $f(n)$ actually does exist and argue until a contradiction is reached. Let

$$f(n) = a_k n^k + a_{k-1} n^{k-1} + \cdots + a_2 n^2 + a_1 n + a_0$$

where all the coefficients $a_0, a_1, \ldots, a_k$ are integers, and $a_k \neq 0$. For a fixed value of (n_0), $p = f(n_0)$ is a prime number. Now, for any integer t, we consider the following expression:

$$\begin{aligned} f(n_0 + tp) &= a_k(n_0 + tp)^k + \cdots + a_1(n_0 + tp) + a_0 \\ &= (a_k n_0^k + \cdots + a_1 n_0 + a_0) + pQ(t) \\ &= f(n_0) + pQ(t) \\ &= p + pQ(t) = p(1 + Q(t)) \end{aligned}$$

where $Q(t)$ is a polynomial in t having integral coefficients. Our reasoning shows that $p \mid f(n_0 + tp)$; hence, from our own assumption that $f(n)$ takes on only prime values, $f(n_0 + tp) = p$ for any integer t. Because a polynomial of degree k cannot assume the same value more than k times, we have obtained the required contradiction.

Recent years have seen a measure of success in the search for prime-producing functions. W. H. Mills proved (1947) that there exists a positive real number r such that the expression $f(n) = [r^{3^n}]$ is prime for $n = 1, 2, 3, \ldots$ (the brackets indicate the greatest integer function). Needless to say, this is strictly an existence theorem and nothing is known about the actual value of r. Mills's function does not produce all the primes.

PROBLEMS 3.3

1. Verify that the integers 1949 and 1951 are twin primes.
2. (a) If 1 is added to a product of twin primes, prove that a perfect square is always obtained.
   (b) Show that the sum of twin primes p and $p + 2$ is divisible by 12, provided that $p > 3$.
3. Find all pairs of primes p and q satisfying $p - q = 3$.
4. Sylvester (1896) rephrased the Goldbach conjecture: Every even integer $2n$ greater than 4 is the sum of two primes, one larger than $n/2$ and the other less than $3n/2$. Verify this version of the conjecture for all even integers between 6 and 76.
5. In 1752, Goldbach submitted the following conjecture to Euler: Every odd integer can be written in the form $p + 2a^2$, where p is either a prime or 1 and $a \geq 0$. Show that the integer 5777 refutes this conjecture.
6. Prove that the Goldbach conjecture that every even integer greater than 2 is the sum of two primes is equivalent to the statement that every integer greater than 5 is the sum of three primes.
   [*Hint:* If $2n - 2 = p_1 + p_2$, then $2n = p_1 + p_2 + 2$ and $2n + 1 = p_1 + p_2 + 3$.]
7. A conjecture of Lagrange (1775) asserts that every odd integer greater than 5 can be written as a sum $p_1 + 2p_2$, where p_1, p_2 are both primes. Confirm this for all odd integers through 75.
8. Given a positive integer n, it can be shown that there exists an even integer a that is representable as the sum of two odd primes in n different ways. Confirm that the integers

60, 78, and 84 can be written as the sum of two primes in six, seven, and eight ways, respectively.

9. (a) For $n > 3$, show that the integers $n, n+2, n+4$ cannot all be prime.
(b) Three integers $p, p+2, p+6$, which are all prime, are called a *prime-triplet*. Find five sets of prime-triplets.

10. Establish that the sequence

$$(n+1)!-2, (n+1)!-3, \ldots, (n+1)!-(n+1)$$

produces n consecutive composite integers for $n > 2$.

11. Find the smallest positive integer n for which the function $f(n) = n^2 + n + 17$ is composite. Do the same for the functions $g(n) = n^2 + 21n + 1$ and $h(n) = 3n^2 + 3n + 23$.

12. Let p_n denote the nth prime number. For $n \geq 3$, prove that $p_{n+3}^2 < p_n p_{n+1} p_{n+2}$.
[*Hint:* Note that $p_{n+3}^2 < 4p_{n+2}^2 < 8p_{n+1}p_{n+2}$.]

13. Apply the same method of proof as in Theorem 3.6 to show that there are infinitely many primes of the form $6n + 5$.

14. Find a prime divisor of the integer $N = 4(3 \cdot 7 \cdot 11) - 1$ of the form $4n + 3$. Do the same for $N = 4(3 \cdot 7 \cdot 11 \cdot 15) - 1$.

15. Another unanswered question is whether there exist an infinite number of sets of five consecutive odd integers of which four are primes. Find five such sets of integers.

16. Let the sequence of primes, with 1 adjoined, be denoted by $p_0 = 1$, $p_1 = 2$, $p_2 = 3$, $p_3 = 5, \ldots$. For each $n \geq 1$, it is known that there exists a suitable choice of coefficients $\epsilon_k = \pm 1$ such that

$$p_{2n} = p_{2n-1} + \sum_{k=0}^{2n-2} \epsilon_k p_k \qquad p_{2n+1} = 2p_{2n} + \sum_{k=0}^{2n-1} \epsilon_k p_k$$

To illustrate:

$$13 = 1 + 2 - 3 - 5 + 7 + 11$$

and

$$17 = 1 + 2 - 3 - 5 + 7 - 11 + 2 \cdot 13$$

Determine similar representations for the primes 23, 29, 31, and 37.

17. In 1848, de Polignac claimed that every odd integer is the sum of a prime and a power of 2. For example, $55 = 47 + 2^3 = 23 + 2^5$. Show that the integers 509 and 877 discredit this claim.

18. (a) If p is a prime and $p \nmid b$, prove that in the arithmetic progression

$$a, a+b, a+2b, a+3b, \ldots$$

every pth term is divisible by p.
[*Hint:* Because $\gcd(p, b) = 1$, there exist integers r and s satisfying $pr + bs = 1$. Put $n_k = kp - as$ for $k = 1, 2, \ldots$ and show that $p \mid (a + n_k b)$.]
(b) From part (a), conclude that if b is an odd integer, then every other term in the indicated progression is even.

19. In 1950, it was proved that any integer $n > 9$ can be written as a sum of distinct odd primes. Express the integers 25, 69, 81, and 125 in this fashion.

20. If p and $p^2 + 8$ are both prime numbers, prove that $p^3 + 4$ is also prime.

21. (a) For any integer $k > 0$, establish that the arithmetic progression

$$a + b, a + 2b, a + 3b, \ldots$$

where $\gcd(a, b) = 1$, contains k consecutive terms that are composite.
[*Hint:* Put $n = (a + b)(a + 2b) \cdots (a + kb)$ and consider the k terms $a + (n + 1)b$, $a + (n + 2)b, \ldots, a + (n + k)b$.]

(b) Find five consecutive composite terms in the arithmetic progression

$$6, 11, 16, 21, 26, 31, 36, \ldots$$

22. Show that 13 is the largest prime that can divide two successive integers of the form $n^2 + 3$.

23. (a) The arithmetic mean of the twin primes 5 and 7 is the triangular number 6. Are there any other twin primes with a triangular mean?

(b) The arithmetic mean of the twin primes 3 and 5 is the perfect square 4. Are there any other twin primes with a square mean?

24. Determine all twin primes p and $q = p + 2$ for which $pq - 2$ is also prime.

25. Let p_n denote the nth prime. For $n > 3$, show that

$$p_n < p_1 + p_2 + \cdots + p_{n-1}$$

[*Hint:* Use induction and the Bertrand conjecture.]

26. Verify the following:

(a) There exist infinitely many primes ending in 33, such as 233, 433, 733, 1033, ... [*Hint:* Apply Dirichlet's theorem.]

(b) There exist infinitely many primes that do not belong to any pair of twin primes. [*Hint:* Consider the arithmetic progression $21k + 5$ for $k = 1, 2, \ldots$.]

(c) There exists a prime ending in as many consecutive 1's as desired. [*Hint:* To obtain a prime ending in n consecutive 1's, consider the arithmetic progression $10^n k + R_n$ for $k = 1, 2, \ldots$.]

(d) There exist infinitely many primes that contain but do not end in the block of digits 123456789. [*Hint:* Consider the arithmetic progression $10^{11}k + 1234567891$ for $k = 1, 2, \ldots$.]

27. Prove that for every $n \geq 2$ there exists a prime p with $p \leq n < 2p$.
[*Hint:* In the case where $n = 2k + 1$, then by the Bertrand conjecture there exists a prime p such that $k < p < 2k$.]

28. (a) If $n > 1$, show that $n!$ is never a perfect square.

(b) Find the values of $n \geq 1$ for which

$$n! + (n + 1)! + (n + 2)!$$

is a perfect square.
[*Hint:* Note that $n! + (n + 1)! + (n + 2)! = n!(n + 2)^2$.]

CHAPTER 4

THE THEORY OF CONGRUENCES

Gauss once said "Mathematics is the queen of the sciences and number-theory the queen of mathematics." If this be true we may add that the Disquisitiones *is the Magna Charta of number-theory.*
M. CANTOR

4.1 CARL FRIEDRICH GAUSS

Another approach to divisibility questions is through the arithmetic of remainders, or the *theory of congruences* as it is now commonly known. The concept, and the notation that makes it such a powerful tool, was first introduced by the German mathematician Carl Friedrich Gauss (1777–1855) in his *Disquisitiones Arithmeticae*; this monumental work, which appeared in 1801 when Gauss was 24 years old, laid the foundations of modern number theory. Legend has it that a large part of the *Disquisitiones Arithmeticae* had been submitted as a memoir to the French Academy the previous year and had been rejected in a manner that, even if the work had been as worthless as the referees believed, would have been inexcusable. (In an attempt to lay this defamatory tale to rest, the officers of the Academy made an exhaustive search of their permanent records in 1935 and concluded that the *Disquisitiones* was never submitted, much less rejected.) "It is really astonishing," said Kronecker, "to think that a single man of such young years was able to bring to light such a wealth of results, and above all to present such a profound and well-organized treatment of an entirely new discipline."

Carl Friedrich Gauss
(1777–1855)

(*Dover Publications, Inc.*)

Gauss was one of those remarkable infant prodigies whose natural aptitude for mathematics soon becomes apparent. As a child of age three, according to a well-authenticated story, he corrected an error in his father's payroll calculations. His arithmetical powers so overwhelmed his schoolmasters that, by the time Gauss was 7 years old, they admitted that there was nothing more they could teach the boy. It is said that in his first arithmetic class Gauss astonished his teacher by instantly solving what was intended to be a "busy work" problem: Find the sum of all the numbers from 1 to 100. The young Gauss later confessed to having recognized the pattern

$$1 + 100 = 101, 2 + 99 = 101, 3 + 98 = 101, \ldots, 50 + 51 = 101$$

Because there are 50 pairs of numbers, each of which adds up to 101, the sum of all the numbers must be $50 \cdot 101 = 5050$. This technique provides another way of deriving the formula

$$1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2}$$

for the sum of the first n positive integers. One need only display the consecutive integers 1 through n in two rows as follows:

$$\begin{array}{ccccccc} 1 & 2 & 3 & \cdots & n-1 & n \\ n & n-1 & n-2 & \cdots & 2 & 1 \end{array}$$

Addition of the vertical columns produces n terms, each of which is equal to $n + 1$; when these terms are added, we get the value $n(n + 1)$. Because the same sum is obtained on adding the two rows horizontally, what occurs is the formula $n(n + 1) = 2(1 + 2 + 3 + \cdots + n)$.

Gauss went on to a succession of triumphs, each new discovery following on the heels of a previous one. The problem of constructing regular polygons with only "Euclidean tools," that is to say, with ruler and compass alone, had long been laid aside in the belief that the ancients had exhausted all the possible constructions. In 1796, Gauss showed that the 17-sided regular polygon is so constructible, the first

advance in this area since Euclid's time. Gauss' doctoral thesis of 1799 provided a rigorous proof of the Fundamental Theorem of Algebra, which had been stated first by Girard in 1629 and then proved imperfectly by d'Alembert (1746), and later by Euler (1749). The theorem (it asserts that a polynomial equation of degree n has exactly n complex roots) was always a favorite of Gauss', and he gave, in all, four distinct demonstrations of it. The publication of *Disquisitiones Arithmeticae* in 1801 at once placed Gauss in the front rank of mathematicians.

The most extraordinary achievement of Gauss was more in the realm of theoretical astronomy than of mathematics. On the opening night of the 19th century, January 1, 1801, the Italian astronomer Piazzi discovered the first of the so-called minor planets (planetoids or asteroids), later called Ceres. But after the course of this newly found body—visible only by telescope—passed the sun, neither Piazzi nor any other astronomer could locate it again. Piazzi's observations extended over a period of 41 days, during which the orbit swept out an angle of only nine degrees. From the scanty data available, Gauss was able to calculate the orbit of Ceres with amazing accuracy, and the elusive planet was rediscovered at the end of the year in almost exactly the position he had forecasted. This success brought Gauss worldwide fame, and led to his appointment as director of Göttingen Observatory.

By the middle of the 19th century, mathematics had grown into an enormous and unwieldy structure, divided into a large number of fields in which only the specialist knew his way. Gauss was the last complete mathematician, and it is no exaggeration to say that he was in some degree connected with nearly every aspect of the subject. His contemporaries regarded him as Princeps Mathematicorum (Prince of Mathematicians), on a par with Archimedes and Isaac Newton. This is revealed in a small incident: On being asked who was the greatest mathematician in Germany, Laplace answered, "Why, Pfaff." When the questioner indicated that he would have thought Gauss was, Laplace replied, "Pfaff is by far the greatest in Germany, but Gauss is the greatest in all Europe."

Although Gauss adorned every branch of mathematics, he always held number theory in high esteem and affection. He insisted that, "Mathematics is the Queen of the Sciences, and the theory of numbers is the Queen of Mathematics."

4.2 BASIC PROPERTIES OF CONGRUENCE

In the first chapter of *Disquisitiones Arithmeticae*, Gauss introduces the concept of congruence and the notation that makes it such a powerful technique (he explains that he was induced to adopt the symbol $\equiv$ because of the close analogy with algebraic equality). According to Gauss, "If a number n measures the difference between two numbers a and b, then a and b are said to be congruent with respect to n; if not, incongruent." Putting this into the form of a definition, we have Definition 4.1.

Definition 4.1. Let n be a fixed positive integer. Two integers a and b are said to be *congruent modulo* n, symbolized by

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

if n divides the difference $a - b$; that is, provided that $a - b = kn$ for some integer k.

To fix the idea, consider $n = 7$. It is routine to check that

$$3 \equiv 24 \pmod 7 \qquad -31 \equiv 11 \pmod 7 \qquad -15 \equiv -64 \pmod 7$$

because $3 - 24 = (-3)7$, $-31 - 11 = (-6)7$, and $-15 - (-64) = 7 \cdot 7$. When $n \nmid (a - b)$, we say that a is *incongruent to b modulo n*, and in this case we write $a \not\equiv b \pmod n$. For a simple example: $25 \not\equiv 12 \pmod 7$, because 7 fails to divide $25 - 12 = 13$.

It is to be noted that any two integers are congruent modulo 1, whereas two integers are congruent modulo 2 when they are both even or both odd. Inasmuch as congruence modulo 1 is not particularly interesting, the usual practice is to assume that $n > 1$.

Given an integer a, let q and r be its quotient and remainder upon division by n, so that

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

Then, by definition of congruence, $a \equiv r \pmod n$. Because there are n choices for r, we see that every integer is congruent modulo n to exactly one of the values $0, 1, 2, \ldots, n - 1$; in particular, $a \equiv 0 \pmod n$ if and only if $n \mid a$. The set of n integers $0, 1, 2, \ldots, n - 1$ is called the set of *least nonnegative residues modulo n*.

In general, a collection of n integers $a_1, a_2, \ldots, a_n$ is said to form a *complete set of residues* (or a *complete system of residues*) *modulo n* if every integer is congruent modulo n to one and only one of the a_k. To put it another way, $a_1, a_2, \ldots, a_n$ are congruent modulo n to $0, 1, 2, \ldots, n - 1$, taken in some order. For instance,

$$-12, -4, 11, 13, 22, 82, 91$$

constitute a complete set of residues modulo 7; here, we have

$$-12 \equiv 2 \quad -4 \equiv 3 \quad 11 \equiv 4 \quad 13 \equiv 6 \quad 22 \equiv 1 \quad 82 \equiv 5 \quad 91 \equiv 0$$

all modulo 7. An observation of some importance is that any n integers form a complete set of residues modulo n if and only if no two of the integers are congruent modulo n. We shall need this fact later.

Our first theorem provides a useful characterization of congruence modulo n in terms of remainders upon division by n.

Theorem 4.1. For arbitrary integers a and b, $a \equiv b \pmod n$ if and only if a and b leave the same nonnegative remainder when divided by n.

Proof. First take $a \equiv b \pmod n$, so that $a = b + kn$ for some integer k. Upon division by n, b leaves a certain remainder r; that is, $b = qn + r$, where $0 \leq r < n$. Therefore,

$$a = b + kn = (qn + r) + kn = (q + k)n + r$$

which indicates that a has the same remainder as b.

On the other hand, suppose we can write $a = q_1 n + r$ and $b = q_2 n + r$, with the same remainder r $(0 \leq r < n)$. Then

$$a - b = (q_1 n + r) - (q_2 n + r) = (q_1 - q_2)n$$

whence $n \mid a - b$. In the language of congruences, we have $a \equiv b \pmod n$.

Example 4.1. Because the integers -56 and -11 can be expressed in the form

$$-56 = (-7)9 + 7 \qquad -11 = (-2)9 + 7$$

with the same remainder 7, Theorem 4.1 tells us that $-56 \equiv -11 \pmod 9$. Going in the other direction, the congruence $-31 \equiv 11 \pmod 7$ implies that -31 and 11 have the same remainder when divided by 7; this is clear from the relations

$$-31 = (-5)7 + 4 \qquad 11 = 1 \cdot 7 + 4$$

Congruence may be viewed as a generalized form of equality, in the sense that its behavior with respect to addition and multiplication is reminiscent of ordinary equality. Some of the elementary properties of equality that carry over to congruences appear in the next theorem.

Theorem 4.2. Let $n > 1$ be fixed and a, b, c, d be arbitrary integers. Then the following properties hold:

(a) $a \equiv a \pmod n$.
(b) If $a \equiv b \pmod n$, then $b \equiv a \pmod n$.
(c) If $a \equiv b \pmod n$ and $b \equiv c \pmod n$, then $a \equiv c \pmod n$.
(d) If $a \equiv b \pmod n$ and $c \equiv d \pmod n$, then $a + c \equiv b + d \pmod n$ and $ac \equiv bd \pmod n$.
(e) If $a \equiv b \pmod n$, then $a + c \equiv b + c \pmod n$ and $ac \equiv bc \pmod n$.
(f) If $a \equiv b \pmod n$, then $a^k \equiv b^k \pmod n$ for any positive integer k.

Proof. For any integer a, we have $a - a = 0 \cdot n$, so that $a \equiv a \pmod n$. Now if $a \equiv b \pmod n$, then $a - b = kn$ for some integer k. Hence, $b - a = -(kn) = (-k)n$ and because $-k$ is an integer, this yields property (b).

Property (c) is slightly less obvious: Suppose that $a \equiv b \pmod n$ and also $b \equiv c \pmod n$. Then there exist integers h and k satisfying $a - b = hn$ and $b - c = kn$. It follows that

$$a - c = (a - b) + (b - c) = hn + kn = (h + k)n$$

which is $a \equiv c \pmod n$ in congruence notation.

In the same vein, if $a \equiv b \pmod n$ and $c \equiv d \pmod n$, then we are assured that $a - b = k_1 n$ and $c - d = k_2 n$ for some choice of k_1 and k_2. Adding these equations, we obtain

$$\begin{aligned}(a + c) - (b + d) &= (a - b) + (c - d) \\ &= k_1 n + k_2 n = (k_1 + k_2)n\end{aligned}$$

or, as a congruence statement, $a + c \equiv b + d \pmod n$. As regards the second assertion of property (d), note that

$$ac = (b + k_1 n)(d + k_2 n) = bd + (bk_2 + dk_1 + k_1 k_2 n)n$$

Because $bk_2 + dk_1 + k_1 k_2 n$ is an integer, this says that $ac - bd$ is divisible by n, whence $ac \equiv bd \pmod n$.

The proof of property (e) is covered by (d) and the fact that $c \equiv c \pmod n$. Finally, we obtain property (f) by making an induction argument. The statement certainly holds for $k = 1$, and we will assume it is true for some fixed k. From (d), we know

that $a \equiv b \pmod{n}$ and $a^k \equiv b^k \pmod{n}$ together imply that $aa^k \equiv bb^k \pmod{n}$, or equivalently $a^{k+1} \equiv b^{k+1} \pmod{n}$. This is the form the statement should take for $k+1$, and so the induction step is complete.

Before going further, we should illustrate that congruences can be a great help in carrying out certain types of computations.

Example 4.2. Let us endeavor to show that 41 divides $2^{20} - 1$. We begin by noting that $2^5 \equiv -9 \pmod{41}$, whence $(2^5)^4 \equiv (-9)^4 \pmod{41}$ by Theorem 4.2(f); in other words, $2^{20} \equiv 81 \cdot 81 \pmod{41}$. But $81 \equiv -1 \pmod{41}$, and so $81 \cdot 81 \equiv 1 \pmod{41}$. Using parts (b) and (e) of Theorem 4.2, we finally arrive at

$$2^{20} - 1 \equiv 81 \cdot 81 - 1 \equiv 1 - 1 \equiv 0 \pmod{41}$$

Thus, $41 \mid 2^{20} - 1$, as desired.

Example 4.3. For another example in the same spirit, suppose that we are asked to find the remainder obtained upon dividing the sum

$$1! + 2! + 3! + 4! + \cdots + 99! + 100!$$

by 12. Without the aid of congruences this would be an awesome calculation. The observation that starts us off is that $4! \equiv 24 \equiv 0 \pmod{12}$; thus, for $k \geq 4$,

$$k! \equiv 4! \cdot 5 \cdot 6 \cdots k \equiv 0 \cdot 5 \cdot 6 \cdots k \equiv 0 \pmod{12}$$

In this way, we find that

$$\begin{aligned} 1! + 2! + 3! + 4! + \cdots + 100! \\ \equiv 1! + 2! + 3! + 0 + \cdots + 0 \equiv 9 \pmod{12} \end{aligned}$$

Accordingly, the sum in question leaves a remainder of 9 when divided by 12.

In Theorem 4.1 we saw that if $a \equiv b \pmod{n}$, then $ca \equiv cb \pmod{n}$ for any integer c. The converse, however, fails to hold. As an example, perhaps as simple as any, note that $2 \cdot 4 \equiv 2 \cdot 1 \pmod{6}$, whereas $4 \not\equiv 1 \pmod{6}$. In brief: One cannot unrestrictedly cancel a common factor in the arithmetic of congruences.

With suitable precautions, cancellation can be allowed; one step in this direction, and an important one, is provided by the following theorem.

Theorem 4.3. If $ca \equiv cb \pmod{n}$, then $a \equiv b \pmod{n/d}$, where $d = \gcd(c, n)$.

Proof. By hypothesis, we can write

$$c(a - b) = ca - cb = kn$$

for some integer k. Knowing that $\gcd(c, n) = d$, there exist relatively prime integers r and s satisfying $c = dr$, $n = ds$. When these values are substituted in the displayed equation and the common factor d canceled, the net result is

$$r(a - b) = ks$$

Hence, $s \mid r(a - b)$ and $\gcd(r, s) = 1$. Euclid's lemma yields $s \mid a - b$, which may be recast as $a \equiv b \pmod{s}$; in other words, $a \equiv b \pmod{n/d}$.

Theorem 4.3 gets its maximum force when the requirement that $\gcd(c, n) = 1$ is added, for then the cancellation may be accomplished without a change in modulus.

Corollary 1. If $ca \equiv cb \pmod{n}$ and $\gcd(c, n) = 1$, then $a \equiv b \pmod{n}$.

We take a moment to record a special case of Corollary 1 that we shall have frequent occasion to use, namely, Corollary 2.

Corollary 2. If $ca \equiv cb \pmod{p}$ and $p \nmid c$, where p is a prime number, then $a \equiv b \pmod{p}$.

Proof. The conditions $p \nmid c$ and p a prime imply that $\gcd(c, p) = 1$.

Example 4.4. Consider the congruence $33 \equiv 15 \pmod{9}$ or, if one prefers, $3 \cdot 11 \equiv 3 \cdot 5 \pmod{9}$. Because $\gcd(3, 9) = 3$, Theorem 4.3 leads to the conclusion that $11 \equiv 5 \pmod{3}$. A further illustration is given by the congruence $-35 \equiv 45 \pmod{8}$, which is the same as $5 \cdot (-7) \equiv 5 \cdot 9 \pmod{8}$. The integers 5 and 8 being relatively prime, we may cancel the factor 5 to obtain a correct congruence $-7 \equiv 9 \pmod{8}$.

Let us call attention to the fact that, in Theorem 4.3, it is unnecessary to stipulate that $c \not\equiv 0 \pmod{n}$. Indeed, if $c \equiv 0 \pmod{n}$, then $\gcd(c, n) = n$ and the conclusion of the theorem would state that $a \equiv b \pmod{1}$; but, as we remarked earlier, this holds trivially for all integers a and b.

There is another curious situation that can arise with congruences: The product of two integers, neither of which is congruent to zero, may turn out to be congruent to zero. For instance, $4 \cdot 3 \equiv 0 \pmod{12}$, but $4 \not\equiv 0 \pmod{12}$ and $3 \not\equiv 0 \pmod{12}$. It is a simple matter to show that if $ab \equiv 0 \pmod{n}$ and $\gcd(a, n) = 1$, then $b \equiv 0 \pmod{n}$: Corollary 1 permits us legitimately to cancel the factor a from both sides of the congruence $ab \equiv a \cdot 0 \pmod{n}$. A variation on this is that when $ab \equiv 0 \pmod{p}$, with p a prime, then either $a \equiv 0 \pmod{p}$ or $b \equiv 0 \pmod{p}$.

PROBLEMS 4.2

1. Prove each of the following assertions:
   (a) If $a \equiv b \pmod{n}$ and $m \mid n$, then $a \equiv b \pmod{m}$.
   (b) If $a \equiv b \pmod{n}$ and $c > 0$, then $ca \equiv cb \pmod{cn}$.
   (c) If $a \equiv b \pmod{n}$ and the integers a, b, n are all divisible by $d > 0$, then $a/d \equiv b/d \pmod{n/d}$.
2. Give an example to show that $a^2 \equiv b^2 \pmod{n}$ need not imply that $a \equiv b \pmod{n}$.
3. If $a \equiv b \pmod{n}$, prove that $\gcd(a, n) = \gcd(b, n)$.
4. (a) Find the remainders when 2^{50} and 41^{65} are divided by 7.
   (b) What is the remainder when the following sum is divided by 4?

$$1^5 + 2^5 + 3^5 + \cdots + 99^5 + 100^5$$

5. Prove that the integer $53^{103} + 103^{53}$ is divisible by 39, and that $111^{333} + 333^{111}$ is divisible by 7.

6. For $n \geq 1$, use congruence theory to establish each of the following divisibility statements:
(a) $7 \mid 5^{2n} + 3 \cdot 2^{5n-2}$.
(b) $13 \mid 3^{n+2} + 4^{2n+1}$.
(c) $27 \mid 2^{5n+1} + 5^{n+2}$.
(d) $43 \mid 6^{n+2} + 7^{2n+1}$.

7. For $n \geq 1$, show that

$$(-13)^{n+1} \equiv (-13)^n + (-13)^{n-1} \pmod{181}$$

[*Hint:* Notice that $(-13)^2 \equiv -13 + 1 \pmod{181}$; use induction on n.]

8. Prove the assertions below:
(a) If a is an odd integer, then $a^2 \equiv 1 \pmod 8$.
(b) For any integer a, $a^3 \equiv 0$, 1, or 6 (mod 7).
(c) For any integer a, $a^4 \equiv 0$ or 1 (mod 5).
(d) If the integer a is not divisible by 2 or 3, then $a^2 \equiv 1 \pmod{24}$.

9. If p is a prime satisfying $n < p < 2n$, show that

$$\binom{2n}{n} \equiv 0 \pmod p$$

10. If $a_1, a_2, \ldots, a_n$ is a complete set of residues modulo n and $\gcd(a, n) = 1$, prove that $aa_1, aa_2, \ldots, aa_n$ is also a complete set of residues modulo n.
[*Hint:* It suffices to show that the numbers in question are incongruent modulo n.]

11. Verify that $0, 1, 2, 2^2, 2^3, \ldots, 2^9$ form a complete set of residues modulo 11, but that $0, 1^2, 2^2, 3^2, \ldots, 10^2$ do not.

12. Prove the following statements:
(a) If $\gcd(a, n) = 1$, then the integers

$$c, c + a, c + 2a, c + 3a, \ldots, c + (n-1)a$$

form a complete set of residues modulo n for any c.
(b) Any n consecutive integers form a complete set of residues modulo n.
[*Hint:* Use part (a).]
(c) The product of any set of n consecutive integers is divisible by n.

13. Verify that if $a \equiv b \pmod{n_1}$ and $a \equiv b \pmod{n_2}$, then $a \equiv b \pmod n$, where the integer $n = \operatorname{lcm}(n_1, n_2)$. Hence, whenever n_1 and n_2 are relatively prime, $a \equiv b \pmod{n_1 n_2}$.

14. Give an example to show that $a^k \equiv b^k \pmod n$ and $k \equiv j \pmod n$ need not imply that $a^j \equiv b^j \pmod n$.

15. Establish that if a is an odd integer, then for any $n \geq 1$

$$a^{2^n} \equiv 1 \pmod{2^{n+2}}$$

[*Hint:* Proceed by induction on n.]

16. Use the theory of congruences to verify that

$$89 \mid 2^{44} - 1 \qquad \text{and} \qquad 97 \mid 2^{48} - 1$$

17. Prove that whenever $ab \equiv cd \pmod n$ and $b \equiv d \pmod n$, with $\gcd(b, n) = 1$, then $a \equiv c \pmod n$.

18. If $a \equiv b \pmod{n_1}$ and $a \equiv c \pmod{n_2}$, prove that $b \equiv c \pmod n$, where the integer $n = \gcd(n_1, n_2)$.

4.3 BINARY AND DECIMAL REPRESENTATIONS OF INTEGERS

One of the more interesting applications of congruence theory involves finding special criteria under which a given integer is divisible by another integer. At their heart, these divisibility tests depend on the notational system used to assign "names" to integers and, more particularly, to the fact that 10 is taken as the base for our number system. Let us, therefore, start by showing that, given an integer $b > 1$, any positive integer N can be written uniquely in terms of powers of b as

$$N = a_m b^m + a_{m-1} b^{m-1} + \cdots + a_2 b^2 + a_1 b + a_0$$

where the coefficients a_k can take on the b different values $0, 1, 2, \ldots, b-1$. For the Division Algorithm yields integers q_1 and a_0 satisfying

$$N = q_1 b + a_0 \qquad 0 \leq a_0 < b$$

If $q_1 \geq b$, we can divide once more, obtaining

$$q_1 = q_2 b + a_1 \qquad 0 \leq a_1 < b$$

Now substitute for q_1 in the earlier equation to get

$$N = (q_2 b + a_1)b + a_0 = q_2 b^2 + a_1 b + a_0$$

As long as $q_2 \geq b$, we can continue in the same fashion. Going one more step: $q_2 = q_3 b + a_2$, where $0 \leq a_2 < b$; hence

$$N = q_3 b^3 + a_2 b^2 + a_1 b + a_0$$

Because $N > q_1 > q_2 > \cdots \geq 0$ is a strictly decreasing sequence of integers, this process must eventually terminate, say, at the $(m-1)$th stage, where

$$q_{m-1} = q_m b + a_{m-1} \qquad 0 \leq a_{m-1} < b$$

and $0 \leq q_m < b$. Setting $a_m = q_m$, we reach the representation

$$N = a_m b^m + a_{m-1} b^{m-1} + \cdots + a_1 b + a_0$$

which was our aim.

To show uniqueness, let us suppose that N has two distinct representations, say,

$$N = a_m b^m + \cdots + a_1 b + a_0 = c_m b^m + \cdots + c_1 b + c_0$$

with $0 \leq a_i < b$ for each i and $0 \leq c_j < b$ for each j (we can use the same m by simply adding terms with coefficients $a_i = 0$ or $c_j = 0$, if necessary). Subtracting the second representation from the first gives the equation

$$0 = d_m b^m + \cdots + d_1 b + d_0$$

where $d_i = a_i - c_i$ for $i = 0, 1, \ldots, m$. Because the two representations for N are assumed to be different, we must have $d_i \neq 0$ for some value of i. Take k to be the smallest subscript for which $d_k \neq 0$. Then

$$0 = d_m b^m + \cdots + d_{k+1} b^{k+1} + d_k b^k$$

and so, after dividing by b^k,

$$d_k = -b(d_m b^{m-k-1} + \cdots + d_{k+1})$$

This tells us that $b \mid d_k$. Now the inequalities $0 \leq a_k < b$ and $0 \leq c_k < b$ lead us to $-b < a_k - c_k < b$, or $|d_k| < b$. The only way of reconciling the conditions $b \mid d_k$ and $|d_k| < b$ is to have $d_k = 0$, which is impossible. From this contradiction, we conclude that the representation of N is unique.

The essential feature in all of this is that the integer N is completely determined by the ordered array $a_m, a_{m-1}, \ldots, a_1, a_0$ of coefficients, with the plus signs and the powers of b being superfluous. Thus, the number

$$N = a_m b^m + a_{m-1} b^{m-1} + \cdots + a_2 b^2 + a_1 b + a_0$$

may be replaced by the simpler symbol

$$N = (a_m a_{m-1} \cdots a_2 a_1 a_0)_b$$

(the right-hand side is not to be interpreted as a product, but only as an abbreviation for N). We call this the *base b place-value notation for N*.

Small values of b give rise to lengthy representation of numbers, but have the advantage of requiring fewer choices for coefficients. The simplest case occurs when the base $b = 2$, and the resulting system of enumeration is called the *binary number system* (from the Latin *binarius*, two). The fact that when a number is written in the binary system only the integers 0 and 1 can appear as coefficients means that every positive integer is expressible in exactly one way as a sum of distinct powers of 2. For example, the integer 105 can be written as

$$\begin{aligned} 105 &= 1 \cdot 2^6 + 1 \cdot 2^5 + 0 \cdot 2^4 + 1 \cdot 2^3 + 0 \cdot 2^2 + 0 \cdot 2 + 1 \\ &= 2^6 + 2^5 + 2^3 + 1 \end{aligned}$$

or, in abbreviated form,

$$105 = (1101001)_2$$

In the other direction, $(1001111)_2$ translates into

$$1 \cdot 2^6 + 0 \cdot 2^5 + 0 \cdot 2^4 + 1 \cdot 2^3 + 1 \cdot 2^2 + 1 \cdot 2 + 1 = 79$$

The binary system is most convenient for use in modern electronic computing machines, because binary numbers are represented by strings of zeros and ones; 0 and 1 can be expressed in the machine by a switch (or a similar electronic device) being either on or off.

We shall frequently wish to calculate the value of $a^k \pmod{n}$ when k is large. Is there a more efficient way of obtaining the least positive residue than multiplying a by itself k times before reducing modulo n? One such procedure, called the *binary exponential algorithm*, relies on successive squarings, with a reduction modulo n after each squaring. More specifically, the exponent k is written in binary form, as $k = (a_m a_{m-1} \ldots a_2 a_1 a_0)_2$, and the values $a^{2^j} \pmod{n}$ are calculated for the powers of 2, which correspond to the 1's in the binary representation. These partial results are then multiplied together to give the final answer.

An illustration should make this process clear.

Example 4.5. To calculate $5^{110} \pmod{131}$, first note that the exponent 110 can be expressed in binary form as

$$110 = 64 + 32 + 8 + 4 + 2 = (110110)_2$$

Thus, we obtain the powers $5^{2^j} \pmod{131}$ for $0 \leq j \leq 6$ by repeatedly squaring while at each stage reducing each result modulo 131:

$$\begin{aligned} 5^2 &\equiv 25 \pmod{131} & 5^{16} &\equiv 27 \pmod{131} \\ 5^4 &\equiv 101 \pmod{131} & 5^{32} &\equiv 74 \pmod{131} \\ 5^8 &\equiv 114 \pmod{131} & 5^{64} &\equiv 105 \pmod{131} \end{aligned}$$

When the appropriate partial results—those corresponding to the 1's in the binary expansion of 110—are multiplied, we see that

$$\begin{aligned} 5^{110} &= 5^{64+32+8+4+2} \\ &= 5^{64} \cdot 5^{32} \cdot 5^8 \cdot 5^4 \cdot 5^2 \\ &\equiv 105 \cdot 74 \cdot 114 \cdot 101 \cdot 25 \equiv 60 \pmod{131} \end{aligned}$$

As a minor variation of the procedure, one might calculate, modulo 131, the powers $5, 5^2, 5^3, 5^6, 5^{12}, 5^{24}, 5^{48}, 5^{96}$ to arrive at

$$5^{110} = 5^{96} \cdot 5^{12} \cdot 5^2 \equiv 41 \cdot 117 \cdot 25 \equiv 60 \pmod{131}$$

which would require two fewer multiplications.

We ordinarily record numbers in the *decimal system* of notation, where $b = 10$, omitting the 10-subscript that specifies the base. For instance, the symbol 1492 stands for the more awkward expression

$$1 \cdot 10^3 + 4 \cdot 10^2 + 9 \cdot 10 + 2$$

The integers 1, 4, 9, and 2 are called the *digits* of the given number, 1 being the thousands digit, 4 the hundreds digit, 9 the tens digit, and 2 the units digit. In technical language we refer to the representation of the positive integers as sums of powers of 10, with coefficients at most 9, as their *decimal representation* (from the Latin *decem*, ten).

We are about ready to derive criteria for determining whether an integer is divisible by 9 or 11, without performing the actual division. For this, we need a result having to do with congruences involving polynomials with integral coefficients.

Theorem 4.4. Let $P(x) = \sum_{k=0}^{m} c_k x^k$ be a polynomial function of x with integral coefficients c_k. If $a \equiv b \pmod{n}$, then $P(a) \equiv P(b) \pmod{n}$.

Proof. Because $a \equiv b \pmod{n}$, part (f) of Theorem 4.2 can be applied to give $a^k \equiv b^k \pmod{n}$ for $k = 0, 1, \ldots, m$. Therefore,

$$c_k a^k \equiv c_k b^k \pmod{n}$$

for all such k. Adding these $m + 1$ congruences, we conclude that

$$\sum_{k=0}^{m} c_k a^k \equiv \sum_{k=0}^{m} c_k b^k \pmod{n}$$

or, in different notation, $P(a) \equiv P(b) \pmod{n}$.

If $P(x)$ is a polynomial with integral coefficients, we say that a is a solution of the congruence $P(x) \equiv 0 \pmod{n}$ if $P(a) \equiv 0 \pmod{n}$.

Corollary. If a is a solution of $P(x) \equiv 0 \pmod{n}$ and $a \equiv b \pmod{n}$, then b also is a solution.

Proof. From the last theorem, it is known that $P(a) \equiv P(b) \pmod{n}$. Hence, if a is a solution of $P(x) \equiv 0 \pmod{n}$, then $P(b) \equiv P(a) \equiv 0 \pmod{n}$, making b a solution.

One divisibility test that we have in mind is this. A positive integer is divisible by 9 if and only if the sum of the digits in its decimal representation is divisible by 9.

Theorem 4.5. Let $N = a_m 10^m + a_{m-1}10^{m-1} + \cdots + a_1 10 + a_0$ be the decimal expansion of the positive integer N, $0 \leq a_k < 10$, and let $S = a_0 + a_1 + \cdots + a_m$. Then $9 \mid N$ if and only if $9 \mid S$.

Proof. Consider $P(x) = \sum_{k=0}^{m} a_k x^k$, a polynomial with integral coefficients. The key observation is that $10 \equiv 1 \pmod{9}$, whence by Theorem 4.4, $P(10) \equiv P(1) \pmod{9}$. But $P(10) = N$ and $P(1) = a_0 + a_1 + \cdots + a_m = S$, so that $N \equiv S \pmod{9}$. It follows that $N \equiv 0 \pmod{9}$ if and only if $S \equiv 0 \pmod{9}$, which is what we wanted to prove.

Theorem 4.4 also serves as the basis for a well-known test for divisibility by 11: an integer is divisible by 11 if and only if the alternating sum of its digits is divisible by 11. We state this more precisely by Theorem 4.6.

Theorem 4.6. Let $N = a_m 10^m + a_{m-1}10^{m-1} + \cdots + a_1 10 + a_0$ be the decimal expansion of the positive integer N, $0 \leq a_k < 10$, and let $T = a_0 - a_1 + a_2 - \cdots + (-1)^m a_m$. Then $11 \mid N$ if and only if $11 \mid T$.

Proof. As in the proof of Theorem 4.5, put $P(x) = \sum_{k=0}^{m} a_k x^k$. Because $10 \equiv -1 \pmod{11}$, we get $P(10) \equiv P(-1) \pmod{11}$. But $P(10) = N$, whereas $P(-1) = a_0 - a_1 + a_2 - \cdots + (-1)^m a_m = T$, so that $N \equiv T \pmod{11}$. The implication is that either both N and T are divisible by 11 or neither is divisible by 11.

Example 4.6. To see an illustration of the last two results, take the integer $N = 1{,}571{,}724$. Because the sum

$$1 + 5 + 7 + 1 + 7 + 2 + 4 = 27$$

is divisible by 9, Theorem 4.5 guarantees that 9 divides N. It also can be divided by 11; for, the alternating sum

$$4 - 2 + 7 - 1 + 7 - 5 + 1 = 11$$

is divisible by 11.

Congruence theory is frequently used to append an extra check digit to identification numbers, in order to recognize transmission errors or forgeries. Personal

identification numbers of some kind appear on passports, credit cards, bank accounts, and a variety of other settings.

Some banks use an eight-digit identification number $a_1a_2 \ldots a_8$ together with a final check digit a_9. The check digit is usually obtained by multiplying the digits $a_i (1 \leq i \leq 8)$ by certain "weights" and calculating the sum of the weighted products modulo 10. For instance, the check digit might be chosen to satisfy

$$a_9 \equiv 7a_1 + 3a_2 + 9a_3 + 7a_4 + 3a_5 + 9a_6 + 7a_7 + 3a_8 \pmod{10}$$

The identification number 81504216 would then have check digit

$$a_9 \equiv 7 \cdot 8 + 3 \cdot 1 + 9 \cdot 5 + 7 \cdot 0 + 3 \cdot 4 + 9 \cdot 2 + 7 \cdot 1 + 3 \cdot 6 \equiv 9 \pmod{10}$$

so that 815042169 would be printed on the check.

This weighting scheme for assigning check digits detects any single-digit error in the identification number. For suppose that the digit a_i is replaced by a different a_i'. By the manner in which the check digit is calculated, the difference between the correct a_9 and the new a_9' is

$$a_9 - a_9' \equiv k(a_i - a_i') \pmod{10}$$

where k is 7, 3, or 9 depending on the position of a_i'. Because $k(a_i - a_i') \not\equiv 0 \pmod{10}$, it follows that $a_9 \neq a_9'$ and the error is apparent. Thus, if the valid number 81504216 were incorrectly entered as 81504316 into a computer programmed to calculate check digits, an 8 would come up rather than the expected 9.

The modulo 10 approach is not entirely effective, for it does not always detect the common error of transposing distinct adjacent entries a and b within the string of digits. To illustrate: the identification numbers 81504216 and 81504261 have the same check digit 9 when our example weights are used. (The problem occurs when $|a - b| = 5$.) More sophisticated methods are available, with larger moduli and different weights, that would prevent this possible error.

PROBLEMS 4.3

1. Use the binary exponentiation algorithm to compute both $19^{53} \pmod{503}$ and $141^{47} \pmod{1537}$.
2. Prove the following statements:
   (a) For any integer a, the units digit of a^2 is 0, 1, 4, 5, 6, or 9.
   (b) Any one of the integers 0, 1, 2, 3, 4, 5, 6, 7, 8, 9 can occur as the units digit of a^3.
   (c) For any integer a, the units digit of a^4 is 0, 1, 5, or 6.
   (d) The units digit of a triangular number is 0, 1, 3, 5, 6, or 8.
3. Find the last two digits of the number 9^{9^9}.
   [*Hint:* $9^9 \equiv 9 \pmod{10}$; hence, $9^{9^9} = 9^{9+10k}$; now use the fact that $9^9 \equiv 89 \pmod{100}$.]
4. Without performing the divisions, determine whether the integers 176,521,221 and 149,235,678 are divisible by 9 or 11.
5. (a) Obtain the following generalization of Theorem 4.6: If the integer N is represented in the base b by

$$N = a_m b^m + \cdots + a_2 b^2 + a_1 b + a_0 \qquad 0 \leq a_k \leq b - 1$$

   then $b - 1 \mid N$ if and only if $b - 1 \mid (a_m + \cdots + a_2 + a_1 + a_0)$.

(b) Give criteria for the divisibility of N by 3 and 8 that depend on the digits of N when written in the base 9.
(c) Is the integer $(447836)_9$ divisible by 3 and 8?

6. Working modulo 9 or 11, find the missing digits in the calculations below:
(a) $51840 \cdot 273581 = 1418243x040$.
(b) $2x99561 = [3(523 + x)]^2$.
(c) $2784x = x \cdot 5569$.
(d) $512 \cdot 1x53125 = 1000000000$.

7. Establish the following divisibility criteria:
(a) An integer is divisible by 2 if and only if its units digit is 0, 2, 4, 6, or 8.
(b) An integer is divisible by 3 if and only if the sum of its digits is divisible by 3.
(c) An integer is divisible by 4 if and only if the number formed by its tens and units digits is divisible by 4.
[*Hint:* $10^k \equiv 0 \pmod 4$ for $k \geq 2$.]
(d) An integer is divisible by 5 if and only if its units digit is 0 or 5.

8. For any integer a, show that $a^2 - a + 7$ ends in one of the digits 3, 7, or 9.

9. Find the remainder when 4444^{4444} is divided by 9.
[*Hint:* Observe that $2^3 \equiv -1 \pmod 9$.]

10. Prove that no integer whose digits add up to 15 can be a square or a cube.
[*Hint:* For any a, $a^3 \equiv 0, 1$, or $8 \pmod 9$.]

11. Assuming that 495 divides $273x49y5$, obtain the digits x and y.

12. Determine the last three digits of the number 7^{999}.
[*Hint:* $7^{4n} \equiv (1 + 400)^n \equiv 1 + 400n \pmod{1000}$.]

13. If t_n denotes the nth triangular number, show that $t_{n+2k} \equiv t_n \pmod k$; hence, t_n and t_{n+20} must have the same last digit.

14. For any $n \geq 1$, prove that there exists a prime with at least n of its digits equal to 0.
[*Hint:* Consider the arithmetic progression $10^{n+1}k + 1$ for $k = 1, 2, \ldots$.]

15. Find the values of $n \geq 1$ for which $1! + 2! + 3! + \cdots + n!$ is a perfect square.
[*Hint:* Problem 2(a).]

16. Show that 2^n divides an integer N if and only if 2^n divides the number made up of the last n digits of N.
[*Hint:* $10^k = 2^k 5^k \equiv 0 \pmod{2^n}$ for $k \geq n$.]

17. Let $N = a_m 10^m + \cdots + a_2 10^2 + a_1 10 + a_0$, where $0 \leq a_k \leq 9$, be the decimal expansion of a positive integer N.
(a) Prove that 7, 11, and 13 all divide N if and only if 7, 11, and 13 divide the integer

$$M = (100a_2 + 10a_1 + a_0) - (100a_5 + 10a_4 + a_3) + (100a_8 + 10a_7 + a_6) - \cdots$$

[*Hint:* If n is even, then $10^{3n} \equiv 1$, $10^{3n+1} \equiv 10$, $10^{3n+2} \equiv 100 \pmod{1001}$; if n is odd, then $10^{3n} \equiv -1$, $10^{3n+1} \equiv -10$, $10^{3n+2} \equiv -100 \pmod{1001}$.]
(b) Prove that 6 divides N if and only if 6 divides the integer

$$M = a_0 + 4a_1 + 4a_2 + \cdots + 4a_m$$

18. Without performing the divisions, determine whether the integer 1010908899 is divisible by 7, 11, and 13.

19. (a) Given an integer N, let M be the integer formed by reversing the order of the digits of N (for example, if $N = 6923$, then $M = 3296$). Verify that $N - M$ is divisible by 9.

(b) A *palindrome* is a number that reads the same backwards as forwards (for instance, 373 and 521125 are palindromes). Prove that any palindrome with an even number of digits is divisible by 11.

20. Given a repunit R_n, show that
(a) $9 \mid R_n$ if and only if $9 \mid n$.
(b) $11 \mid R_n$ if and only if n is even.

21. Factor the repunit $R_6 = 111111$ into a product of primes.
[*Hint:* Problem 17(a).]

22. Explain why the following curious calculations hold:

$$\begin{aligned}
1 \cdot 9 + 2 &= 11 \\
12 \cdot 9 + 3 &= 111 \\
123 \cdot 9 + 4 &= 1111 \\
1234 \cdot 9 + 5 &= 11111 \\
12345 \cdot 9 + 6 &= 111111 \\
123456 \cdot 9 + 7 &= 1111111 \\
1234567 \cdot 9 + 8 &= 11111111 \\
12345678 \cdot 9 + 9 &= 111111111 \\
123456789 \cdot 9 + 10 &= 1111111111
\end{aligned}$$

[*Hint:* Show that

$$(10^{n-1} + 2 \cdot 10^{n-2} + 3 \cdot 10^{n-3} + \cdots + n)(10 - 1) + (n + 1) = \frac{10^{n+1} - 1}{9}.]$$

23. An old and somewhat illegible invoice shows that 72 canned hams were purchased for $\$x\,67.9y$. Find the missing digits.

24. If 792 divides the integer $13xy\,45z$, find the digits x, y, and z.
[*Hint:* By Problem 17, $8 \mid 45z$.]

25. For any prime $p > 3$ prove that 13 divides $10^{2p} - 10^p + 1$.

26. Consider the eight-digit bank identification number $a_1a_2 \ldots a_8$, which is followed by a ninth check digit a_9 chosen to satisfy the congruence

$$a_9 \equiv 7a_1 + 3a_2 + 9a_3 + 7a_4 + 3a_5 + 9a_6 + 7a_7 + 3a_8 \pmod{10}$$

(a) Obtain the check digits that should be appended to the two numbers 55382006 and 81372439.
(b) The bank identification number $237a_418538$ has an illegible fourth digit. Determine the value of the obscured digit.

27. The International Standard Book Number (ISBN) used in many libraries consists of nine digits $a_1a_2 \ldots a_9$ followed by a tenth check digit a_{10}, which satisfies

$$a_{10} \equiv \sum_{k=1}^{9} ka_k \pmod{11}$$

Determine whether each of the ISBNs below is correct:
(a) 0-07-232569-0 (United States).
(b) 91-7643-497-5 (Sweden).
(c) 1-56947-303-10 (England).

28. When printing the ISBN $a_1a_2 \ldots a_9$, two unequal digits were transposed. Show that the check digits detected this error.

4.4 LINEAR CONGRUENCES AND THE CHINESE REMAINDER THEOREM

This is a convenient place in our development of number theory at which to investigate the theory of linear congruences: An equation of the form $ax \equiv b \pmod{n}$ is called a *linear congruence*, and by a solution of such an equation we mean an integer x_0 for which $ax_0 \equiv b \pmod{n}$. By definition, $ax_0 \equiv b \pmod{n}$ if and only if $n \mid ax_0 - b$ or, what amounts to the same thing, if and only if $ax_0 - b = ny_0$ for some integer y_0. Thus, the problem of finding all integers that will satisfy the linear congruence $ax \equiv b \pmod{n}$ is identical with that of obtaining all solutions of the linear Diophantine equation $ax - ny = b$. This allows us to bring the results of Chapter 2 into play.

It is convenient to treat two solutions of $ax \equiv b \pmod{n}$ that are congruent modulo n as being "equal" even though they are not equal in the usual sense. For instance, $x = 3$ and $x = -9$ both satisfy the congruence $3x \equiv 9 \pmod{12}$; because $3 \equiv -9 \pmod{12}$, they are not counted as different solutions. In short: When we refer to the number of solutions of $ax \equiv b \pmod{n}$, we mean the number of incongruent integers satisfying this congruence.

With these remarks in mind, the principal result is easy to state.

Theorem 4.7. The linear congruence $ax \equiv b \pmod{n}$ has a solution if and only if $d \mid b$, where $d = \gcd(a, n)$. If $d \mid b$, then it has d mutually incongruent solutions modulo n.

Proof. We already have observed that the given congruence is equivalent to the linear Diophantine equation $ax - ny = b$. From Theorem 2.9, it is known that the latter equation can be solved if and only if $d \mid b$; moreover, if it is solvable and x_0, y_0 is one specific solution, then any other solution has the form

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

for some choice of t.

Among the various integers satisfying the first of these formulas, consider those that occur when t takes on the successive values $t = 0, 1, 2, \ldots, d - 1$:

$$x_0, x_0 + \frac{n}{d}, x_0 + \frac{2n}{d}, \ldots, x_0 + \frac{(d-1)n}{d}$$

We claim that these integers are incongruent modulo n, and all other such integers x are congruent to some one of them. If it happened that

$$x_0 + \frac{n}{d}t_1 \equiv x_0 + \frac{n}{d}t_2 \pmod{n}$$

where $0 \leq t_1 < t_2 \leq d - 1$, then we would have

$$\frac{n}{d}t_1 \equiv \frac{n}{d}t_2 \pmod{n}$$

Now $\gcd(n/d, n) = n/d$, and therefore by Theorem 4.3 the factor n/d could be canceled to arrive at the congruence

$$t_1 \equiv t_2 \pmod{d}$$

which is to say that $d \mid t_2 - t_1$. But this is impossible in view of the inequality $0 < t_2 - t_1 < d$.

It remains to argue that any other solution $x_0 + (n/d)t$ is congruent modulo n to one of the d integers listed above. The Division Algorithm permits us to write t as $t = qd + r$, where $0 \leq r \leq d - 1$. Hence

$$\begin{aligned} x_0 + \frac{n}{d}t &= x_0 + \frac{n}{d}(qd + r) \\ &= x_0 + nq + \frac{n}{d}r \\ &\equiv x_0 + \frac{n}{d}r \pmod{n} \end{aligned}$$

with $x_0 + (n/d)r$ being one of our d selected solutions. This ends the proof.

The argument that we gave in Theorem 4.7 brings out a point worth stating explicitly: If x_0 is any solution of $ax \equiv b \pmod{n}$, then the $d = \gcd(a, n)$ incongruent solutions are given by

$$x_0, x_0 + \frac{n}{d}, x_0 + 2\left(\frac{n}{d}\right), \ldots, x_0 + (d-1)\left(\frac{n}{d}\right)$$

For the reader's convenience, let us also record the form Theorem 4.7 takes in the special case in which a and n are assumed to be relatively prime.

Corollary. If $\gcd(a, n) = 1$, then the linear congruence $ax \equiv b \pmod{n}$ has a unique solution modulo n.

Given relatively prime integers a and n, the congruence $ax \equiv 1 \pmod{n}$ has a unique solution. This solution is sometimes called the (multiplicative) inverse of a modulo n.

We now pause to look at two concrete examples.

Example 4.7. First consider the linear congruence $18x \equiv 30 \pmod{42}$. Because $\gcd(18, 42) = 6$ and 6 surely divides 30, Theorem 4.7 guarantees the existence of exactly six solutions, which are incongruent modulo 42. By inspection, one solution is found to be $x = 4$. Our analysis tells us that the six solutions are as follows:

$$x \equiv 4 + (42/6)t \equiv 4 + 7t \pmod{42} \qquad t = 0, 1, \ldots, 5$$

or, plainly enumerated,

$$x \equiv 4, 11, 18, 25, 32, 39 \pmod{42}$$

Example 4.8. Let us solve the linear congruence $9x \equiv 21 \pmod{30}$. At the outset, because $\gcd(9, 30) = 3$ and $3 \mid 21$, we know that there must be three incongruent solutions.

One way to find these solutions is to divide the given congruence through by 3, thereby replacing it by the equivalent congruence $3x \equiv 7 \pmod{10}$. The relative primeness of 3 and 10 implies that the latter congruence admits a unique solution modulo 10. Although it is not the most efficient method, we could test the integers

0, 1, 2, . . . ,9 in turn until the solution is obtained. A better way is this: Multiply both sides of the congruence $3x \equiv 7 \pmod{10}$ by 7 to get

$$21x \equiv 49 \pmod{10}$$

which reduces to $x \equiv 9 \pmod{10}$. (This simplification is no accident, for the multiples $0 \cdot 3,\ 1 \cdot 3,\ 2 \cdot 3, \ldots, 9 \cdot 3$ form a complete set of residues modulo 10; hence, one of them is necessarily congruent to 1 modulo 10.) But the original congruence was given modulo 30, so that its incongruent solutions are sought among the integers 0, 1, 2, . . . , 29. Taking $t = 0, 1, 2$, in the formula

$$x = 9 + 10t$$

we obtain 9, 19, 29, whence

$$x \equiv 9 \pmod{30} \qquad x \equiv 19 \pmod{30} \qquad x \equiv 29 \pmod{30}$$

are the required three solutions of $9x \equiv 21 \pmod{30}$.

A different approach to the problem is to use the method that is suggested in the proof of Theorem 4.7. Because the congruence $9x \equiv 21 \pmod{30}$ is equivalent to the linear Diophantine equation

$$9x - 30y = 21$$

we begin by expressing $3 = \gcd(9, 30)$ as a linear combination of 9 and 30. It is found, either by inspection or by using the Euclidean Algorithm, that $3 = 9(-3) + 30 \cdot 1$, so that

$$21 = 7 \cdot 3 = 9(-21) - 30(-7)$$

Thus, $x = -21$, $y = -7$ satisfy the Diophantine equation and, in consequence, all solutions of the congruence in question are to be found from the formula

$$x = -21 + (30/3)t = -21 + 10t$$

The integers $x = -21 + 10t$, where $t = 0, 1, 2$, are incongruent modulo 30 (but all are congruent modulo 10); thus, we end up with the incongruent solutions

$$x \equiv -21 \pmod{30} \qquad x \equiv -11 \pmod{30} \qquad x \equiv -1 \pmod{30}$$

or, if one prefers positive numbers, $x \equiv 9, 19, 29 \pmod{30}$.

Having considered a single linear congruence, it is natural to turn to the problem of solving a system of simultaneous linear congruences:

$$a_1x \equiv b_1 \pmod{m_1},\ a_2x \equiv b_2 \pmod{m_2},\ \ldots,\ a_rx \equiv b_r \pmod{m_r}$$

We shall assume that the moduli m_k are relatively prime in pairs. Evidently, the system will admit no solution unless each individual congruence is solvable; that is, unless $d_k \mid b_k$ for each k, where $d_k = \gcd(a_k, m_k)$. When these conditions are satisfied, the factor d_k can be canceled in the kth congruence to produce a new system having the same set of solutions as the original one:

$$a_1'x \equiv b_1' \pmod{n_1},\ a_2'x \equiv b_2' \pmod{n_2},\ \ldots,\ a_r'x \equiv b_r' \pmod{n_r}$$

where $n_k = m_k/d_k$ and $\gcd(n_i, n_j) = 1$ for $i \neq j$; in addition, $\gcd(a_i', n_i) = 1$. The solutions of the individual congruences assume the form

$$x \equiv c_1 \pmod{n_1}, x \equiv c_2 \pmod{n_2}, \ldots, x \equiv c_r \pmod{n_r}$$

Thus, the problem is reduced to one of finding a simultaneous solution of a system of congruences of this simpler type.

The kind of problem that can be solved by simultaneous congruences has a long history, appearing in the Chinese literature as early as the 1st century A.D. Sun-Tsu asked: Find a number that leaves the remainders 2, 3, 2 when divided by 3, 5, 7, respectively. (Such mathematical puzzles are by no means confined to a single cultural sphere; indeed, the same problem occurs in the *Introductio Arithmeticae* of the Greek mathematician Nicomachus, circa 100 A.D.) In honor of their early contributions, the rule for obtaining a solution usually goes by the name of the Chinese Remainder Theorem.

Theorem 4.8 Chinese Remainder Theorem. Let $n_1, n_2, \ldots, n_r$ be positive integers such that $\gcd(n_i, n_j) = 1$ for $i \neq j$. Then the system of linear congruences

$$\begin{aligned} x &\equiv a_1 \pmod{n_1} \\ x &\equiv a_2 \pmod{n_2} \\ &\vdots \\ x &\equiv a_r \pmod{n_r} \end{aligned}$$

has a simultaneous solution, which is unique modulo the integer $n_1 n_2 \cdots n_r$.

Proof. We start by forming the product $n = n_1 n_2 \cdots n_r$. For each $k = 1, 2, \ldots, r$, let

$$N_k = \frac{n}{n_k} = n_1 \cdots n_{k-1} n_{k+1} \cdots n_r$$

In words, N_k is the product of all the integers n_i with the factor n_k omitted. By hypothesis, the n_i are relatively prime in pairs, so that $\gcd(N_k, n_k) = 1$. According to the theory of a single linear congruence, it is therefore possible to solve the congruence $N_k x \equiv 1 \pmod{n_k}$; call the unique solution x_k. Our aim is to prove that the integer

$$\bar{x} = a_1 N_1 x_1 + a_2 N_2 x_2 + \cdots + a_r N_r x_r$$

is a simultaneous solution of the given system.

First, observe that $N_i \equiv 0 \pmod{n_k}$ for $i \neq k$, because $n_k \mid N_i$ in this case. The result is

$$\bar{x} = a_1 N_1 x_1 + \cdots + a_r N_r x_r \equiv a_k N_k x_k \pmod{n_k}$$

But the integer x_k was chosen to satisfy the congruence $N_k x \equiv 1 \pmod{n_k}$, which forces

$$\bar{x} \equiv a_k \cdot 1 \equiv a_k \pmod{n_k}$$

This shows that a solution to the given system of congruences exists.

As for the uniqueness assertion, suppose that x' is any other integer that satisfies these congruences. Then

$$\bar{x} \equiv a_k \equiv x' \pmod{n_k} \qquad k = 1, 2, \ldots, r$$

and so $n_k \mid \bar{x} - x'$ for each value of k. Because $\gcd(n_i, n_j) = 1$, Corollary 2 to Theorem 2.4 supplies us with the crucial point that $n_1 n_2 \cdots n_r \mid \bar{x} - x'$; hence $\bar{x} \equiv x' \pmod{n}$. With this, the Chinese Remainder Theorem is proven.

Example 4.9. The problem posed by Sun-Tsu corresponds to the system of three congruences

$$x \equiv 2 \pmod 3$$
$$x \equiv 3 \pmod 5$$
$$x \equiv 2 \pmod 7$$

In the notation of Theorem 4.8, we have $n = 3 \cdot 5 \cdot 7 = 105$ and

$$N_1 = \frac{n}{3} = 35 \qquad N_2 = \frac{n}{5} = 21 \qquad N_3 = \frac{n}{7} = 15$$

Now the linear congruences

$$35x \equiv 1 \pmod 3 \qquad 21x \equiv 1 \pmod 5 \qquad 15x \equiv 1 \pmod 7$$

are satisfied by $x_1 = 2$, $x_2 = 1$, $x_3 = 1$, respectively. Thus, a solution of the system is given by

$$x = 2 \cdot 35 \cdot 2 + 3 \cdot 21 \cdot 1 + 2 \cdot 15 \cdot 1 = 233$$

Modulo 105, we get the unique solution $x = 233 \equiv 23 \pmod{105}$.

Example 4.10. For a second illustration, let us solve the linear congruence

$$17x \equiv 9 \pmod{276}$$

Because $276 = 3 \cdot 4 \cdot 23$, this is equivalent to finding a solution for the system of congruences

$$\begin{aligned} 17x &\equiv 9 \pmod 3 \quad \text{or} \quad x \equiv 0 \pmod 3 \\ 17x &\equiv 9 \pmod 4 \qquad\quad x \equiv 1 \pmod 4 \\ 17x &\equiv 9 \pmod{23} \qquad 17x \equiv 9 \pmod{23} \end{aligned}$$

Note that if $x \equiv 0 \pmod 3$, then $x = 3k$ for any integer k. We substitute into the second congruence of the system and obtain

$$3k \equiv 1 \pmod 4$$

Multiplication of both sides of this congruence by 3 gives us

$$k \equiv 9k \equiv 3 \pmod 4$$

so that $k = 3 + 4j$, where j is an integer. Then

$$x = 3(3 + 4j) = 9 + 12j$$

For x to satisfy the last congruence, we must have

$$17(9 + 12j) \equiv 9 \pmod{23}$$

or $204j \equiv -144 \pmod{23}$, which reduces to $3j \equiv 6 \pmod{23}$; in consequence, $j \equiv 2 \pmod{23}$. This yields $j = 2 + 23t$, with t an integer, whence

$$x = 9 + 12(2 + 23t) = 33 + 276t$$

All in all, $x \equiv 33 \pmod{276}$ provides a solution to the system of congruences and, in turn, a solution to $17x \equiv 9 \pmod{276}$.

We should say a few words about linear congruences in two variables; that is, congruences of the form

$$ax + by \equiv c \pmod{n}$$

In analogy with Theorem 4.7, such a congruence has a solution if and only if $\gcd(a, b, n)$ divides c. The condition for solvability holds if either $\gcd(a, n) = 1$ or $\gcd(b, n) = 1$. Say $\gcd(a, n) = 1$. When the congruence is expressed as

$$ax \equiv c - by \pmod{n}$$

the corollary to Theorem 4.7 guarantees a unique solution x for each of the n incongruent values of y. Take as a simple illustration $7x + 4y \equiv 5 \pmod{12}$, that would be treated as $7x \equiv 5 - 4y \pmod{12}$. Substitution of $y \equiv 5 \pmod{12}$ gives $7x \equiv -15 \pmod{12}$; but this is equivalent to $-5x \equiv -15 \pmod{12}$ so that $x \equiv 3 \pmod{12}$. It follows that $x \equiv 3 \pmod{12}, y \equiv 5 \pmod{12}$ is one of the 12 incongruent solutions of $7x + 4y \equiv 5 \pmod{12}$. Another solution having the same value of x is $x \equiv 3 \pmod{12}, y \equiv 8 \pmod{12}$.

The focus of our concern here is how to solve a system of two linear congruences in two variables with the same modulus. The proof of the coming theorem adopts the familiar procedure of eliminating one of the unknowns.

Theorem 4.9. The system of linear congruences

$$ax + by \equiv r \pmod{n}$$
$$cx + dy \equiv s \pmod{n}$$

has a unique solution modulo n whenever $\gcd(ad - bc, n) = 1$.

Proof. Let us multiply the first congruence of the system by d, the second congruence by b, and subtract the lower result from the upper. These calculations yield

$$(ad - bc)x \equiv dr - bs \pmod{n} \tag{1}$$

The assumption $\gcd(ad - bc, n) = 1$ ensures that the congruence

$$(ad - bc)z \equiv 1 \pmod{n}$$

posseses a unique solution; denote the solution by t. When congruence (1) is multiplied by t, we obtain

$$x \equiv t(dr - bs) \pmod{n}$$

A value for y is found by a similar elimination process. That is, multiply the first congruence of the system by c, the second one by a, and subtract to end up with

$$(ad - bc)y \equiv as - cr \pmod{n} \tag{2}$$

Multiplication of this congruence by t leads to

$$y \equiv t(as - cr) \pmod{n}$$

A solution of the system is now established.

We close this section with an example illustrating Theorem 4.9.

Example 4.11. Consider the system

$$7x + 3y \equiv 10 \pmod{16}$$
$$2x + 5y \equiv 9 \pmod{16}$$

Because $\gcd(7 \cdot 5 - 2 \cdot 3, 16) = \gcd(29, 16) = 1$, a solution exists. It is obtained by the method developed in the proof of Theorem 4.9. Multiplying the first congruence by 5, the second one by 3, and subtracting, we arrive at

$$29x \equiv 5 \cdot 10 - 3 \cdot 9 \equiv 23 \pmod{16}$$

or, what is the same thing, $13x \equiv 7 \pmod{16}$. Multiplication of this congruence by 5 (noting that $5 \cdot 13 \equiv 1 \pmod{16}$) produces $x \equiv 35 \equiv 3 \pmod{16}$. When the variable x is eliminated from the system of congruences in a like manner, it is found that

$$29y \equiv 7 \cdot 9 - 2 \cdot 10 \equiv 43 \pmod{16}$$

But then $13y \equiv 11 \pmod{16}$, which upon multiplication by 5, results in $y \equiv 55 \equiv 7 \pmod{16}$. The unique solution of our system turns out to be

$$x \equiv 3 \pmod{16} \qquad y \equiv 7 \pmod{16}$$

PROBLEMS 4.4

1. Solve the following linear congruences:
   (a) $25x \equiv 15 \pmod{29}$.
   (b) $5x \equiv 2 \pmod{26}$.
   (c) $6x \equiv 15 \pmod{21}$.
   (d) $36x \equiv 8 \pmod{102}$.
   (e) $34x \equiv 60 \pmod{98}$.
   (f) $140x \equiv 133 \pmod{301}$.
   [*Hint:* $\gcd(140, 301) = 7$.]
2. Using congruences, solve the Diophantine equations below:
   (a) $4x + 51y = 9$.
   [*Hint:* $4x \equiv 9 \pmod{51}$ gives $x = 15 + 51t$, whereas $51y \equiv 9 \pmod{4}$ gives $y = 3 + 4s$. Find the relation between s and t.]
   (b) $12x + 25y = 331$.
   (c) $5x - 53y = 17$.
3. Find all solutions of the linear congruence $3x - 7y \equiv 11 \pmod{13}$.
4. Solve each of the following sets of simultaneous congruences:
   (a) $x \equiv 1 \pmod{3}$, $x \equiv 2 \pmod{5}$, $x \equiv 3 \pmod{7}$.
   (b) $x \equiv 5 \pmod{11}$, $x \equiv 14 \pmod{29}$, $x \equiv 15 \pmod{31}$.
   (c) $x \equiv 5 \pmod{6}$, $x \equiv 4 \pmod{11}$, $x \equiv 3 \pmod{17}$.
   (d) $2x \equiv 1 \pmod{5}$, $3x \equiv 9 \pmod{6}$, $4x \equiv 1 \pmod{7}$, $5x \equiv 9 \pmod{11}$.
5. Solve the linear congruence $17x \equiv 3 \pmod{2 \cdot 3 \cdot 5 \cdot 7}$ by solving the system

$$17x \equiv 3 \pmod{2} \qquad 17x \equiv 3 \pmod{3}$$
$$17x \equiv 3 \pmod{5} \qquad 17x \equiv 3 \pmod{7}$$

6. Find the smallest integer $a > 2$ such that

$$2 \mid a,\ 3 \mid a + 1,\ 4 \mid a + 2, 5 \mid a + 3, 6 \mid a + 4$$

7. (a) Obtain three consecutive integers, each having a square factor.
[*Hint:* Find an integer a such that $2^2 \mid a, 3^2 \mid a+1, 5^2 \mid a+2$.]
(b) Obtain three consecutive integers, the first of which is divisible by a square, the second by a cube, and the third by a fourth power.

8. (Brahmagupta, 7th century A.D.) When eggs in a basket are removed 2, 3, 4, 5, 6 at a time there remain, respectively, 1, 2, 3, 4, 5 eggs. When they are taken out 7 at a time, none are left over. Find the smallest number of eggs that could have been contained in the basket.

9. The basket-of-eggs problem is often phrased in the following form: One egg remains when the eggs are removed from the basket 2, 3, 4, 5, or 6 at a time; but, no eggs remain if they are removed 7 at a time. Find the smallest number of eggs that could have been in the basket.

10. (Ancient Chinese Problem.) A band of 17 pirates stole a sack of gold coins. When they tried to divide the fortune into equal portions, 3 coins remained. In the ensuing brawl over who should get the extra coins, one pirate was killed. The wealth was redistributed, but this time an equal division left 10 coins. Again an argument developed in which another pirate was killed. But now the total fortune was evenly distributed among the survivors. What was the least number of coins that could have been stolen?

11. Prove that the congruences

$$x \equiv a \pmod{n} \qquad \text{and} \qquad x \equiv b \pmod{m}$$

admit a simultaneous solution if and only if $\gcd(n, m) \mid a - b$; if a solution exists, confirm that it is unique modulo $\operatorname{lcm}(n, m)$.

12. Use Problem 11 to show that the following system does not possess a solution:

$$x \equiv 5 \pmod{6} \qquad \text{and} \qquad x \equiv 7 \pmod{15}$$

13. If $x \equiv a \pmod{n}$, prove that either $x \equiv a \pmod{2n}$ or $x \equiv a + n \pmod{2n}$.

14. A certain integer between 1 and 1200 leaves the remainders 1, 2, 6 when divided by 9, 11, 13, respectively. What is the integer?

15. (a) Find an integer having the remainders 1, 2, 5, 5 when divided by 2, 3, 6, 12, respectively. (Yih-hing, died 717).
(b) Find an integer having the remainders 2, 3, 4, 5 when divided by 3, 4, 5, 6, respectively. (Bhaskara, born 1114).
(c) Find an integer having the remainders 3, 11, 15 when divided by 10, 13, 17, respectively. (Regiomontanus, 1436–1476).

16. Let t_n denote the nth triangular number. For which values of n does t_n divide

$$t_1^2 + t_2^2 + \cdots + t_n^2$$

[*Hint:* Because $t_1^2 + t_2^2 + \cdots + t_n^2 = t_n(3n^3 + 12n^2 + 13n + 2)/30$, it suffices to determine those n satisfying $3n^3 + 12n^2 + 13n + 2 \equiv 0 \pmod{2 \cdot 3 \cdot 5}$.]

17. Find the solutions of the system of congruences:

$$3x + 4y \equiv 5 \pmod{13}$$
$$2x + 5y \equiv 7 \pmod{13}$$

18. Obtain the two incongruent solutions modulo 210 of the system

$$2x \equiv 3 \pmod{5}$$
$$4x \equiv 2 \pmod{6}$$
$$3x \equiv 2 \pmod{7}$$

19. Obtain the eight incongruent solutions of the linear congruence $3x + 4y \equiv 5 \pmod 8$

20. Find the solutions of each of the following systems of congruences:

(a) $5x + 3y \equiv 1 \pmod 7$

$3x + 2y \equiv 4 \pmod 7$.

(b) $7x + 3y \equiv 6 \pmod{11}$

$4x + 2y \equiv 9 \pmod{11}$.

(c) $11x + 5y \equiv 7 \pmod{20}$

$6x + 3y \equiv 8 \pmod{20}$.

CHAPTER 5

FERMAT'S THEOREM

And perhaps posterity will thank me for having shown it that the ancients did not know everything.
P. DE FERMAT

5.1 PIERRE DE FERMAT

What the ancient world had known was largely forgotten during the intellectual torpor of the Dark Ages, and it was only after the 12th century that Western Europe again became conscious of mathematics. The revival of classical scholarship was stimulated by Latin translations from the Greek and, more especially, from the Arabic. The Latinization of Arabic versions of Euclid's great treatise, the *Elements*, first appeared in 1120. The translation was not a faithful rendering of the *Elements*, having suffered successive, inaccurate translations from the Greek—first into Arabic, then into Castilian, and finally into Latin—done by copyists not versed in the content of the work. Nevertheless, this much-used copy, with its accumulation of errors, served as the foundation of all editions known in Europe until 1505, when the Greek text was recovered.

With the fall of Constantinople to the Turks in 1453, the Byzantine scholars who had served as the major custodians of mathematics brought the ancient masterpieces of Greek learning to the West. It is reported that a copy of what survived of Diophantus' *Arithmetica* was found in the Vatican library around 1462 by Johannes Müller (better known as Regiomontanus from the Latin name of his native town, Königsberg). Presumably, it had been brought to Rome by the refugees from Byzantium. Regiomontanus observed that "In these books the very flower of the

Pierre de Fermat
(1601–1665)

(*David Eugene Smith Collection, Rare Book and Manuscript Library, Columbia University*)

whole of arithmetic lies hid," and tried to interest others in translating it. Notwithstanding the attention that was called to the work, it remained practically a closed book until 1572 when the first translation and printed edition was brought out by the German professor Wilhelm Holzmann, who wrote under the Grecian form of his name, Xylander. The *Arithmetica* became fully accessible to European mathematicians when Claude Bachet—borrowing liberally from Xylander—published (1621) the original Greek text, along with a Latin translation containing notes and comments. The Bachet edition probably has the distinction of being the work that first directed the attention of Fermat to the problems of number theory.

Few if any periods were so fruitful for mathematics as was the 17th century; Northern Europe alone produced as many men of outstanding ability as had appeared during the preceding millennium. At a time when such names as Desargues, Descartes, Pascal, Wallis, Bernoulli, Leibniz, and Newton were becoming famous, a certain French civil servant, Pierre de Fermat (1601–1665), stood as an equal among these brilliant scholars. Fermat, the "Prince of Amateurs," was the last great mathematician to pursue the subject as a sideline to a nonscientific career. By profession a lawyer and magistrate attached to the provincial parliament at Toulouse, he sought refuge from controversy in the abstraction of mathematics. Fermat evidently had no particular mathematical training and he evidenced no interest in its study until he was past 30; to him, it was merely a hobby to be cultivated in leisure time. Yet no practitioner of his day made greater discoveries or contributed more to the advancement of the discipline: one of the inventors of analytic geometry (the actual term was coined in the early 19th century), he laid the technical foundations of differential and integral calculus and, with Pascal, established the conceptual guidelines of the theory of probability. Fermat's real love in mathematics was undoubtedly number theory, which he rescued from the realm of superstition and occultism where it had long been imprisoned. His contributions here overshadow all else; it may well be said that the revival of interest in the abstract side of number theory began with Fermat.

Fermat preferred the pleasure he derived from mathematical research itself to any reputation that it might bring him; indeed, he published only one major manuscript during his lifetime and that just 5 years before his death, using the concealing initials M.P.E.A.S. Adamantly refusing to put his work in finished form, he thwarted several efforts by others to make the results available in print under his name. In partial compensation for his lack of interest in publication, Fermat carried on a voluminous correspondence with contemporary mathematicians. Most of what little we know about his investigations is found in the letters to friends with whom he exchanged problems and to whom he reported his successes. They did their best to publicize Fermat's talents by passing these letters from hand to hand or by making copies, which were dispatched over the Continent.

As his parliamentary duties demanded an ever greater portion of his time, Fermat was given to inserting notes in the margin of whatever book he happened to be using. Fermat's personal copy of the Bachet edition of Diophantus held in its margin many of his famous theorems in number theory. These were discovered by his son Samuel 5 years after Fermat's death. His son brought out a new edition of the *Arithmetica* incorporating Fermat's celebrated marginalia. Because there was little space available, Fermat's habit had been to jot down some result and omit all steps leading to the conclusion. Posterity has wished many times that the margins of the *Arithmetica* had been wider or that Fermat had been a little less secretive about his methods.

5.2 FERMAT'S LITTLE THEOREM AND PSEUDOPRIMES

The most significant of Fermat's correspondents in number theory was Bernhard Frénicle de Bessy (1605–1675), an official at the French mint who was renowned for his gift of manipulating large numbers. (Frénicle's facility in numerical calculation is revealed by the following incident: On hearing that Fermat had proposed the problem of finding cubes that when increased by their proper divisors become squares, as is the case with $7^3 + (1 + 7 + 7^2) = 20^2$, he immediately gave four different solutions, and supplied six more the next day.) Though in no way Fermat's equal as a mathematician, Frénicle alone among his contemporaries could challenge Fermat in number theory and Frénicle's challenges had the distinction of coaxing out of Fermat some of his carefully guarded secrets. One of the most striking is the theorem that states: If p is a prime and a is any integer not divisible by p, then p divides $a^{p-1} - 1$. Fermat communicated the result in a letter to Frénicle dated October 18, 1640, along with the comment, "I would send you the demonstration, if I did not fear its being too long." This theorem has since become known as "Fermat's Little Theorem," or just "Fermat's Theorem," to distinguish it from Fermat's "Great" or "Last Theorem," which is the subject of Chapter 12. Almost 100 years were to elapse before Euler published the first proof of the little theorem in 1736. Leibniz, however, seems not to have received his share of recognition, for he left an identical argument in an unpublished manuscript sometime before 1683.

We now proceed to a proof of Fermat's theorem.

Theorem 5.1 Fermat's theorem. Let p be a prime and suppose that $p \nmid a$. Then $a^{p-1} \equiv 1 \pmod{p}$.

Proof. We begin by considering the first $p-1$ positive multiples of a; that is, the integers

$$a, 2a, 3a, \ldots, (p-1)a$$

None of these numbers is congruent modulo p to any other, nor is any congruent to zero. Indeed, if it happened that

$$ra \equiv sa \pmod{p} \qquad 1 \leq r < s \leq p-1$$

then a could be canceled to give $r \equiv s \pmod{p}$, which is impossible. Therefore, the previous set of integers must be congruent modulo p to $1, 2, 3, \ldots, p-1$, taken in some order. Multiplying all these congruences together, we find that

$$a \cdot 2a \cdot 3a \cdots (p-1)a \equiv 1 \cdot 2 \cdot 3 \cdots (p-1) \pmod{p}$$

whence

$$a^{p-1}(p-1)! \equiv (p-1)! \pmod{p}$$

Once $(p-1)!$ is canceled from both sides of the preceding congruence (this is possible because since $p \nmid (p-1)!$), our line of reasoning culminates in the statement that $a^{p-1} \equiv 1 \pmod{p}$, which is Fermat's theorem.

This result can be stated in a slightly more general way in which the requirement that $p \nmid a$ is dropped.

Corollary. If p is a prime, then $a^p \equiv a \pmod{p}$ for any integer a.

Proof. When $p \mid a$, the statement obviously holds; for, in this setting, $a^p \equiv 0 \equiv a \pmod{p}$. If $p \nmid a$, then according to Fermat's theorem, we have $a^{p-1} \equiv 1 \pmod{p}$. When this congruence is multiplied by a, the conclusion $a^p \equiv a \pmod{p}$ follows.

There is a different proof of the fact that $a^p \equiv a \pmod{p}$, involving induction on a. If $a = 1$, the assertion is that $1^p \equiv 1 \pmod{p}$, which clearly is true, as is the case $a = 0$. Assuming that the result holds for a, we must confirm its validity for $a+1$. In light of the binomial theorem,

$$(a+1)^p = a^p + \binom{p}{1} a^{p-1} + \cdots + \binom{p}{k} a^{p-k} + \cdots + \binom{p}{p-1} a + 1$$

where the coefficient $\binom{p}{k}$ is given by

$$\binom{p}{k} = \frac{p!}{k!(p-k)!} = \frac{p(p-1)\cdots(p-k+1)}{1 \cdot 2 \cdot 3 \cdots k}$$

Our argument hinges on the observation that $\binom{p}{k} \equiv 0 \pmod{p}$ for $1 \leq k \leq p-1$. To see this, note that

$$k! \binom{p}{k} = p(p-1)\cdots(p-k+1) \equiv 0 \pmod{p}$$

by virtue of which $p \mid k!$ or $p \mid \binom{p}{k}$. But $p \mid k!$ implies that $p \mid j$ for some j satisfying $1 \leq j \leq k \leq p-1$, an absurdity. Therefore, $p \mid \binom{p}{k}$ or, converting to a congruence statement,

$$\binom{p}{k} \equiv 0 \pmod{p}$$

The point we wish to make is that

$$(a+1)^p \equiv a^p + 1 \equiv a + 1 \pmod{p}$$

where the rightmost congruence uses our inductive assumption. Thus, the desired conclusion holds for $a+1$ and, in consequence, for all $a \geq 0$. If a happens to be a negative integer, there is no problem: because $a \equiv r \pmod{p}$ for some r, where $0 \leq r \leq p-1$, we get $a^p \equiv r^p \equiv r \equiv a \pmod{p}$.

Fermat's theorem has many applications and is central to much of what is done in number theory. In the least, it can be a labor-saving device in certain calculations. If asked to verify that $5^{38} \equiv 4 \pmod{11}$, for instance, we take the congruence $5^{10} \equiv 1 \pmod{11}$ as our starting point. Knowing this,

$$\begin{aligned} 5^{38} = 5^{10 \cdot 3 + 8} &= (5^{10})^3 (5^2)^4 \\ &\equiv 1^3 \cdot 3^4 \equiv 81 \equiv 4 \pmod{11} \end{aligned}$$

as desired.

Another use of Fermat's theorem is as a tool in testing the primality of a given integer n. If it could be shown that the congruence

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

fails to hold for some choice of a, then n is necessarily composite. As an example of this approach, let us look at $n = 117$. The computation is kept under control by selecting a small integer for a, say, $a = 2$. Because 2^{117} may be written as

$$2^{117} = 2^{7 \cdot 16 + 5} = (2^7)^{16} 2^5$$

and $2^7 = 128 \equiv 11 \pmod{117}$, we have

$$2^{117} \equiv 11^{16} \cdot 2^5 \equiv (121)^8 2^5 \equiv 4^8 \cdot 2^5 \equiv 2^{21} \pmod{117}$$

But $2^{21} = (2^7)^3$, which leads to

$$2^{21} \equiv 11^3 \equiv 121 \cdot 11 \equiv 4 \cdot 11 \equiv 44 \pmod{117}$$

Combining these congruences, we finally obtain

$$2^{117} \equiv 44 \not\equiv 2 \pmod{117}$$

so that 117 must be composite; actually, $117 = 13 \cdot 9$.

It might be worthwhile to give an example illustrating the failure of the converse of Fermat's theorem to hold, in other words, to show that if $a^{n-1} \equiv 1 \pmod{n}$ for some integer a, then n need not be prime. As a prelude we require a technical lemma.

Lemma. If p and q are distinct primes with $a^p \equiv a \pmod{q}$ and $a^q \equiv a \pmod{p}$, then $a^{pq} \equiv a \pmod{pq}$.

Proof. The last corollary tells us that $(a^q)^p \equiv a^q \pmod{p}$, whereas $a^q \equiv a \pmod{p}$ holds by hypothesis. Combining these congruences, we obtain $a^{pq} \equiv a \pmod{p}$ or, in different terms, $p \mid a^{pq} - a$. In an entirely similar manner, $q \mid a^{pq} - a$. Corollary 2 to Theorem 2.4 now yields $pq \mid a^{pq} - a$, which can be recast as $a^{pq} \equiv a \pmod{pq}$.

Our contention is that $2^{340} \equiv 1 \pmod{341}$, where $341 = 11 \cdot 31$. In working toward this end, notice that $2^{10} = 1024 = 31 \cdot 33 + 1$. Thus,

$$2^{11} = 2 \cdot 2^{10} \equiv 2 \cdot 1 \equiv 2 \pmod{31}$$

and

$$2^{31} = 2(2^{10})^3 \equiv 2 \cdot 1^3 \equiv 2 \pmod{11}$$

Exploiting the lemma,

$$2^{11 \cdot 31} \equiv 2 \pmod{11 \cdot 31}$$

or $2^{341} \equiv 2 \pmod{341}$. After canceling a factor of 2, we pass to

$$2^{340} \equiv 1 \pmod{341}$$

so that the converse to Fermat's theorem is false.

The historical interest in numbers of the form $2^n - 2$ resides in the claim made by Chinese mathematicians over 25 centuries ago that n is prime if and only if $n \mid 2^n - 2$ (in point of fact, this criterion is reliable for all integers $n \leq 340$). Our example, where $341 \mid 2^{341} - 2$, although $341 = 11 \cdot 31$, lays the conjecture to rest; this was discovered in the year 1819. The situation in which $n \mid 2^n - 2$ occurs often enough to merit a name, though: A composite integer n is called *pseudoprime* whenever $n \mid 2^n - 2$. It can be shown that there are infinitely many pseudoprimes, the smallest four being 341, 561, 645, and 1105.

Theorem 5.2 allows us to construct an increasing sequence of pseudoprimes.

Theorem 5.2. If n is an odd pseudoprime, then $M_n = 2^n - 1$ is a larger one.

Proof. Because n is a composite number, we can write $n = rs$, with $1 < r \leq s < n$. Then, according to Problem 21, Section 2.3, $2^r - 1 \mid 2^n - 1$, or equivalently $2^r - 1 \mid M_n$, making M_n composite. By our hypotheses, $2^n \equiv 2 \pmod{n}$; hence $2^n - 2 = kn$ for some integer k. It follows that

$$2^{M_n - 1} = 2^{2^n - 2} = 2^{kn}$$

This yields

$$\begin{aligned} 2^{M_n - 1} - 1 &= 2^{kn} - 1 \\ &= (2^n - 1)(2^{n(k-1)} + 2^{n(k-2)} + \cdots + 2^n + 1) \\ &= M_n(2^{n(k-1)} + 2^{n(k-2)} + \cdots + 2^n + 1) \\ &\equiv 0 \pmod{M_n} \end{aligned}$$

We see immediately that $2^{M_n} - 2 \equiv 0 \pmod{M_n}$, in light of which M_n is a pseudoprime.

More generally, a composite integer n for which $a^n \equiv a \pmod{n}$ is called a *pseudoprime to the base a*. (When $a = 2$, n is simply said to be a pseudoprime.) For instance, 91 is the smallest pseudoprime to base 3, whereas 217 is the smallest such to base 5. It has been proved (1903) that there are infinitely many pseudoprimes to any given base.

These "prime imposters" are much rarer than are actual primes. Indeed, there are only 245 pseudoprimes smaller than one million, in comparison with 78498 primes. The first example of an even pseudoprime, namely, the number

$$161038 = 2 \cdot 73 \cdot 1103$$

was found in 1950.

There exist composite numbers n that are pseudoprimes to every base a; that is, $a^n \equiv a \pmod{n}$ for all integers a. The least such is 561. These exceptional numbers are called *absolute pseudoprimes* or *Carmichael numbers*, for R. D. Carmichael, who was the first to notice their existence. In his first paper on the subject, published in 1910, Carmichael indicated four absolute pseudoprimes including the well-known $561 = 3 \cdot 11 \cdot 17$; the others are $1105 = 5 \cdot 13 \cdot 17, 2821 = 7 \cdot 13 \cdot 31$, and $15841 = 7 \cdot 31 \cdot 73$. Two years later he presented 11 more having three prime factors and discovered one absolute pseudoprime with four factors, specifically, $16046641 = 13 \cdot 37 \cdot 73 \cdot 457$. The largest number of this kind known to date is the product of 1101518 distinct odd primes: It has 16142049 digits.

To see that $561 = 3 \cdot 11 \cdot 17$ must be an absolute pseudoprime, notice that $\gcd(a, 561) = 1$ gives

$$\gcd(a, 3) = \gcd(a, 11) = \gcd(a, 17) = 1$$

An application of Fermat's theorem leads to the congruences

$$a^2 \equiv 1 \pmod{3} \qquad a^{10} \equiv 1 \pmod{11} \qquad a^{16} \equiv 1 \pmod{17}$$

and, in turn, to

$$\begin{aligned} a^{560} &\equiv (a^2)^{280} \equiv 1 \pmod{3} \\ a^{560} &\equiv (a^{10})^{56} \equiv 1 \pmod{11} \\ a^{560} &\equiv (a^{16})^{35} \equiv 1 \pmod{17} \end{aligned}$$

These give rise to the single congruence $a^{560} \equiv 1 \pmod{561}$, where $\gcd(a, 561) = 1$. But then $a^{561} \equiv a \pmod{561}$ for all a, showing 561 to be an absolute pseudoprime.

Any absolute pseudoprime is square-free. This is easy to prove. Suppose that $a^n \equiv a \pmod{n}$ for every integer a, but $k^2 \mid n$ for some $k > 1$. If we let $a = k$, then $k^n \equiv k \pmod{n}$. Because $k^2 \mid n$, this last congruence holds modulo k^2; that is, $k \equiv k^n \equiv 0 \pmod{k^2}$, whence $k^2 \mid k$, which is impossible. Thus, n must be square-free.

Next we present a theorem that furnishes a means for producing absolute pseudoprimes.

Theorem 5.3. Let n be a composite square-free integer, say, $n = p_1 p_2 \cdots p_r$, where the p_i are distinct primes. If $p_i - 1 \mid n - 1$ for $i = 1, 2, \ldots, r$, then n is an absolute pseudoprime.

Proof. Suppose that a is an integer satisfying $\gcd(a, n) = 1$, so that $\gcd(a, p_i) = 1$ for each i. Then Fermat's theorem yields $p_i \mid a^{p_i - 1} - 1$. From the divisibility hypothesis $p_i - 1 \mid n - 1$, we have $p_i \mid a^{n-1} - 1$, and therefore $p_i \mid a^n - a$ for all a and $i = 1, 2, \ldots, r$. As a result of Corollary 2 to Theorem 2.4, we end up with $n \mid a^n - a$, which makes n an absolute pseudoprime.

Examples of integers that satisfy the conditions of Theorem 5.3 are

$$1729 = 7 \cdot 13 \cdot 19 \qquad 6601 = 7 \cdot 23 \cdot 41 \qquad 10585 = 5 \cdot 29 \cdot 73$$

It was proven in 1994 that infinitely many absolute pseudoprimes exist, but that they are fairly rare. There are just 43 of them less than one million, and 105212 less than 10^{15}.

PROBLEMS 5.2

1. Use Fermat's theorem to verify that 17 divides $11^{104} + 1$.

2. (a) If $\gcd(a, 35) = 1$, show that $a^{12} \equiv 1 \pmod{35}$.
[*Hint:* From Fermat's theorem $a^6 \equiv 1 \pmod 7$ and $a^4 \equiv 1 \pmod 5$.]
(b) If $\gcd(a, 42) = 1$, show that $168 = 3 \cdot 7 \cdot 8$ divides $a^6 - 1$.
(c) If $\gcd(a, 133) = \gcd(b, 133) = 1$, show that $133 \mid a^{18} - b^{18}$.

3. From Fermat's theorem deduce that, for any integer $n \geq 0$, $13 \mid 11^{12n+6} + 1$.

4. Derive each of the following congruences:
(a) $a^{21} \equiv a \pmod{15}$ for all a.
[*Hint:* By Fermat's theorem, $a^5 \equiv a \pmod 5$.]
(b) $a^7 \equiv a \pmod{42}$ for all a.
(c) $a^{13} \equiv a \pmod{3 \cdot 7 \cdot 13}$ for all a.
(d) $a^9 \equiv a \pmod{30}$ for all a.

5. If $\gcd(a, 30) = 1$, show that 60 divides $a^4 + 59$.

6. (a) Find the units digit of 3^{100} by the use of Fermat's theorem.
(b) For any integer a, verify that a^5 and a have the same units digit.

7. If $7 \nmid a$, prove that either $a^3 + 1$ or $a^3 - 1$ is divisible by 7.

8. The three most recent appearances of Halley's comet were in the years 1835, 1910, and 1986; the next occurrence will be in 2061. Prove that

$$1835^{1910} + 1986^{2061} \equiv 0 \pmod 7$$

9. (a) Let p be a prime and $\gcd(a, p) = 1$. Use Fermat's theorem to verify that $x \equiv a^{p-2}b \pmod p$ is a solution of the linear congruence $ax \equiv b \pmod p$.
(b) By applying part (a), solve the congruences $2x \equiv 1 \pmod{31}$, $6x \equiv 5 \pmod{11}$, and $3x \equiv 17 \pmod{29}$.

10. Assuming that a and b are integers not divisible by the prime p, establish the following:
(a) If $a^p \equiv b^p \pmod p$, then $a \equiv b \pmod p$.
(b) If $a^p \equiv b^p \pmod p$, then $a^p \equiv b^p \pmod{p^2}$.
[*Hint:* By (a), $a = b + pk$ for some k, so that $a^p - b^p = (b + pk)^p - b^p$; now show that p^2 divides the latter expression.]

11. Employ Fermat's theorem to prove that, if p is an odd prime, then
(a) $1^{p-1} + 2^{p-1} + 3^{p-1} + \cdots + (p-1)^{p-1} \equiv -1 \pmod p$.
(b) $1^p + 2^p + 3^p + \cdots + (p-1)^p \equiv 0 \pmod p$.
[*Hint:* Recall the identity $1 + 2 + 3 + \cdots + (p-1) = p(p-1)/2$.]

12. Prove that if p is an odd prime and k is an integer satisfying $1 \leq k \leq p-1$, then the binomial coefficient

$$\binom{p-1}{k} \equiv (-1)^k \pmod{p}$$

13. Assume that p and q are distinct odd primes such that $p-1 \mid q-1$. If $\gcd(a, pq) = 1$, show that $a^{q-1} \equiv 1 \pmod{pq}$.

14. If p and q are distinct primes, prove that

$$p^{q-1} + q^{p-1} \equiv 1 \pmod{pq}$$

15. Establish the statements below:

(a) If the number $M_p = 2^p - 1$ is composite, where p is a prime, then M_p is a pseudoprime.

(b) Every composite number $F_n = 2^{2^n} + 1$ is a pseudoprime ($n = 0, 1, 2, \ldots$).
[*Hint:* By Problem 21, Section 2.3, $2^{n+1} \mid 2^{2^n}$ implies that $2^{2^{n+1}} - 1 \mid 2^{F_n - 1} - 1$; but $F_n \mid 2^{2^{n+1}} - 1$.]

16. Confirm that the following integers are absolute pseudoprimes:

(a) $1105 = 5 \cdot 13 \cdot 17$.

(b) $2821 = 7 \cdot 13 \cdot 31$.

(c) $2465 = 5 \cdot 17 \cdot 29$.

17. Show that the smallest pseudoprime 341 is not an absolute pseudoprime by showing that $11^{341} \not\equiv 11 \pmod{341}$.
[*Hint:* $31 \nmid 11^{341} - 11$.]

18. (a) When $n = 2p$, where p is an odd prime, prove that $a^{n-1} \equiv a \pmod{n}$ for any integer a.

(b) For $n = 195 = 3 \cdot 5 \cdot 13$, verify that $a^{n-2} \equiv a \pmod{n}$ for any integer a.

19. Prove that any integer of the form

$$n = (6k+1)(12k+1)(18k+1)$$

is an absolute pseudoprime if all three factors are prime; hence, $1729 = 7 \cdot 13 \cdot 19$ is an absolute pseudoprime.

20. Show that $561 \mid 2^{561} - 2$ and $561 \mid 3^{561} - 3$. It is an unanswered question whether there exist infinitely many composite numbers n with the property that $n \mid 2^n - 2$ and $n \mid 3^n - 3$.

21. Establish the congruence

$$2222^{5555} + 5555^{2222} \equiv 0 \pmod{7}$$

[*Hint:* First evaluate 1111 modulo 7.]

5.3 WILSON'S THEOREM

We now turn to another milestone in the development of number theory. In his *Meditationes Algebraicae* of 1770, the English mathematician Edward Waring (1734–1798) announced several new theorems. Foremost among these is an interesting property of primes reported to him by one of his former students, a certain John Wilson. The property is the following: If p is a prime number, then p divides $(p-1)! + 1$. Wilson appears to have guessed this on the basis of numerical computations; at any rate, neither he nor Waring knew how to prove it. Confessing his inability to supply a demonstration, Waring added, "Theorems of this kind will be

very hard to prove, because of the absence of a notation to express prime numbers." (Reading the passage, Gauss uttered his telling comment on "notationes versus notiones," implying that in questions of this nature it was the notion that really mattered, not the notation.) Despite Waring's pessimistic forecast, soon afterward Lagrange (1771) gave a proof of what in literature is called "Wilson's theorem" and observed that the converse also holds. Perhaps it would be more just to name the theorem after Leibniz, for there is evidence that he was aware of the result almost a century earlier, but published nothing on the subject.

Now we give a proof of Wilson's theorem.

Theorem 5.4 Wilson. If p is a prime, then $(p-1)! \equiv -1 \pmod{p}$.

Proof. Dismissing the cases $p = 2$ and $p = 3$ as being evident, let us take $p > 3$. Suppose that a is any one of the $p - 1$ positive integers

$$1, 2, 3, \ldots, p-1$$

and consider the linear congruence $ax \equiv 1 \pmod{p}$. Then $\gcd(a, p) = 1$. By Theorem 4.7, this congruence admits a unique solution modulo p; hence, there is a unique integer a', with $1 \leq a' \leq p-1$, satisfying $aa' \equiv 1 \pmod{p}$.

Because p is prime, $a = a'$ if and only if $a = 1$ or $a = p - 1$. Indeed, the congruence $a^2 \equiv 1 \pmod{p}$ is equivalent to $(a-1) \cdot (a+1) \equiv 0 \pmod{p}$. Therefore, either $a - 1 \equiv 0 \pmod{p}$, in which case $a = 1$, or $a + 1 \equiv 0 \pmod{p}$, in which case $a = p - 1$.

If we omit the numbers 1 and $p - 1$, the effect is to group the remaining integers $2, 3, \ldots, p-2$ into pairs a, a', where $a \neq a'$, such that their product $aa' \equiv 1 \pmod{p}$. When these $(p-3)/2$ congruences are multiplied together and the factors rearranged, we get

$$2 \cdot 3 \cdots (p-2) \equiv 1 \pmod{p}$$

or rather

$$(p-2)! \equiv 1 \pmod{p}$$

Now multiply by $p - 1$ to obtain the congruence

$$(p-1)! \equiv p - 1 \equiv -1 \pmod{p}$$

as was to be proved.

Example 5.1. A concrete example should help to clarify the proof of Wilson's theorem. Specifically, let us take $p = 13$. It is possible to divide the integers $2, 3, \ldots, 11$ into $(p-3)/2 = 5$ pairs, each product of which is congruent to 1 modulo 13. To write these congruences out explicitly:

$$2 \cdot 7 \equiv 1 \pmod{13}$$
$$3 \cdot 9 \equiv 1 \pmod{13}$$
$$4 \cdot 10 \equiv 1 \pmod{13}$$
$$5 \cdot 8 \equiv 1 \pmod{13}$$
$$6 \cdot 11 \equiv 1 \pmod{13}$$

Multiplying these congruences gives the result

$$11! = (2 \cdot 7)(3 \cdot 9)(4 \cdot 10)(5 \cdot 8)(6 \cdot 11) \equiv 1 \pmod{13}$$

and so

$$12! \equiv 12 \equiv -1 \pmod{13}$$

Thus, $(p-1)! \equiv -1 \pmod{p}$, with $p = 13$.

The converse of Wilson's theorem is also true. If $(n-1)! \equiv -1 \pmod{n}$, then n must be prime. For, if n is not a prime, then n has a divisor d with $1 < d < n$. Furthermore, because $d \leq n-1$, d occurs as one of the factors in $(n-1)!$, whence $d \mid (n-1)!$. Now we are assuming that $n \mid (n-1)! + 1$, and so $d \mid (n-1)! + 1$, too. The conclusion is that $d \mid 1$, which is nonsense.

Taken together, Wilson's theorem and its converse provide a necessary and sufficient condition for determining primality; namely, an integer $n > 1$ is prime if and only if $(n-1)! \equiv -1 \pmod{n}$. Unfortunately, this test is of more theoretical than practical interest because as n increases, $(n-1)!$ rapidly becomes unmanageable in size.

We would like to close this chapter with an application of Wilson's theorem to the study of quadratic congruences. [It is understood that *quadratic congruence* means a congruence of the form $ax^2 + bx + c \equiv 0 \pmod{n}$, with $a \not\equiv 0 \pmod{n}$.] This is the content of Theorem 5.5.

Theorem 5.5. The quadratic congruence $x^2 + 1 \equiv 0 \pmod{p}$, where p is an odd prime, has a solution if and only if $p \equiv 1 \pmod{4}$.

Proof. Let a be any solution of $x^2 + 1 \equiv 0 \pmod{p}$, so that $a^2 \equiv -1 \pmod{p}$. Because $p \nmid a$, the outcome of applying Fermat's theorem is

$$1 \equiv a^{p-1} \equiv (a^2)^{(p-1)/2} \equiv (-1)^{(p-1)/2} \pmod{p}$$

The possibility that $p = 4k + 3$ for some k does not arise. If it did, we would have

$$(-1)^{(p-1)/2} = (-1)^{2k+1} = -1$$

hence, $1 \equiv -1 \pmod{p}$. The net result of this is that $p \mid 2$, which is patently false. Therefore, p must be of the form $4k + 1$.

Now for the opposite direction. In the product

$$(p-1)! = 1 \cdot 2 \cdots \frac{p-1}{2} \cdot \frac{p+1}{2} \cdots (p-2)(p-1)$$

we have the congruences

$$\begin{aligned} p - 1 &\equiv -1 \pmod{p} \\ p - 2 &\equiv -2 \pmod{p} \\ &\vdots \\ \frac{p+1}{2} &\equiv -\frac{p-1}{2} \pmod{p} \end{aligned}$$

Rearranging the factors produces

$$(p-1)! \equiv 1 \cdot (-1) \cdot 2 \cdot (-2) \cdots \frac{p-1}{2} \cdot \left(-\frac{p-1}{2}\right) \pmod{p}$$

$$\equiv (-1)^{(p-1)/2} \left(1 \cdot 2 \cdots \frac{p-1}{2}\right)^2 \pmod{p}$$

because there are $(p-1)/2$ minus signs involved. It is at this point that Wilson's theorem can be brought to bear; for, $(p-1)! \equiv -1 \pmod{p}$, whence

$$-1 \equiv (-1)^{(p-1)/2} \left[\left(\frac{p-1}{2}\right)!\right]^2 \pmod{p}$$

If we assume that p is of the form $4k+1$, then $(-1)^{(p-1)/2} = 1$, leaving us with the congruence

$$-1 \equiv \left[\left(\frac{p-1}{2}\right)!\right]^2 \pmod{p}$$

The conclusion is that the integer $[(p-1)/2]!$ satisfies the quadratic congruence $x^2 + 1 \equiv 0 \pmod{p}$.

Let us take a look at an actual example, say, the case $p = 13$, which is a prime of the form $4k+1$. Here, we have $(p-1)/2 = 6$, and it is easy to see that

$$6! = 720 \equiv 5 \pmod{13}$$

and

$$5^2 + 1 = 26 \equiv 0 \pmod{13}$$

Thus, the assertion that $[((p-1)/2)!]^2 + 1 \equiv 0 \pmod{p}$ is correct for $p = 13$.

Wilson's theorem implies that there exists an infinitude of composite numbers of the form $n! + 1$. On the other hand, it is an open question whether $n! + 1$ is prime for infinitely many values of n. The only values of n in the range $1 \leq n \leq 100$ for which $n! + 1$ is known to be a prime number are $n = 1, 2, 3, 11, 27, 37, 41, 73$, and 77. Currently, the largest prime of the form $n! + 1$ is $6380! + 1$, discovered in 2000.

PROBLEMS 5.3

1. (a) Find the remainder when 15! is divided by 17.
   (b) Find the remainder when 2(26!) is divided by 29.
2. Determine whether 17 is a prime by deciding whether $16! \equiv -1 \pmod{17}$.
3. Arrange the integers $2, 3, 4, \ldots, 21$ in pairs a and b that satisfy $ab \equiv 1 \pmod{23}$.
4. Show that $18! \equiv -1 \pmod{437}$.
5. (a) Prove that an integer $n > 1$ is prime if and only if $(n-2)! \equiv 1 \pmod{n}$.
   (b) If n is a composite integer, show that $(n-1)! \equiv 0 \pmod{n}$, except when $n = 4$.
6. Given a prime number p, establish the congruence

$$(p-1)! \equiv p - 1 \pmod{1 + 2 + 3 + \cdots + (p-1)}$$

7. If p is a prime, prove that for any integer a,

$$p \mid a^p + (p-1)!a \qquad \text{and} \qquad p \mid (p-1)!a^p + a$$

[*Hint:* By Wilson's theorem, $a^p + (p-1)!a \equiv a^p - a \pmod{p}$.]

8. Find two odd primes $p \leq 13$ for which the congruence $(p-1)! \equiv -1 \pmod{p^2}$ holds.

9. Using Wilson's theorem, prove that for any odd prime p,

$$1^2 \cdot 3^2 \cdot 5^2 \cdots (p-2)^2 \equiv (-1)^{(p+1)/2} \pmod{p}$$

[*Hint:* Because $k \equiv -(p-k) \pmod{p}$, it follows that

$$2 \cdot 4 \cdot 6 \cdots (p-1) \equiv (-1)^{(p-1)/2} 1 \cdot 3 \cdot 5 \cdots (p-2) \pmod{p}.]$$

10. (a) For a prime p of the form $4k+3$, prove that either

$$\left(\frac{p-1}{2}\right)! \equiv 1 \pmod{p} \qquad \text{or} \qquad \left(\frac{p-1}{2}\right)! \equiv -1 \pmod{p}$$

hence, $[(p-1)/2]!$ satisfies the quadratic congruence $x^2 \equiv 1 \pmod{p}$.

(b) Use part (a) to show that if $p = 4k+3$ is prime, then the product of all the even integers less than p is congruent modulo p to either 1 or -1.
[*Hint:* Fermat's theorem implies that $2^{(p-1)/2} \equiv \pm 1 \pmod{p}$.]

11. Apply Theorem 5.5 to obtain two solutions to each of the quadratic congruences $x^2 \equiv -1 \pmod{29}$ and $x^2 \equiv -1 \pmod{37}$.

12. Show that if $p = 4k+3$ is prime and $a^2 + b^2 \equiv 0 \pmod{p}$, then $a \equiv b \equiv 0 \pmod{p}$.
[*Hint:* If $a \not\equiv 0 \pmod{p}$, then there exists an integer c such that $ac \equiv 1 \pmod{p}$; use this fact to contradict Theorem 5.5.]

13. Supply any missing details in the following proof of the irrationality of $\sqrt{2}$: Suppose $\sqrt{2} = a/b$, with $\gcd(a, b) = 1$. Then $a^2 = 2b^2$, so that $a^2 + b^2 = 3b^2$. But $3 \mid (a^2 + b^2)$ implies that $3 \mid a$ and $3 \mid b$, a contradiction.

14. Prove that the odd prime divisors of the integer $n^2 + 1$ are of the form $4k+1$.
[*Hint:* Theorem 5.5.]

15. Verify that $4(29!) + 5!$ is divisible by 31.

16. For a prime p and $0 \leq k \leq p-1$, show that $k!(p-k-1)! \equiv (-1)^{k+1} \pmod{p}$.

17. If p and q are distinct primes, prove that for any integer a,

$$pq \mid a^{pq} - a^p - a^q + a$$

18. Prove that if p and $p+2$ are a pair of twin primes, then

$$4((p-1)! + 1) + p \equiv 0 \pmod{p(p+2)}$$

5.4 THE FERMAT-KRAITCHIK FACTORIZATION METHOD

In a fragment of a letter, written in all probability to Father Marin Mersenne in 1643, Fermat described a technique of his for factoring large numbers. This represented the first real improvement over the classical method of attempting to find a factor of n by dividing by all primes not exceeding $\sqrt{n}$. Fermat's factorization scheme has at its heart the observation that the search for factors of an odd integer n (because powers of 2 are easily recognizable and may be removed at the outset, there is no loss in assuming that n is odd) is equivalent to obtaining integral solutions x and y of the equation

$$n = x^2 - y^2$$

If n is the difference of two squares, then it is apparent that n can be factored as

$$n = x^2 - y^2 = (x + y)(x - y)$$

Conversely, when n has the factorization $n = ab$, with $a \geq b \geq 1$, then we may write

$$n = \left(\frac{a+b}{2}\right)^2 - \left(\frac{a-b}{2}\right)^2$$

Moreover, because n is taken to be an odd integer, a and b are themselves odd; hence $(a + b)/2$ and $(a - b)/2$ will be nonnegative integers.

One begins the search for possible x and y satisfying the equation $n = x^2 - y^2$, or what is the same thing, the equation

$$x^2 - n = y^2$$

by first determining the smallest integer k for which $k^2 \geq n$. Now look successively at the numbers

$$k^2 - n, (k + 1)^2 - n, (k + 2)^2 - n, (k + 3)^2 - n, \ldots$$

until a value of $m \geq \sqrt{n}$ is found making $m^2 - n$ a square. The process cannot go on indefinitely, because we eventually arrive at

$$\left(\frac{n+1}{2}\right)^2 - n = \left(\frac{n-1}{2}\right)^2$$

the representation of n corresponding to the trivial factorization $n = n \cdot 1$. If this point is reached without a square difference having been discovered earlier, then n has no factors other than n and 1, in which case it is a prime.

Fermat used the procedure just described to factor

$$2027651281 = 44021 \cdot 46061$$

in only 11 steps, as compared with making 4580 divisions by the odd primes up to 44021. This was probably a favorable case devised on purpose to show the chief virtue of his method: It does not require one to know all the primes less than $\sqrt{n}$ to find factors of n.

Example 5.2. To illustrate the application of Fermat's method, let us factor the integer $n = 119143$. From a table of squares, we find that $345^2 < 119143 < 346^2$; thus it suffices to consider values of $k^2 - 119143$ for those k that satisfy the inequality $346 \leq k < (119143 + 1)/2 = 59572$. The calculations begin as follows:

$$346^2 - 119143 = 119716 - 119143 = 573$$
$$347^2 - 119143 = 120409 - 119143 = 1266$$
$$348^2 - 119143 = 121104 - 119143 = 1961$$
$$349^2 - 119143 = 121801 - 119143 = 2658$$
$$350^2 - 119143 = 122500 - 119143 = 3357$$
$$351^2 - 119143 = 123201 - 119143 = 4058$$
$$352^2 - 119143 = 123904 - 119143 = 4761 = 69^2$$

This last line exhibits the factorization

$$119143 = 352^2 - 69^2 = (352 + 69)(352 - 69) = 421 \cdot 283$$

the two factors themselves being prime. In only seven trials, we have obtained the prime factorization of the number 119143. Of course, one does not always fare so luckily; it may take many steps before a difference turns out to be a square.

Fermat's method is most effective when the two factors of n are of nearly the same magnitude, for in this case a suitable square will appear quickly. To illustrate, let us suppose that $n = 23449$ is to be factored. The smallest square exceeding n is 154^2, so that the sequence $k^2 - n$ starts with

$$154^2 - 23449 = 23716 - 23449 = 267$$
$$155^2 - 23449 = 24025 - 23449 = 576 = 24^2$$

Hence, factors of 23449 are

$$23449 = (155 + 24)(155 - 24) = 179 \cdot 131$$

When examining the differences $k^2 - n$ as possible squares, many values can be immediately excluded by inspection of the final digits. We know, for instance, that a square must end in one of the six digits 0, 1, 4, 5, 6, 9 (Problem 2(a), Section 4.3). This allows us to exclude all values in Example 5.2, save for 1266, 1961, and 4761. By calculating the squares of the integers from 0 to 99 modulo 100, we see further that, for a square, the last two digits are limited to the following 22 possibilities:

00	21	41	64	89
01	24	44	69	96
04	25	49	76	
09	29	56	81	
16	36	61	84	

The integer 1266 can be eliminated from consideration in this way. Because 61 is among the last two digits allowable in a square, it is only necessary to look at the numbers 1961 and 4761; the former is not a square, but $4761 = 69^2$.

There is a generalization of Fermat's factorization method that has been used with some success. Here, we look for distinct integers x and y such that $x^2 - y^2$ is a multiple of n rather than n itself; that is,

$$x^2 \equiv y^2 \pmod{n}$$

Having obtained such integers, $d = \gcd(x - y, n)$ (or $d = \gcd(x + y, n)$) can be calculated by means of the Euclidean Algorithm. Clearly, d is a divisor of n, but is it a nontrivial divisor? In other words, do we have $1 < d < n$?

In practice, n is usually the product of two primes p and q, with $p < q$, so that d is equal to 1, p, q, or pq. Now the congruence $x^2 \equiv y^2 \pmod{n}$ translates into $pq \mid (x - y)(x + y)$. Euclid's lemma tells us that p and q must divide one of the factors. If it happened that $p \mid x - y$ and $q \mid x - y$, then $pq \mid x - y$, or expressed as

a congruence $x \equiv y \pmod{n}$. Also, $p \mid x + y$ and $q \mid x + y$ yield $x \equiv -y \pmod{n}$. By seeking integers x and y satisfying $x^2 \equiv y^2 \pmod{n}$, where $x \not\equiv \pm y \pmod{n}$, these two situations are ruled out. The result of all this is that d is either p or q, giving us a nontrivial divisor of n.

Example 5.3. Suppose we wish to factor the positive integer $n = 2189$ and happen to notice that $579^2 \equiv 18^2 \pmod{2189}$. Then we compute

$$\gcd(579 - 18, 2189) = \gcd(561, 2189) = 11$$

using the Euclidean Algorithm:

$$\begin{aligned} 2189 &= 3 \cdot 561 + 506 \\ 561 &= 1 \cdot 506 + 55 \\ 506 &= 9 \cdot 55 + 11 \\ 55 &= 5 \cdot 11 \end{aligned}$$

This leads to the prime divisor 11 of 2189. The other factor, namely 199, can be obtained by observing that

$$\gcd(579 + 18, 2189) = \gcd(597, 2189) = 199$$

The reader might wonder how we ever arrived at a number, such as 579, whose square modulo 2189 also turns out to be a perfect square. In looking for squares close to multiples of 2189, it was observed that

$$81^2 - 3 \cdot 2189 = -6 \qquad \text{and} \qquad 155^2 - 11 \cdot 2189 = -54$$

which translates into

$$81^2 \equiv -2 \cdot 3 \pmod{2189} \qquad \text{and} \qquad 155^2 \equiv -2 \cdot 3^3 \pmod{2189}$$

When these congruences are multiplied, they produce

$$(81 \cdot 155)^2 \equiv (2 \cdot 3^2)^2 \pmod{2189}$$

Because the product $81 \cdot 155 = 12555 \equiv -579 \pmod{2189}$, we ended up with the congruence $579^2 \equiv 18^2 \pmod{2189}$.

The basis of our approach is to find several x_i having the property that each x_i^2 is, modulo n, the product of small prime powers, and such that their product's square is congruent to a perfect square.

When n has more than two prime factors, our factorization algorithm may still be applied; however, there is no guarantee that a particular solution of the congruence $x^2 \equiv y^2 \pmod{n}$, with $x \not\equiv \pm y \pmod{n}$, will result in a nontrivial divisor of n. Of course the more solutions of this congruence that are available, the better the chance of finding the desired factors of n.

Our next example provides a considerably more efficient variant of this last factorization method. It was introduced by Maurice Kraitchik in the 1920s and became the basis of such modern methods as the quadratic sieve algorithm.

Example 5.4. Let $n = 12499$ be the integer to be factored. The first square just larger than n is $112^2 = 12544$. So we begin by considering the sequence of numbers $x^2 - n$

for $x = 112, 113, \ldots$. As before, our interest is in obtaining a set of values x_1, $x_2, \ldots, x_k$ for which the product $(x_i - n) \cdots (x_k - n)$ is a square, say y^2. Then $(x_1 \cdots x_k)^2 \equiv y^2 \pmod{n}$, which might lead to a nontrivial factor of n.

A short search reveals that

$$112^2 - 12499 = 45$$

$$117^2 - 12499 = 1190$$

$$121^2 - 12499 = 2142$$

or, written as congruences,

$$112^2 \equiv 3^2 \cdot 5 \pmod{12499}$$

$$117^2 \equiv 2 \cdot 5 \cdot 7 \cdot 17 \pmod{12499}$$

$$121^2 \equiv 2 \cdot 3^2 \cdot 7 \cdot 17 \pmod{12499}$$

Multiplying these together results in the congruence

$$(112 \cdot 117 \cdot 121)^2 \equiv (2 \cdot 3^2 \cdot 5 \cdot 7 \cdot 17)^2 \pmod{12499}$$

that is,

$$1585584^2 \equiv 10710^2 \pmod{12499}$$

But we are unlucky with this square combination. Because

$$1585584 \equiv 10710 \pmod{12499}$$

only a trivial divisor of 12499 will be found. To be specific,

$$\gcd(1585584 + 10710, 12499) = 1$$

$$\gcd(1585584 - 10710, 12499) = 12499$$

After further calculation, we notice that

$$113^2 \equiv 2 \cdot 5 \cdot 3^3 \pmod{12499}$$

$$127^2 \equiv 2 \cdot 3 \cdot 5 \cdot 11^2 \pmod{12499}$$

which gives rise to the congruence

$$(113 \cdot 127)^2 \equiv (2 \cdot 3^2 \cdot 5 \cdot 11)^2 \pmod{12499}$$

This reduces modulo 12499 to

$$1852^2 \equiv 990^2 \pmod{12499}$$

and fortunately $1852 \not\equiv \pm 990 \pmod{12499}$. Calculating

$$\gcd(1852 - 990, 12499) = \gcd(862, 12499) = 431$$

produces the factorization $12499 = 29 \cdot 431$.

PROBLEMS 5.4

1. Use Fermat's method to factor each of the following numbers:
(a) 2279.
(b) 10541.
(c) 340663 [*Hint:* The smallest square just exceeding 340663 is 584^2.]

2. Prove that a perfect square must end in one of the following pairs of digits: 00, 01, 04, 09, 16, 21, 24, 25, 29, 36, 41, 44, 49, 56, 61, 64, 69, 76, 81, 84, 89, 96.
[*Hint:* Because $x^2 \equiv (50 + x)^2 \pmod{100}$ and $x^2 \equiv (50 - x)^2 \pmod{100}$, it suffices to examine the final digits of x^2 for the 26 values $x = 0, 1, 2, \ldots, 25$.]

3. Factor the number $2^{11} - 1$ by Fermat's factorization method.

4. In 1647, Mersenne noted that when a number can be written as a sum of two relatively prime squares in two distinct ways, it is composite and can be factored as follows: If $n = a^2 + b^2 = c^2 + d^2$, then

$$n = \frac{(ac + bd)(ac - bd)}{(a + d)(a - d)}$$

Use this result to factor the numbers

$$493 = 18^2 + 13^2 = 22^2 + 3^2$$

and

$$38025 = 168^2 + 99^2 = 156^2 + 117^2$$

5. Employ the generalized Fermat method to factor each of the following numbers:
(a) 2911 [*Hint:* $138^2 \equiv 67^2 \pmod{2911}$.]
(b) 4573 [*Hint:* $177^2 \equiv 92^2 \pmod{4573}$.]
(c) 6923 [*Hint:* $208^2 \equiv 93^2 \pmod{6923}$.]

6. Factor 13561 with the help of the congruences

$$233^2 \equiv 3^2 \cdot 5 \pmod{13561} \qquad \text{and} \qquad 1281^2 \equiv 2^4 \cdot 5 \pmod{13561}$$

7. (a) Factor the number 4537 by searching for x such that

$$x^2 - k \cdot 4537$$

is the product of small prime powers.
(b) Use the procedure indicated in part (a) to factor 14429.
[*Hint:* $120^2 - 14429 = -29$ and $3003^2 - 625 \cdot 14429 = -116$.]

8. Use Kraitchik's method to factor the number 20437.