CHAPTER 10

INTRODUCTION TO CRYPTOGRAPHY

I am fairly familiar with all forms of secret writings and am myself the author of a trifling manuscript on the subject.
SIR ARTHUR CONAN DOYLE

10.1 FROM CAESAR CIPHER TO PUBLIC KEY CRYPTOGRAPHY

Classically, the making and breaking of secret codes has usually been confined to diplomatic and military practices. With the growing quantity of digital data stored and communicated by electronic data-processing systems, organizations in both the public and commercial sectors have felt the need to protect information from unwanted intrusion. Indeed, the widespread use of electronic funds transfers has made privacy a pressing concern in most financial transactions. There thus has been a recent surge of interest by mathematicians and computer scientists in *cryptography* (from the Greek *kryptos* meaning *hidden* and *graphein* meaning *to write*), the science of making communications unintelligible to all except authorized parties. Cryptography is the only known practical means for protecting information transmitted through public communications networks, such as those using telephone lines, microwaves, or satellites.

In the language of cryptography, where codes are called *ciphers*, the information to be concealed is called *plaintext*. After transformation to a secret form, a message is called *ciphertext*. The process of converting from plaintext to ciphertext is said to be *encrypting* (or *enciphering*), whereas the reverse process of changing from ciphertext back to plaintext is called *decrypting* (or *deciphering*).

One of the earliest cryptographic systems was used by the great Roman emperor Julius Caesar around 50 B.C. Caesar wrote to Marcus Cicero using a rudimentary substitution cipher in which each letter of the alphabet is replaced by the letter that occurs three places down the alphabet, with the last three letters cycled back to the first three letters. If we write the ciphertext equivalent underneath the plaintext letter, the substitution alphabet for the *Caesar cipher* is given by

Plaintext: A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

Ciphertext: D E F G H I J K L M N O P Q R S T U V W X Y Z A B C

For example, the plaintext message

CAESAR WAS GREAT

is transformed into the ciphertext

FDHVDU ZDV JUHDW

The Caesar cipher can be described easily using congruence theory. Any plaintext is first expressed numerically by translating the characters of the text into digits by means of some correspondence such as the following:

A	B	C	D	E	F	G	H	I	J	K	L	M
00	01	02	03	04	05	06	07	08	09	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

If P is the digital equivalent of a plaintext letter and C is the digital equivalent of the corresponding ciphertext letter, then

$$C \equiv P + 3 \pmod{26}$$

Thus, for instance, the letters of the message in Eq. (1) are converted to their equivalents:

02 00 04 18 00 17 22 00 18 06 17 04 00 19

Using the congruence $C \equiv P + 3 \pmod{26}$, this becomes the ciphertext

05 03 07 21 03 20 25 03 21 09 20 07 03 22

To recover the plaintext, the procedure is simply reversed by means of the congruence

$$P \equiv C - 3 \equiv C + 23 \pmod{26}$$

The Caesar cipher is very simple and, hence, extremely insecure. Caesar himself soon abandoned this scheme—not only because of its insecurity, but also because he did not trust Cicero, with whom he necessarily shared the secret of the cipher.

An encryption scheme in which each letter of the original message is replaced by the same cipher substitute is known as a *monoalphabetic cipher*. Such cryptographic systems are extremely vulnerable to statistical methods of attack because they preserve the frequency, or relative commonness, of individual letters. In a *polyalphabetic cipher,* a plaintext letter has more than one ciphertext equivalent: the letter E, for instance, might be represented by J, Q, or X, depending on where it occurs in the message.

General fascination with cryptography had its initial impetus with the short story *The Gold Bug*, published in 1843 by the American writer Edgar Allan Poe. It is a fictional tale of the use of a table of letter frequencies to decipher directions for finding Captain Kidd's buried treasure. Poe fancied himself a cryptologist far beyond the ordinary. Writing for *Alexander's Weekly*, a Philadelphia newspaper, he once issued a claim that he could solve "forthwith" any monoalphabetic substitution cipher sent in by readers. The challenge was taken up by one G. W. Kulp, who submitted a 43-word ciphertext in longhand. Poe showed in a subsequent column that the entry was not genuine, but rather a "jargon of random characters having no meaning whatsoever." When Kulp's cipher submission was finally decoded in 1975, the reason for the difficulty became clear; the submission contained a major error on Kulp's part, along with 15 minor errors, which were most likely printer's mistakes in reading Kulp's longhand.

The most famous example of a polyalphabetic cipher was published by the French cryptographer Blaise de Vigenère (1523–1596) in his *Traicté de Chiffres* of 1586. To implement this system, the communicating parties agree on an easily remembered word or phrase. With the standard alphabet numbered from A = 00 to Z = 25, the digital equivalent of the keyword is repeated as many times as necessary beneath that of the plaintext message. The message is then enciphered by adding, modulo 26, each plaintext number to the one immediately beneath it. The process may be illustrated with the keyword READY, whose numerical version is 17 04 00 03 24. Repetitions of this sequence are arranged below the numerical plaintext of the message

ATTACK AT ONCE

to produce the array

00	19	19	00	02	10	00	19	14	13	02	04
17	04	00	03	24	17	04	00	03	24	17	04

When the columns are added modulo 26, the plaintext message is encrypted as

17	23	19	03	00	01	04	19	17	11	19	08

or, converted to letters,

RXTDAB ET RLTI

Notice that a given letter of plaintext is represented by different letters in ciphertext. The double T in the word ATTACK no longer appears as a double letter when ciphered, while the ciphertext letter R first corresponds to A and then to O in the original message.

In general, any sequence of n letters with numerical equivalents $b_1, b_2, \ldots, b_n$ ($00 \leq b_i \leq 25$) will serve as the keyword. The plaintext message is expressed as successive blocks $P_1 P_2 \cdots P_n$ of n two-digit integers P_i, and then converted to ciphertext blocks $C_1 C_2 \cdots C_n$ by means of the congruences

$$C_i \equiv P_i + b_i \pmod{26} \qquad 1 \leq i \leq n$$

Decryption is carried out by using the relations

$$P_i \equiv C_i - b_i \pmod{26} \qquad 1 \leq i \leq n$$

A weakness in Vigenère's approach is that once the length of the keyword has been determined, a coded message can be regarded as a number of separate monoalphabetic ciphers, each subject to straightforward frequency analysis. A variant to the continued repetition of the keyword is what is called a *running key*, a random assignment of ciphertext letters to plaintext letters. A favorite procedure for generating such keys is to use the text of a book, where both sender and recipient know the title of the book and the starting point of the appropriate lines. Because a running key cipher completely obscures the underlying structure of the original message, the system was long thought to be secure. But it does not, as *Scientific American* once claimed, produce ciphertext that is "impossible of translation."

A clever modification that Vigenère contrived for his polyalphabetic cipher is currently called the *autokey* ("automatic key"). This approach makes use of the plaintext message itself in constructing the encryption key. The idea is to start off the keyword with a short *seed* or *primer* (generally a single letter) followed by the plaintext, whose ending is truncated by the length of the seed. The autokey cipher enjoyed considerable popularity in the 16th and 17th centuries, since all it required of a legitimate pair of users was to remember the seed, which could easily be changed.

Let us give a simple example of the method.

Example 10.1. Assume that the message

ONE IF BY DAWN

is to be encrypted. Taking the letter K as the seed, the keyword becomes

KONEIFBYDAW

When both the plaintext and keyword are converted to numerical form, we obtain the array

14	13	04	08	05	01	24	03	00	22	13
10	14	13	04	08	05	01	24	03	00	22

Adding the integers in matching positions modulo 26 yields the ciphertext

24	01	17	12	13	06	25	01	03	22	09

or, changing back to letters:

YBR MN GZ BDWJ

Decipherment is achieved by returning to the numerical form of both the plaintext and its ciphertext. Suppose that the plaintext has digital equivalents $P_1 P_2 \ldots P_n$ and the ciphertext $C_1 C_2 \ldots C_n$. If S indicates the seed, then the first plaintext number is

$$P_1 = C_1 - S = 24 - 10 \equiv 14 \pmod{26}$$

Thus, the deciphering transformation becomes

$$P_k = C_k - P_{k-1} \pmod{26}, 2 \leq k \leq n$$

This recovers, for example, the integers

$$P_2 \equiv 01 - 14 = -13 \equiv 13 \pmod{26}$$

$$P_3 \equiv 17 - 13 \equiv 4 \pmod{26}$$

where, to maintain the two-digit format, the 4 is written 04.

A way to ensure greater security in alphabetic substitution ciphers was devised in 1929 by Lester Hill, an assistant professor of mathematics at Hunter College. Briefly, Hill's approach is to divide the plaintext message into blocks of n letters (possibly filling out the last block by adding "dummy" letters such as X's), and then to encrypt block by block using a system of n linear congruences in n variables. In its simplest form, when $n = 2$, the procedure takes two successive letters and transforms their numerical equivalents P_1P_2 into a block C_1C_2 of ciphertext numbers via the pair of congruences

$$C_1 \equiv aP_1 + bP_2 \pmod{26}$$

$$C_2 \equiv cP_1 + dP_2 \pmod{26}$$

To permit decipherment, the four coefficients a, b, c, d must be selected so the $\gcd(ad - bc, 26) = 1$.

Example 10.2. To illustrate Hill's cipher, let us use the congruences

$$C_1 \equiv 2P_1 + 3P_2 \pmod{26}$$

$$C_2 \equiv 5P_1 + 8P_2 \pmod{26}$$

to encrypt the message BUY NOW. The first block BU of two letters is numerically equivalent to 01 20. This is replaced by

$$2(01) + 3(20) \equiv 62 \equiv 10 \pmod{26}$$

$$5(01) + 8(20) \equiv 165 \equiv 09 \pmod{26}$$

Continuing two letters at a time, we find that the completed ciphertext is

$$10 \quad 09 \quad 09 \qquad 16 \quad 16 \quad 12$$

which can be expressed alphabetically as KJJ QQM.

Decipherment requires solving the original system of congruences for P_1 and P_2 in terms of C_1 and C_2. It follows from the proof of Theorem 4.9 that the plaintext block P_1P_2 can be recovered from the ciphertext block C_1C_2 by means of the congruences

$$P_1 \equiv 8C_1 - 3C_2 \pmod{26}$$

$$P_2 \equiv -5C_1 + 2C_2 \pmod{26}$$

For the block 10 09 of ciphertext, we calculate

$$P_1 \equiv 8(10) - 3(09) \equiv 53 \equiv 01 \pmod{26}$$

$$P_2 \equiv -5(10) + 2(09) \equiv -32 \equiv 20 \pmod{26}$$

which is the same as the letter-pair BU. The remaining plaintext can be restored in a similar manner.

An influential nonalphabetic cipher was devised by Gilbert S. Verman in 1917 while he was employed by the American Telephone and Telegraph Company (AT&T). Verman was interested in safeguarding information sent by the newly developed teletypewriter. At that time, wire messages were transmitted in the Baudot code, a code named after its French inventor J. M. E. Baudot. Baudot represented each letter of the alphabet by a five-element sequence of two symbols. If we take the two symbols to be 1 and 0, then the complete table is given by

A = 11000	J = 11010	S = 10100
B = 10011	K = 11110	T = 00001
C = 01110	L = 01001	U = 11100
D = 10010	M = 00111	V = 01111
E = 10000	N = 00110	W = 11001
F = 10110	O = 00011	X = 10111
G = 01011	P = 01101	Y = 10101
H = 00101	Q = 11101	Z = 10001
I = 01100	R = 01010	

Any plaintext message such as

ACT NOW

would first be transformed into a sequence of binary digits:

1100001110000010011000011110 01

Verman's innovation was to take as the encryption key an arbitrary sequence of 1's and 0's with length the same as that of the numerical plaintext. A typical key might appear as

1010010111001000100011110 01011

where the digits could be chosen by flipping a coin with heads as 1 and tails as 0. Finally, the ciphertext is formed by adding modulo 2 the digits in equivalent places in the two binary strings. The result in this instance becomes

0110011001001010111011111 10010

A crucial point is that the intended recipient must possess in advance the encryption key, for then the numerical plaintext can be reconstructed by merely adding modulo 2 corresponding digits of the encryption key and ciphertext.

In the early applications of Verman's telegraph cipher, the keys were written on numbered sheets of paper and then bound into pads held by both correspondents. A sheet was torn out and destroyed after its key had been used just once. For this reason, the Verman enciphering procedure soon became known as the one-time system or one-time pad. The cryptographic strength of Verman's method of enciphering resided in the possibly extreme length of the encryption key and the absence of any pattern within its entries. This assured security that was attractive to the military or

diplomatic services of many countries. In 1963, for instance, a teleprinter hot line was established between Washington and Moscow using a one-time tape.

In conventional cryptographic systems, such as Caesar's cipher, the sender and receiver jointly have a secret *key*. The sender uses the key to encrypt the plaintext to be sent, and the receiver uses the same key to decrypt the ciphertext obtained. Public-key cryptography differs from conventional cryptography in that it uses two keys, an encryption key and a decryption key. Although the two keys effect inverse operations and are therefore related, there is no easily computed method of deriving the decryption key from the encryption key. Thus, the encryption key can be made public without compromising the decryption key; each user can encrypt messages, but only the intended recipient (whose decryption key is kept secret) can decipher them. A major advantage of a public-key cryptosystem is that it is unnecessary for senders and receivers to exchange a key in advance of their decision to communicate with each other.

In 1977, R. Rivest, A. Shamir, and L. Adleman proposed a public-key cryptosystem that uses only elementary ideas from number theory. Their enciphering system is called *RSA*, after the initials of the algorithm's inventors. Its security depends on the assumption that in the current state of computer technology, the factorization of composite numbers with large prime factors is prohibitively time-consuming.

Each user of the RSA system chooses a pair of distinct primes, p and q, large enough that the factorization of their product $n = pq$, called the *enciphering modulus*, is beyond all current computational capabilities. For instance, one might pick p and q with 200 digits each, so that n has roughly 400 digits. Having selected n, the user then chooses a random positive integer k, the *enciphering exponent*, satisfying $\gcd(k, \phi(n)) = 1$. The pair (n, k) is placed in a public file, analogous to a telephone directory, as the user's personal encryption key. This allows anyone else in the communication network to encrypt and send a message to that individual. Notice that whereas n is openly revealed, the listed public key does not mention the factors p and q of n.

The encryption process begins with the conversion of the message to be sent into an integer M by means of a "digital alphabet" in which each letter, number, or punctuation mark of the plaintext is replaced by a two-digit integer. One standard procedure is to use the following assignment:

A = 00	K = 10	U = 20	1 = 30
B = 01	L = 11	V = 21	2 = 31
C = 02	M = 12	W = 22	3 = 32
D = 03	N = 13	X = 23	4 = 33
E = 04	O = 14	Y = 24	5 = 34
F = 05	P = 15	Z = 25	6 = 35
G = 06	Q = 16	, = 26	7 = 36
H = 07	R = 17	. = 27	8 = 37
I = 08	S = 18	? = 28	9 = 38
J = 09	T = 19	0 = 29	! = 39

with 99 indicating a space between words. In this scheme, the message

The brown fox is quick

is transformed into the numerical string

$$M = 19070499011714221399051423990818991620080210 27$$

It is assumed that the plaintext number $M < n$, where n is the enciphering modulus. Otherwise it would be impossible to distinguish M from any larger integer congruent to it modulo n. When the message is too long to be handled as a single number $M < n$, then M is broken up into blocks of digits $M_1, M_2, \ldots, M_s$ of the appropriate size. Each block is encrypted separately.

Looking up the intended recipient's encryption key (n, k) in the public directory, the sender disguises the plaintext number M as a ciphertext number r by raising M to the kth power and then reducing the result modulo n; that is,

$$M^k \equiv r \pmod{n}$$

A 200-character message can be encrypted in seconds on a high-speed computer. Recall that the public enciphering exponent k was originally selected so that $\gcd(k, \phi(n)) = 1$. Although there are many suitable choices for k, an obvious suggestion is to pick k to be any prime larger than both p and q.

At the other end, the authorized recipient deciphers the transmitted information by first determining the integer j, the secret *recovery exponent*, for which

$$kj \equiv 1 \pmod{\phi(n)}$$

Because $\gcd(k, \phi(n)) = 1$, this linear congruence has a unique solution modulo $\phi(n)$. In fact, the Euclidean algorithm produces j as a solution x to the equation

$$kx + \phi(n)y = 1$$

The recovery exponent can only be calculated by someone who knows both k and $\phi(n) = (p-1)(q-1)$ and, hence, knows the prime factors p and q of n. Thus, j is secure from an illegitimate third party whose knowledge is limited to the public key (n, k).

Matters have been arranged so that the recipient can now retrieve M from r by simply calculating r^j modulo n. Because $kj = 1 + \phi(n)t$ for some integer t, it follows that

$$\begin{aligned} r^j &\equiv (M^k)^j \equiv M^{1+\phi(n)t} \\ &\equiv M(M^{\phi(n)})^t \equiv M \cdot 1^t \equiv M \pmod{n} \end{aligned}$$

whenever $\gcd(M, n) = 1$. In other words, raising the ciphertext number to the jth power and reducing it modulo n recovers the original plaintext number M.

The assumption that $\gcd(M, n) = 1$ was made to use Euler's theorem. In the unlikely event that M and n are not relatively prime, a similar argument establishes that $r^j \equiv M \pmod{p}$ and $r^j \equiv M \pmod{q}$, which then yields the desired congruence $r^j \equiv M \pmod{n}$. We omit the details.

The major advantage of this ingenious procedure is that the encryption of a message does not require the knowledge of the two primes p and q, but only their

product n; there is no need for anyone other than the receiver of the message ever to know the prime factors critical to the decryption process.

Example 10.3. For the reader to gain familiarity with the RSA public-key algorithm, let us work an example in detail. We first select two primes

$$p = 29 \qquad q = 53$$

of an unrealistically small size, to get an easy-to-handle illustration. In practice, p and q would be large enough so that the factorization of the nonsecret $n = pq$ is not feasible. Our enciphering modulus is $n = 29 \cdot 53 = 1537$ and $\phi(n) = 28 \cdot 52 = 1456$. Because $\gcd(47, 1456) = 1$, we may choose $k = 47$ to be the enciphering exponent. Then the recovery exponent, the unique integer j satisfying the congruence $kj \equiv 1 \pmod{\phi(n)}$, is $j = 31$. To encrypt the message

NO WAY

first translate each letter into its digital equivalent using the substitution mentioned earlier; this yields the plaintext number

$$M = 131499220024$$

We want each plaintext block to be an integer less than 1537. Given this restriction, it seems reasonable to split M into blocks of three digits each. The first block, 131, encrypts as the ciphertext number

$$131^{47} \equiv 570 \pmod{1537}$$

These are the first digits of the secret transmission. At the other end, knowing that the recovery exponent is $j = 31$, the authorized recipient begins to recover the plaintext number by computing

$$570^{31} \equiv 131 \pmod{1537}$$

The total ciphertext of our message is

0570 1222 0708 1341

For the RSA cryptosystem to be secure it must not be computationally feasible to recover the plaintext M from the information assumed to be known to a third party, namely, the listed public-key (n, k). The direct method of attack would be to attempt to factor n, an integer of huge magnitude; for once the factors are determined, the recovery exponent j can be calculated from $\phi(n) = (p-1)(q-1)$ and k. Our confidence in the RSA system rests on what is known as the work factor, the expected amount of computer time needed to factor the product of two large primes. Factoring is computationally more difficult than distinguishing between primes and composites. On today's fastest computers, a 200-digit number can routinely be tested for primality in less than 20 seconds, whereas the running time required to factor a composite number of the same size is prohibitive. It has been estimated that the quickest factoring algorithm known can use approximately $(1.2)10^{23}$ computer operations to resolve an integer with 200 digits into its prime factors; assuming that each operation takes 1 nanosecond (10^{-9} seconds), the factorization time would be about $(3.8)10^6$ years. Given unlimited computing time and some unimaginably efficient factoring algorithm, the RSA cryptosystem could be broken, but for the present it

appears to be quite safe. All we need do is choose larger primes p and q for the enciphering moduli, always staying ahead of the current state of the art in factoring integers.

A greater threat is posed by the use of widely distributed networks of computers, working simultaneously on pieces of data necessary for a factorization and communicating their results to a central site. This is seen in the factoring of RSA-129, one of the most famous problems in cryptography.

To demonstrate that their cryptosystem could withstand any attack on its security, the three inventors submitted a ciphertext message to *Scientific American*, with an offer of $100 to anyone who could decode it. The message depended on a 129-digit enciphering modulus that was the product of two primes of approximately the same length. This large number acquired the name RSA-129. Taking into account the most powerful factoring methods and fastest computers available at the time, it was estimated that at least 40 quadrillion years would be required to break down RSA-129 and decipher the message. However, by devoting enough computing power to the task the factorization was realized in 1994. A worldwide network of some 600 volunteers participated in the project, running more than 1600 computers over an 8-month period. What seemed utterly beyond reach in 1977 was accomplished a mere 17 years later. The plaintext message is the sentence

"The magic words are squeamish ossifrage."

(An ossifrage, by the way, is a kind of hawk.)

Drawn up in 1991, the 42 numbers in the RSA Challenge List serve as something of a test for recent advances in factorization methods. The latest factoring success showed that the 174-digit number (576 binary digits) RSA-576 could be written as the product of two primes having 87 digits each.

PROBLEMS 10.1

1. Encrypt the message *RETURN HOME* using the Caesar cipher.
2. If the Caesar cipher produced *KDSSB ELUWKGDB*, what is the plaintext message?
3. (a) A linear cipher is defined by the congruence $C \equiv aP + b \pmod{26}$, where a and b are integers with $\gcd(a, 26) = 1$. Show that the corresponding decrypting congruence is $P \equiv a'(C - b) \pmod{26}$, where the integer a' satisfies $aa' \equiv 1 \pmod{26}$.
   (b) Using the linear cipher $C \equiv 5P + 11 \pmod{26}$, encrypt the message *NUMBER THEORY IS EASY*.
   (c) Decrypt the message *RXQTGU HOZTKGH FJ KTMMTG*, which was produced using the linear cipher $C \equiv 3P + 7 \pmod{26}$.
4. In a lengthy ciphertext message, sent using a linear cipher $C \equiv aP + b \pmod{26}$, the most frequently occurring letter is Q and the second most frequent is J.
   (a) Break the cipher by determining the values of a and b.
   [*Hint:* The most often used letter in English text is E, followed by T.]
   (b) Write out the plaintext for the intercepted message *WCPQ JZQO MX*.
5. (a) Encipher the message *HAVE A NICE TRIP* using a Vigenère cipher with the keyword *MATH*.
   (b) The ciphertext *BS FMX KFSGR JAPWL* is known to have resulted from a Vigenère cipher whose keyword is *YES*. Obtain the deciphering congruences and read the message.

6. (a) Encipher the message HAPPY DAYS ARE HERE using the autokey cipher with seed Q.
(b) Decipher the message BBOT XWBZ AWUVGK, which was produced by the autokey cipher with seed RX.

7. (a) Use the Hill cipher

$$C_1 \equiv 5P_1 + 2P_2 \pmod{26}$$

$$C_2 \equiv 3P_1 + 4P_2 \pmod{26}$$

to encipher the message *GIVE THEM TIME.*
(b) The ciphertext *ALXWU VADCOJO* has been enciphered with the cipher

$$C_1 \equiv 4P_1 + 11P_2 \pmod{26}$$

$$C_2 \equiv 3P_1 + 8P_2 \pmod{26}$$

Derive the plaintext.

8. A long string of ciphertext resulting from a Hill cipher

$$C_1 \equiv aP_1 + bP_2 \pmod{26}$$

$$C_2 \equiv cP_1 + dP_2 \pmod{26}$$

revealed that the most frequently occurring two-letter blocks were *HO* and *PP*, in that order.
(a) Find the values of a, b, c, and d.
[*Hint:* The most common two-letter blocks in the English language are *TH*, followed by *HE*.]
(b) What is the plaintext for the intercepted message *PPIH HOG RAPVT?*

9. Suppose that the message GO SOX is to be enciphered using Verman's telegraph cipher.
(a) Express the message in Baudot code.
(b) If the enciphering key is

$$01110101111010101001100 10$$

obtain the alphabetic form of the ciphertext.

10. A plaintext message expressed in Baudot code has been converted by the Verman cipher into the string

$$11000111000011101010010 1111111$$

If it is known that the key used for encipherment was

$$01110101100101111000100 1101010$$

recover the message in its alphabetic form.

11. If $n = pq = 274279$ and $\phi(n) = 272376$, find the primes p and q.
[*Hint*: Note that

$$p + q = n - \phi(n) + 1$$

$$p - q = [(p+q)^2 - 4n]^{1/2}.]$$

12. When the RSA algorithm is based on the key $(n, k) = (3233, 37)$, what is the recovery exponent for the cryptosystem?

13. Encrypt the plaintext message *GOLD MEDAL* using the RSA algorithm with key $(n, k) = (2419, 3)$.

14. The ciphertext message produced by the RSA algorithim with key $(n, k) = (1643, 223)$ is

$$0833 \quad 0823 \quad 1130 \quad 0055 \quad 0329 \quad 1099$$

Determine the original plaintext message.
[*Hint:* The recovery exponent is $j = 7$.]

15. Decrypt the ciphertext

$$1369 \quad 1436 \quad 0119 \quad 0385 \quad 0434 \quad 1580 \quad 0690$$

that was encrypted using the RSA algorithm with key $(n, k) = (2419, 211)$.
[*Hint:* The recovery exponent is 11. Note that it may be necessary to fill out a plaintext block by adding zeros on the left.]

10.2 THE KNAPSACK CRYPTOSYSTEM

A public-key cryptosystem also can be based on the classic problem in combinatorics known as the *knapsack problem*, or the subset sum problem. This problem may be stated as follows: Given a knapsack of volume V and n items of various volumes $a_1, a_2, \ldots, a_n$, can a subset of these items be found that will completely fill the knapsack? There is an alternative formulation: For positive integers $a_1, a_2, \ldots, a_n$ and a sum V, solve the equation

$$V = a_1x_2 + a_2x_2 + \cdots + a_nx_n$$

where $x_i = 0$ or 1 for $i = 1, 2, \ldots, n$.

There might be no solution, or more than one solution, to the problem, depending on the choice of the sequence $a_1, a_2, \ldots, a_n$ and the integer V. For instance, the knapsack problem

$$22 = 3x_1 + 7x_2 + 9x_3 + 11x_4 + 20x_5$$

is not solvable; but

$$27 = 3x_1 + 7x_2 + 9x_3 + 11x_4 + 20x_5$$

has two distinct solutions, namely

$$x_2 = x_3 = x_4 = 1 \qquad x_1 = x_5 = 0$$

and

$$x_2 = x_5 = 1 \qquad x_1 = x_3 = x_4 = 0$$

Finding a solution to a randomly chosen knapsack problem is notoriously difficult. None of the known methods for attacking the problem are substantially less time-consuming than is conducting an exhaustive direct search, that is, by testing all the 2^n possibilities for $x_1, x_2, \ldots, x_n$. This is computationally impracticable for n greater than 100, or so.

However, if the sequence of integers $a_1, a_2, \ldots, a_n$ happens to have some special properties, the knapsack problem becomes much easier to solve. We call a sequence

$a_1, a_2, \ldots, a_n$ *superincreasing* when each a_i is larger than the sum of all the preceding ones; that is,

$$a_i > a_1 + a_2 + \cdots + a_{i-1} \qquad i = 2, 3, \ldots, n$$

A simple illustration of a superincreasing sequence is 1, 2, 4, 8, ..., 2^n, where $2^i > 2^i - 1 = 1 + 2 + 4 + \cdots + 2^{i-1}$. For the corresponding knapsack problem,

$$V = x_1 + 2x_2 + 4x_3 + \cdots + 2^n x_n \qquad V < 2^{n+1}$$

the unknowns x_i are just the digits in the binary expansion of V.

Knapsack problems based on superincreasing sequences are uniquely solvable whenever they are solvable at all, as our next example shows.

Example 10.4. Let us solve the superincreasing knapsack problem

$$28 = 3x_1 + 5x_2 + 11x_3 + 20x_4 + 41x_5$$

We start with the largest coefficient in this equation, namely 41. Because $41 > 28$, it cannot be part of our subset sum; hence $x_5 = 0$. The next-largest coefficient is 20, with $20 < 28$. Now the sum of the preceding coefficients is $3 + 5 + 11 < 28$, so that these cannot fill the knapsack; therefore 20 must be included in the sum, and so $x_4 = 1$. Knowing the values of x_4 and x_5, the original problem may be rewritten as

$$8 = 3x_1 + 5x_2 + 11x_3$$

A repetition of our earlier reasoning now determines whether 11 should be in our knapsack sum. In fact, the inequality $11 > 8$ forces us to take $x_3 = 0$. To clinch matters, we are reduced to solving the equation $8 = 3x_1 + 5x_2$, which has the obvious solution $x_1 = x_2 = 1$. This identifies a subset of 3, 5, 11, 20, 41 having the desired sum:

$$28 = 3 + 5 + 20$$

It is not difficult to see how the procedure described in Example 10.4 operates, in general. Suppose that we wish to solve the knapsack problem

$$V = a_1x_1 + a_2x_2 + \cdots + a_nx_n$$

where $a_1, a_2, \ldots, a_n$ is a superincreasing sequence of integers. Assume that V can be obtained by using some subset of the sequence, so that V is not larger than the sum $a_1 + a_2 + \cdots + a_n$. Working from right to left in our sequence, we begin by letting $x_n = 1$ if $V \geq a_n$ and $x_n = 0$ if $V < a_n$. Then obtain $x_{n-1}, x_{n-2}, \ldots, x_1$, in turn, by choosing

$$x_i = \begin{cases} 1 & \text{if } V - (a_{i+1}x_{i+1} + \cdots + a_nx_n) \geq a_i \\ 0 & \text{if } V - (a_{i+1}x_{i+1} + \cdots + a_nx_n) < a_i \end{cases}$$

With this algorithm, knapsack problems using superincreasing sequences can be solved quite readily.

A public-key cryptosystem based on the knapsack problem was devised by R. Merkle and M. Hellman in 1978. It works as follows. A typical user of the system starts by choosing a superincreasing sequence $a_1, a_2, \ldots, a_n$. Now select a modulus $m > 2a_n$ and a multiplier a, with $0 < a < m$ and $\gcd(a, m) = 1$. This ensures that

the congruence $ax \equiv 1 \pmod{m}$ has a unique solution, say, $x \equiv c \pmod{m}$. Finally, form the sequence of integers $b_1, b_2, \ldots, b_n$ defined by

$$b_i \equiv aa_i \pmod{m} \qquad i = 1, 2, \ldots, n$$

where $0 < b_i < m$. Carrying out this last transformation generally destroys the superincreasing property enjoyed by the a_i.

The user keeps secret the original sequence $a_1, a_2, \ldots, a_n$, and the numbers m and a, but publishes $b_1, b_2, \ldots, b_n$ in a public directory. Anyone wishing to send a message to the user employs the publicly available sequence as the encryption key.

The sender begins by converting the plaintext message into a string M of 0's and 1's using the binary equivalent of letters:

Letter	Binary equivalent	Letter	Binary equivalent
A	00000	N	01101
B	00001	O	01110
C	00010	P	01111
D	00011	Q	10000
E	00100	R	10001
F	00101	S	10010
G	00110	T	10011
H	00111	U	10100
I	01000	V	10101
J	01001	W	10110
K	01010	X	10111
L	01011	Y	11000
M	01100	Z	11001

For example, the message

First Place

would be converted into the numerical representation

$$M = 00101\ \ 01000\ \ 10001\ \ 10010\ \ 10011\ \ 01111\ \ 01011\ \ 00000$$
$$00010\ \ 00100$$

The string is then split into blocks of n binary digits, with the last block being filled out with 1's at the end, if necessary. The public encrypting sequence $b_1, b_2, \ldots, b_n$ is next used to transform a given plaintext block, say $x_1x_2 \cdots x_n$, into the sum

$$S = b_1x_1 + b_2x_2 + \cdots + b_nx_n$$

The number S is the hidden information that the sender transmits over a communication channel, which is presumed to be insecure.

Notice that because each x_i is either 0 or 1, the problem of recreating the plaintext block from S is equivalent to solving an apparently difficult knapsack problem ("difficult" because the sequence $b_1, b_2, \ldots, b_n$ is not necessarily superincreasing). On first impression, the intended recipient and any eavesdropper are faced with the same task. However, with the aid of the private decryption key, the recipient can change the difficult knapsack problem into an easy one. No one without the private key can make this change.

Knowing c and m, the recipient computes

$$S' \equiv cS \pmod{m} \qquad 0 \leq S' < m$$

or, expanding this,

$$\begin{aligned} S' &\equiv cb_1x_1 + cb_2x_2 + \cdots + cb_nx_n \pmod{m} \\ &\equiv caa_1x_1 + caa_2x_2 + \cdots + caa_nx_n \pmod{m} \end{aligned}$$

Now $ca \equiv 1 \pmod{m}$, so that the previous congruence becomes

$$S' \equiv a_1x_1 + a_2x_2 + \cdots + a_nx_n \pmod{m}$$

Because m was initially chosen to satisfy $m > 2a_n > a_1 + a_2 + \cdots + a_n$, we obtain $a_1x_1 + a_2x_2 + \cdots + a_nx_n < m$. In light of the condition $0 \leq S' < m$, the equality

$$S' = a_1x_1 + a_2x_2 + \cdots + a_nx_n$$

must hold. The solution to this superincreasing knapsack problem furnishes the solution to the difficult problem, and the plaintext block $x_1x_2 \cdots x_n$ of n digits is thereby recovered from S.

To help make the technique clearer, we consider a small-scale example with $n = 5$.

Example 10.5. Suppose that a typical user of this cryptosystem selects as a secret key the superincreasing sequence 3, 5, 11, 20, 41, the modulus $m = 85$, and the multiplier $a = 44$. Each member of the superincreasing sequence is multiplied by 44 and reduced modulo 85 to yield 47, 50, 59, 30, 19. This is the encryption key that the user submits to the public directory.

Someone who wants to send a plaintext message to the user, such as

HELP US

first converts it into the following string of 0's and 1's:

$$M = 00111 \quad 00100 \quad 01011 \quad 01111 \quad 10100 \quad 10010$$

The string is then broken up into blocks of digits, in the current case blocks of length 5. Using the listed public key to encrypt, the sender transforms the successive blocks into

$$\begin{aligned} 108 &= 47 \cdot 0 + 50 \cdot 0 + 59 \cdot 1 + 30 \cdot 1 + 19 \cdot 1 \\ 59 &= 47 \cdot 0 + 50 \cdot 0 + 59 \cdot 1 + 30 \cdot 0 + 19 \cdot 0 \\ 99 &= 47 \cdot 0 + 50 \cdot 1 + 59 \cdot 0 + 30 \cdot 1 + 19 \cdot 1 \\ 158 &= 47 \cdot 0 + 50 \cdot 1 + 59 \cdot 1 + 30 \cdot 1 + 19 \cdot 1 \\ 106 &= 47 \cdot 1 + 50 \cdot 0 + 59 \cdot 1 + 30 \cdot 0 + 19 \cdot 0 \\ 77 &= 47 \cdot 1 + 50 \cdot 0 + 59 \cdot 0 + 30 \cdot 1 + 19 \cdot 0 \end{aligned}$$

The transmitted ciphertext consists of the sequence of positive integers

108 59 99 158 106 77

To read the message, the legitimate receiver first solves the congruence $44x \equiv 1 \pmod{85}$, yielding $x \equiv 29 \pmod{85}$. Then each ciphertext number is multiplied by 29 and reduced modulo 85, to produce a superincreasing knapsack problem. For instance,

108 is converted to 72, because $108 \cdot 29 \equiv 72 \pmod{85}$; and the corresponding knapsack problem is

$$72 = 3x_1 + 5x_2 + 11x_3 + 20x_4 + 41x_5$$

The procedure for handling superincreasing knapsack problems quickly produces the solution $x_1 = x_2 = 0, x_3 = x_4 = x_5 = 1$. In this way, the first block 00111 of the binary equivalent of the plaintext is recovered.

The Merkle-Hellman cryptosystem aroused a great deal of interest when it was first proposed, because it was based on a provably difficult problem. However, in 1982 A. Shamir invented a reasonably fast algorithm for solving knapsack problems that involved sequences $b_1, b_2, \ldots, b_n$, where $b_i \equiv aa_i \pmod{m}$ and $a_1, a_2, \ldots, a_n$ is superincreasing. The weakness of the system is that the public encryption key $b_1, b_2, \ldots, b_n$ is too special; multiplying by a and reducing modulo m does not completely disguise the sequence $a_1, a_2, \ldots, a_n$. The system can be made somewhat more secure by iterating the modular multiplication method with different values of a and m, so that the public and private sequences differ by several transformations. But even this construction was successfully broken in 1985. Although most variations of the Merkle-Hellman scheme have been shown to be insecure, there are a few that have, so far, resisted attack.

PROBLEMS 10.2

1. Obtain all solutions of the knapsack problem
$$21 = 2x_1 + 3x_2 + 5x_3 + 7x_4 + 9x_5 + 11x_6$$
2. Determine which of the sequences below are superincreasing:
   (a) 3, 13, 20, 37, 81.
   (b) 5, 13, 25, 42, 90.
   (c) 7, 27, 47, 97, 197, 397.
3. Find the unique solution of each of the following superincreasing knapsack problems:
   (a) $118 = 4x_1 + 5x_2 + 10x_3 + 20x_4 + 41x_5 + 99x_6$.
   (b) $51 = 3x_1 + 5x_2 + 9x_3 + 18x_4 + 37x_5$.
   (c) $54 = x_1 + 2x_2 + 5x_3 + 9x_4 + 18x_5 + 40x_6$.
4. Consider a sequence of positive integers $a_1, a_2, \ldots, a_n$, where $a_{i+1} > 2a_i$ for $i = 1, 2, \ldots, n-1$. Show that the sequence is superincreasing.
5. A user of the knapsack cryptosystem has the sequence 49, 32, 30, 43 as a listed encryption key. If the user's private key involves the modulus $m = 50$ and multiplier $a = 33$, determine the secret superincreasing sequence.
6. The ciphertext message produced by the knapsack cryptosystem employing the superincreasing sequence 1, 3, 5, 11, 35, modulus $m = 73$, and multiplier $a = 5$ is 55, 15, 124, 109, 25, 34. Obtain the plaintext message.
   [*Hint:* Note that $5 \cdot 44 \equiv 1 \pmod{73}$.]
7. A user of the knapsack cryptosystem has a private key consisting of the superincreasing sequence 2, 3, 7, 13, 27, modulus $m = 60$, and multiplier $a = 7$.
   (a) Find the user's listed public key.
   (b) With the aid of the public key, encrypt the message *SEND MONEY*.

10.3 AN APPLICATION OF PRIMITIVE ROOTS TO CRYPTOGRAPHY

Most modern cryptographic schemes rely on the presumed difficulty of solving some particular number theoretic problem within a reasonable length of time. For instance, the security underlying the widely used RSA cryptosystem discussed in Section 10.1 is the sheer effort required to factor large numbers. In 1985, Taher ElGamal introduced a method of encrypting messages based on a version of the so-called discrete logarithm problem: that is, the problem of finding the power $0 < x < \phi(n)$, if it exists, which satisfies the congruence $r^x \equiv y \pmod{n}$ for given r, y, and n. The exponent x is said to be discrete logarithm of y to the base r, modulo n. The advantage of requiring that the base r be a primitive root of prime number n is the assurance that y will always have a well-defined discrete logarithm. The logarithm could be found by exhaustive search; that is, by calculating the successive powers of r until $y \equiv r^x \pmod{n}$ is reached. Of course, this would generally not be practical for a large modulus n of several hundred digits.

Example 8.4 indicates that, say, the discrete logarithm of 7 to the base 2 modulo 13 is 11; expressed otherwise, 11 is the smallest positive integer x for which $2^x \equiv 7 \pmod{13}$. In that example, we used the classical notation $11 = \text{ind}_2 7 \pmod{13}$ and spoke of 11 as being the index of 7, rather than employing the more current terminology.

The ElGamal cryptosystem, like the RSA system, requires that each user possess both a public and a private (secret) key. The means needed to transmit a ciphered message between parties is announced openly, even published in a directory. However, deciphering can be done only by the intended recipient using a private key. Because knowledge of the public key and the method of encipherment is not sufficient to discover the other key, confidential information can be communicated over an insecure channel.

A typical user of this system begins by selecting a prime number p along with one of its primitive roots r. Then an integer k, where $2 \leq k \leq p - 2$, is randomly chosen to serve as the secret key; thereafter,

$$a \equiv r^k \pmod{p} \quad 0 \leq a \leq p - 1$$

is calculated. The triple of integers (p, r, a) becomes the person's public key, made available to all others for cryptographic purposes. The value of the exponent k is never revealed. For an unauthorized party to discover k would entail solving a discrete logarithm problem that would be nearly intractable for large values of a and p.

Before looking at the enciphering procedure, we illustrate the selection of the public key.

Example 10.6. Suppose that an individual begins by picking the prime $p = 113$ and its smallest primitive root $r = 3$. The choice $k = 37$ is then made for the integer satisfying $2 \leq k \leq 111$. It remains to calculate $a \equiv 3^{37} \pmod{113}$. The exponentiation can be readily accomplished by the technique of repeated squaring, reducing

modulo 113 at each step:

$$\begin{aligned} 3^1 &\equiv 3 \pmod{113} & 3^8 &\equiv 7 \pmod{113} \\ 3^2 &\equiv 9 \pmod{113} & 3^{16} &\equiv 49 \pmod{113} \\ 3^4 &\equiv 81 \pmod{113} & 3^{32} &\equiv 28 \pmod{113} \end{aligned}$$

and so

$$a = 3^{37} = 3^1 \cdot 3^4 \cdot 3^{32} \equiv 3 \cdot 81 \cdot 28 \equiv 6304 \equiv 24 \pmod{113}$$

The triple (113, 3, 24) serves as the public key, while the integer 37 becomes the secret deciphering key.

Here is how ElGamal encryption works. Assume that a message is to be sent to someone who has public key (p, r, a) and also the corresponding private key k. The transmission is a string of integers smaller than p. Thus, the literal message is first converted to its numerical equivalent M by some standard convention such as letting a = 00, b = 01, ..., z = 25. If $M \geq p$, then M is split into successive blocks, each block containing the same (even) number of digits. It may be necessary to add extra digits (say, $25 = z$), to fill out the final block.

The blocks of digits are encrypted separately. If B denotes the first block, then the sender—who is aware of the recipient's public key—arbitrarily selects an integer $2 \leq j \leq p - 2$ and computes two values:

$$C_1 \equiv r^j \pmod{p} \quad \text{and} \quad C_2 \equiv Ba^j \pmod{p}, \quad 0 \leq C_1, C_2 \leq p - 1$$

The numerical ciphertext associated with the block B is the pair of integers (C_1, C_2). It is possible, in case greater security is needed, for the choice of j to be changed from block to block.

The recipient of the ciphertext can recover the block B by using the secret key k. All that needs to be done is to evaluate $C_1^{p-1-k} \pmod{p}$ and then $P \equiv C_2 C_1^{p-1-k} \pmod{p}$; for

$$\begin{aligned} P \equiv C_2 C_1^{p-1-k} &\equiv (Ba^j)(r^j)^{p-1-k} \\ &\equiv B(r^k)^j (r^{j(p-1)-jk}) \\ &\equiv B(r^{p-1})^j \\ &\equiv B \pmod{p} \end{aligned}$$

where the final congruence results from the Fermat identity $r^{p-1} \equiv 1 \pmod{p}$. The main point is that the decryption can be carried out by someone who knows the value of k.

Let us work through the steps of the encryption algorithm, using a reasonably small prime number for simplicity.

Example 10.7. Assume that the user wishes to deliver the message

SELL NOW

to a person who has the secret key $k = 15$ and public encryption key $(p, r, a) = (43, 3, 22)$, where $22 \equiv 3^{15} \pmod{43}$. The literal plaintext is first converted to the string of digits

$$M = 18041111131422$$

To create the ciphertext, the sender selects an integer j satisfying $2 \leq j \leq 41$, perhaps $j = 23$, and then calculates

$$r^j = 3^{23} \equiv 34 \pmod{43} \quad \text{and} \quad a^j = 22^{23} \equiv 32 \pmod{43}$$

Thereafter, the product $a^j B \equiv 32B \pmod{43}$ is computed for each two-digit block B of M. The initial block, for instance, is encrypted as $32.18 \equiv 17 \pmod{43}$. The entered digital message M is transformed in this way into a new string

$$M' = 17420808291816$$

The ciphertext that goes forward takes the form

$$(34, 17)\,(34, 42)\,(34, 08)\,(34, 08)\,(34, 29)\,(34, 18)\,(34, 16)$$

On the arrival of the message, the recipient uses the secret key to obtain

$$(r^j)^{p-1-k} \equiv 34^{27} \equiv 39 \pmod{43}$$

Each second entry in the ciphertext pairs is decrypted on multiplication by this last value. The first letter, S, in the sender's original message would be recovered from the congruence $18 \equiv 39 \cdot 17 \pmod{43}$, and so on.

An important aspect of a cryptosystem should be its ability to confirm the integrity of a message; because everyone knows how to send a message, the recipient must be sure that the encryption was really issued by an authorized person. The usual method of protecting against possible third-party forgeries is for the person sending the message to have a digital "signature," the electronic analog of a handwritten signature. It should be difficult to tamper with the digital signature, but its authenticity should be easy to recognize. Unlike a handwritten signature, it should be possible to vary a digital signature from one communication to another.

A feature of the ElGamal cryptosystem is an efficient procedure for authenticating messages. Consider a user of the system who has public key (p, r, a), private key k, and encrypted message M. The first step toward supplying a signature is to choose an integer $1 \leq j \leq p - 1$ where $\gcd(j, p - 1) = 1$. Taking a piece of the plaintext message M—for instance, the first block B—the user next computes

$$c \equiv r^j \pmod{p}, \quad 0 \leq j \leq p - 1$$

and then obtains a solution of the linear congruence

$$jd + kc \equiv B \pmod{p - 1}, \quad 0 \leq d \leq p - 2$$

The solution d can be found using the Euclidean algorithm. The pair of integers (c, d) is the required digital signature appended to the message. It can be created only by someone aware of the private key k, the random integer j, and the message M.

The recipient uses the sender's public key (p, r, a) to confirm the purported signature. It is simply a matter of calculating the two values

$$V_1 \equiv a^c c^d \pmod{p}, \quad V_2 \equiv r^B \pmod{p}, \quad 0 \leq V_1, V_2 \leq p - 1$$

The signature is accepted as legitimate when $V_1 = V_2$. That this equality should take place follows from the congruence

$$\begin{aligned} V_1 \equiv a^c c^d &\equiv (r^k)^c (r^j)^d \\ &\equiv r^{kc+jd} \\ &\equiv r^B \equiv V_2 \pmod{p} \end{aligned}$$

Notice that the personal identification does not require the recipient to know the sender's private key k.

Example 10.8. The person having public key (43, 3, 22) and private key $k = 15$ wants to sign and reply to the message SELL NOW. This is carried out by first choosing an integer $0 \leq j \leq 42$ with $\gcd(j, 42) = 1$, say $j = 25$. If the first block of the encoded reply is $B = 13$, then the person calculates

$$c \equiv 3^{25} \equiv 5 \pmod{43}$$

and thereafter solves the congruence

$$25d \equiv 13 - 5 \cdot 15 \pmod{42}$$

for the value $d \equiv 16 \pmod{42}$. The digital signature attached to the reply consists of the pair (5, 16). On its arrival, the signature is confirmed by checking the equality of the integers V_1 and V_2:

$$V_1 \equiv 22^5 \cdot 5^{16} \equiv 39 \cdot 40 \equiv 12 \pmod{43}$$
$$V_2 \equiv 3^{13} \equiv 12 \pmod{43}$$

PROBLEMS 10.3

1. The message REPLY TODAY is to be encrypted in the ElGamal cryptosystem and forwarded to a user with public key (47, 5, 10) and private key $k = 19$.

(a) If the random integer chosen for encryption is $j = 13$, determine the ciphertext.

(b) Indicate how the ciphertext can be decrypted using the recipient's private key.

2. Suppose that the following ciphertext is received by a person having ElGamal public key (71, 7, 32) and private key $k = 30$:

(56, 45) (56, 38) (56, 29) (56, 03) (56, 67)
(56, 05) (56, 27) (56, 31) (56, 38) (56, 29)

Obtain the plaintext message.

3. The message NOT NOW (numerically 131419131422) is to be sent to a user of the ElGamal system who has public key (37, 2, 18) and private key $k = 17$. If the integer j used to construct the ciphertext is changed over successive four-digit blocks from $j = 13$ to $j = 28$ to $j = 11$, what is the encrypted message produced?

4. Assume that a person has ElGamal public key (2633, 3, 1138) and private key $k = 965$. If the person selects the random interger $j = 583$ to encrypt the message BEWARE OF THEM, obtain the resulting ciphertext.

[*Hint:* $3^{583} \equiv 1424 \pmod{2633}$, $1138^{583} \equiv 97 \pmod{2633}$.]

5. (a) A person with public key (31, 2, 22) and private key $k = 17$ wishes to sign a message whose first plaintext block is $B = 14$. If 13 is the integer chosen to construct the signature, obtain the signature produced by the ElGamal algorithm.

(b) Confirm the validity of this signature.

CHAPTER 11

NUMBERS OF SPECIAL FORM

In most sciences one generation tears down what another has built and what one has established another undoes. In Mathematics alone each generation builds a new story to the old structure.
HERMANN HANKEL

11.1 MARIN MERSENNE

The earliest instance we know of a regular gathering of mathematicians is the group held together by an unlikely figure—the French priest Father Marin Mersenne (1588–1648). The son of a modest farmer, Mersenne received a thorough education at the Jesuit College of La Flèche. In 1611, after two years studying theology at the Sorbonne, he joined the recently founded Franciscan Order of Minims. Mersenne entered the Minim Convent in Paris in 1619 where, except for short trips, he remained for the rest of his life.

Mersenne lamented the absence of any sort of formal organization to which scholars might resort. He responded to this need by making his own rooms at the Minim convent available as a meeting place for those drawn together by common interests, eager to discuss their respective discoveries and hear of similar activity elsewhere. The learned circle he fostered—composed mainly of Parisian mathematicians and scientists but augmented by colleagues passing through the city—seems to have met almost continuously from 1635 until Mersenne's death in 1648. At one of these meetings the precocious 14-year-old Blaise Pascal distributed his handbill *Essay pour les coniques* containing his famous "mystic hexagram" theorem; Descartes could only grumble that he could not "pretend to be interested in the

work of a boy." After Mersenne's death, the august sessions continued to be held at private homes in and around Paris, including Pascal's. It is customary to regard the Académie Royale des Sciences, chartered in 1666, as the more or less direct successor of these informal gatherings.

From 1625 onwards, Mersenne made it his business to become acquainted with everyone of note in the European intellectual world. He carried out this plan through an elaborate network of correspondence which lasted over 20 years. In essence he became an individual clearinghouse of mathematical and scientific information, trading news of current advances in return for more news. It was Mersenne who, following a 1645 visit to Torricelli in Italy, made widely known that the physicist's demonstration of atmospheric pressure through the rising of a column of mercury in a vacuum tube. Mersenne's communications, dispersed over the Continent by passing from hand to hand, were the vital link between isolated members of the emerging scientific community at a time when the publication of learned journals still lay in the future.

After Mersenne's death letters from 78 correspondents scattered over Western Europe were found in his Parisian quarters. Among his correspondents were Huygens in Holland, Torricelli and Galileo in Italy, Pell and Hobbes in England, and the Pascals, father and son, in France. He had also served as the main channel of communication between the French number theorists Fermat, Frénicle and Descartes; their exchanged letters determined the sorts of problems these three chose to investigate.

Mersenne was not himself a serious contributor to the subject, rather a remarkable interested person prodding others with questions and conjectures. His own queries tended to be rooted in the classical Greek concern with divisibility. For instance, in a letter written in 1643, he sent the number 100895598169 to Fermat with a request for its factors. (Fermat responded almost immediately that it is the product of the two primes 898423 and 112303.) On another occasion he asked for a number which has exactly 360 divisors. Mersenne was also interested in whether or not there exists a so called "perfect number" with 20 or 21 digits, the underlying question really being to find out whether $2^{37} - 1$ is prime. Fermat discovered that the only prime divisors of $2^{37} - 1$ are of the form $74k + 1$ and that 223 is such a factor, thereby supplying a negative answer to Mersenne.

Mersenne was the author of various works dealing with the mathematical sciences, including *Synopsis Mathematica* (1626), *Traité de l'Harmonie Universelle* (1636–37) and *Universae Geometriae Synopsis* (1644). A believer in the new Copernican theory of the earth's motion, he was virtually Galileo's representative in France. He brought out (1634), under the title *Les Mécaniques de Galilée*, a version of Galileo's early lectures on mechanics; and, in 1639, a year after its original publication, he translated Galileo's *Discorsi*—a treatise analyzing projectile motion and gravitational acceleration—into French. As Italian was little understood abroad, Mersenne was instrumental in popularizing Galileo's investigations. It is notable that he did this as a faithful member of a Catholic religious order at the height of the Church's hostility to Galileo, and its condemnation of his writings. Perhaps Mersenne's greatest contribution to the scientific movement lay in his rejection of the traditional interpretation of natural phenomena, which had stressed the action of "occult" powers, by insisting instead upon purely rational explanations.

Marin Mersenne
(1588–1648)

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

11.2 PERFECT NUMBERS

The history of the theory of numbers abounds with famous conjectures and open questions. The present chapter focuses on some of the intriguing conjectures associated with perfect numbers. A few of these have been satisfactorily answered, but most remain unresolved; all have stimulated the development of the subject as a whole.

The Pythagoreans considered it rather remarkable that the number 6 is equal to the sum of its positive divisors, other than itself:

$$6 = 1 + 2 + 3$$

The next number after 6 having this feature is 28; for the positive divisors of 28 are found to be 1, 2, 4, 7, 14, and 28, and

$$28 = 1 + 2 + 4 + 7 + 14$$

In line with their philosophy of attributing mystical qualities to numbers, the Pythagoreans called such numbers "perfect." We state this precisely in Definition 11.1.

Definition 11.1. A positive integer n is said to be *perfect* if n is equal to the sum of all its positive divisors, excluding n itself.

The sum of the positive divisors of an integer n, each of them less than n, is given by $\sigma(n) - n$. Thus, the condition "n is perfect" amounts to asking that $\sigma(n) - n = n$, or equivalently, that

$$\sigma(n) = 2n$$

For example, we have

$$\sigma(6) = 1 + 2 + 3 + 6 = 2 \cdot 6$$

and

$$\sigma(28) = 1 + 2 + 4 + 7 + 14 + 28 = 2 \cdot 28$$

so that 6 and 28 are both perfect numbers.

For many centuries, philosophers were more concerned with the mystical or religious significance of perfect numbers than with their mathematical properties. Saint Augustine explains that although God could have created the world all at once, He preferred to take 6 days because the perfection of the work is symbolized by the (perfect) number 6. Early commentators on the Old Testament argued that the perfection of the Universe is represented by 28, the number of days it takes the moon to circle the earth. In the same vein, the 8th century theologian Alcuin of York observed that the whole human race is descended from the 8 souls on Noah's Ark and that this second Creation is less perfect than the first, 8 being an imperfect number.

Only four perfect numbers were known to the ancient Greeks. Nicomachus in his *Introductio Arithmeticae* (circa 100 A.D.) lists

$$P_1 = 6 \qquad P_2 = 28 \qquad P_3 = 496 \qquad P_4 = 8128$$

He says that they are formed in an "orderly" fashion, one among the units, one among the tens, one among the hundreds, and one among the thousands (that is, less than 10,000). Based on this meager evidence, it was conjectured that

1. The nth perfect number P_n contains exactly n digits; and

2. The even perfect numbers end, alternately, in 6 and 8.

Both assertions are wrong. There is no perfect number with 5 digits; the next perfect number (first given correctly in an anonymous 15th century manuscript) is

$$P_5 = 33550336$$

Although the final digit of P_5 is 6, the succeeding perfect number, namely,

$$P_6 = 8589869056$$

also ends in 6, not 8 as conjectured. To salvage something in the positive direction, we shall show later that the even perfect numbers do always end in 6 or 8—but not necessarily alternately.

If nothing else, the magnitude of P_6 should convince the reader of the rarity of perfect numbers. It is not yet known whether there are finitely many or infinitely many of them.

The problem of determining the general form of all perfect numbers dates back almost to the beginning of mathematical time. It was partially solved by Euclid when in Book IX of the *Elements* he proved that if the sum

$$1 + 2 + 2^2 + 2^3 + \cdots + 2^{k-1} = p$$

is a prime number, then $2^{k-1}p$ is a perfect number (of necessity even). For instance, $1 + 2 + 4 = 7$ is a prime; hence, $4 \cdot 7 = 28$ is a perfect number. Euclid's argument

makes use of the formula for the sum of a geometric progression

$$1 + 2 + 2^2 + 2^3 + \cdots + 2^{k-1} = 2^k - 1$$

which is found in various Pythagorean texts. In this notation, the result reads as follows: If $2^k - 1$ is prime ($k > 1$), then $n = 2^{k-1}(2^k - 1)$ is a perfect number. About 2000 years after Euclid, Euler took a decisive step in proving that all even perfect numbers must be of this type. We incorporate both these statements in our first theorem.

Theorem 11.1. If $2^k - 1$ is prime ($k > 1$), then $n = 2^{k-1}(2^k - 1)$ is perfect and every even perfect number is of this form.

Proof. Let $2^k - 1 = p$, a prime, and consider the integer $n = 2^{k-1}p$. Inasmuch as $\gcd(2^{k-1}, p) = 1$, the multiplicativity of σ (as well as Theorem 6.2) entails that

$$\begin{aligned}\sigma(n) &= \sigma(2^{k-1}p) = \sigma(2^{k-1})\sigma(p) \\ &= (2^k - 1)(p + 1) \\ &= (2^k - 1)2^k = 2n\end{aligned}$$

making n a perfect number.

For the converse, assume that n is an even perfect number. We may write n as $n = 2^{k-1}m$, where m is an odd integer and $k \geq 2$. It follows from $\gcd(2^{k-1}, m) = 1$ that

$$\sigma(n) = \sigma(2^{k-1}m) = \sigma(2^{k-1})\sigma(m) = (2^k - 1)\sigma(m)$$

whereas the requirement for a number to be perfect gives

$$\sigma(n) = 2n = 2^k m$$

Together, these relations yield

$$2^k m = (2^k - 1)\sigma(m)$$

which is simply to say that $(2^k - 1) \mid 2^k m$. But $2^k - 1$ and 2^k are relatively prime, whence $(2^k - 1) \mid m$; say, $m = (2^k - 1)M$. Now the result of substituting this value of m into the last-displayed equation and canceling $2^k - 1$ is that $\sigma(m) = 2^k M$. Because m and M are both divisors of m (with $M < m$), we have

$$2^k M = \sigma(m) \geq m + M = 2^k M$$

leading to $\sigma(m) = m + M$. The implication of this equality is that m has only two positive divisors, to wit, M and m itself. It must be that m is prime and $M = 1$; in other words, $m = (2^k - 1)M = 2^k - 1$ is a prime number, completing the present proof.

Because the problem of finding even perfect numbers is reduced to the search for primes of the form $2^k - 1$, a closer look at these integers might be fruitful. One thing that can be proved is that if $2^k - 1$ is a prime number, then the exponent k must itself be prime. More generally, we have the following lemma.

Lemma. If $a^k - 1$ is prime ($a > 0$, $k \geq 2$), then $a = 2$ and k is also prime.

Proof. It can be verified without difficulty that

$$a^k - 1 = (a-1)(a^{k-1} + a^{k-2} + \cdots + a + 1)$$

where, in the present setting,

$$a^{k-1} + a^{k-2} + \cdots + a + 1 \geq a + 1 > 1$$

Because by hypothesis $a^k - 1$ is prime, the other factor must be 1; that is, $a - 1 = 1$ so that $a = 2$.

If k were composite, then we could write $k = rs$, with $1 < r$ and $1 < s$. Thus,

$$\begin{aligned} a^k - 1 &= (a^r)^s - 1 \\ &= (a^r - 1)(a^{r(s-1)} + a^{r(s-2)} + \cdots + a^r + 1) \end{aligned}$$

and each factor on the right is plainly greater than 1. But this violates the primality of $a^k - 1$, so that by contradiction k must be prime.

For $p = 2, 3, 5, 7$, the values 3, 7, 31, 127 of $2^p - 1$ are primes, so that

$$\begin{aligned} 2(2^2 - 1) &= 6 \\ 2^2(2^3 - 1) &= 28 \\ 2^4(2^5 - 1) &= 496 \\ 2^6(2^7 - 1) &= 8128 \end{aligned}$$

are all perfect numbers.

Many early writers erroneously believed that $2^p - 1$ is prime for every choice of the prime number p. But in 1536, Hudalrichus Regius in a work entitled *Utriusque Arithmetices* exhibits the correct factorization

$$2^{11} - 1 = 2047 = 23 \cdot 89$$

If this seems a small accomplishment, it should be realized that his calculations were in all likelihood carried out in Roman numerals, with the aid of an abacus (not until the late 16th century did the Arabic numeral system win complete ascendancy over the Roman one). Regius also gave $p = 13$ as the next value of p for which the expression $2^p - 1$ is a prime. From this, we obtain the fifth perfect number

$$2^{12}(2^{13} - 1) = 33550336$$

One of the difficulties in finding further perfect numbers was the unavailability of tables of primes. In 1603, Pietro Cataldi, who is remembered chiefly for his invention of the notation for continued fractions, published a list of all primes less than 5150. By the direct procedure of dividing by all primes not exceeding the square root of a number, Cataldi determined that $2^{17} - 1$ was prime and, in consequence, that

$$2^{16}(2^{17} - 1) = 8589869056$$

is the sixth perfect number.

A question that immediately springs to mind is whether there are infinitely many primes of the type $2^p - 1$, with p a prime. If the answer were in the affirmative, then there would exist an infinitude of (even) perfect numbers. Unfortunately, this is another famous unresolved problem.

This appears to be as good a place as any at which to prove our theorem on the final digits of even perfect numbers.

Theorem 11.2. An even perfect number n ends in the digit 6 or 8; equivalently, either $n \equiv 6 \pmod{10}$ or $n \equiv 8 \pmod{10}$.

Proof. Being an even perfect number, n may be represented as $n = 2^{k-1}(2^k - 1)$, where $2^k - 1$ is a prime. According to the last lemma, the exponent k must also be prime. If $k = 2$, then $n = 6$, and the asserted result holds. We may therefore confine our attention to the case $k > 2$. The proof falls into two parts, according as k takes the form $4m + 1$ or $4m + 3$.

If k is of the form $4m + 1$, then

$$\begin{aligned} n &= 2^{4m}(2^{4m+1} - 1) \\ &= 2^{8m+1} - 2^{4m} = 2 \cdot 16^{2m} - 16^m \end{aligned}$$

A straightforward induction argument will make it clear that $16^t \equiv 6 \pmod{10}$ for any positive integer t. Utilizing this congruence, we get

$$n \equiv 2 \cdot 6 - 6 \equiv 6 \pmod{10}$$

Now, in the case in which $k = 4m + 3$,

$$\begin{aligned} n &= 2^{4m+2}(2^{4m+3} - 1) \\ &= 2^{8m+5} - 2^{4m+2} = 2 \cdot 16^{2m+1} - 4 \cdot 16^m \end{aligned}$$

Falling back on the fact that $16^t \equiv 6 \pmod{10}$, we see that

$$n \equiv 2 \cdot 6 - 4 \cdot 6 \equiv -12 \equiv 8 \pmod{10}$$

Consequently, every even perfect number has a last digit equal to 6 or to 8.

A little more argument establishes a sharper result, namely, that any even perfect number $n = 2^{k-1}(2^k - 1)$ always ends in the digits 6 or 28. Because an integer is congruent modulo 100 to its last two digits, it suffices to prove that, if k is of the form $4m + 3$, then $n \equiv 28 \pmod{100}$. To see this, note that

$$2^{k-1} = 2^{4m+2} = 16^m \cdot 4 \equiv 6 \cdot 4 \equiv 4 \pmod{10}$$

Moreover, for $k > 2$, we have $4 \mid 2^{k-1}$, and therefore the number formed by the last two digits of 2^{k-1} is divisible by 4. The situation is this: The last digit of 2^{k-1} is 4, and 4 divides the last two digits. Modulo 100, the various possibilities are

$$2^{k-1} \equiv 4, 24, 44, 64, \text{or } 84$$

But this implies that

$$2^k - 1 = 2 \cdot 2^{k-1} - 1 \equiv 7, 47, 87, 27, \text{or } 67 \pmod{100}$$

whence

$$\begin{aligned} n &= 2^{k-1}(2^k - 1) \\ &\equiv 4 \cdot 7, 24 \cdot 47, 44 \cdot 87, 64 \cdot 27, \text{or } 84 \cdot 67 \pmod{100} \end{aligned}$$

It is a modest exercise, which we bequeath to the reader, to verify that each of the products on the right-hand side of the last congruence is congruent to 28 modulo 100.

PROBLEMS 11.2

1. Prove that the integer $n = 2^{10}(2^{11} - 1)$ is not a perfect number by showing that $\sigma(n) \neq 2n$.
   [*Hint:* $2^{11} - 1 = 23 \cdot 89$.]
2. Verify each of the statements below:
   (a) No power of a prime can be a perfect number.
   (b) A perfect square cannot be a perfect number.
   (c) The product of two odd primes is never a perfect number.
   [*Hint:* Expand the inequality $(p - 1)(q - 1) > 2$ to get $pq > p + q + 1$.]
3. If n is a perfect number, prove that $\sum_{d \mid n} 1/d = 2$.
4. Prove that every even perfect number is a triangular number.
5. Given that n is an even perfect number, for instance $n = 2^{k-1}(2^k - 1)$, show that the integer $n = 1 + 2 + 3 + \cdots + (2^k - 1)$ and also that $\phi(n) = 2^{k-1}(2^{k-1} - 1)$.
6. For an even perfect number $n > 6$, show the following:
   (a) The sum of the digits of n is congruent to 1 modulo 9.
   [*Hint:* The congruence $2^6 \equiv 1 \pmod 9$ and the fact that any prime $p \geq 5$ is of the form $6k + 1$ or $6k + 5$ imply that $n = 2^{p-1}(2^p - 1) \equiv 1 \pmod 9$.]
   (b) The integer n can be expressed as a sum of consecutive odd cubes.
   [*Hint:* Use Section 1.1, Problem 1(e) to establish the identity below for all $k \geq 1$:

$$1^3 + 3^3 + 5^3 + \cdots + (2^k - 1)^3 = 2^{2k-2}(2^{2k-1} - 1).]$$

7. Show that no proper divisor of a perfect number can be perfect.
   [*Hint:* Apply the result of Problem 3.]
8. Find the last two digits of the perfect number

$$n = 2^{19936}(2^{19937} - 1)$$

9. If $\sigma(n) = kn$, where $k \geq 3$, then the positive integer n is called a *k-perfect number* (sometimes, *multiply perfect*). Establish the following assertions concerning k-perfect numbers:
   (a) $523{,}776 = 2^9 \cdot 3 \cdot 11 \cdot 31$ is 3-perfect.
   $30{,}240 = 2^5 \cdot 3^3 \cdot 5 \cdot 7$ is 4-perfect.
   $14{,}182{,}439{,}040 = 2^7 \cdot 3^4 \cdot 5 \cdot 7 \cdot 11^2 \cdot 17 \cdot 19$ is 5-perfect.
   (b) If n is a 3-perfect number and $3 \nmid n$, then $3n$ is 4-perfect.
   (c) If n is a 5-perfect number and $5 \nmid n$, then $5n$ is 6-perfect.
   (d) If $3n$ is a $4k$-perfect number and $3 \nmid n$, then n is $3k$-perfect.
   For each k, it is conjectured that there are only finitely many k-perfect numbers. The largest one discovered has 558 digits and is 9-perfect.
10. Show that 120 and 672 are the only 3-perfect numbers of the form $n = 2^k \cdot 3 \cdot p$, where p is an odd prime.
11. A positive integer n is *multiplicatively perfect* if n is equal to the product of all its positive divisors, excluding n itself; in other words, $n^2 = \prod_{d \mid n} d$. Find all multiplicatively perfect numbers.
    [*Hint:* Notice that $n^2 = n^{\tau(n)/2}$.]
12. (a) If $n > 6$ is an even perfect number, prove that $n \equiv 4 \pmod 6$.
    [*Hint:* $2^{p-1} \equiv 1 \pmod 3$ for an odd prime p.]
    (b) Prove that if $n \neq 28$ is an even perfect number, then $n \equiv 1$ or $-1 \pmod 7$.
13. For any even perfect number $n = 2^{k-1}(2^k - 1)$, show that $2^k \mid \sigma(n^2) + 1$.

14. Numbers n such that $\sigma(\sigma(n)) = 2n$ are called *superperfect numbers*.
(a) If $n = 2^k$ with $2^{k+1} - 1$ a prime, prove that n is superperfect; hence, 16 and 64 are superperfect.
(b) Find all even perfect numbers $n = 2^{k-1}(2^k - 1)$ which are also superperfect.
[*Hint:* First establish the equality $\sigma(\sigma(n)) = 2^k(2^{k+1} - 1)$.]

15. The *harmonic mean* $H(n)$ of the divisors of a positive integer n is defined by the formula

$$\frac{1}{H(n)} = \frac{1}{\tau(n)} \sum_{d \mid n} \frac{1}{d}$$

Show that if n is a perfect number, then $H(n)$ must be an integer.
[*Hint:* Observe that $H(n) = n\tau(n)/\sigma(n)$.]

16. The twin primes 5 and 7 are such that one half their sum is a perfect number. Are there any other twin primes with this property?
[*Hint:* Given the twin primes p and $p + 2$, with $p > 5$, $\frac{1}{2}(p + p + 2) = 6k$ for some $k > 1$.]

17. Prove that if $2^k - 1$ is prime, then the sum

$$2^{k-1} + 2^k + 2^{k+1} + \cdots + 2^{2k-2}$$

will yield a perfect number. For instance, $2^3 - 1$ is prime and $2^2 + 2^3 + 2^4 = 28$, which is perfect.

18. Assuming that n is an even perfect number, say $n = 2^{k-1}(2^k - 1)$, prove that the product of the positive divisors of n is equal to n^k; in symbols,

$$\prod_{d \mid n} d = n^k$$

19. If $n_1, n_2, \cdots, n_r$ are distinct even perfect numbers, establish that

$$\phi(n_1 n_2 \cdots n_r) = 2^{r-1}\phi(n_1)\phi(n_2)\cdots\phi(n_r)$$

[*Hint:* See Problem 5.]

20. Given an even perfect number $n = 2^{k-1}(2^k - 1)$, show that

$$\phi(n) = n - 2^{2k-2}$$

11.3 MERSENNE PRIMES AND AMICABLE NUMBERS

It has become traditional to call numbers of the form

$$M_n = 2^n - 1 \qquad n \geq 1$$

Mersenne numbers after Father Marin Mersenne who made an incorrect but provocative assertion concerning their primality. Those Mersenne numbers that happen to be prime are said to be *Mersenne primes*. By what we proved in Section 11.2, the determination of Mersenne primes M_n—and, in turn, of even perfect numbers—is narrowed down to the case in which n is itself prime.

In the preface of his *Cogitata Physica-Mathematica* (1644), Mersenne stated that M_p is prime for $p = 2, 3, 5, 7, 13, 17, 19, 31, 67, 127, 257$ and composite for all other primes $p < 257$. It was obvious to other mathematicians that Mersenne could not have tested for primality all the numbers he had announced; but neither could they. Euler verified (1772) that M_{31} was prime by examining all primes up to

46339 as possible divisors, but M_{67}, M_{127}, and M_{257} were beyond his technique; in any event, this yielded the eighth perfect number

$$2^{30}(2^{31} - 1) = 2305843008139952128$$

It was not until 1947, after tremendous labor caused by unreliable desk calculators, that the examination of the prime or composite character of M_p for the 55 primes in the range $p \leq 257$ was completed. We know now that Mersenne made five mistakes. He erroneously concluded that M_{67} and M_{257} are prime and excluded M_{61}, M_{89}, and M_{107} from his predicted list of primes. It is rather astonishing that over 300 years were required to set the good friar straight.

All the composite numbers M_n with $n \leq 257$ have now been completely factored. The most difficult factorization, that of M_{251}, was obtained in 1984 after a 32-hour search on a supercomputer.

An historical curiosity is that, in 1876, Edouard Lucas worked a test whereby he was able to prove that the Mersenne number M_{67} was composite; but he could not produce the actual factors.

Lucas was the first to devise an efficient "primality test"; that is, a procedure that guarantees whether a number is prime or composite without revealing its factors, if any. His primality criteria for the Mersenne and Fermat numbers were developed in a series of 13 papers published between January of 1876 and January of 1878. Despite an outpouring of research Lucas never obtained a major academic position in his native France, instead spending his career in various secondary schools. A freak, unfortunate accident led to Lucas's death from infection at the early age of 49: a piece of a plate dropped at a banquet flew up and gashed his cheek.

At the October 1903 meeting of the American Mathematical Society, the American mathematician Frank Nelson Cole had a paper on the program with the somewhat unassuming title "On the Factorization of Large Numbers." When called upon to speak, Cole walked to a board and, saying nothing, proceeded to raise the integer 2 to the 67th power; then he carefully subtracted 1 from the resulting number and let the figure stand. Without a word he moved to a clean part of the board and multiplied, longhand, the product

$$193{,}707{,}721 \times 761{,}838{,}257{,}287$$

The two calculations agreed. The story goes that, for the first and only time on record, this venerable body rose to give the presenter of a paper a standing ovation. Cole took his seat without having uttered a word, and no one bothered to ask him a question. (Later, he confided to a friend that it took him 20 years of Sunday afternoons to find the factors of M_{67}.)

In the study of Mersenne numbers, we come upon a strange fact: When each of the first four Mersenne primes (namely, 3, 7, 31, and 127) is substituted for n in the formula $2^n - 1$, a higher Mersenne prime is obtained. Mathematicians had hoped that this procedure would give rise to an infinite set of Mersenne primes; in other words, the conjecture was that if the number M_n is prime, then M_{M_n} is also a prime. Alas, in 1953 a high-speed computer found the next possibility

$$M_{M_{13}} = 2^{M_{13}} - 1 = 2^{8191} - 1$$

(a number with 2466 digits) to be composite.

There are various methods for determining whether certain special types of Mersenne numbers are prime or composite. One such test is presented next.

Theorem 11.3. If p and $q = 2p + 1$ are primes, then either $q \mid M_p$ or $q \mid M_p + 2$, but not both.

Proof. With reference to Fermat's theorem, we know that

$$2^{q-1} - 1 \equiv 0 \pmod{q}$$

and, factoring the left-hand side, that

$$\begin{aligned}(2^{(q-1)/2} - 1)(2^{(q-1)/2} + 1) &= (2^p - 1)(2^p + 1) \\ &\equiv 0 \pmod{q}\end{aligned}$$

What amounts to the same thing:

$$M_p(M_p + 2) \equiv 0 \pmod{q}$$

The stated conclusion now follows directly from Theorem 3.1. We cannot have both $q \mid M_p$ and $q \mid M_p + 2$, for then $q \mid 2$, which is impossible.

A single application should suffice to illustrate Theorem 11.3: If $p = 23$, then $q = 2p + 1 = 47$ is also a prime, so that we may consider the case of M_{23}. The question reduces to one of whether $47 \mid M_{23}$ or, to put it differently, whether $2^{23} \equiv 1 \pmod{47}$. Now, we have

$$2^{23} = 2^3(2^5)^4 \equiv 2^3(-15)^4 \pmod{47}$$

But

$$(-15)^4 = (225)^2 \equiv (-10)^2 \equiv 6 \pmod{47}$$

Putting these two congruences together, we see that

$$2^{23} \equiv 2^3 \cdot 6 \equiv 48 \equiv 1 \pmod{47}$$

whence M_{23} is composite.

We might point out that Theorem 11.3 is of no help in testing the primality of M_{29}, say; in this instance, $59 \nmid M_{29}$, but instead $59 \mid M_{29} + 2$.

Of the two possibilities $q \mid M_p$ or $q \mid M_p + 2$, is it reasonable to ask: What conditions on q will ensure that $q \mid M_p$? The answer is to be found in Theorem 11.4.

Theorem 11.4. If $q = 2n + 1$ is prime, then we have the following:

(a) $q \mid M_n$, provided that $q \equiv 1 \pmod{8}$ or $q \equiv 7 \pmod{8}$.
(b) $q \mid M_n + 2$, provided that $q \equiv 3 \pmod{8}$ or $q \equiv 5 \pmod{8}$.

Proof. To say that $q \mid M_n$ is equivalent to asserting that

$$2^{(q-1)/2} = 2^n \equiv 1 \pmod{q}$$

In terms of the Legendre symbol, the latter condition becomes the requirement that

$(2/q) = 1$. But according to Theorem 9.6, $(2/q) = 1$ when we have $q \equiv 1 \pmod 8$ or $q \equiv 7 \pmod 8$. The proof of (b) proceeds along similar lines.

Let us consider an immediate consequence of Theorem 11.4.

Corollary. If p and $q = 2p + 1$ are both odd primes, with $p \equiv 3 \pmod 4$, then $q \mid M_p$.

Proof. An odd prime p is either of the form $4k + 1$ or $4k + 3$. If $p = 4k + 3$, then $q = 8k + 7$ and Theorem 11.4 yields $q \mid M_p$. In the case in which $p = 4k + 1$, $q = 8k + 3$ so that $q \nmid M_p$.

The following is a partial list of those prime numbers $p \equiv 3 \pmod 4$ where $q = 2p + 1$ is also prime: $p = 11, 23, 83, 131, 179, 191, 239, 251$. In each instance, M_p is composite.

Exploring the matter a little further, we next tackle two results of Fermat that restrict the divisors of M_p. The first is Theorem 11.5.

Theorem 11.5. If p is an odd prime, then any prime divisor of M_p is of the form $2kp + 1$.

Proof. Let q be any prime divisor of M_p, so that $2^p \equiv 1 \pmod q$. If 2 has order k modulo q (that is, if k is the smallest positive integer that satisfies $2^k \equiv 1 \pmod q$), then Theorem 8.1 tells us that $k \mid p$. The case $k = 1$ cannot arise; for this would imply that $q \mid 1$, an impossible situation. Therefore, because both $k \mid p$ and $k > 1$, the primality of p forces $k = p$.

In compliance with Fermat's theorem, we have $2^{q-1} \equiv 1 \pmod q$, and therefore, thanks to Theorem 8.1 again, $k \mid q - 1$. Knowing that $k = p$, the net result is $p \mid q - 1$. To be definite, let us put $q - 1 = pt$; then $q = pt + 1$. The proof is completed by noting that if t were an odd integer, then q would be even and a contradiction occurs. Hence, we must have $q = 2kp + 1$ for some choice of k, which gives q the required form.

As a further sieve to screen out possible divisors of M_p, we cite the following result.

Theorem 11.6. If p is an odd prime, then any prime divisor q of M_p is of the form $q \equiv \pm 1 \pmod 8$.

Proof. Suppose that q is a prime divisor of M_p, so that $2^p \equiv 1 \pmod q$. According to Theorem 11.5, q is of the form $q = 2kp + 1$ for some integer k. Thus, using Euler's criterion, $(2/q) \equiv 2^{(q-1)/2} \equiv 1 \pmod q$, whence $(2/q) = 1$. Theorem 9.6 can now be brought into play again to conclude that $q \equiv \pm 1 \pmod 8$.

For an illustration of how these theorems can be used, one might look at M_{17}. Those integers of the form $34k + 1$ that are less than $362 < \sqrt{M_{17}}$ are

$$35, 69, 103, 137, 171, 205, 239, 273, 307, 341$$

Because the smallest (nontrivial) divisor of M_{17} must be prime, we need only consider the primes among the foregoing 10 numbers; namely,

$$103, 137, 239, 307$$

The work can be shortened somewhat by noting that $307 \not\equiv \pm 1 \pmod 8$, and therefore we may delete 307 from our list. Now either M_{17} is prime or one of the three remaining possibilities divides it. With a little calculation, we can check that M_{17} is divisible by none of 103, 137, and 239; the result: M_{17} is prime.

After giving the eighth perfect number $2^{30}(2^{31} - 1)$, Peter Barlow, in his book *Theory of Numbers* (published in 1811), concludes from its size that it "is the greatest that ever will be discovered; for as they are merely curious, without being useful, it is not likely that any person will ever attempt to find one beyond it." The very least that can be said is that Barlow underestimated obstinate human curiosity. Although the subsequent search for larger perfect numbers provides us with one of the fascinating chapters in the history of mathematics, an extended discussion would be out of place here.

It is worth remarking, however, that the first 12 Mersenne primes (hence, 12 perfect numbers) have been known since 1914. The 11th in order of discovery, namely, M_{89}, was the last Mersenne prime disclosed by hand calculation; its primality was verified by both Powers and Cunningham in 1911, working independently and using different techniques. The prime M_{127} was found by Lucas in 1876 and for the next 75 years was the largest number actually known to be a prime.

Calculations whose mere size and tedium repel the mathematician are just grist for the mill of electronic computers. Starting in 1952, 22 additional Mersenne primes (all huge) have come to light. The 25th Mersenne prime, M_{21701}, was discovered in 1978 by two 18-year-old high school students, Laura Nickel and Curt Noll, using 440 hours on a large computer. A few months later, Noll confirmed that M_{23209} is also prime. With the advent of much faster computers, even this record prime did not stand for long.

During the last 10 years, a flurry of computer activity confirmed the primality of nine more Mersenne numbers, each in turn becoming the largest number currently known to be prime. (In the never-ending pursuit of bigger and bigger primes, the record holder has usually been a Mersenne number.) Forty-one Mersenne primes have been identified. The most recent is $M_{24036583}$, discovered in 2004. It has 7235733 decimal digits, nearly a million more than the previous largest known prime, the 6320430-digit $M_{20996011}$. The year-long search for $M_{24036583}$ used the spare time of several hundred thousand volunteers and their computers, each assigned a different set of candidates to test for primality. The newest champion prime gave rise to the 41st even perfect number

$$P_{41} = 2^{24036582}(2^{24036583} - 1)$$

an immense number of 14591877 digits.

It is not likely that every prime in the vast expanse $p < 24036583$ has been tested to see if M_p is prime. One should be wary, for in 1989 a systematic computer search found the overlooked Mersenne prime M_{110503} lurking between M_{86243} and

M_{216091}. What is more probable is that enthusiasts with the time and inclinatio forge on through higher values to new records.

	Mersenne number	Number of digits	Date of discovery
1	$2^2 - 1$	1	unknown
2	$2^3 - 1$	1	unknown
3	$2^5 - 1$	2	unknown
4	$2^7 - 1$	3	unknown
5	$2^{13} - 1$	4	1456
6	$2^{17} - 1$	6	1588
7	$2^{19} - 1$	6	1588
8	$2^{31} - 1$	10	1772
9	$2^{61} - 1$	19	1883
10	$2^{89} - 1$	27	1911
11	$2^{107} - 1$	33	1914
12	$2^{127} - 1$	39	1876
13	$2^{521} - 1$	157	1952
14	$2^{607} - 1$	183	1952
15	$2^{1279} - 1$	386	1952
16	$2^{2203} - 1$	664	1952
17	$2^{2281} - 1$	687	1952
18	$2^{3217} - 1$	969	1957
19	$2^{4253} - 1$	1281	1961
20	$2^{4423} - 1$	1332	1961
21	$2^{9689} - 1$	2917	1963
22	$2^{9941} - 1$	2993	1963
23	$2^{11213} - 1$	3376	1963
24	$2^{19937} - 1$	6002	1971
25	$2^{21701} - 1$	6533	1978
26	$2^{23209} - 1$	6987	1978
27	$2^{44497} - 1$	13395	1979
28	$2^{86243} - 1$	25962	1983
29	$2^{110503} - 1$	33265	1989
30	$2^{132049} - 1$	39751	1983
31	$2^{216091} - 1$	65050	1985
32	$2^{756839} - 1$	227832	1992
33	$2^{859433} - 1$	258716	1994
34	$2^{1257787} - 1$	378632	1996
35	$2^{1398269} - 1$	420921	1996
36	$2^{2976221} - 1$	895932	1996
37	$2^{3021377} - 1$	909526	1998
38	$2^{6972593} - 1$	2098960	1999
39	$2^{13466917} - 1$	4059346	2001
40	$2^{20996011} - 1$	6320430	2003
41	$2^{24036583} - 1$	7235733	2004

An algorithm frequently used for testing the primality of M_p is the Lucas-Le test. It relies on the inductively defined sequence

$$S_1 = 4 \qquad S_{k+1} = S_k^2 - 2 \qquad k \geq 1$$

Thus, the sequence begins with the values 4, 14, 194, 37634, ... The basic theorem, as perfected by Derrick Lehmer in 1930 from the pioneering results of Lucas, is this: For $p > 2$, M_p is prime if and only if $S_{p-1} \equiv 0 \pmod{M_p}$. An equivalent formulation is that M_p is prime if and only if $S_{p-2} \equiv \pm 2^{(p+1)/2} \pmod{M_p}$.

A simple example is provided by the Mersenne number $M_7 = 2^7 - 1 = 127$. Working modulo 127, the computation runs as follows:

$$S_1 \equiv 4 \qquad S_2 \equiv 14 \qquad S_3 \equiv 67 \qquad S_4 \equiv 42 \qquad S_5 \equiv -16 \qquad S_6 \equiv 0$$

This establishes that M_7 is prime.

The largest of the numbers on Mersenne's "original" list, the 78-digit M_{257}, was found to be composite in 1930 when Lehmer succeeded in showing that $S_{256} \not\equiv 0 \pmod{257}$; this arithmetic achievement was announced in print in 1930, although no factor of the number was known. In 1952, the National Bureau of Standards Western Automatic Computer (SWAC) confirmed Lehmer's efforts of 20 years earlier. The electronic computer accomplished in 68 seconds what had taken Lehmer over 700 hours using a calculating machine. The smallest prime factor of M_{257}, namely,

$$535006138814359$$

was obtained in 1979 and the remaining two factors exhibited in 1980, 50 years after the composite nature of the number had been revealed.

For the reader's convenience, we have listed the 41 Mersenne primes, the number of digits in each, and its approximate date of discovery.

Most mathematicians believe that there are infinitely many Mersenne primes, but a proof of this seems hopelessly beyond reach. Known Mersenne primes M_p clearly become more scarce as p increases. It has been conjectured that about two primes M_p should be expected for all primes p in an interval $x < p < 2x$; the numerical evidence tends to support this.

One of the celebrated problems of number theory is whether there exist any odd perfect numbers. Although no odd perfect number has been produced thus far, nonetheless, it is possible to find certain conditions for the existence of odd perfect numbers. The oldest of these we owe to Euler, who proved that if n is an odd perfect number, then

$$n = p^{\alpha} q_1^{2\beta_1} q_2^{2\beta_2} \cdots q_r^{2\beta_r}$$

where $p, q_1, \ldots, q_r$ are distinct odd primes and $p \equiv \alpha \equiv 1 \pmod 4$. In 1937, Steuerwald showed that not all β_i's can be equal to 1; that is, if $n = p^{\alpha} q_1^2 q_2^2 \cdots q_r^2$ is an odd number with $p \equiv \alpha \equiv 1 \pmod 4$, then n is not perfect. Four years later, Kanold established that not all β_i's can be equal to 2, nor is it possible to have one β_i equal to 2 and all the others equal to 1. The last few years have seen further progress: Hagis and McDaniel (1972) found that it is impossible to have $\beta_i = 3$ for all i.

With these comments out of the way, let us prove Euler's result.

Theorem 11.7 Euler. If n is an odd perfect number, then

$$n = p_1^{k_1} p_2^{2j_2} \cdots p_r^{2j_r}$$

where the p_i's are distinct odd primes and $p_1 \equiv k_1 \equiv 1 \pmod 4$.

Proof. Let $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ be the prime factorization of n. Because n is perfect, we can write

$$2n = \sigma(n) = \sigma(p_1^{k_1})\sigma(p_2^{k_2}) \cdots \sigma(p_r^{k_r})$$

Being an odd integer, either $n \equiv 1 \pmod 4$ or $n \equiv 3 \pmod 4$; in any event, $2n \equiv 2 \pmod 4$. Thus, $\sigma(n) = 2n$ is divisible by 2, but not by 4. The implication is that one of the $\sigma(p_i^{k_i})$, say $\sigma(p_1^{k_1})$, must be an even integer (but not divisible by 4), and all the remaining $\sigma(p_i^{k_i})$'s are odd integers.

For a given p_i, there are two cases to be considered: $p_i \equiv 1 \pmod 4$ and $p_i \equiv 3 \pmod 4$. If $p_i \equiv 3 \equiv -1 \pmod 4$, we would have

$$\begin{aligned}\sigma(p_i^{k_i}) &= 1 + p_i + p_i^2 + \cdots + p_i^{k_i} \\ &\equiv 1 + (-1) + (-1)^2 + \cdots + (-1)^{k_i} \pmod 4 \\ &\equiv \begin{cases} 0 \pmod 4 & \text{if } k_i \text{ is odd} \\ 1 \pmod 4 & \text{if } k_i \text{ is even} \end{cases}\end{aligned}$$

Because $\sigma(p_1^{k_1}) \equiv 2 \pmod 4$, this tells us that $p_1 \not\equiv 3 \pmod 4$ or, to put it affirmatively, $p_1 \equiv 1 \pmod 4$. Furthermore, the congruence $\sigma(p_i^{k_i}) \equiv 0 \pmod 4$ signifies that 4 divides $\sigma(p_i^{k_i})$, which is not possible. The conclusion: If $p_i \equiv 3 \pmod 4$, where $i = 2, \ldots, r$, then its exponent k_i is an even integer.

Should it happen that $p_i \equiv 1 \pmod 4$—which is certainly true for $i = 1$—then

$$\begin{aligned}\sigma(p_i^{k_i}) &= 1 + p_i + p_i^2 + \cdots + p_i^{k_i} \\ &\equiv 1 + 1^1 + 1^2 + \cdots + 1^{k_i} \pmod 4 \\ &\equiv k_i + 1 \pmod 4\end{aligned}$$

The condition $\sigma(p_1^{k_1}) \equiv 2 \pmod 4$ forces $k_1 \equiv 1 \pmod 4$. For the other values of i, we know that $\sigma(p_i^{k_i}) \equiv 1$ or $3 \pmod 4$, and therefore $k_i \equiv 0$ or $2 \pmod 4$; in any case, k_i is an even integer. The crucial point is that, regardless of whether $p_i \equiv 1 \pmod 4$ or $p_i \equiv 3 \pmod 4$, k_i is always even for $i \neq 1$. Our proof is now complete.

In view of the preceding theorem, any odd perfect number n can be expressed as

$$\begin{aligned}n &= p_1^{k_1} p_2^{2j_2} \cdots p_r^{2j_r} \\ &= p_1^{k_1} (p_2^{j_2} \cdots p_r^{j_r})^2 \\ &= p_1^{k_1} m^2\end{aligned}$$

This leads directly to the following corollary.

Corollary. If n is an odd perfect number, then n is of the form

$$n = p^k m^2$$

where p is a prime, $p \nmid m$, and $p \equiv k \equiv 1 \pmod 4$; in particular, $n \equiv 1 \pmod 4$.

Proof. Only the last assertion is not obvious. Because $p \equiv 1 \pmod 4$, we have $p^k \equiv 1 \pmod 4$. Notice that m must be odd; hence, $m \equiv 1$ or $3 \pmod 4$, and therefore upon squaring, $m^2 \equiv 1 \pmod 4$. It follows that

$$n = p^k m^2 \equiv 1 \cdot 1 \equiv 1 \pmod 4$$

establishing our corollary.

Another line of investigation involves estimating the size of an odd perfect number n. The classical lower bound was obtained by Turcaninov in 1908: n has at least four distinct prime factors and exceeds $2 \cdot 10^6$. With the advent of electronic computers, the lower bound has been improved to $n > 10^{300}$. Recent investigations have shown that n must be divisible by at least eight distinct primes, the largest of which is greater than 10^7, and the next largest exceeds 10^4; if $3 \nmid n$, then the number of distinct prime factors of n is at least 11.

Although all of this lends support to the belief that there are no odd perfect numbers, only a proof of their nonexistence would be conclusive. We would then be in the curious position of having built up a whole theory for a class of numbers that did not exist. "It must always," wrote the mathematician Joseph Sylvester in 1888, "stand to the credit of the Greek geometers that they succeeded in discovering a class of perfect numbers which in all probability are the only numbers which are perfect."

Another group of numbers that has had a continuous history extended from the early Greeks to the present time comprises the *amicable numbers*. Two numbers such as 220 and 284 are called *amicable*, or friendly, because they have the remarkable property that each number is "contained" within the other, in the sense that each number is equal to the sum of all the positive divisors of the other, not counting the number itself. Thus, as regards the divisors of 220,

$$1 + 2 + 4 + 5 + 10 + 11 + 20 + 22 + 44 + 55 + 110 = 284$$

and for 284,

$$1 + 2 + 4 + 71 + 142 = 220$$

In terms of the σ function, amicable numbers m and n (or an *amicable pair*) are defined by the equations

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

or what amounts to the same thing:

$$\sigma(m) = m + n = \sigma(n)$$

Down through their quaint history, amicable numbers have been important in magic and astrology, and in casting horoscopes, making talismans, and concocting

love potions. The Greeks believed that these numbers had a particular influence in establishing friendships between individuals. The philosopher Iamblichus of Chalcis (ca. A.D. 250–A.D. 330) ascribed a knowledge of the pair 220 and 284 to the Pythagoreans. He wrote:

> They [the Pythagoreans] call certain numbers amicable numbers, adopting virtues and social qualities to numbers, as 284 and 220; for the parts of each have the power to generate the other....

Biblical commentators spotted 220, the lesser of the classical pair, in Genesis 32:14 as numbering Jacob's present to Esau of 200 she-goats and 20 he-goats. According to one commentator, Jacob wisely counted out his gift (a "hidden secret arrangement") to secure the friendship of Esau. An Arab of the 11th century, El Madschriti of Madrid, related that he had put to the test the erotic effect of these numbers by giving someone a confection in the shape of the smaller number, 220, to eat, while he himself ate the larger, 284. He failed, however, to describe whatever success the ceremony brought.

It is a mark of the slow development of number theory that until the 1630s no one had been able to add to the original pair of amicable numbers discovered by the Greeks. The first explicit rule described for finding certain types of amicable pairs is due to Thabit ibn Qurra, an Arabian mathematician of the 9th century. In a manuscript composed at that time, he indicated:

> If the three numbers $p = 3 \cdot 2^{n-1} - 1$, $q = 3 \cdot 2^n - 1$, and $r = 9 \cdot 2^{2n-1} - 1$ are all prime and $n \geq 2$, then $2^n pq$ and $2^n r$ are amicable numbers.

It was not until its rediscovery centuries later by Fermat and Descartes that Thabit's rule produced the second and third pairs of amicable numbers. In a letter to Mersenne in 1636, Fermat announced that 17,296 and 18,416 were an amicable pair, and Descartes wrote to Mersenne in 1638 that he had found the pair 9363584 and 9437056. Fermat's pair resulted from taking $n = 4$ in Thabit's rule ($p = 23$, $q = 47$, $r = 1151$ are all prime) and Descartes' from $n = 7$ ($p = 191$, $q = 383$, $r = 73727$ are all prime).

In the 1700s, Euler drew up at one clip a list of 64 amicable pairs; two of these new pairs were later found to be "unfriendly," one in 1909 and one in 1914. Adrien Marie Legendre, in 1830, found another pair, 2172649216 and 2181168896.

Extensive computer searches have currently revealed more than 50000 amicable pairs, some of them running to 320 digits; these include all those with values less than 10^{11}. It has not yet been established whether the number of amicable pairs is finite or infinite, nor has a pair been produced in which the numbers are relatively prime. What has been proved is that each integer in a pair of relatively prime amicable numbers must be greater than 10^{25}, and their product must be divisible by at least 22 distinct primes. Part of the difficulty is that in contrast with the single formula for generating (even) perfect numbers, there is no known rule for finding all amicable pairs of numbers.

Another inaccessible question, already considered by Euler, is whether there are amicable pairs of opposite parity—that is, with one integer even and the other odd.

"Most" amicable pairs in which both members of the pair are even have their sums divisible by 9. A simple example is $220 + 284 = 504 \equiv 0 \pmod 9$. The smallest known even amicable pair whose sum fails to enjoy this feature is 666030256 and 696630544.

PROBLEMS 11.3

1. Prove that the Mersenne number M_{13} is a prime; hence, the integer $n = 2^{12}(2^{13} - 1)$ is perfect.
   [*Hint:* Because $\sqrt{M_{13}} < 91$, Theorem 11.5 implies that the only candidates for prime divisors of M_{13} are 53 and 79.]
2. Prove that the Mersenne number M_{19} is a prime; hence, the integer $n = 2^{18}(2^{19} - 1)$ is perfect.
   [*Hint:* By Theorems 11.5 and 11.6, the only prime divisors to test are 191, 457, and 647.]
3. Prove that the Mersenne number M_{29} is composite.
4. A positive integer n is said to be a *deficient number* if $\sigma(n) < 2n$ and an *abundant number* if $\sigma(n) > 2n$. Prove each of the following:
   (a) There are infinitely many deficient numbers.
   [*Hint:* Consider the integers $n = p^k$, where p is an odd prime and $k \geq 1$.]
   (b) There are infinitely many even abundant numbers.
   [*Hint:* Consider the integers $n = 2^k \cdot 3$, where $k > 1$.]
   (c) There are infinitely many odd abundant numbers.
   [*Hint:* Consider the integers $n = 945 \cdot k$, where k is any positive integer not divisible by 2, 3, 5, or 7. Because $945 = 3^3 \cdot 5 \cdot 7$, it follows that $\gcd(945, k) = 1$ and so $\sigma(n) = \sigma(945)\sigma(k)$.]
5. Assuming that n is an even perfect number and $d \mid n$, where $1 < d < n$, show that d is deficient.
6. Prove that any multiple of a perfect number is abundant.
7. Confirm that the pairs of integers listed below are amicable:
   (a) $220 = 2^2 \cdot 5 \cdot 11$ and $284 = 2^2 \cdot 71$. (Pythagoras, 500 B.C.)
   (b) $17296 = 2^4 \cdot 23 \cdot 47$ and $18416 = 2^4 \cdot 1151$. (Fermat, 1636)
   (c) $9363584 = 2^7 \cdot 191 \cdot 383$ and $9437056 = 2^7 \cdot 73727$. (Descartes, 1638)
8. For a pair of amicable numbers m and n, prove that

$$\left(\sum_{d \mid m} 1/d\right)^{-1} + \left(\sum_{d \mid n} 1/d\right)^{-1} = 1$$

9. Establish the following statements concerning amicable numbers:
   (a) A prime number cannot be one of an amicable pair.
   (b) The larger integer in any amicable pair is a deficient number.
   (c) If m and n are an amicable pair, with m even and n odd, then n is a perfect square.
   [*Hint:* If p is an odd prime, then $1 + p + p^2 + \cdots + p^k$ is odd only when k is an even integer.]
10. In 1886, a 16-year-old Italian boy announced that $1184 = 2^5 \cdot 37$ and $1210 = 2 \cdot 5 \cdot 11^2$ form an amicable pair of numbers, but gave no indication of the method of discovery. Verify his assertion.

11. Prove "Thabit's rules" for amicable pairs: If $p = 3 \cdot 2^{n-1} - 1$, $q = 3 \cdot 2^n - 1$, and $r = 9 \cdot 2^{2n-1} - 1$ are all prime numbers, where $n \geq 2$, then $2^n pq$ and $2^n r$ are an amicable pair of numbers. This rule produces amicable numbers for $n = 2$, 4, and 7, but for no other $n \leq 20{,}000$.

12. By an *amicable triple* of numbers is meant three integers such that the sum of any two is equal to the sum of the divisors of the remaining integer, excluding the number itself. Verify that $2^5 \cdot 3 \cdot 13 \cdot 293 \cdot 337$, $2^5 \cdot 3 \cdot 5 \cdot 13 \cdot 16561$, and $2^5 \cdot 3 \cdot 13 \cdot 99371$ are an amicable triple.

13. A finite sequence of positive integers is said to be a *sociable chain* if each is the sum of the positive divisors of the preceding integer, excluding the number itself (the last integer is considered as preceding the first integer in the chain). Show that the following integers form a sociable chain:

$$14288, 15472, 14536, 14264, 12496$$

Only two sociable chains were known until 1970, when nine chains of four integers each were found.

14. Prove that

(a) Any odd perfect number n can be represented in the form $n = pa^2$, where p is a prime.

(b) If $n = pa^2$ is an odd perfect number, then $n \equiv p \pmod 8$.

15. If n is an odd perfect number, prove that n has at least three distinct prime factors. [*Hint:* Assume that $n = p^k q^{2j}$, where $p \equiv k \equiv 1 \pmod 4$. Use the inequality $2 = \sigma(n)/n \leq [p/(p-1)][q/(q-1)]$ to reach a contradiction.]

16. If the integer $n > 1$ is a product of distinct Mersenne primes, show that $\sigma(n) = 2^k$ for some k.

11.4 FERMAT NUMBERS

To round out the picture, let us mention another class of numbers that provides a rich source of conjectures, the Fermat numbers. These may be considered as a special case of the integers of the form $2^m + 1$. We observe that if $2^m + 1$ is an odd prime, then $m = 2^n$ for some $n \geq 0$. Assume to the contrary that m had an odd divisor $2k + 1 > 1$, say $m = (2k + 1)r$; then $2^m + 1$ would admit the nontrivial factorization

$$\begin{aligned} 2^m + 1 &= 2^{(2k+1)r} + 1 = (2^r)^{2k+1} + 1 \\ &= (2^r + 1)(2^{2kr} - 2^{(2k-1)r} + \cdots + 2^{2r} - 2^r + 1) \end{aligned}$$

which is impossible. In brief, $2^m + 1$ can be prime only if m is a power of 2.

Definition 11.2. A *Fermat number* is an integer of the form

$$F_n = 2^{2^n} + 1 \qquad n \geq 0$$

If F_n is prime, it is said to be a *Fermat prime*.

Fermat, whose mathematical intuition was usually reliable, observed that all the integers

$$F_0 = 3 \qquad F_1 = 5 \qquad F_2 = 17 \qquad F_3 = 257 \qquad F_4 = 65537$$

are primes and expressed his belief that F_n is prime for each value of n. In writing to Mersenne, he confidently announced: "I have found that numbers of the form $2^{2^n} + 1$ are always prime numbers and have long since signified to analysts the truth of this theorem." However, Fermat bemoaned his inability to come up with a proof and, in subsequent letters, his tone of growing exasperation suggests that he was continually trying to do so. The question was resolved negatively by Euler in 1732 when he found

$$F_5 = 2^{2^5} + 1 = 4294967297$$

to be divisible by 641. To us, such a number does not seem very large; but in Fermat's time, the investigation of its primality was difficult, and obviously he did not carry it out.

The following elementary proof that $641 \mid F_5$ does not explicitly involve division and is due to G. Bennett.

Theorem 11.8. The Fermat number F_5 is divisible by 641.

Proof. We begin by putting $a = 2^7$ and $b = 5$, so that

$$1 + ab = 1 + 2^7 \cdot 5 = 641$$

It is easily seen that

$$1 + ab - b^4 = 1 + (a - b^3)b = 1 + 3b = 2^4$$

But this implies that

$$\begin{aligned} F_5 = 2^{2^5} + 1 &= 2^{32} + 1 \\ &= 2^4 a^4 + 1 \\ &= (1 + ab - b^4)a^4 + 1 \\ &= (1 + ab)a^4 + (1 - a^4 b^4) \\ &= (1 + ab)[a^4 + (1 - ab)(1 + a^2 b^2)] \end{aligned}$$

which gives $641 \mid F_n$.

To this day it is not known whether there are infinitely many Fermat primes or, for that matter, whether there is at least one Fermat prime beyond F_4. The best "guess" is that all Fermat numbers $F_n > F_4$ are composite.

Part of the interest in Fermat primes stems from the discovery that they have a remarkable connection with the ancient problem of determining all regular polygons that can be constructed with ruler and compass alone (where the former is used only to draw straight lines and the latter only to draw arcs). In the seventh and last section of the *Disquisitiones Arithmeticae*, Gauss proved that a regular polygon of n sides is so constructible if and only if either

$$n = 2^k \qquad \text{or} \qquad n = 2^k p_1 p_2 \cdots p_r$$

where $k \geq 0$ and $p_1, p_2, \ldots, p_r$ are distinct Fermat primes. The construction of regular polygons of 2^k, $2^k \cdot 3$, $2^k \cdot 5$ and $2^k \cdot 15$ sides had been known since the time of the Greek geometers. In particular, they could construct regular n-sided polygons

for $n = 3, 4, 5, 6, 8, 10, 12, 15$, and 16. What no one suspected before Gauss was that a regular 17-sided polygon can also be constructed by ruler and compass. Gauss was so proud of his discovery that he requested that a regular polygon of 17 sides be engraved on his tombstone; for some reason, this wish was never fulfilled, but such a polygon is inscribed on the side of a monument to Gauss erected in Brunswick, Germany, his birthplace.

A useful property of Fermat numbers is that they are relatively prime to each other.

Theorem 11.9. For Fermat numbers F_n and F_m, where $m > n \geq 0$, $\gcd(F_m, F_n) = 1$.

Proof. Put $d = \gcd(F_m, F_n)$. Because Fermat numbers are odd integers, d must be odd. If we set $x = 2^{2^n}$ and $k = 2^{m-n}$, then

$$\frac{F_m - 2}{F_n} = \frac{(2^{2^n})^{2^{m-n}} - 1}{2^{2^n} + 1}$$

$$= \frac{x^k - 1}{x + 1} = x^{k-1} - x^{k-2} + \cdots - 1$$

whence $F_n \mid (F_m - 2)$. From $d \mid F_n$, it follows that $d \mid (F_m - 2)$. Now use the fact that $d \mid F_m$ to obtain $d \mid 2$. But d is an odd integer, and so $d = 1$, establishing the result claimed.

This leads to a pleasant little proof of the infinitude of primes. We know that each of the Fermat numbers $F_0, F_1, \ldots, F_n$ is divisible by a prime that, according to Theorem 11.9, does not divide any of the other F_k. Thus, there are at least $n + 1$ distinct primes not exceeding F_n. Because there are infinitely many Fermat numbers, the number of primes is also infinite.

In 1877, the Jesuit priest T. Pepin devised the practical test (Pepin's test) for determining the primality of F_n that is embodied in the following theorem.

Theorem 11.10 Pepin's test. For $n \geq 1$, the Fermat number $F_n = 2^{2^n} + 1$ is prime if and only if

$$3^{(F_n - 1)/2} \equiv -1 \pmod{F_n}$$

Proof. First let us assume that

$$3^{(F_n - 1)/2} \equiv -1 \pmod{F_n}$$

Upon squaring both sides, we get

$$3^{F_n - 1} \equiv 1 \pmod{F_n}$$

The same congruence holds for any prime p that divides F_n:

$$3^{F_n - 1} \equiv 1 \pmod{p}$$

Now let k be the order of 3 modulo p. Theorem 8.1 indicates that $k \mid F_n - 1$, or in other words, that $k \mid 2^{2^n}$; therefore k must be a power of 2.

It is not possible that $k = 2^r$ for any $r \leq 2^n - 1$. For if this were so, repeated squaring of the congruence $3^k \equiv 1 \pmod{p}$ would yield

$$3^{2^{2^n-1}} \equiv 1 \pmod{p}$$

or, what is the same thing,

$$3^{(F_n-1)/2} \equiv 1 \pmod{p}$$

We would then arrive at $1 \equiv -1 \pmod{p}$, resulting in $p = 2$, which is a contradiction. Thus the only possibility open to us is that

$$k = 2^{2^n} = F_n - 1$$

Fermat's theorem tells us now that $k \leq p - 1$, which means, in turn, that $F_n = k + 1 \leq p$. Because $p \mid F_n$, we also have $p \leq F_n$. Together these inequalities mean that $F_n = p$, so that F_n is a prime.

On the other hand, suppose that F_n, $n \geq 1$, is prime. The Quadratic Reciprocity Law gives

$$(3/F_n) = (F_n/3) = (2/3) = -1$$

when we use the fact that $F_n \equiv (-1)^{2^n} + 1 = 2 \pmod{3}$. Applying Euler's Criterion, we end up with

$$3^{(F_n-1)/2} \equiv -1 \pmod{F_n}$$

Let us demonstrate the primality of $F_3 = 257$ using Pepin's test. Working modulo 257, we have

$$\begin{aligned} 3^{(F_3-1)/2} &= 3^{128} = 3^3(3^5)^{25} \\ &\equiv 27(-14)^{25} \\ &\equiv 27 \cdot 14^{24}(-14) \\ &\equiv 27(17)(-14) \\ &\equiv 27 \cdot 19 \equiv 513 \equiv -1 \pmod{257} \end{aligned}$$

so that F_3 is prime.

We have already observed that Euler proved the Fermat number F_5 to be composite, with the factorization $F_5 = 2^{32} + 1 = 641 \cdot 6700417$. As for F_6, in 1880, F. Landry announced that

$$\begin{aligned} F_6 &= 2^{64} + 1 \\ &= 274177 \cdot 67280421310721 \end{aligned}$$

This accomplishment is all the more remarkable when we consider that Landry was 82 years old at the time. Landry never published an account of his work on factoring F_6, but it is unlikely that he resorted to the process of trial division; for, several years earlier, he had estimated that any attempt to show the primality of F_6 by testing numbers of the form $128k + 1$ could take up to 3000 years.

In 1905, J. C. Morehead and A. E. Western independently performed Pepin's test on F_7 and communicated its composite character almost simultaneously. It took

66 years, until 1971, before Brillhart and Morrison discovered the prime factorization

$$\begin{aligned} F_7 &= 2^{128} + 1 \\ &= 59649589127497217 \cdot 5704689200685129054721 \end{aligned}$$

(The possibility of arriving at such a factorization without recourse to fast computers with large memories is remote.) Morehead and Western carried out (in 1909) a similar calculation for the compositeness of F_8, each doing half the work; but the actual factors were not found until 1980, when Brent and Pollard showed the smallest prime divisor of F_8 to be

$$1238926361552897$$

The other factor of F_8 is 62 digits long, and shortly afterward was shown to be prime. A large F_n to which Pepin's test has been applied is F_{14}, a number of 4933 digits; this Fermat number was determined to be composite by Selfridge and Hurwitz in 1963, although at present no divisor is known.

Our final theorem, due to Euler and Lucas, is a valuable aid in determining the divisors of Fermat numbers. As early as 1747, Euler established that every prime factor of F_n must be of the form $k \cdot 2^{n+1} + 1$; over 100 years later, in 1879, the French number theorist Edouard Lucas improved upon this result by showing that k can be taken to be even. From this, we have the following theorem.

Theorem 11.11. Any prime divisor p of the Fermat number $F_n = 2^{2^n} + 1$, where $n \geq 2$, is of the form $p = k \cdot 2^{n+2} + 1$.

Proof. For a prime divisor p of F_n,

$$2^{2^n} \equiv -1 \pmod{p}$$

which is to say, upon squaring, that

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

If h is the order of 2 modulo p, this congruence tells us that

$$h \mid 2^{n+1}$$

We cannot have $h = 2^r$ where $1 \leq r \leq n$, for this would lead to

$$2^{2^n} \equiv 1 \pmod{p}$$

and, in turn, to the contradiction that $p = 2$. This lets us conclude that $h = 2^{n+1}$. Because the order of 2 modulo p divides $\phi(p) = p - 1$, we may further conclude that $2^{n+1} \mid p - 1$. The point is that for $n \geq 2$, $p \equiv 1 \pmod{8}$, and therefore, by Theorem 9.6, the Legendre symbol $(2/p) = 1$. Using Euler's criterion, we immediately pass to

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

An appeal to Theorem 8.1 finishes the proof; it asserts that $h \mid (p-1)/2$, or equivalently, $2^{n+1} \mid (p-1)/2$. This forces $2^{n+2} \mid p - 1$, and we obtain $p = k \cdot 2^{n+2} + 1$ for some integer k.

Theorem 11.11 enables us to determine quickly the nature of $F_4 = 2^{16} + 1 = 65537$. The prime divisors of F_4 must take the form $2^6k + 1 = 64k + 1$. There is only one prime of this kind that is less than or equal to $\sqrt{F_4}$, namely, the prime 193. Because this trial divisor fails to be a factor of F_4, we may conclude that F_4 is itself a prime.

The increasing power and availability of computing equipment has allowed the search for prime factors of the Fermat numbers to be extended significantly. For example, the first prime factor of F_{28} was found in 1997. It is now known that F_n is composite for $5 \leq n \leq 30$, and for some 140 additional values of n. The largest composite Fermat number found to date is F_{303088}, with divisor $3 \cdot 2^{303093} + 1$.

The complete prime factorization of F_n has been obtained for $5 \leq n \leq 11$ and no other n. After the factorization of F_8, it was little suspected that F_{11}, 629 digits long, would be the next Fermat number to be completely factored; but this was carried out by Brent and Morain in 1988. The factorization of the 155-digit F_9 by the joint efforts of Lenstra, Manasse, and Pollard in 1990 was noteworthy for having employed approximately 700 workstations at various locations around the world. The complete factorization took about 4 months. Not long thereafter (1996), Brent determined the remaining two prime factors of the 310-digit F_{10}. The reason for arriving at the factorization of F_{11} before that of F_9 and F_{10} was that size of the second-largest prime factor of F_{11} made the calculations much easier. The second-largest prime factor of F_{11} contains 22 digits, whereas those of F_9 and F_{10} have lengths of 49 and 40 digits, respectively.

The enormous F_{31}, with a decimal expansion of over 600 million digits, was proved to be composite in 2001. It was computationally fortunate that F_{31} had a prime factor of only 23 digits. For F_{33}, the challenge remains: it is the smallest Fermat number whose character is in doubt. Considering that F_{33} has more than two trillion digits, the matter may not be settled for some time.

A resume of the current primality status for the Fermat numbers F_n, where $0 \leq n \leq 33$, is given below.

n	Character of F_n
0, 1, 2, 3, 4	prime
5, 6, 7, 8, 9, 10, 11	completely factored
12, 13, 15, 16, 18, 19, 25, 27, 30	two or more prime factors known
17, 21, 23, 26, 28, 29, 31, 32	only one prime factor known
14, 20, 22, 24	composite, but no factor known
33	character unknown

The case for F_{16} was settled in 1953 and lays to rest the tantalizing conjecture that all the terms of the sequence

$$2 + 1, 2^2 + 1, 2^{2^2} + 1, 2^{2^{2^2}} + 1, 2^{2^{2^{2^2}}} + 1, \ldots$$

are prime numbers. What is interesting is that none of the known prime factors p of a Fermat number F_n gives rise to a square factor p^2; indeed, it is speculated that the Fermat numbers are square-free. This is in contrast to the Mersenne numbers where, for example, 9 divides M_{6n}.

Numbers of the form $k \cdot 2^n + 1$, which occur in the search for prime factors of Fermat numbers, are of considerable interest in their own right. The smallest n for which $k \cdot 2^n + 1$ is prime may be quite large in some cases; for instance, the first time $47 \cdot 2^n + 1$ is prime is when $n = 583$. But there also exist values of k such that $k \cdot 2^n + 1$ is always composite. Indeed, in 1960 it was proved that there exist infinitely many odd integers k with $k \cdot 2^n + 1$ composite for all $n \geq 1$. The problem of determining the least such value of k remains unsolved. Up to now, $k = 78557$ is the smallest known k for which $k \cdot 2^n + 1$ is never prime for any n.

PROBLEMS 11.4

1. By taking fourth powers of the congruence $5 \cdot 2^7 \equiv -1 \pmod{641}$, deduce that $2^{32} + 1 \equiv 0 \pmod{641}$; hence, $641 \mid F_5$.

2. Gauss (1796) discovered that a regular polygon with p sides, where p is a prime, can be constructed with ruler and compass if and only if $p - 1$ is a power of 2. Show that this condition is equivalent to requiring that p be a Fermat prime.

3. For $n > 0$, prove the following:

(a) There are infinitely many composite numbers of the form $2^{2^n} + 3$.
[*Hint:* Use the fact that $2^{2n} = 3k + 1$ for some k to establish that $7 \mid 2^{2^{2n+1}} + 3$.]

(b) Each of the numbers $2^{2^n} + 5$ is composite.

4. Composite integers n for which $n \mid 2^n - 2$ are called *pseudoprimes*. Show that every Fermat number F_n is either a prime or a pseudoprime.
[*Hint:* Raise the congruence $2^{2^n} \equiv -1 \pmod{F_n}$ to the $2^{2^n - n}$ power.]

5. For $n \geq 2$, show that the last digit of the Fermat number $F_n = 2^{2^n} + 1$ is 7.
[*Hint:* By induction on n, verify that $2^{2^n} \equiv 6 \pmod{10}$ for $n \geq 2$.]

6. Establish that $2^{2^n} - 1$ has at least n distinct prime divisors.
[*Hint:* Use induction on n and the fact that

$$2^{2^n} - 1 = (2^{2^{n-1}} + 1)(2^{2^{n-1}} - 1).]$$

7. In 1869, Landry wrote: "No one of our numerous factorizations of the numbers $2^n \pm 1$ gave us as much trouble and labor as that of $2^{58} + 1$." Verify that $2^{58} + 1$ can be factored rather easily using the identity

$$4x^4 + 1 = (2x^2 - 2x + 1)(2x^2 + 2x + 1)$$

8. From Problem 5, conclude the following:

(a) The Fermat number F_n is never a perfect square.

(b) For $n > 0$, F_n is never a triangular number.

9. (a) For any odd integer n, show that $3 \mid 2^n + 1$.

(b) Prove that if p and q are both odd primes and $q \mid 2^p + 1$, then either $q = 3$ or $q = 2kp + 1$ for some integer k.
[*Hint:* Because $2^{2p} \equiv 1 \pmod{q}$, the order of 2 modulo q is either 2 or $2p$; in the latter case, $2p \mid \phi(q)$.]

(c) Find the smallest prime divisor $q > 3$ of each of the integers $2^{29} + 1$ and $2^{41} + 1$.

10. Determine the smallest odd integer $n > 1$ such that $2^n - 1$ is divisible by a pair of twin primes p and q, where $3 < p < q$.
[*Hint:* Being the first member of a pair of twin primes, $p \equiv -1 \pmod 6$. Because $(2/p) = (2/q) = 1$, Theorem 9.6 gives $p \equiv q \equiv \pm 1 \pmod 8$; hence, $p \equiv -1 \pmod{24}$ and $q \equiv 1 \pmod{24}$. Now use the fact that the orders of 2 modulo p and q must divide n.]

11. Find all prime numbers p such that p divides $2^p + 1$; do the same for $2^p - 1$.

12. Let $p = 3 \cdot 2^n + 1$ be a prime, where $n \geq 1$. (Twenty-nine primes of this form are currently known, the smallest occurring when $n = 1$ and the largest when $n = 303093$.) Prove each of the following assertions:
(a) The order of 2 modulo p is either 3, 2^k or $3 \cdot 2^k$ for some $0 \leq k \leq n$.
(b) Except when $p = 13$, 2 is not a primitive root of p.
[*Hint:* If 2 is a primitive root of p, then $(2/p) = -1$.]
(c) The order of 2 modulo p is not divisible by 3 if and only if p divides a Fermat number F_k with $0 \leq k \leq n - 1$.
[*Hint:* Use the identity $2^{2^k} - 1 = F_0 F_1 F_2 \ldots F_{k-1}$.]
(d) There is no Fermat number that is divisible by 7, 13, or 97.

13. For any Fermat number $F_n = 2^{2^n} + 1$ with $n > 0$, establish that $F_n \equiv 5$ or $8 \pmod 9$ according as n is odd or even.
[*Hint:* Use induction to show, first, that $2^{2^n} \equiv 2^{2^{n-2}} \pmod 9$ for $n \geq 3$.]

14. Use the fact that the prime divisors of F_5 are of the form $2^7 k + 1 = 128k + 1$ to confirm that $641 \mid F_5$.

15. For any prime $p > 3$, prove the following:
(a) $\frac{1}{3}(2^p + 1)$ is not divisible by 3.
[*Hint:* Consider the identity

$$\frac{2^p + 1}{2 + 1} = 2^{p-1} - 2^{p-2} + \cdots - 2 + 1.]$$

(b) $\frac{1}{3}(2^p + 1)$ has a prime divisor greater than p.
[*Hint:* Problem 9(b).]
(c) The integers $\frac{1}{3}(2^{19} + 1)$ and $\frac{1}{3}(2^{23} + 1)$ are both prime.

16. From the previous problem, deduce that there are infinitely many prime numbers.

17. (a) Prove that 3, 5, and 7 are quadratic nonresidues of any Fermat prime F_n, where $n \geq 2$.
[*Hint:* Pepin's test and Problem 15, Section 9.3.]
(b) Show that every quadratic nonresidue of a Fermat prime F_n is a primitive root of F_n.

18. Establish that any Fermat prime F_n can be written as the difference of two squares, but not of two cubes.
[*Hint:*

$$F_n = 2^{2^n} + 1 = (2^{2^n - 1} + 1)^2 - (2^{2^n - 1})^2.]$$

19. For $n \geq 1$, show that $\gcd(F_n, n) = 1$.
[*Hint:* Theorem 11.11.]

20. Use Theorems 11.9 and 11.11 to deduce that there are infinitely many primes of the form $4k + 1$.

CHAPTER 12

CERTAIN NONLINEAR DIOPHANTINE EQUATIONS

He who seeks for methods without having a definite problem in mind seeks for the most part in vain.
D. HILBERT

12.1 THE EQUATION $x^2 + y^2 = z^2$

Fermat, whom many regard as a father of modern number theory, nevertheless, had a custom peculiarly ill-suited to this role. He published very little personally, preferring to communicate his discoveries in letters to friends (usually with no more than the terse statement that he possessed a proof) or to keep them to himself in notes. A number of such notes were jotted down in the margin of his copy of Bachet's translation of Diophantus's *Arithmetica*. By far the most famous of these marginal comments is the one—presumably written about 1637—which states:

> It is impossible to write a cube as a sum of two cubes, a fourth power as a sum of two fourth powers, and, in general, any power beyond the second as a sum of two similar powers. For this, I have discovered a truly wonderful proof, but the margin is too small to contain it.

In this tantalizing aside, Fermat was simply asserting that, if $n > 2$, then the Diophantine equation

$$x^n + y^n = z^n$$

has no solution in the integers, other than the trivial solutions in which at least one of the variables is zero.

The quotation just cited has come to be known as Fermat's Last Theorem or, more accurately, Fermat's conjecture. By the 1800s, all the assertions appearing in the margin of his *Arithmetica* had either been proved or refuted—with the one exception of the Last Theorem (hence the name). The claim has fascinated many generations of mathematicians, professional and amateur alike, because it is so simple to understand yet so difficult to establish. If Fermat really did have a "truly wonderful proof," it has never come to light. Whatever demonstration he thought he possessed very likely contained a flaw. Indeed, Fermat himself may have subsequently discovered the error, for there is no reference to the proof in his correspondence with other mathematicians.

Fermat did, however, leave a proof of his Last Theorem for the case $n = 4$. To carry through the argument, we first undertake the task of identifying all solutions in the positive integers of the equation

$$x^2 + y^2 = z^2 \tag{1}$$

Because the length z of the hypotenuse of a right triangle is related to the lengths x and y of the sides by the famous Pythagorean equation $x^2 + y^2 = z^2$, the search for all positive integers that satisfy Eq. (1) is equivalent to the problem of finding all right triangles with sides of integral length. The latter problem was raised in the days of the Babylonians and was a favorite with the ancient Greek geometers. Pythagoras himself has been credited with a formula for infinitely many such triangles, namely,

$$x = 2n + 1 \qquad y = 2n^2 + 2n \qquad z = 2n^2 + 2n + 1$$

where n is an arbitrary positive integer. This formula does not account for all right triangles with integral sides, and it was not until Euclid wrote his *Elements* that a complete solution to the problem appeared.

The following definition gives us a concise way of referring to the solutions of Eq. (1).

Definition 12.1. A *Pythagorean triple* is a set of three integers x, y, z such that $x^2 + y^2 = z^2$; the triple is said to be *primitive* if $\gcd(x, y, z) = 1$.

Perhaps the best-known examples of primitive Pythagorean triples are 3, 4, 5 and 5, 12, 13, whereas a less obvious one is 12, 35, 37.

There are several points that need to be noted. Suppose that x, y, z is any Pythagorean triple and $d = \gcd(x, y, z)$. If we write $x = dx_1$, $y = dy_1$, $z = dz_1$, then it is easily seen that

$$x_1^2 + y_1^2 = \frac{x^2 + y^2}{d^2} = \frac{z^2}{d^2} = z_1^2$$

with $\gcd(x_1, y_1, z_1) = 1$. In short, x_1, y_1, z_1 form a primitive Pythagorean triple. Thus, it is enough to occupy ourselves with finding all primitive Pythagorean triples; any Pythagorean triple can be obtained from a primitive one upon multiplying by a suitable nonzero integer. The search may be confined to those primitive Pythagorean

triples x, y, z in which $x > 0$, $y > 0$, $z > 0$, inasmuch as all others arise from the positive ones through a simple change of sign.

Our development requires two preparatory lemmas, the first of which sets forth a basic fact regarding primitive Pythagorean triples.

Lemma 1. If x, y, z is a primitive Pythagorean triple, then one of the integers x or y is even, while the other is odd.

Proof. If x and y are both even, then $2 \mid (x^2 + y^2)$ or $2 \mid z^2$, so that $2 \mid z$. The inference is that $\gcd(x, y, z) \geq 2$, which we know to be false. If, on the other hand, x and y should both be odd, then $x^2 \equiv 1 \pmod 4$ and $y^2 \equiv 1 \pmod 4$, leading to

$$z^2 = x^2 + y^2 \equiv 2 \pmod 4$$

But this is equally impossible, because the square of any integer must be congruent either to 0 or to 1 modulo 4.

Given a primitive Pythagorean triple x, y, z, exactly one of these integers is even, the other two being odd (if x, y, z were all odd, then $x^2 + y^2$ would be even, whereas z^2 is odd). The foregoing lemma indicates that the even integer is either x or y; to be definite, we shall hereafter write our Pythagorean triples so that x is even and y is odd; then, of course, z is odd.

It is worth noticing (and we will use this fact) that each pair of the integers x, y, and z must be relatively prime. Were it the case that $\gcd(x, y) = d > 1$, then there would exist a prime p with $p \mid d$. Because $d \mid x$ and $d \mid y$, we would have $p \mid x$ and $p \mid y$, whence $p \mid x^2$ and $p \mid y^2$. But then $p \mid (x^2 + y^2)$, or $p \mid z^2$, giving $p \mid z$. This would conflict with the assumption that $\gcd(x, y, z) = 1$, and so $d = 1$. In like manner, one can verify that $\gcd(y, z) = \gcd(x, z) = 1$.

By virtue of Lemma 1, there exists no primitive Pythagorean triple x, y, z all of whose values are prime numbers. There are primitive Pythagorean triples in which z and one of x or y is a prime; for instance, 3, 4, 5; 11, 60, 61; and 19, 180, 181. It is unknown whether there exist infinitely many such triples.

The next hurdle that stands in our way is to establish that if a and b are relatively prime positive integers having a square as their product, then a and b are themselves squares. With an assist from the Fundamental Theorem of Arithmetic, we can prove considerably more, to wit, Lemma 2.

Lemma 2. If $ab = c^n$, where $\gcd(a, b) = 1$, then a and b are nth powers; that is, there exist positive integers a_1, b_1 for which $a = a_1^n$, $b = b_1^n$.

Proof. There is no harm in assuming that $a > 1$ and $b > 1$. If

$$a = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r} \qquad b = q_1^{j_1} q_2^{j_2} \cdots q_s^{j_s}$$

are the prime factorizations of a and b, then, bearing in mind that $\gcd(a, b) = 1$, no p_i can occur among the q_i. As a result, the prime factorization of ab is given by

$$ab = p_1^{k_1} \cdots p_r^{k_r} q_1^{j_1} \cdots q_s^{j_s}$$

Let us suppose that c can be factored into primes as $c = u_1^{l_1} u_2^{l_2} \cdots u_t^{l_t}$. Then the condition $ab = c^n$ becomes

$$p_1^{k_1} \cdots p_r^{k_r} q_1^{j_1} \cdots q_s^{j_s} = u_1^{nl_1} \cdots u_t^{nl_t}$$

From this we see that the primes $u_1, \ldots, u_t$ are $p_1, \ldots, p_r, q_1, \ldots, q_s$ (in some order) and $nl_1, \ldots, nl_t$ are the corresponding exponents $k_1, \ldots, k_r, j_1, \ldots, j_s$. The conclusion: Each of the integers k_i and j_i must be divisible by n. If we now put

$$a_1 = p_1^{k_1/n} p_2^{k_2/n} \cdots p_r^{k_r/n}$$
$$b_1 = q_1^{j_1/n} q_2^{j_2/n} \cdots q_s^{j_s/n}$$

then $a_1^n = a$, $b_1^n = b$, as desired.

With the routine work now out of the way, the characterization of all primitive Pythagorean triples is fairly straightforward.

Theorem 12.1. All the solutions of the Pythagorean equation

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

satisfying the conditions

$$\gcd(x, y, z) = 1 \qquad 2 \mid x \qquad x > 0, y > 0, z > 0$$

are given by the formulas

$$x = 2st \qquad y = s^2 - t^2 \qquad z = s^2 + t^2$$

for integers $s > t > 0$ such that $\gcd(s, t) = 1$ and $s \not\equiv t \pmod 2$.

Proof. To start, let x, y, z be a (positive) primitive Pythagorean triple. Because we have agreed to take x even, and y and z both odd, $z - y$ and $z + y$ are even integers; say, $z - y = 2u$ and $z + y = 2v$. Now the equation $x^2 + y^2 = z^2$ may be rewritten as

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

whence

$$\left(\frac{x}{2}\right)^2 = \left(\frac{z - y}{2}\right)\left(\frac{z + y}{2}\right) = uv$$

Notice that u and v are relatively prime; indeed, if $\gcd(u, v) = d > 1$, then $d \mid (u - v)$ and $d \mid (u + v)$, or equivalently, $d \mid y$ and $d \mid z$, which violates the fact that $\gcd(y, z) = 1$. Taking Lemma 2 into consideration, we may conclude that u and v are each perfect squares; to be specific, let

$$u = t^2 \qquad v = s^2$$

where s and t are positive integers. The result of substituting these values of u and v reads

$$z = v + u = s^2 + t^2$$
$$y = v - u = s^2 - t^2$$
$$x^2 = 4vu = 4s^2t^2$$

or, in the last case $x = 2st$. Because a common factor of s and t divides both y and z, the condition $\gcd(y, z) = 1$ forces $\gcd(s, t) = 1$. It remains for us to observe that if s and t were both even, or both odd, then this would make each of y and z even, which is an impossibility. Hence, exactly one of the pair s, t is even, and the other is odd; in symbols, $s \not\equiv t \pmod 2$.

Conversely, let s and t be two integers subject to the conditions described before. That $x = 2st$, $y = s^2 - t^2$, $z = s^2 + t^2$ form a Pythagorean triple follows from the easily verified identity

$$x^2 + y^2 = (2st)^2 + (s^2 - t^2)^2 = (s^2 + t^2)^2 = z^2$$

To see that this triple is primitive, we assume that $\gcd(x, y, z) = d > 1$ and take p to be any prime divisor of d. Observe that $p \neq 2$, because p divides the odd integer z (one of s and t is odd, and the other is even, hence, $s^2 + t^2 = z$ must be odd). From $p \mid y$ and $p \mid z$, we obtain $p \mid (z + y)$ and $p \mid (z - y)$, or put otherwise, $p \mid 2s^2$ and $p \mid 2t^2$. But then $p \mid s$ and $p \mid t$, which is incompatible with $\gcd(s, t) = 1$. The implication of all this is that $d = 1$ and so x, y, z constitutes a primitive Pythagorean triple. Theorem 12.1 is thus proven.

The table below lists some primitive Pythagorean triples arising from small values of s and t. For each value of $s = 2, 3, \ldots, 7$, we have taken those values of t that are relatively prime to s, less than s, and even whenever s is odd.

		x	y	z
s	t	$(2st)$	$(s^2 - t^2)$	$(s^2 + t^2)$
2	1	4	3	5
3	2	12	5	13
4	1	8	15	17
4	3	24	7	25
5	2	20	21	29
5	4	40	9	41
6	1	12	35	37
6	5	60	11	61
7	2	28	45	53
7	4	56	33	65
7	6	84	13	85

From this, or from a more extensive table, the reader might be led to suspect that if x, y, z is a primitive Pythagorean triple, then exactly one of the integers x or y is divisible by 3. This is, in fact, the case. For, by Theorem 12.1, we have

$$x = 2st \qquad y = s^2 - t^2 \qquad z = s^2 + t^2$$

where $\gcd(s, t) = 1$. If either $3 \mid s$ or $3 \mid t$, then evidently $3 \mid x$, and we need go no further. Suppose that $3 \nmid s$ and $3 \nmid t$. Fermat's theorem asserts that

$$s^2 \equiv 1 \pmod 3 \qquad t^2 \equiv 1 \pmod 3$$

and so

$$y = s^2 - t^2 \equiv 0 \pmod 3$$

In other words, y is divisible by 3, which is what we were required to show.

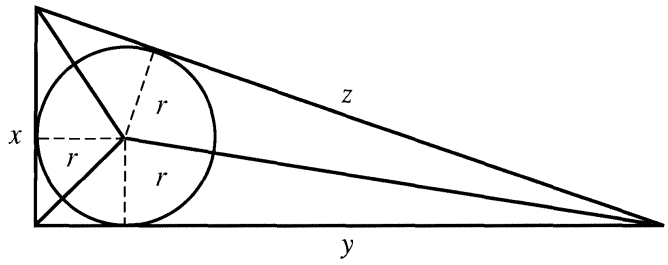
Let us define a *Pythagorean triangle* to be a right triangle whose sides are of integral length. Our findings lead to an interesting geometric fact concerning Pythagorean triangles, recorded as Theorem 12.2.

Theorem 12.2. The radius of the inscribed circle of a Pythagorean triangle is always an integer.

Proof. Let r denote the radius of the circle inscribed in a right triangle with hypotenuse of length z and sides of lengths x and y. The area of the triangle is equal to the sum of the areas of the three triangles having common vertex at the center of the circle; hence,

$$\frac{1}{2}xy = \frac{1}{2}rx + \frac{1}{2}ry + \frac{1}{2}rz = \frac{1}{2}r(x + y + z)$$

The situation is illustrated below:



Now $x^2 + y^2 = z^2$. But we know that the positive integral solutions of this equation are given by

$$x = 2kst \qquad y = k(s^2 - t^2) \qquad z = k(s^2 + t^2)$$

for an appropriate choice of positive integers k, s, t. Replacing x, y, z in the equation $xy = r(x + y + z)$ by these values and solving for r, it will be found that

$$\begin{aligned} r &= \frac{2k^2st(s^2 - t^2)}{k(2st + s^2 - t^2 + s^2 + t^2)} \\ &= \frac{kt(s^2 - t^2)}{s + t} \\ &= kt(s - t) \end{aligned}$$

which is an integer.

We take the opportunity to mention another result relating to Pythagorean triangles. Notice that it is possible for different Pythagorean triangles to have the same area; for instance, the right triangles associated with the primitive Pythagorean triples 20, 21, 29 and 12, 35, 37 each have an area equal to 210. Fermat proved: For any integer $n > 1$, there exist n Pythagorean triangles with different hypotenuses and the same area. The details of this are omitted.

PROBLEMS 12.1

1. (a) Find three different Pythagorean triples, not necessarily primitive, of the form $16, y, z$.

(b) Obtain all primitive Pythagorean triples x, y, z in which $x = 40$; do the same for $x = 60$.

2. If x, y, z is a primitive Pythagorean triple, prove that $x + y$ and $x - y$ are congruent modulo 8 to either 1 or 7.

3. (a) Prove that if $n \not\equiv 2 \pmod 4$, then there is a primitive Pythagorean triple x, y, z in which x or y equals n.

(b) If $n \geq 3$ is arbitrary, find a Pythagorean triple (not necessarily primitive) having n as one of its members.

[*Hint:* Assuming n is odd, consider the triple $n, \frac{1}{2}(n^2 - 1), \frac{1}{2}(n^2 + 1)$; for n even, consider the triple $n, (n^2/4) - 1, (n^2/4) + 1$.]

4. Prove that in a primitive Pythagorean triple x, y, z, the product xy is divisible by 12, hence $60 \mid xyz$.

5. For a given positive integer n, show that there are at least n Pythagorean triples having the same first member.

[*Hint:* Let $y_k = 2^k(2^{2n-2k} - 1)$ and $z_k = 2^k(2^{2n-2k} + 1)$ for $k = 0, 1, 2, \ldots, n - 1$. Then $2^{n+1}, y_k, z_k$ are all Pythagorean triples.]

6. Verify that 3, 4, 5 is the only primitive Pythagorean triple involving consecutive positive integers.

7. Show that $3n, 4n, 5n$ where $n = 1, 2, \ldots$ are the only Pythagorean triples whose terms are in arithmetic progression.

[*Hint:* Call the triple in question $x - d, x, x + d$, and solve for x in terms of d.]

8. Find all Pythagorean triangles whose areas are equal to their perimeters.

[*Hint:* The equations $x^2 + y^2 = z^2$ and $x + y + z = \frac{1}{2}xy$ imply that $(x - 4)(y - 4) = 8$.]

9. (a) Prove that if x, y, z is a primitive Pythagorean triple in which x and z are consecutive positive integers, then

$$x = 2t(t + 1) \qquad y = 2t + 1 \qquad z = 2t(t + 1) + 1$$

for some $t > 0$.

[*Hint:* The equation $1 = z - x = s^2 + t^2 - 2st$ implies that $s - t = 1$.]

(b) Prove that if x, y, z is a primitive Pythagorean triple in which the difference $z - y = 2$, then

$$x = 2t \qquad y = t^2 - 1 \qquad z = t^2 + 1$$

for some $t > 1$.

10. Show that there exist infinitely many primitive Pythagorean triples x, y, z whose even member x is a perfect square.

[*Hint:* Consider the triple $4n^2, n^4 - 4, n^4 + 4$, where n is an arbitrary odd integer.]

11. For an arbitrary positive integer n, show that there exists a Pythagorean triangle the radius of whose inscribed circle is n.

[*Hint:* If r denotes the radius of the circle inscribed in the Pythagorean triangle having sides a and b and hypotenuse c, then $r = \frac{1}{2}(a + b - c)$. Now consider the triple $2n + 1$, $2n^2 + 2n, 2n^2 + 2n + 1$.]

12. (a) Establish that there exist infinitely many primitive Pythagorean triples x, y, z in which x and y are consecutive positive integers. Exhibit five of these.

[*Hint:* If $x, x + 1, z$ forms a Pythagorean triple, then so does the triple $3x + 2z + 1$, $3x + 2z + 2, 4x + 3z + 2$.]

(b) Show that there exist infinitely many Pythagorean triples x, y, z in which x and y are consecutive triangular numbers. Exhibit three of these.
[*Hint:* If x, $x+1$, z forms a Pythagorean triple, then so does t_{2x}, t_{2x+1}, $(2x+1)z$.]

13. Use Problem 12 to prove that there exist infinitely many triangular numbers that are perfect squares. Exhibit five such triangular numbers.
[*Hint:* If x, $x+1$, z forms a Pythagorean triple, then upon setting $u = z - x - 1$, $v = x + \frac{1}{2}(1-z)$, one obtains $u(u+1)/2 = v^2$.]

12.2 FERMAT'S LAST THEOREM

With our knowledge of Pythagorean triples, we are now prepared to take up the one case in which Fermat himself had a proof of his conjecture, the case $n = 4$. The technique used in the proof is a form of induction sometimes called "Fermat's method of infinite descent." In brief, the method may be described as follows: It is assumed that a solution of the problem in question is possible in the positive integers. From this solution, one constructs a new solution in smaller positive integers, which then leads to a still smaller solution, and so on. Because the positive integers cannot be decreased in magnitude indefinitely, it follows that the initial assumption must be false and therefore no solution is possible.

Instead of giving a proof of the Fermat conjecture for $n = 4$, it turns out to be easier to establish a fact that is slightly stronger, namely, the impossibility of solving the equation $x^4 + y^4 = z^2$ in the positive integers.

Theorem 12.3 Fermat. The Diophantine equation $x^4 + y^4 = z^2$ has no solution in positive integers x, y, z.

Proof. With the idea of deriving a contradiction, let us assume that there exists a positive solution x_0, y_0, z_0 of $x^4 + y^4 = z^2$. Nothing is lost in supposing also that $\gcd(x_0, y_0) = 1$; otherwise, put $\gcd(x_0, y_0) = d$, $x_0 = dx_1$, $y_0 = dy_1$, $z_0 = d^2 z_1$ to get $x_1^4 + y_1^4 = z_1^2$ with $\gcd(x_1, y_1) = 1$.

Expressing the supposed equation $x_0^4 + y_0^4 = z_0^2$ in the form

$$(x_0^2)^2 + (y_0^2)^2 = z_0^2$$

we see that x_0^2, y_0^2, z_0 meet all the requirements of a primitive Pythagorean triple, and therefore Theorem 12.1 can be brought into play. In such triples, one of the integers x_0^2 or y_0^2 is necessarily even, whereas the other is odd. Taking x_0^2 (and hence x_0) to be even, there exist relatively prime integers $s > t > 0$ satisfying

$$x_0^2 = 2st$$
$$y_0^2 = s^2 - t^2$$
$$z_0 = s^2 + t^2$$

where exactly one of s and t is even. If it happens that s is even, then we have

$$1 \equiv y_0^2 = s^2 - t^2 \equiv 0 - 1 \equiv 3 \pmod 4$$

which is an impossibility. Therefore, s must be the odd integer and, in consequence, t is the even one. Let us put $t = 2r$. Then the equation $x_0^2 = 2st$ becomes $x_0^2 = 4sr$,

which says that

$$\left(\frac{x_0}{2}\right)^2 = sr$$

But Lemma 2 asserts that the product of two relatively prime integers [note that $\gcd(s, t) = 1$ implies that $\gcd(s, r) = 1$] is a square only if each of the integers itself is a square; hence, $s = z_1^2$, $r = w_1^2$ for positive integers z_1, w_1.

We wish to apply Theorem 12.1 again, this time to the equation

$$t^2 + y_0^2 = s^2$$

Because $\gcd(s, t) = 1$, it follows that $\gcd(t, y_0, s) = 1$, making t, y_0, s a primitive Pythagorean triple. With t even, we obtain

$$t = 2uv$$
$$y_0 = u^2 - v^2$$
$$s = u^2 + v^2$$

for relatively prime integers $u > v > 0$. Now the relation

$$uv = \frac{t}{2} = r = w_1^2$$

signifies that u and v are both squares (Lemma 2 serves its purpose once more); say, $u = x_1^2$ and $v = y_1^2$. When these values are substituted into the equation for s, the result is

$$z_1^2 = s = u^2 + v^2 = x_1^4 + y_1^4$$

A crucial point is that, z_1 and t being positive, we also have the inequality

$$0 < z_1 \leq z_1^2 = s \leq s^2 < s^2 + t^2 = z_0$$

What has happened is this. Starting with one solution x_0, y_0, z_0 of $x^4 + y^4 = z^2$, we have constructed another solution x_1, y_1, z_1 such that $0 < z_1 < z_0$. Repeating the whole argument, our second solution would lead to a third solution x_2, y_2, z_2 with $0 < z_2 < z_1$, which, in turn, gives rise to a fourth. This process can be carried out as many times as desired to produce an infinite decreasing sequence of positive integers

$$z_0 > z_1 > z_2 > \cdots$$

Because there is only a finite supply of positive integers less than z_0, a contradiction occurs. We are forced to conclude that $x^4 + y^4 = z^2$ is not solvable in the positive integers.

As an immediate result, one gets the following corollary.

Corollary. The equation $x^4 + y^4 = z^4$ has no solution in the positive integers.

Proof. If x_0, y_0, z_0 were a positive solution of $x^4 + y^4 = z^4$, then x_0, y_0, z_0^2 would satisfy the equation $x^4 + y^4 = z^2$, in conflict with Theorem 12.3.

If $n > 2$, then n is either a power of 2 or divisible by an odd prime p. In the first case, $n = 4k$ for some $k \geq 1$ and the Fermat equation $x^n + y^n = z^n$ can be written as

$$(x^k)^4 + (y^k)^4 = (z^k)^4$$

We have just seen that this equation is impossible in the positive integers. When $n = pk$, the Fermat equation is the same as

$$(x^k)^p + (y^k)^p = (z^k)^p$$

If it could be shown that the equation $u^p + v^p = w^p$ has no solution, then, in particular, there would be no solution of the form $u = x^k$, $v = y^k$, $w = z^k$; hence, $x^n + y^n = z^n$ would not be solvable. Therefore, Fermat's conjecture reduces to this: For no odd prime p does the equation

$$x^p + y^p = z^p$$

admit a solution in the positive integers.

Although the problem has challenged the foremost mathematicians of the last 300 years, their efforts tended to produce partial results and proofs of individual cases. Euler gave the first proof of the Fermat conjecture for the prime $p = 3$ in the year 1770; the reasoning was incomplete at one stage, but Legendre later supplied the missing steps. Using the method of infinite descent, Dirichlet and Legendre independently settled the case $p = 5$ around 1825. Not long thereafter, in 1839, Lamé proved the conjecture for seventh powers. With the increasing complexity of the arguments came the realization that a successful resolution of the general case called for different techniques. The best hope seemed to lie in extending the meaning of "integer" to include a wider class of numbers and, by attacking the problem within this enlarged system, obtaining more information than was possible by using ordinary integers only.

The German mathematician Kummer made the major breakthrough. In 1843, he submitted to Dirichlet a purported proof of Fermat's conjecture based upon an extension of the integers to include the so-called "algebraic numbers" (that is, complex numbers satisfying polynomials with rational coefficients). Having spent considerable time on the problem himself, Dirichlet was immediately able to detect the flaw in the reasoning: Kummer had taken for granted that algebraic numbers admit a unique factorization similar to that of the ordinary integers, which is not always true.

But Kummer was undeterred by this perplexing situation and returned to his investigations with redoubled effort. To restore unique factorization to the algebraic numbers, he was led to invent the concept of *ideal numbers*. By adjoining these new entities to the algebraic numbers, Kummer successfully proved Fermat's conjecture for a large class of primes that he termed *regular primes* (that this represented an enormous achievement is reflected in the fact that the only irregular primes less than 100 are 37, 59, and 67). Unfortunately, it is still not known whether there are an infinite number of regular primes, whereas in the other direction, Jensen (1915) established that there exist infinitely many irregular ones. Almost all the subsequent progress on the problem was within the framework suggested by Kummer.

In 1983, a 29-year-old West German mathematician, Gerd Faltings, proved that for each exponent $n > 2$, the Fermat equation $x^n + y^n = z^n$ can have at most a finite number (as opposed to an infinite number) of integral solutions. At first glance, this may not seem like much of an advance; but if it could be shown that the finite number of solutions was zero in each case, then the Fermat's conjecture would be laid to rest once and for all.

Another striking result, established in 1987, was that Fermat's assertion is true for "almost all" values of n; that is, as n increases the percentage of cases in which the conjecture could fail approaches zero.

With the advent of computers, various numerical tests were devised to verify Fermat's conjecture for specific values of n. In 1977, S. S. Wagstaff took over 2 years, using computing time on four machines on weekends and holidays, to show that the conjecture held for all $n \leq 125000$. Since that time, the range of exponents for which the result was determined to be true has been extended repeatedly. By 1992, Fermat's conjecture was known to be true for exponents up to 4000000.

For a moment in the summer of 1993, it appeared that the final breakthrough had been made. At the conclusion of 3 days of lectures in Cambridge, England, Andrew Wiles of Princeton University stunned his colleagues by announcing that he could favorably resolve Fermat's conjecture. His proposed proof, which had taken 7 years to prepare, was an artful blend of many sophisticated techniques developed by other mathematicians only within the preceding decade. The key insight was to link equations of the kind posed by Fermat with the much-studied theory of elliptic curves; that is, curves determined by cubic polynomials of the form $y^2 = x^3 + ax + b$, where a and b are integers.

The overall structure and strategy of Wiles's argument was so compelling that mathematicians hailed it as almost certainly correct. But when the immensely complicated 200-page manuscript was carefully scrutinized for hidden errors, it revealed a subtle snag. No one claimed that the flaw was fatal, and bridging the gap was felt to be feasible. Over a year later, Wiles provided a corrected, refined, and shorter (125-page) version of his original proof to the enthusiastic reviewers. The revised argument was seen to be sound, and Fermat's seemingly simple claim was finally settled.

The failure of Wiles's initial attempt is not really surprising or unusual in mathematical research. Normally, proposed proofs are privately circulated and examined for possible flaws months in advance of any formal announcement. In Wiles's case, the notoriety of one of number theory's most elusive conjectures brought premature publicity and temporary disappointment to the mathematical community.

To round out our historical digression, we might mention that in 1908 a prize of 100,000 marks was bequeathed to the Academy of Science at Göttingen to be paid for the first complete proof of Fermat's conjecture. The immediate result was a deluge of incorrect demonstrations by amateur mathematicians. Because only printed solutions were eligible, Fermat's conjecture is reputed to be the mathematical problem for which the greatest number of false proofs have been published; indeed, between 1908 and 1912 over 1000 alleged proofs appeared, mostly printed as private pamphlets. Suffice it to say, interest declined as the German inflation of the 1920s wiped out the monetary value of the prize. (With the introduction of the Reichsmark and Deutsche Mark [DM] and after various currency revaluations, the award was worth about DM 75,000 or $40,000 when it was presented to Wiles in 1997.)

From $x^4 + y^4 = z^2$, we move on to a closely related Diophantine equation, namely, $x^4 - y^4 = z^2$. The proof of its insolubility parallels that of Theorem 12.3, but we give a slight variation in the method of infinite descent.

Theorem 12.4 Fermat. The Diophantine equation $x^4 - y^4 = z^2$ has no solution in positive integers x, y, z.

Proof. The proof proceeds by contradiction. Let us assume that the equation admits a solution in the positive integers and among these solutions x_0, y_0, z_0 is one with a least value of x; in particular, this supposition forces x_0 to be odd (Why?). Were $\gcd(x_0, y_0) = d > 1$, then putting $x_0 = dx_1$, $y_0 = dy_1$, we would have $d^4(x_1^4 - y_1^4) = z_0^2$, whence $d^2 \mid z_0$ or $z_0 = d^2 z_1$ for some $z_1 > 0$. It follows that x_1, y_1, z_1 provides a solution to the equation under consideration with $0 < x_1 < x_0$, which is an impossible situation. Thus, we are free to assume a solution x_0, y_0, z_0 in which $\gcd(x_0, y_0) = 1$. The ensuing argument falls into two stages, depending on whether y_0 is odd or even.

First, consider the case of an odd integer y_0. If the equation $x_0^4 - y_0^4 = z_0^2$ is written in the form $z_0^2 + (y_0^2)^2 = (x_0^2)^2$, we see that z_0, y_0^2, x_0^2 constitute a primitive Pythagorean triple. Theorem 12.1 asserts the existence of relatively prime integers $s > t > 0$ for which

$$\begin{aligned} z_0 &= 2st \\ y_0^2 &= s^2 - t^2 \\ x_0^2 &= s^2 + t^2 \end{aligned}$$

Thus, it appears that

$$s^4 - t^4 = (s^2 + t^2)(s^2 - t^2) = x_0^2 y_0^2 = (x_0 y_0)^2$$

making s, t, $x_0 y_0$ a (positive) solution to the equation $x^4 - y^4 = z^2$. Because

$$0 < s < \sqrt{s^2 + t^2} = x_0$$

we arrive at a contradiction to the minimal nature of x_0.

For the second part of the proof, assume that y_0 is an even integer. Using the formulas for primitive Pythagorean triples, we now write

$$\begin{aligned} y_0^2 &= 2st \\ z_0 &= s^2 - t^2 \\ x_0^2 &= s^2 + t^2 \end{aligned}$$

where s may be taken to be even and t to be odd. Then, in the relation $y_0^2 = 2st$, we have $\gcd(2s, t) = 1$. The now-customary application of Lemma 2 tells us that $2s$ and t are each squares of positive integers; say, $2s = w^2$, $t = v^2$. Because w must of necessity be an even integer, set $w = 2u$ to get $s = 2u^2$. Therefore,

$$x_0^2 = s^2 + t^2 = 4u^4 + v^4$$

and so $2u^2$, v^2, x_0 forms a primitive Pythagorean triple. Falling back on Theorem 12.1 again, there exist integers $a > b > 0$ for which

$$\begin{aligned} 2u^2 &= 2ab \\ v^2 &= a^2 - b^2 \\ x_0 &= a^2 + b^2 \end{aligned}$$

where $\gcd(a, b) = 1$. The equality $u^2 = ab$ ensures that a and b are perfect squares, so that $a = c^2$ and $b = d^2$. Knowing this, the rest of the proof is easy; for, upon substituting,

$$v^2 = a^2 - b^2 = c^4 - d^4$$

The result is a new solution c, d, v of the given equation $x^4 - y^4 = z^2$ and what is more, a solution in which

$$0 < c = \sqrt{a} < a^2 + b^2 = x_0$$

contrary to our assumption regarding x_0.

The only resolution of these contradictions is that the equation $x^4 - y^4 = z^2$ cannot be satisfied in the positive integers.

In the margin of his copy of Diophantus's *Arithmetica*, Fermat states and proves the following: The area of a right triangle with rational sides cannot be the square of a rational number. Clearing of fractions, this reduces to a theorem about Pythagorean triangles, to wit, Theorem 12.5.

Theorem 12.5. The area of a Pythagorean triangle can never be equal to a perfect (integral) square.

Proof. Consider a Pythagorean triangle whose hypotenuse has length z and other two sides have lengths x and y, so that $x^2 + y^2 = z^2$. The area of the triangle in question is $\frac{1}{2}xy$, and if this were a square, say u^2, it would follow that $2xy = 4u^2$. By adding and subtracting the last-written equation from $x^2 + y^2 = z^2$, we are led to

$$(x + y)^2 = z^2 + 4u^2 \qquad \text{and} \qquad (x - y)^2 = z^2 - 4u^2$$

When these last two equations are multiplied together, the outcome is that two fourth powers have as their difference a square:

$$(x^2 - y^2)^2 = z^4 - 16u^4 = z^4 - (2u)^4$$

Because this amounts to an infringement on Theorem 12.4, there can be no Pythagorean triangle whose area is a square.

There are a number of simple problems pertaining to Pythagorean triangles that still await solution. The corollary to Theorem 12.3 may be expressed by saying that there exists no Pythagorean triangle all the sides of which are squares. However, it is not difficult to produce Pythagorean triangles whose sides, if increased by 1, are squares; for instance, the triangles associated with the triples $13^2 - 1$, $10^2 - 1$, $14^2 - 1$, and $287^2 - 1$, $265^2 - 1$, $329^2 - 1$. An obvious—and as yet unanswered—question is whether there are an infinite number of such triangles. We can find Pythagorean triangles each side of which is a triangular number. [By a triangular number, we mean an integer of the form $t_n = n(n + 1)/2$.] An example of such is the triangle corresponding to t_{132}, t_{143}, t_{164}. It is not known if infinitely many Pythagorean triangles of this type exist.

As a closing comment, we should observe that all the effort expended on attempting to prove Fermat's conjecture has been far from wasted. The new mathematics that was developed as a by-product laid the foundations for algebraic number theory and the ideal theory of modern abstract algebra. It seems fair to say that the value of these far exceeds that of the conjecture itself.

Another challenge to number theorists, somewhat akin to Fermat's conjecture, concerns the Catalan equation. Consider for the moment the squares and cubes of

positive integers in increasing order:

$$1, 4, 8, 9, 16, 25, 27, 36, 49, 64, 81, 100, \ldots$$

We notice that 8 and 9 are consecutive integers in this sequence. The medieval astronomer Levi ben Gerson (1288–1344) proved that there are no other consecutive powers of 2 and 3; to put it another way, he showed that if $3^m - 2^n = \pm 1$, with $m > 1$ and $n > 1$, then $m = 2$ and $n = 3$. In 1738, Euler, using Fermat's method of infinite descent, dealt with the equation $x^3 - y^2 = \pm 1$, proving that $x = 2$ and $y = 3$. Catalan himself contributed little more to the consecutive-power problem than the assertion (1844) that the only solution of the equation $x^m - y^n = 1$ in integers x, y, m, n, all greater than 1, is $m = y = 2, n = x = 3$. This statement, now known as Catalan's conjecture, was proved, in 2002.

Over the years, the Catalan equation $x^m - y^n = 1$ had been shown to be impossible of solution for special values of m and n. For example in 1850, V. A. Lebesgue proved that $x^m - y^2 = 1$ admits no solution in the positive integers for $m \neq 3$; but, it remained until 1964 to show that the more difficult equation $x^2 - y^n = 1$ is not solvable for $n \neq 3$. The cases $x^3 - y^n = 1$ and $x^m - y^3 = 1$, with $m \neq 2$, were successfully resolved in 1921. The most striking result, obtained by R. Tijdeman in 1976, is that $x^m - y^n = 1$ has only a finite number of solutions, all of which are smaller than some computable constant $C > 0$; that is, $x^m, y^n < C$.

Suppose that Catalan's equation did have a solution other than $3^2 - 2^3 = 1$. If p and q are primes dividing m and n respectively, then $x^{m/p}$ and $y^{n/q}$ would provide a solution to the equation $u^p - v^q = 1$. What needed to be shown was that this equation was not solvable in integers $u, v \geq 2$ and distinct primes $p, q \geq 5$. One approach called for obtaining explicit bounds on the possible size of the exponents. A series of investigations continually sharpened the restrictions until by the year 2000 it was known that $3 \cdot 10^8 < p < (7.15)10^{11}$ and $3.10^8 < q < (7.75)10^{16}$. Thus, the Catalan conjecture could in principle be settled by exhaustive computer calculations; but until the upper bound was lowered, this would take a long time.

In 2000, Preda Mihailescu proved that for a Catalan solution to exist, p and q must satisfy the simultaneous congruences

$$p^{q-1} \equiv 1 (\mathrm{mod}\, q^2) \quad \text{and} \quad q^{p-1} \equiv 1 (\mathrm{mod}\, p^2)$$

These are known as double Wieferich primes, after Arthur Wieferich, who investigated (1909) the congruence $2^{p-1} \equiv 1 \pmod{p^2}$. Such pairs of primes are rare, with only six pairs having been identified by the year 2001. Furthermore, as each of these 12 primes is less than $3 \cdot 10^8$, none satisfied the known restrictions. Taking advantage of his results on Wieferich primes, Mihailescu continued to work on the problem. He finally settled the famous question early in the following year: the only consecutive powers are 8 and 9.

One interesting consequence of these results is that no Fermat number $F_n = 2^{2^n} + 1$ can be a power of another integer, the exponent being greater than 1. For if $F_n = a^m$, with $m \geq 2$, then $a^m - (2^{2^{n-1}})^2 = 1$, which would imply that the equation $x^m - y^2 = 1$ has a solution.

PROBLEMS 12.2

1. Show that the equation $x^2 + y^2 = z^3$ has infinitely many solutions for x, y, z positive integers.
   [*Hint:* For any $n \geq 2$, let $x = n(n^2 - 3)$ and $y = 3n^2 - 1$.]
2. Prove the theorem: The only solutions in nonnegative integers of the equation $x^2 + 2y^2 = z^2$, with $\gcd(x, y, z) = 1$, are given by
   $$x = \pm(2s^2 - t^2) \qquad y = 2st \qquad z = 2s^2 + t^2$$
   where s, t are arbitrary nonnegative integers.
   [*Hint:* If u, v, w are such that $y = 2w$, $z + x = 2u$, $z - x = 2v$, then the equation becomes $2w^2 = uv$.]
3. In a Pythagorean triple x, y, z, prove that not more than one of x, y, or z can be a perfect square.
4. Prove each of the following assertions:
   (a) The system of simultaneous equations
   $$x^2 + y^2 = z^2 - 1 \qquad \text{and} \qquad x^2 - y^2 = w^2 - 1$$
   has infinitely many solutions in positive integers x, y, z, w.
   [*Hint:* For any integer $n \geq 1$, take $x = 2n^2$ and $y = 2n$.]
   (b) The system of simultaneous equations
   $$x^2 + y^2 = z^2 \qquad \text{and} \qquad x^2 - y^2 = w^2$$
   admits no solution in positive integers x, y, z, w.
   (c) The system of simultaneous equations
   $$x^2 + y^2 = z^2 + 1 \qquad \text{and} \qquad x^2 - y^2 = w^2 + 1$$
   has infinitely many solutions in positive integers x, y, z, w.
   [*Hint:* For any integer $n \geq 1$, take $x = 8n^4 + 1$ and $y = 8n^3$.]
5. Use Problem 4 to establish that there is no solution in positive integers of the simultaneous equations
   $$x^2 + y^2 = z^2 \qquad \text{and} \qquad x^2 + 2y^2 = w^2$$
   [*Hint:* Any solution of the given system also satisfies $z^2 + y^2 = w^2$ and $z^2 - y^2 = x^2$.]
6. Show that there is no solution in positive integers of the simultaneous equations
   $$x^2 + y^2 = z^2 \qquad \text{and} \qquad x^2 + z^2 = w^2$$
   hence, there exists no Pythagorean triangle whose hypotenuse and one of whose sides form the sides of another Pythagorean triangle.
   [*Hint:* Any solution of the given system also satisfies $x^4 + (wy)^2 = z^4$.]
7. Prove that the equation $x^4 - y^4 = 2z^2$ has no solutions in positive integers x, y, z.
   [*Hint:* Because x, y must be both odd or both even, $x^2 + y^2 = 2a^2$, $x + y = 2b^2$, $x - y = 2c^2$ for some a, b, c; hence, $a^2 = b^4 + c^4$.]
8. Verify that the only solution in relatively prime positive integers of the equation $x^4 + y^4 = 2z^2$ is $x = y = z = 1$.
   [*Hint:* Any solution of the given equation also satisfies the equation
   $$z^4 - (xy)^4 = \left(\frac{x^4 - y^4}{2}\right)^2 .]$$