Chapter 1

Topics in Number Theory

We assume familiarity with the number systems. The notion of a number line, which extends from $-\infty$ to $+\infty$, represents the ordering of the *real numbers.* Among these, the counting numbers, 1, 2, 3, ... are better known as the *natural numbers.* There are also the *integers,* which extend the natural numbers by including zero and negative natural numbers. In other words, natural numbers are precisely the positive integers.

The integers come in two kinds, even and odd. The even numbers are

$$0,\ \pm 2,\ \pm 4,\ \pm 6,\ \pm 8,\ \pm 10,\ \pm 12,\ \ldots$$

and the rest of the integers are odd:

$$\pm 1,\ \pm 3,\ \pm 5,\ \pm 7,\ \pm 9,\ \pm 11,\ \pm 13,\ \ldots$$

Observe that the sequence of even numbers can be written in the form

$$\ldots,\ 2\times -1,\ 2\times 0,\ 2\times 1,\ 2\times 2,\ 2\times 3,\ \ldots$$

So the two classes of integers may be defined as follows.

Definition. An integer n is *even* if $n = 2m$, where m is again integer. On the other hand, n is *odd* if $n = 2m + 1$ for some integer m.

For instance, 26 is even because $26 = 2 \times 13$, and 13 is integer. But, the number 17 is not even because $17 = 2 \times 8.5$, where 8.5 is not an integer. Note that 17 is odd because $17 = 2 \times 8 + 1$, where 8 is an integer.

Question. With these definitions, can an integer be *both* even and odd? Why or why not?

The ratio of two integers, written a/b, with $b \neq 0$, is what we call a *rational number.* Sometimes, a rational number can actually be an integer, e.g., $21/3$ is the integer 7. In general, however, the rational numbers form a bigger set which contains the integers as a subset.

Real numbers which are not rational are called *irrational numbers.* Thus, irrational numbers are real numbers which cannot be expressed as the ratio of two integers. An example of irrational numbers is given by $\sqrt{2}$. We will see in Section 2.3.4 a proof of the fact that $\sqrt{2}$ is indeed irrational.

The integers are the domain of number theory. In particular, number theory is concerned with the properties of the natural numbers. How can we know if a given natural number n is the product of two smaller numbers, which are called *factors* of n? Is there an algorithm to find all common factors of a given pair (m, n)? These are two questions one may ask in number theory.

1.1 Integers in Various Bases

We start by introducing different systems in which we may represent counting numbers. The way we are used to count is based on a ten-digit system, called *decimal,* i.e., using the digits 0 to 9. In computer language, however, it is more convenient to use the *binary* number system, in which we employ only 0 and 1. Computers rely on switches to perceive quantities, and a swith can be *off* or *on*—thus the reason for the binary digits of zeros and ones.

Hence, to enumerate the natural numbers in binary, we begin with

$$1,\ 10,\ 11,\ 100,\ 101,\ 110,\ 111,\ 1000,\ 1001,\ 1010,\ \ldots$$

Note that 111, for instance, corresponds to the number 7 in decimal. We express this relation by writing $111_2 = 7_{10}$. The first question that arises is, given a binary number, how do we know its equivalent in decimal? The key to the algorithm for finding the answer is the following observation.

In decimal, every digit acts as a counter, where from right to left we have the number of ones, then the number of tens (ten ones), the number of hundreds (ten tens), and on. For example,

$$\begin{aligned} 5,467 &= 5,000 + 400 + 60 + 7 \\ &= 5 \times 10^3 + 4 \times 10^2 + 6 \times 10^1 + 7 \times 10^0 \end{aligned}$$

This principle holds in the binary number system as well, except that powers

of 10 are replaced by powers of 2. Hence,

$$\begin{aligned} 111_2 &= 1 \times 2^2 + 1 \times 2^1 + 1 \times 2^0 \\ &= 4 + 2 + 1 \\ &= 7_{10} \end{aligned}$$

Example. Convert the binary number 1100101 to decimal.

Solution. Multiply each digit by the appropriate power of 2, ignoring the zeros since they do not add anything:

$$\begin{aligned} 1100101_2 &= 1 \times 2^6 + 1 \times 2^5 + 1 \times 2^2 + 1 \times 2^0 \\ &= 2^6 + 2^5 + 2^2 + 2^0 \\ &= 64 + 32 + 4 + 1 \\ &= 101_{10} \end{aligned}$$

Note that without the indices, writing $1100101 = 101$ would have been misleading!

Exercise 1.1. Convert the binary numbers to decimal.
a) 1101111
b) 1110111
c) 100000001
d) 1101111000

Test 1.2. Which binary number represents an odd number?
a) 1100101100
b) 111010010101010
c) 1010010010101011
d) 1010100101111111100

Going in the other direction, how do we convert a decimal number to binary? The reverse algorithm will now involve *divisions* by powers of 2.

Example. Convert the decimal number 101 to binary.

Solution. Ahead of time, we do not know the largest power of 2 which divides into 101. So we will divide 101 by 2 repeatedly, as follows.

$$\begin{aligned} 101 \div 2 &= 50 && \text{with remainder } 1 \\ 50 \div 2 &= 25 && \text{with remainder } 0 \\ 25 \div 2 &= 12 && \text{with remainder } 1 \\ 12 \div 2 &= 6 && \text{with remainder } 0 \\ 6 \div 2 &= 3 && \text{with remainder } 0 \\ 3 \div 2 &= 1 && \text{with remainder } 1 \\ 1 \div 2 &= 0 && \text{with remainder } 1 \end{aligned}$$

Note that the remainders determine the digits of the sought binary number; and we recover the relation $101_{10} = 1100101_2$ by reading these remainders from the last one up.

Exercise 1.3. Convert the decimal numbers to binary.

a) 99
b) 129
c) 999
d) 2730

In principle, the idea of a base-10 or base-2 number system can be generalized to any base-n number system, where n is the number of digits used. Two other common number systems for the computing language are the *hexadecimal* and *octal* systems—using 16 and 8 digits, respectively.

In hexadecimal, we count using the sixteen "digits" 0 to 9 and A to F, in this order. From 1 to 20, for instance, we write,

$$1,\ 2,\ 3,\ 4,\ 5,\ 6,\ 7,\ 8,\ 9,\ A,\ B,\ C,\ D,\ E,\ F,\ 10,\ 11,\ 12,\ 13,\ 14$$

The fact that 14_{16} is equivalent to 20_{10} can be explained by the same principle of "multiples of powers," which has been demonstrated in decimal as well as in binary, i.e., $14_{16} = 1 \times 16^1 + 4 \times 16^0 = 16 + 4 = 20_{10}$.

Example. Convert the hexadecimal number $1A5E$ to decimal.

Solution. This time, multiply each digit by the appropriate power of 16:

$$\begin{aligned} 1A5E_{16} &= 1 \times 16^3 + 10 \times 16^2 + 5 \times 16^1 + 14 \times 16^0 \\ &= 4096 + 2560 + 80 + 14 \\ &= 6750_{10} \end{aligned}$$

Exercise 1.4. Convert each hexadecimal number given below to decimal.

a) AA
b) CEF
c) $2BAD$
d) 10101

Test 1.5. Which hexadecimal number represents an even number?

a) A625B
b) FF79C3
c) E020ADD
d) 37B951FE

The conversion from decimal to hexadecimal is now through iterative division by 16, analogous to that from decimal to binary.

Example. Convert the decimal number 6750 to hexadecimal.

Solution. We use division with remainder, like in grade school, and find,

$$\begin{aligned} 6750 \div 16 &= 421 && \text{with remainder } 14 \\ 421 \div 16 &= 26 && \text{with remainder } 5 \\ 26 \div 16 &= 1 && \text{with remainder } 10 \\ 1 \div 16 &= 0 && \text{with remainder } 1 \end{aligned}$$

The answer, again, is read from last to first: $6750_{10} = 1A5E_{16}$.

Question. How do we find these remainders in the calculator?

Exercise 1.6. Convert the decimal numbers to hexadecimal.

a) 999
b) 10001
c) 98765
d) 522958

The *octal* number system mentioned earlier employs only the digits 0 to 7. Again, the principles of conversion between two bases remain valid.

Exercise 1.7. Convert the octal numbers to decimal.

a) 777
b) 1234
c) 5702
d) 52543

Exercise 1.8. Convert the decimal numbers to octal.

a) 99
b) 999
c) 10001
d) 98765

The hexadecimal and octal number systems are chosen for the following practical reason. Note the relation $2^4 = 16^1$, which indirectly says that four binary digits, or *bits,* are equivalent to one hexadecimal digit. With the help of Table 1.1, this provides a fast method of conversion between base-16 and base-2.

Example. Convert the hexadecimal number $1A5E$ to binary.

Table 1.1: The numbers 0 to 15 in hexadecimal and in binary.

0	1	2	3	4	5	6	7
0000	0001	0010	0011	0100	0101	0110	0111
8	9	*A*	*B*	*C*	*D*	*E*	*F*
1000	1001	1010	1011	1100	1101	1110	1111

Solution. In fact, we simply replace each hexadecimal digit, 1, A, 5, E, by the corresponding four bits shown in Table 1.1, then we juxtapose these binary digits to form the answer.

$$1A5E_{16} = 0001, 1010, 0101, 1110_2$$

The comas are inserted for better reading, and the answer can well be written without them, i.e., 1101001011110.

Exercise 1.9. Convert the hexadecimal numbers of Exercise 1.4 to binary.

To convert from binary to hexadecimal, simply reverse this action. In the case where the binary digits are not evenly grouped into fours, we simply add extra zeros to the left of the quantity.

Example. Convert the binary number 11011000111100 to hexadecimal.

Solution. There are 14 digits; to group them into fours we need to have two extra zeros on the left. With Table 1.1 again, we get the following answer.

$$0011, 0110, 0011, 1100_2 = 363C_{16}$$

Question. Would it be wrong if we pad zeros to the right?

Exercise 1.10. Convert the binary numbers to hexadecimal.

a) 1101111
b) 11111111111
c) 100000000001
d) 111110000111001

Exercise* 1.11. Elias has carelessly added two extra zeros to the right, instead of to the left of the binary digits and come up with his wrong hexadecimal answer, $ACE8$. What is supposed to be the correct answer?

For base-8, similarly, we have the relation $2^3 = 8^1$. Since this implies that every octal digit corresponds to three bits, there is also a quick way to convert between binary and octal.

Exercise 1.12. Convert the binary numbers to octal, or vice versa.

a) 1101111_2
b) 10111001011_2
c) 264_8
d) 10101_8

Now suppose we wish to convert a hexadecimal number to octal. One way to do this is to convert first to decimal and then to octal—but why not to binary first, and then from binary to octal?

Exercise 1.13. Convert the hexadecimal numbers to octal, or vice versa.

a) $A2C_{16}$
b) $E7DC2_{16}$
c) 5764_8
d) 7777777_8

Test 1.14. We are given a number in the base-4 system, 1231231_4. What is this number in hexadecimal?

a) 6DB1
b) 1B6D
c) 6DB4
d) 1BCD

Exercise* 1.15. The base-26 number system uses the letters of the alphabet, i.e., from A to Z, to represent the digits 0 through 25. How do we represent the decimal number 62534 in base-26?

Exercise* 1.16. Amira is a very wealthy businesswoman who has built a modern village in the suburb of Jakarta. Being superstitious, she refuses to use the digit 4 in numbering the floors of her high-rise office building, the top floor being the 69th. How many floors up is that, if Amira were not afraid to count with 4? Of course, there is no 13th floor either. Can you write a computer program to do this conversion, in either direction?

Appendix: Representing Non-Integer Numbers

We have been concerned with conversion of natural numbers between number systems of different bases. There are ways in which binary digits are used to represent negative integers or even non-integer rational numbers.

In the decimal system, a rational number can be written using a dot (period sign) properly inserted among the digits, e.g., 3.1415. The part to the right of the dot is called the *fractional* part. We observe that the digits

of the fractional part represent multiples of negative powers of 10. In this example,

$$\begin{aligned} 3.1415 &= 3 + 0.1 + 0.04 + 0.001 + 0.0005 \\ &= 3 \times 10^0 + 1 \times 10^{-1} + 4 \times 10^{-2} + 1 \times 10^{-3} + 5 \times 10^{-4} \end{aligned}$$

If we keep this principle for the binary number system, then we may represent certain rational numbers by association with negative powers of 2.

Example. Convert the binary number 0.1011 to decimal.

Solution. We do not need to write down the multiples of zero:

$$\begin{aligned} 0.1011_2 &= 2^{-1} + 2^{-3} + 2^{-4} \\ &= 0.5 + 0.125 + 0.0625 \\ &= 0.6875_{10} \end{aligned}$$

Exercise 1.17. Convert the binary numbers to decimal.

a) 0.01
b) 0.10001
c) 0.11111
d) 0.000001

From decimal to binary, converting the fractional part of a rational number would be through repeated multiplication by 2, where in each step we keep record of the integer part.

Example. Convert the decimal number 0.6875 to binary.

Solution. We write the integer parts in the far right column.

$$\begin{aligned} 0.6875 \times 2 &= 1 + 0.375 && 1 \\ 0.375 \times 2 &= 0 + 0.75 && 0 \\ 0.75 \times 2 &= 1 + 0.5 && 1 \\ 0.5 \times 2 &= 1 + 0 && 1 \end{aligned}$$

This time, the correct answer is obtained by reading the integer parts downward from the top, following the dot: 0.1011_2 .

Note that in the above example we stop the algorithm when we reach 0 in the fractional part. In general, however, the iterations may never terminate with a zero. The situations parallel those in decimal, where a rational number may be represented by an infinite, but always periodic, extension of digits, e.g., $1/3 = 0.333\ldots = 0.\overline{3}$ and $5/11 = 0.\overline{45}$.

Exercise 1.18. Convert the decimal numbers to binary and to hexadecimal.

a) 0.03125
b) 0.765625
c) 5/8
d) 1/3

1.2 Divisibility

We return to the studies of integers. It is clear that adding or multiplying two integers results in another integer. Dividing an integer by another, on the other hand, sometimes yields an integer value but sometimes does not. The relation in which an integer divides another integer (resulting in another integer) is an important concept in the theory of numbers.

First, we need to introduce some functions which have their domain or range in the set of integers. For instance, there are times when we need to extract the integer part of a non-integer number. This particular operation is performed by the floor function.

Definition. The *floor function* $f(x) = \lfloor x \rfloor$ takes any real number x and returns the greatest integer n with condition $n \leq x$. The quantity $\lfloor x \rfloor$ may be called the *floor* of x.

For example, we have $\lfloor 3.1415 \rfloor = 3$ and $\lfloor -100/7 \rfloor = -15$. Note that $\lfloor x \rfloor = x$ if, and only if, x is already an integer. Furthermore, the inequalities $\lfloor x \rfloor \leq x < \lfloor x \rfloor + 1$ hold for any real number x.

A companion to the floor function is the ceiling function, defined as follows.

Definition. The *ceiling function* $f(x) = \lceil x \rceil$ takes any real number x and returns the least integer n with condition $n \geq x$. We may call $\lceil x \rceil$ the *ceiling* of x.

Hence, to illustrate, $\lceil 3.1415 \rceil = 4$ and $\lceil -20/3 \rceil = -6$. Similar to the floor function, we also have $\lceil x \rceil = x$ if and only if x is an integer.

Exercise* 1.19. Order the following quantities, from the smallest to the largest.

$$x,\ \lfloor x \rfloor,\ \lfloor x \rfloor + 1,\ \lfloor x \rfloor - 1,\ \lceil x \rceil,\ \lceil x \rceil + 1,\ \lceil x \rceil - 1$$

1.2.1 The Mod Operation

The floor function is needed to define the next, very useful operation with integers.

Definition. With two integers m and n, where $n > 0$, we define the operation m *mod* n by

$$m \bmod n = m - \left\lfloor \frac{m}{n} \right\rfloor \times n$$

In some programming language, like C++ or Java, the notation $m \bmod n$ is written $m \,\%\, n$.

Example. Compute 12345 mod 7.

Solution. According the to definition,

$$\begin{aligned} 12345 \bmod 7 &= 12345 - \left\lfloor \frac{12345}{7} \right\rfloor \times 7 \\ &= 12345 - \lfloor 1763.571429\ldots \rfloor \times 7 \\ &= 12345 - (1763 \times 7) \\ &= 12345 - 12341 \\ &= 4 \end{aligned}$$

Exercise 1.20. Perform the following mod operations.

a) 678 mod 5
b) 35 mod 217
c) 3393 mod 29
d) 99999 mod 111

Test 1.21. Which one of these four quantities is the largest?

a) 100 mod 7
b) 234 mod 9
c) 11 mod 29
d) 20 mod 11

As you may have suspected by now, the operation $m \bmod n$ actually returns the remainder upon dividing m by n via the division-with-remainder method. In the preceding example, dividing 12345 by 7 will give us the integer output 1763, which we call the *quotient,* and the remainder 4—a fact we may express as an equation,

$$12345 = (1763) \times 7 + (4)$$

The brackets are added merely to emphazise where the quotient and the remainder are, respectively.

The next theorem, whose proof is left as an easy challenge, states some basic properties of the mod operation which are familiar facts concerning the remainder of a division.

Theorem 1.1. Let m and $n > 0$ be fixed integers. Then

1) $0 \leq m \bmod n < n$.

2) $m \bmod n = m$, if $0 \leq m < n$.

3) $m \bmod n = 0$, if m/n is an integer.

4) m/n is an integer, if $m \bmod n = 0$.

The relation $m \bmod n = 0$, appearing in the above theorem, is an important and useful concept in working with integers. This leads us to the next definition.

Definition. The following statements all have one and the same meaning, namely that $m \bmod n = 0$.

a) m is a *multiple* of n
b) m is *divisible* by n
c) n is a *divisor*, or *factor,* of m
d) n *divides* m

In view of Theorem 1.1, this definition also means that m/n is an integer, i.e., there is an integer k such that $m = nk$.

Example. The following examples illustrate the newly defined terms.

a) The fact that $40/8 = 5$, an integer, allows us to say that 8 divides 40 and that 40 is a multiple of 8 or is divisible by 8.
b) The numbers 10, 20, 30, 40, 50, ... are all divisible by 2 and 5.
c) Even numbers are multiples of 2. In contrast, no odd number has a factor of 2.
d) The number 17 has no divisors other than 1 and 17.

Test 1.22. Which number is a multiple of 24?

a) 0
b) 8
c) 16
d) 84

Another important and useful concept involving the mod operation is the relation between integers which have the same remainder upon division by a fixed number $n > 0$.

Definition. If a and b are two integers such that $a \bmod n = b \bmod n$, then we write $a \equiv b \pmod{n}$, and say that a is *congruent* to $b \bmod n$. The relation $a \equiv b \pmod{n}$, which is equivalent to $b \equiv a \pmod{n}$, is called a *congruence* $\bmod n$.

For example, since $23 \bmod 7 = 2$ and $100 \bmod 7 = 2$, we have $100 \equiv 23 \pmod 7$. In this new notation, we can say that $m \equiv 0 \pmod n$ precisely when n divides m.

Test 1.23. Which one of the following numbers is congruent to 99 mod 13?
a) 0
b) 69
c) 96
d) 112

1.2.2 An Application in Check Digits

The mod operation is used in many modern applications of identification number assignment, as for a bank account, credit card, airline ticket, product bar code, or a vehicle license plate. In particular, such ID numbers come with a *check digit* (usually the right-most digit) whose purpose is to alert us when an error has occured in typing the number. We illustrate here the use of check digits in assigning the International Standard Book Number (ISBN) for book publications.

An ISBN consists of 10 digits which are separated into four groups by a hyphen between them, e.g., 1-4196-8735-2. These four groups represent the codes for, from left to right, language (0 or 1 means English), publisher, book title, and check digit. In this case, the check digit can also be a capital letter X, and it is determined according to the following algorithm.

Let $a_1, a_2 \ldots, a_{10}$ represent the ten digits of the ISBN, in the order from left to right, and let S be defined by

$$S = (10a_1 + 9a_2 + 8a_3 + 7a_4 + 6a_5 + 5a_6 + 4a_7 + 3a_8 + 2a_9) \bmod 11$$

The check digit will then be given by

$$a_{10} = (11 - S) \bmod 11$$

In addition, due to the range $0 \le a_{10} \le 10$, we agree to replace $a_{10} = 10$ by the letter X.

For example, having determined that the first three codes for the ISBN of a book to be 1-4196-8735-x, we proceed to assigning the check digit x:

$$\begin{aligned} S &= \big((10 \times 1) + (9 \times 4) + (8 \times 1) + (7 \times 9) + (6 \times 6) \\ &\quad + (5 \times 8) + (4 \times 7) + (3 \times 3) + (2 \times 5)\big) \bmod 11 \\ &= (10 + 36 + 8 + 63 + 36 + 40 + 28 + 9 + 10) \bmod 11 \\ &= 240 \bmod 11 = 9 \end{aligned}$$

Thus, $x = (11 - 9) \bmod 11 = 2$, and 1-4196-8735-2 is the complete ISBN.

Exercise 1.24. Determine the check digit for each of the following incomplete ISBN's.

a) 3-314-00783-x
b) 957-747-134-x
c) 962-244-122-x
d) 977-230-154-x

It is not hard to show that the algorithm we have used to produce the check digit a_{10} can be summarized with a single formula,

$$a_{10} = (1a_1 + 2a_2 + 3a_3 + 4a_4 + 5a_5 + 6a_6 + 7a_7 + 8a_8 + 9a_9) \bmod 11$$

It can also be verified that a common typing error like a mistake in just one of the ten digits, or two digits reversely placed, will always be detected by this formula.

Test 1.25. Which one of the following ISBN's is in error?

a) 0-310-91291-1
b) 0-87509-701-4
c) 0-88368-324-X
d) 0-9629049-0-2

Exercise* 1.26. Is it possible, hypothetically, to have two consecutive ISBN's? Think of an example or explain why it is not possible.

As of 1 January 2007, however, all ISBN's have been extended to 13 digits, now called EAN-13, in compliance with the European Article Number for product codes. The conversion is done by prefixing the digit 978 (the code for all books) and readjusting the check digit, according to the following rule.

Let S now be the sum of the first 12 digits, after first multiplying a_2, a_4, a_6, a_8, a_{10}, and a_{12}, each by 3. Then the check digit a_{13} is chosen such that $(S + a_{13}) \bmod 10 = 0$.

Example. Convert the ISBN 1-4196-8735-2 to the corresponding 13-digit EAN.

Solution. The EAN-13 looks like 978-1-4196-8735-x. To determine the check digit, we first calculate S:

$$\begin{aligned} S &= 9 + (7 \times 3) + 8 + (1 \times 3) + 4 + (1 \times 3) \\ &\quad + 9 + (6 \times 3) + 8 + (7 \times 3) + 3 + (5 \times 3) \\ &= 9 + 21 + 8 + 3 + 4 + 3 + 9 + 18 + 8 + 21 + 3 + 15 \\ &= 122 \end{aligned}$$

Hence we choose the digit $x = 8$ in order to make the sum $122 + 8 = 130$, a multiple of 10. The complete EAN-13 for this book is then 978-1-4196-8735-8 or, as normally written without the hyphens, 9781419687358.

Exercise 1.27. Convert each of the ISBN's in Exercise 1.24 to its corresponding EAN-13.

Question. Do we ever need the letter X in an EAN-13?

Exercise 1.28. A number theory textbook shows on its back cover, ISBN 0-471-62546-9. Elias converted this to EAN-13, ignorantly, by simply adding the prefix: 9780471625469. Kindly correct his answer.

Exercise 1.29. A newly published paperback has 9781449976613 for its EAN-13. What would have been the book's ISBN had it been released before the year 2007?

Exercise* 1.30. Is it possible, hypothetically, to have two consecutive EAN-13's? Think of an example or explain why it is not possible.

1.2.3 GCD and LCM

With two integers, it is useful sometimes to find a divisor common to both. For example, 5 is a divisor of both 10 and 25. The next theorem says something about a property of a common divisor.

Theorem 1.2. Suppose d is a divisor of both m and n. Then d divides $am + bn$ for any integers a and b.

Proof. Since m/d and n/d are both integers, the number

$$\frac{am + bn}{d} = a \times \frac{m}{d} \; + \; b \times \frac{n}{d}$$

is also an integer, if a and b are. ▽

Now, given an integer $m \neq 0$, there exist only a finite number of divisors. This is so because if m/n is an integer then $|n| \leq |m|$. The next function will take two integers m and n and returns the greatest of all divisors common to both.

Definition. Let m and n be two integers, not both zero. The *greatest common divisor* of m and n is the largest integer d which divides both m and n. We shall denote this quantity by writing $d = \gcd(m, n)$.

For example, $\gcd(18, 30) = 6$ because 6 divides both 18 and 30, and 6 is the largest number with such a property.

Exercise 1.31. Evaluate $\gcd(m, n)$ given below.

a) $\gcd(125, 200)$
b) $\gcd(12345, 0)$
c) $\gcd(-12, 145)$
d) $\gcd(2, 10000)$

The following theorem will be essential in evaluating $\gcd(m, n)$ for arbitrary values of m and n, even if they are very large.

Theorem 1.3. We have $\gcd(m, n) = \gcd(n, m \bmod n)$.

Proof. Any common divisor of m and n also divides $m \bmod n = m - \lfloor m/n \rfloor n$ by Theorem 1.2. Conversely, any common divisor of n and $m \bmod n$ also divides $m = m \bmod n + \lfloor m/n \rfloor n$ by the same theorem. Hence, both pairs (m, n) and $(n, m \bmod n)$ share the same set of all divisors common to them and, in particular, equal common divisor of greatest value. ▽

Applying Theorem 1.3 twice gives us $\gcd(m, n) = \gcd(m \bmod n, n \bmod (m \bmod n))$. By iteration, the pair decreases in size quite rapidly. This iterative procedure is called the *Euclidean algorithm,* a very efficient method for computing gcd.

Example. Evaluate $\gcd(12345, 6789)$ by the Euclidean algorithm.

Solution. Repeated application of Theorem 1.3 allows us to write

$$\begin{aligned} \gcd(12345, 6789) &= \gcd(6789, 5556) && \text{since } 12345 \bmod 6789 = 5556 \\ &= \gcd(5556, 1233) && \text{since } 6789 \bmod 5556 = 1233 \\ &= \gcd(1233, 624) && \text{since } 5556 \bmod 1233 = 624 \\ &= \cdots \end{aligned}$$

Or we may opt to write only the sequence of remainders:

$$12345,\ 6789,\ 5556,\ 1233,\ 624,\ 609,\ 15,\ 9,\ 6,\ 3,\ 0$$

The last pair tells us that $\gcd(12345, 6789) = \gcd(3, 0) = 3$.

Question. Does the Euclidean algorithm always terminate with a zero remainder?

Exercise 1.32. Use the Euclidean algorithm to evaluate $\gcd(m, n)$.

a) $\gcd(12345, 67890)$
b) $\gcd(12345, 54321)$
c) $\gcd(88888, 555)$
d) $\gcd(234, 60970)$

We conclude this section with one more integer function which complements the gcd function, i.e., the least common multiple.

Definition. With positive integers m and n, we define their *least common multiple* to be the least positive integer which is divisible by both m and n, denoted by $\text{lcm}(m, n)$.

We have $\text{lcm}(12, 15) = 60$, for instance, since 60 is a common multiple of 12 and 15, and it is the smallest of such.

We do not have a particular algorithm to evaluate $\text{lcm}(m, n)$, but the following equality reveals a nice relation between $\gcd(m, n)$ and $\text{lcm}(m, n)$ which can well be used to evaluate one given the other.

Theorem 1.4. For positive integers m and n, we have

$$\gcd(m, n) \times \text{lcm}(m, n) = m \times n$$

We postpone the proof of this claim until later when we reestablish this result following Theorem 1.9 in this chapter.

For example, to evaluate $\text{lcm}(12, 15)$ we may first note that $\gcd(12, 15) = 3$, from which we conclude that $\text{lcm}(12, 15) = 12 \times 15/3 = 60$.

Exercise 1.33. Evaluate $\text{lcm}(m, n)$ by first evaluating $\gcd(m, n)$.

a) $\text{lcm}(275, 115)$
b) $\text{lcm}(144, 456)$
c) $\text{lcm}(999, 123)$
d) $\text{lcm}(725, 1000)$

1.3 Solving Linear Equations

Given integers m, n, and c, we are interested in finding solutions to the linear equation in two variables, x and y, of the form

$$mx + ny = c \tag{1.1}$$

By solutions we mean integer solutions. It turns out that the main ingredient in solving equations of this kind is in fact the Euclidean algorithm.

Theorem 1.2 reminds us that if d is a common divisor of m and n, then d divides $mx + ny$ for any integer values of x and y. Therefore, the first condition for Equation (1.1) to have a solution is that c must be divisible by d and, in particular, by $\gcd(m, n)$.

Theorem 1.5. If the linear equation $mx + ny = c$ has a solution for x and y which are both integers, then $\gcd(m, n)$ must divide c.

Conversely, when c is a multiple of $\gcd(m,n)$, we claim that integer solutions x and y for Equation (1.1) always exist. How do we find at least one such solution pair? First, we claim that integers a and b exist such that

$$ma + nb = \gcd(m,n) \tag{1.2}$$

Then if $c/\gcd(m,n)$ is an integer, we multiply through Equation 1.2 by this integer to obtain

$$m\left(\frac{ac}{\gcd(m,n)}\right) \;+\; n\left(\frac{bc}{\gcd(m,n)}\right) = c$$

thereby producing a solution (x,y) for Equation (1.1).

And how do we find an integer pair (a,b) for Equation (1.2)? We need an extension of the Euclidean algorithm, thus called the *extended Euclidean algorithm*, which we illustrate in the next example.

Example. Find integers a and b such that $123a + 45b = \gcd(123, 45)$.

Solution. We start by writing rows of three integers, labeled (d_i, a_i, b_i) for each row $i \geq 1$, beginning with

	d_i	a_i	b_i
1	123	1	0
2	45	0	1

To determine the third row, subtract $\lfloor 123/45 \rfloor = 2$ times the entire second row from the first. In particular, we will have $d_3 = 123 - \lfloor 123/45 \rfloor 45 = 123 \bmod 45 = 33$. Similarly, for the fourth row, we substract $\lfloor 45/33 \rfloor = 1$ times the entire third row from the second, so that $d_4 = 45 \bmod 33 = 12$.

In this way, down the first column we have the sequence of remainders which we would have upon computing $\gcd(123, 45)$ using the Euclidean algorithm, i.e.,

$$123,\ 45,\ 33,\ 12,\ 9,\ 3,\ 0$$

The completed table with the seven rows is thus obtained:

	d_i	a_i	b_i
	123	1	0
(-2)	45	0	1
(-1)	33	1	-2
(-2)	12	-1	3
(-1)	9	3	-8
(-3)	3	-4	11
	0	15	-41

In such table, we claim that each row obeys the relation

$$d_i = 123a_i + 45b_i \tag{1.3}$$

In particular, the row before the last gives us $\gcd(123, 45) = 3 = 123(-4) + 45(11)$. Thus, we have found our solution of $a = -4$ and $b = 11$.

Question. Can you *prove* why the relation (1.3) holds in each row?

Exercise 1.34. For each given pair (m, n), find integers a and b such that $ma + nb = \gcd(m, n)$.
a) $(345, 215)$
b) $(826, 112)$
c) $(2890, 843)$
d) $(529, 6739)$

Example. Find integers x and y such that $123x + 45y = 66$.

Solution. In the last example, we have found that $123(-4) + 45(11) = 3$. Simply multiply by $66/3 = 22$, and we have a particular solution $x = -88$ and $y = 242$.

Test 1.35. Which equation has integer solutions?
a) $12x + 27y = 35$
b) $12x + 27y = 15$
c) $12x + 20y = 35$
d) $12x + 20y = 15$

Exercise 1.36. For each pair (m, n) given in Exercise 1.34, find integers x and y such that $mx + ny = c$.
a) $c = 95$
b) $c = 98$
c) $c = 11$
d) $c = 99$

In remark, a solution pair for (1.1) in general is not unique. In the preceding table, for instance, if we multiply the third row by 2, then $123(2) + 45(-4) = 66$, providing another solution pair to $123x + 45y = 66$.

Under the condition that $\gcd(m, n)$ divides c, it is now established that Equation (1.1) has at least one solution, or a *particular solution*, denoted by (x_0, y_0). The next theorem describes how to find *all* the solutions.

Theorem 1.6. The equation $mx + ny = c$ has a solution if and only if $\gcd(m, n)$ divides c, in which case all its solutions are given in the form

$$x = x_0 - \frac{nk}{\gcd(m, n)} \quad \text{and} \quad y = y_0 + \frac{mk}{\gcd(m, n)}$$

for any particular solution (x_0, y_0) and for any integer k.

Proof. If we were working over the real numbers, the solutions to $mx+ny = c$ would be represented by a straight line passing through the point (x_0, y_0) and with a slope equals $-m/n$. An arbitrary point on this line is therefore given by (x, y), where

$$x = x_0 - t \quad \text{and} \quad y = y_0 + tm/n$$

for any real number t. We want points on this line which have integer coordinates, so we require that both t and tm/n be integers. We leave as an exercise to verify that this desired condition is achieved precisely when t is a multiple of $n/\gcd(m, n)$, in order to complete the proof. ▽

Example. Find *all* integers x and y such that $123x + 45y = 66$.

Solution. Since we have found a particular solution $(-88, 242)$, and since $\gcd(123, 45) = 3$, the general solutions are now given by

$$x = -88 - 15k \quad \text{and} \quad y = 242 + 41k$$

for any integer k. For example, with $k = -6$ we have the particular solution $x = 2$ and $y = -4$, of which we have remarked earlier.

Exercise 1.37. Complete Exercise 1.36 by finding the general solutions.

Exercise* 1.38. Elias placed a take-out order from Tea Kitchen Chinese restaurant, where a bowl of seafood fried rice costs 3 dinars, a plate of General Tso's chicken is 5.5 dinars, and individually wrapped spring rolls sell for 20 piasters (0.2 dinar) a piece. Elias spent exactly 100 dinars, and he remembered there were exactly 100 items in the bag. Can you break down the receipt for him?

1.4 Prime Numbers and Factorization

The term *factorization* refers to the process of expressing a positive integer as the product of two smaller numbers. For instance, we *factor* the number 91 when we write $91 = 7 \times 13$. In this sense, factorization is the reverse action of multiplication. A prime number can be thought of as an integer which cannot be factored. More precisely,

Definition. An integer $p \geq 2$ is called *prime* or a *prime number,* if it has no divisor strictly between 1 and p. The list of prime numbers begins with

$$2,\ 3,\ 5,\ 7,\ 11,\ 13,\ 17,\ 19,\ 23,\ 29,\ 31,\ 37,\ 41,\ 43,\ \ldots$$

An integer $n \geq 2$ which is not prime is called a *composite*.

1.4.1 Unique Factorization into Primes

Prime numbers are the building blocks of the integers, in the sense that every integer can be written as a product of primes, and that in an essentially unique way. We now observe some properties of primes which will lead to the establishment of this claim.

Theorem 1.7. Let p be a prime number. If p divides a product of integers, then p must divide one of them.

Proof. Assume that p divides mn. If p does not divide m, we will show that p divides n. Look at $\gcd(m, p)$. Being a divisor of p, this quantity is either 1 or p. So, if p does not divide m, then $\gcd(m, p) = 1$. Using the extended Euclidean algorithm, we can find integers a and b such that $ma + pb = 1$. Multiply this equality by n/p to get

$$\left(\frac{mn}{p}\right) a + nb = \frac{n}{p}$$

The quantity on the left-hand side is an integer, since p divides mn; hence so is n/p an integer, i.e., p divides n.

This argument can be repeated to prove the theorem for the case where the product involves three integers or more. ▽

By definition, a composite n can be factored as $n = a \times b$, where $1 < a, b < n$. If a or b is again composite, we can factor it again, and again, and with each step the factors decrease in size. After a finite number of steps, the final stage in this process will be something like

$$n = p_1 \times p_2 \times p_3 \times \cdots \times p_k$$

where each p_i is a prime number. But is it possible, for the same n, another person comes down to a *different* factorization, other than mere reordering of the primes? Well, suppose there are two such results:

$$p_1 \times p_2 \times p_3 \times \cdots \times p_k = q_1 \times q_2 \times q_3 \times \cdots \times q_h \tag{1.4}$$

We may cancel off common primes from each left and right, and if the p's and the q's are really different, then we end up with an equality like (1.4) in which none of the p's equals any of the q's.

However, by Theorem 1.7, p_1 must divide one of the q's. This cannot happen as distinct primes do not divide each other. And that can only mean that the factorization of n into primes involves a unique collection of prime factors. We have proved the *fundamental theorem of arithmetic*.

Theorem 1.8 (The Fundamental Theorem of Arithmetic)**.** Every integer $n \geq 2$ can be factored into prime numbers in a unique way, apart from reordering of the prime factors.

For example, in factoring the number 936 into primes, one may obtain $936 = 3 \times 2 \times 3 \times 13 \times 2 \times 2$, while another $936 = 13 \times 2 \times 2 \times 3 \times 2 \times 3$. But, it would be impossible to find a prime factor outside the collection $\{2, 2, 2, 3, 3, 13\}$. We normally write the final factorization, where all the factors are primes, using the exponential notation in order to clearly display the repeated primes, e.g.,

$$936 = 2^3 \times 3^2 \times 13 \tag{1.5}$$

Exercise* 1.39. Amira claims that she has found a counter-example to the fundamental theorem of arithmetic by showing a different factorization: $936 = 2 \times 3 \times 167$, which she insists is correct—only that it is not written in decimal. Which integer base does Amira have in mind? Does her finding really contradict Theorem 1.8?

Exercise 1.40. Factor these numbers into primes.

a) 888
b) 36000
c) 63756
d) 111111

We have sensed here that factoring in general is harder than multiplying. The most basic, and slowest, factoring algorithm is the *trial division*, where we repeatedly divide n by the primes 2, 3, 5, 7, ... in an attempt to discover a prime factor. Note that only primes up to $\sqrt{n}$ need to be considered, and if no such factor is found then we may conclude that n is itself prime.

Question. Why don't we need to consider prime factors larger than $\sqrt{n}$?

Example. Determine whether the number 577 is prime or composite, using trial division.

Solution. We have $\sqrt{577} \approx 24.02$. The only prime numbers up to 24 are 2, 3, 5, 7, 11, 13, 17, 19, and 23. After a little bit of checking, we see that none of these primes divides 577. Hence, 577 is itself a prime number.

Exercise 1.41. Determine prime or composite by trial division. If composite, factor the number into primes.

a) 239
b) 841
c) 911
d) 1147

1.4.2 GCD and LCM via Factorization

It is sometimes convenient to express the factorization of n into primes using the product notation,

$$n = \prod_{i \geq 1} p_i^{e_i} = p_1^{e_1} \times p_2^{e_2} \times p_3^{e_3} \times \cdots$$

where the product ranges over all prime numbers, $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, ... The exponents e_i will be zero except for finitely many of them. For example with $n = 936$, Equation (1.5) shows that $e_1 = 3$, $e_2 = 2$, $e_6 = 1$, and $e_i = 0$ for all the rest.

Now let $d = \prod p_i^{d_i}$ be the prime factorization of another integer d. As a consequence of Theorem 1.7 and the fundamental theorem of arithmetic, if d divides $n = \prod p_i^{e_i}$ then it is necessary that $d_i \leq e_i$. This fact leads to a more explicit way of evaluating the functions $\gcd(m, n)$ and $\operatorname{lcm}(m, n)$, provided that the factorizations of m and n have been established.

Theorem 1.9. Let $m = \prod p_i^{f_i}$ and $n = \prod p_i^{e_i}$, and let $\min(e_i, f_i)$ and $\max(e_i, f_i)$ denote the lesser and the greater, respectively, of e_i and f_i. Then,

$$\gcd(m, n) = \prod p_i^{\min(e_i, f_i)} \quad \text{and} \quad \operatorname{lcm}(m, n) = \prod p_i^{\max(e_i, f_i)}$$

Proof. Suppose d divides n, where $d = \prod p_i^{d_i}$. We have argued that a necessary condition for d is that $d_i \leq e_i$. Now if d also divides m then as well $d_i \leq f_i$. Hence the greatest common divisor of m and n is such an integer d for which $d_i = e_i$ or $d_i = f_i$, whichever is smaller. This gives $d_i = \min(e_i, f_i)$. The proof for $\operatorname{lcm}(m, n)$ is very similar. ▽

For example, having factored $m = 2^5 \times 3 \times 7^2 \times 13^8 \times 37 \times 101$ and $n = 2^{11} \times 3^2 \times 5^9 \times 11 \times 13^4 \times 23 \times 37$, we readily conclude that

$$\begin{aligned} \gcd(m, n) &= 2^5 \times 3 \times 13^4 \times 37 \\ \operatorname{lcm}(m, n) &= 2^{11} \times 3^2 \times 5^9 \times 7^2 \times 11 \times 13^8 \times 23 \times 37 \times 101 \end{aligned}$$

Thus Theorem 1.9 provides a second method for evaluating $\gcd(m, n)$ without the use of the Euclidean algorithm. Even so, factorization in general is extremely time-consuming—while in contrast, the Euclidean algorithm is particularly a very efficient algorithm.

Exercise 1.42. Redo Exercise 1.32, this time evaluate $\gcd(m, n)$ by factoring m and n.

Note that with Theorem 1.9, we are now able to derive the relation

$$\gcd(m,n) \times \operatorname{lcm}(m,n) = m \times n \tag{1.6}$$

thereby proving Theorem 1.4. Details are asked in the next exercise.

Exercise 1.43. Redo Exercise 1.33, this time evaluate both $\gcd(m,n)$ and $\operatorname{lcm}(m,n)$ by way of factoring m and n. In each case, verify that (1.6) holds and then try to write a proper proof of Theorem 1.4.

As a further consequence of the fundamental theorem of arithmetic, it is not difficult to show that the list of prime numbers never ends. This claim is stated in the next theorem, whose proof was first given by Euclid some 2500 years ago. Our proof here is a slightly modified version of his.

Theorem 1.10. There are infinitely many prime numbers.

Proof. Form the following sequence of integers.

$$\begin{aligned} a_1 &= 2 \\ a_2 &= a_1 + 1 = 3 \\ a_3 &= a_1 a_2 + 1 = 7 \\ a_4 &= a_1 a_2 a_3 + 1 = 43 \\ &\vdots \\ a_k &= a_1 a_2 a_3 \cdots a_{k-1} + 1 \end{aligned}$$

We claim that every pair (a_m, a_n) of two numbers taken from this sequence has $\gcd(a_m, a_n) = 1$. To see why this is true, assuming $m > n$, we can write

$$a_m = a_1 a_2 a_3 \cdots a_n \cdots a_{m-1} + 1$$

which shows that $a_m \bmod a_n = 1$. By Theorem 1.3, we have $\gcd(a_m, a_n) = \gcd(a_n, 1) = 1$. This says that each successive term in the sequence a_k yields a completely new set of prime factors, proving their infinitude. ▽

Question. Does this theorem imply that there are only finitely many composites?

1.4.3 Power Mod Computations

We are to observe that in computing $ab \bmod n$, we may first reduce a and b by replacing them with their respective remainders mod n. The congruence notation, which was introduced in Section 1.2.1, provides a convenient way to state this theorem.

Theorem 1.11. Let $n > 0$ be a fixed integer. For any integers a and b,

$$(a \bmod n)(b \bmod n) \equiv ab \pmod{n}$$

Proof. By definition, we have

$$\begin{aligned}(a \bmod n)(b \bmod n) &= \left(a - \lfloor \frac{a}{n} \rfloor n\right)\left(b - \lfloor \frac{b}{n} \rfloor n\right) \\ &= ab + n\left(\lfloor \frac{a}{n} \rfloor \lfloor \frac{b}{n} \rfloor n - a\lfloor \frac{b}{n} \rfloor - b\lfloor \frac{a}{n} \rfloor\right)\end{aligned}$$

Moreover, since $ab = ab \bmod n + \lfloor ab/n \rfloor n$, we are then allowed to write

$$(a \bmod n)(b \bmod n) = ab \bmod n + nk$$

for some integer k. It follows that $(a \bmod n)(b \bmod n) \bmod n = ab \bmod n$, proving the congruence. ▽

Now some applications, like in cryptography, involve the task of computing an expression of the form $a^k \bmod n$ with a very large exponent k, e.g., $2^{1000} \bmod 7$. Note that in this example, while the power 2^{1000} is quite large, its remainder mod 7 will not exceed 6!

With Theorem 1.11, we will evaluate $a^k \bmod n$ by iteratively multiplying a to itself, k times, while in each step reducing the product mod n, in order to keep the calculations manageable. Being more clever, the *successive squaring algorithm*, described next, achieves this goal in much less time.

Example. Compute $3^{234} \bmod 25$ by the successive squaring algorithm.

Solution. We will form a sequence of successive squares with initial term 3, in which each term is reduced mod 25. In displaying the result below, we omit writing "mod 25" for better readability.

$$\begin{aligned}3^2 &= 9 \\ 3^4 &= 9^2 = 6 \\ 3^8 &= 6^2 = 11 \\ 3^{16} &= 11^2 = 21 \\ 3^{32} &= 21^2 = 16 \\ 3^{64} &= 16^2 = 6 \\ 3^{128} &= 6^2 = 11\end{aligned}$$

The next square, 3^{256}, is bigger than 3^{234}, so we stop here. Next, we express the exponent 234 in binary, which is really the sum of powers of 2, i.e.,

$$234 = 11101010_2 = 128 + 64 + 32 + 8 + 2$$

Finally, we rely on Theorem 1.11 to conclude that

$$\begin{aligned} 3^{234} \bmod 25 &= (3^{128} \times 3^{64} \times 3^{32} \times 3^8 \times 3^2) \bmod 25 \\ &= (11 \times 6 \times 16 \times 11 \times 9) \bmod 25 = 19 \end{aligned}$$

Exercise 1.44. Use the successive squaring algorithm for each power mod.
a) $2^{22} \bmod 10$
b) $5^{99} \bmod 36$
c) $23^{333} \bmod 100$
d) $2^{2249} \bmod 23$

Test 1.45. What is the *unit digit*, i.e., right-most digit, of the number 7^{99}?
a) 1
b) 3
c) 7
d) 9

From the theoretical point of view, power mod operation touches on an elegant theorem of Fermat, which plays an important role in the RSA cryptography of the next section. However, the theorem will not be proved until later in the text—twice, in fact, restated as Theorems 3.30 and 4.15.

Theorem 1.12 (Fermat's Little Theorem)**.** Suppose that a is an integer not divisible by the prime p. Then $a^{p-1} \bmod p = 1$.

For example, knowing that 5647 is prime, Fermat's little theorem assures us that $89^{5646} \bmod 5647 = 1$.

Exercise 1.46. Compute the following powers mod 23, a prime, mentally—with the help of Fermat's little theorem.
a) $100^{22} \bmod 23$
b) $5^{24} \bmod 23$
c) $3^{47} \bmod 23$
d) $2^{2249} \bmod 23$

Exercise* 1.47. If p is a prime number, prove that $a^p \equiv a \pmod{p}$ for every integer a.

Exercise 1.48. Prove that 779 is composite without factoring it, but by showing that $2^{778} \bmod 779 \neq 1$, thereby failing the statement of Fermat's little theorem.

Exercise* 1.49. Is it possible to have $2^{p-1} \bmod p = 1$, but p is composite? Find an example or explain why it is not possible.

1.4.4 An Application in Cryptography

The technology of data transfer has become an inseparable part of the modern life, be it over the Internet, email, or mobile telephone. At times it becomes necessary to send sensitive data, such as a credit card number, over a secure line.

Cryptography is a field of study wherein we analyze different algorithms by which we convert such a sensitive numeric into a secret number which can be read only by the intended recipient who possesses the secret key to it. (A non-numerical message can be treated numerically, usually by assigning a value to each character such as that based on the ASCII table.) One application we wish to present here is the RSA algorithm, named after its three inventors, Rivest, Shamir, and Adleman in 1976.

Let's say Amira represents an online company which involves receiving important data from its users. She secretly selects two distinct, very large prime numbers p and q (of at least 100 digits each) and another positive integer e such that

$$\gcd((p-1)(q-1), e) = 1$$

Of course, Amira uses the Euclidean algorithm to check this gcd condition. In fact, she employs the extended Euclidean algorithm, which gives her two more integers, $a < 0$ and $b > 0$, such that

$$(p-1)(q-1)a + eb = 1$$

Question. What if the algorithm does not yield $a < 0$ and $b > 0$?

Amira then computes $n = p \times q$ and goes on to post on her web site the two values of n and e, with the following instruction: Everyone who wishes to send her an integer m (the sensitive message) must first convert m into a secret number s, based on the formula

$$s = m^e \bmod n$$

This can be performed efficiently using the successive squaring algorithm. And when Amira receives this value of s, she uses her secret key b to recover the intended message m, also using the successive squaring algorithm, i.e.,

$$s^b \bmod n = m \tag{1.7}$$

Why is this true? First, by Fermat's little theorem, we have

$$m^{(p-1)(q-1)} \bmod p = (m^{p-1})^{q-1} \bmod p = 1^{q-1} \bmod p = 1$$
$$m^{(p-1)(q-1)} \bmod q = (m^{q-1})^{p-1} \bmod q = 1^{p-1} \bmod q = 1$$

These two equations imply that $m^{(p-1)(q-1)} - 1$ is a common multiple of p and q. Being distinct, both p and q must appear in the prime factorization of $m^{(p-1)(q-1)} - 1$. Hence, $m^{(p-1)(q-1)} - 1$ is actually a multiple of pq, and

$$m^{(p-1)(q-1)} \bmod pq = 1$$

Remembering that $p \times q = n$, we observe that

$$m^{eb} = m^{1-(p-1)(q-1)a} = m \times (m^{(p-1)(q-1)})^{-a}$$

and therefore, proving (1.7),

$$s^b \bmod n = m^{eb} \bmod n = m(1)^{-a} \bmod n = m$$

assuming that $m < n$. With the size of n being very large, this is probably the case, but if $m > n$ then m needs to be cut up into two or more blocks of smaller integers and sent one at a time.

Question. Where has Theorem 1.11 been used again in this algorithm?

However, just how secure is this RSA algorithm? Recall that only n and e are known to the public. In the worst case, an enemy can also steal s when it is transmitted across the Internet. Knowing n, e, and s, can the enemy recover the secret key b and/or the intended message m?

The only known feasible way to retrieve b is to first find the factors p and q; and that is exactly the strength of RSA: While multiplying takes a quadratic time, with respect to the number of digits in p and q, factoring takes an exponential time. To illustrate, with the size of n around 200 digits, if multiplying p and q took only one second, then factoring n would take 10^{18} years!

Example. Let us suppose, for a small example, that $p = 29$ and $q = 101$. Hence, $n = 29 \times 101 = 2929$ and $(p-1)(q-1) = 2800$. Amira selects $e = 13$ and runs the extended Euclidean algorithm, arriving at the result

$$2800(-5) + 13(1077) = 1$$

Her secret key is $b = 1077$, whereas the values of $n = 2929$ and $e = 13$ are made public.

Now suppose Elias is an online customer who wishes to send securely to Amira the number $m = 888$. He first computes

$$888^{13} \bmod 2929 = 2705$$

then sends her this number $s = 2705$. Upon receiving s, Amira computes

$$2705^{1077} \bmod 2929 = 888$$

which is the correct intended number (message) from Elias.

Exercise 1.50. In this mini RSA exercise, Amira uses $n = 391$ and $e = 5$.

a) Elias is to give her the message $m = 234$. What is the value of s which he sends to Amira?
b) Find p and q using trial division.
c) Find Amira's secret key b and verify that $s^b \bmod 391 = 234$.
d) Another time Amira receives $s = 319$. Discover the intended message m and cross-check that $m^5 \bmod 391 = 319$.

Exercise* 1.51. The statement $a^{p-1} \bmod p = 1$ in Fermat's little theorem relies on the assumption that p does not divide a. The RSA algorithm, however, assumes the theorem without knowing whether p or q divides m. In theory, the probability of such occurrence is extremely small in view of the abundance of primes their size. Nevertheless, please modify the RSA argument to confirm that (1.7) remains valid even if p or q divides m.

1.4.5 Recognizing Large Composites

We have seen that with trial division we can factor any integer, at least theoretically, or prove that it is prime. There are times, as in RSA, when we need to distinguish large primes from composites. We will see two algorithms which can be used to identify large composites without resorting to factorization. While they may not work for *all* composites, these algorithms are still far superior than trial division in time efficiency.

The first such algorithm is based on Fermat's little theorem. The statement of Theorem 1.12 holds whenever p is prime; so if it fails for some integer $p = n$, whose primality is to be determined, then we may safely conclude that n is composite.

Example. Given $n = 989$. Choosing $a = 2$, we use the successive squaring algorithm to discover that $2^{988} \bmod 989 = 213 \neq 1$, a result which would violate Fermat's little theorem if 989 were prime. Hence, we conclude that 989 is composite.

Question. Have you wondered why Fermat's theorem is called *little*?

Fermat's little theorem, however, is not designed to recognize a prime number. What this means is, if $a^{n-1} \bmod n = 1$, we are not allowed to hastily conclude that n is a prime. See, for instance, that $2^{340} \bmod 341 = 1$, and yet 341 is genuinely composite, as $341 = 11 \times 31$. What we can do in such a case is perhaps try another value of a, e.g., $3^{340} \bmod 341 = 56 \neq 1$, which confirms that 341 is indeed composite.

Exercise 1.52. Which ones of the following numbers are recognized as composites using Fermat's little theorem with base $a = 2$ and/or $a = 3$?

a) 561
b) 779
c) 1013
d) 1387

Definition. Suppose that $a^{n-1} \bmod n = 1$ for some integer $a \geq 2$ and some odd number n. If the number n is composite, then we call n a *Fermat pseudoprime* base a.

As we have just seen, the number 341 is a Femat pseudoprime base 2, but not base 3. The worst kind of a Fermat pseudoprime is when $a^{n-1} \bmod n = 1$ holds for many values of a. In fact, the Carmichael numbers n, defined next, are Fermat pseudoprimes to all bases a as long as $\gcd(a, n) = 1$.

Definition. A composite n is called a *Carmichael number* when n factors into distinct primes such that for each prime factor p, the number $p - 1$ divides $n - 1$.

For example, 561 is a Carmichael number because $561 = 3 \times 11 \times 17$, all distinct primes, and 560 is divisible by 2, by 10, and by 16. In fact, 561 is actually the smallest Carmichael number.

Exercise 1.53. Use trial division to factor each number, then verify that the composite is a Carmichael number.
a) 1729
b) 2465
c) 6601
d) 8911

Exercise 1.54. Find two examples of a prime $p < 100$ such that the number $n = 7 \times 31 \times p$ is Carmichael.

Exercise* 1.55. Show why a Carmichael number must be odd.

Theorem 1.13. Suppose that $\gcd(a, n) = 1$. If n is a Carmichael number, then n is a Fermat pseudoprime base a.

Proof. We will demonstrate the claim for $n = 561$ in a structural way which readily applies to all Carmichael numbers n in general.

Let $\gcd(a, 561) = 1$, so a is not a multiple of 3, 11, or 17. By Fermat's little theorem we have $a^{p-1} \bmod p = 1$ for each $p = 3$, 11, and 17. Since

$$a^{560} = (a^2)^{280} = (a^{10})^{56} = (a^{16})^{35}$$

we see by Theorem 1.11 that $a^{560} \bmod p = 1$ for each $p = 3$, 11, and 17. It follows that 3, 11, and 17 are all prime factors of the number $a^{560} - 1$. And as $3 \times 11 \times 17 = 561$, we conclude that $a^{560} \bmod 561 = 1$. $\triangledown$

Although rare, it has been discovered that Carmichael numbers are infinitely many. If the job is to catch composites, Fermat's little theorem is therefore rather weak at it. A stronger compositeness test is based on the following observation.

Theorem 1.14. If p is a prime and $x^2 \bmod p = 1$ for some integer x, then either $x \bmod p = 1$ or $x \bmod p = p - 1$.

Proof. We have p dividing $x^2 - 1 = (x + 1)(x - 1)$. By Theorem 1.7, either p divides $x + 1$ or $x - 1$; the former implies $x \bmod p = p - 1$ and the latter $x \bmod p = 1$. ▽

Theorem 1.14 may not hold for composites, e.g., $5^2 \bmod 12 = 1$, where neither $5 \bmod 12 = 1$ nor $5 \bmod 12 = 11$ is true. In fact, this is the idea: if $a^{n-1} \bmod n = 1$ and we suspect that n might be a pseudoprime, we will look at $a^{(n-1)/2} \bmod n$. If this last quantity is neither 1 nor $n - 1$ then, failing the theorem, n must be a composite. The full algorithm is given as the next compositeness test.

Theorem 1.15 (Miller-Rabin Test)**.** Let n be an odd integer whose primality is to be determined, and fix a base number a such that $\gcd(a, n) = 1$. Write $n - 1 = 2^e \times d$ where d is odd, and consider the sequence given by

$$a^d \bmod n,\ a^{2d} \bmod n,\ a^{4d} \bmod n,\ a^{8d} \bmod n,\ \ldots\ ,\ a^{n-1} \bmod n$$

If a term equals 1 and is preceded by neither 1 nor $n-1$, then n is composite.

Proof. Each successive term is obtained by squaring the previous one, hence by Theorem 1.14, a 1 must be preceded by 1 or $n - 1$, if n be prime. ▽

Note that the sequence consists of $e + 1$ numbers in all, the last term being $a^{2^e \times d} \bmod n$. Moreover, if this last term is not 1, then n is composite, but that is Fermat's little theorem.

Example. We try the Carmichael number 561 for Miller-Rabin test with $a = 2$. Since $560 = 2^4 \times 35$, there are 5 terms in our sequence:

$$2^{35} \bmod 561,\ 2^{70} \bmod 561,\ 2^{140} \bmod 561,\ 2^{280} \bmod 561,\ 2^{560} \bmod 561$$

Using successive squaring algorithm, this sequence turns out to be

$$263,\ 166,\ 67,\ 1,\ 1$$

Note the term 1 preceded by 67, so we conclude that 561 is composite.

Exercise 1.56. Test the Carmichael numbers given in Exercise 1.53 using Theorem 1.15. Which ones are recognized as composites?

Still, Miller-Rabin test may miss some composites which go undetected by Theorem 1.15. We call such odd composites *strong pseudoprimes* base a. The smallest strong pseudoprime base 2 is $2047 = 23 \times 89$. You may verify, with $2046 = 2 \times 1023$, that the two terms in the sequence are just 1 and 1.

Exercise 1.57. The following composites are all Fermat pseudoprimes base 2. Which ones are also strong pseudoprimes base 2?

a) 1105
b) 2821
c) 3277
d) 4033

Exercise* 1.58. Explain why every strong pseudoprime is necessarily a Fermat pseudoprime, to the same base.

As a final remark, although strong pseudoprimes do exist, Theorem 1.15 can nevertheless be used to recognize primes within certain bounds. It has been tested, for instance, that there are no strong pseudoprimes less than 2 trillion to the bases 2, 3, 5, 7, and 11 simultaneously. Hence, within this huge interval, a number n which "passes" Miller-Rabin test to these five bases must be a genuine prime.

Books to Read

1. D. M. Bressoud, *Factorization and Primality Testing,* Springer 1989.

2. S. C. Coutinho, *The Mathematics of Ciphers: Number Theory and RSA Cryptography,* A K Peters 1999.

3. O. Ore, *Number Theory and Its History,* 1948, Dover Publications 1988.

4. W. Trappe and L. C. Washington, *Introduction to Cryptography with Coding Theory,* Second Edition, Prentice Hall 2005.