Chapter 1

Divisibility

Number theory is concerned with the properties of the integers. By the word *integers* we mean the counting numbers 1, 2, 3, . . . , together with their negatives and zero. Accordingly the word *number,* loosely used or symbolically denoted throughout this book, will be understood an integer, unless otherwise stated.

1.1 Divisors and Residues

It is reasonable to claim without proof that performing an addition, subtraction, or multiplication with two integers will result in another integer. Dividing an integer by another, however, does not always return an integer value—and that is exactly where we begin the study of numbers.

We shall denote the output in dividing m by d using the notation $\frac{m}{d}$ or m/d. In general, for $d \neq 0$, the quantity m/d is called a *rational number.*

Definition. We say that the integer d *divides* m, or that m is *divisible* by d, if m/d is again an integer.[1] Such a relation may be written $d \mid m$, or $d \nmid m$ if it is not true. When $d \mid m$, we also say that d is a *divisor* or a *factor* of m, whereas we will call m a *multiple* of d.

Example. To illustrate the idea, let us consider a few examples.

1. The number 3 divides 18 since $18/3 = 6$, an integer. We write $3 \mid 18$.
2. We have $5 \nmid 18$ because $18/5 = 3.6$, not an integer. Hence, 5 is not a divisor of 18.

[1] Alternately, d divides m if there is an integer c such that $cd = m$. This is the more versatile definition since, for one thing, division requires borrowing from the higher field of rational numbers. The two definitions differ in one minor case—can you identify it?

3. Both the numbers 28 and 42 have 7 as a common factor. We can see this by writing $28 = 7 \times 4$ and $42 = 7 \times 6$.

4. Multiples of 2 are integers of the form $2k$. These are the numbers $0, \pm 2, \pm 4, \pm 6, \ldots$, which we call the *even* numbers. The remaining, noneven integers are the *odd* numbers, i.e., not divisible by 2.

EXERCISE 1.1. Does 7 divide 19392?[2]

Note that 0 cannot divide any number, for division by 0 is not allowed. However, the number 0 is always divisible by other integers! This and some other elementary facts about divisibility are listed next.

Proposition 1.1. The following statements hold.

1) The number 1 divides all integers.

2) If $d \neq 0$, then $d \mid 0$ and $d \mid d$.

3) If $d \mid m$ and $m \mid n$, then $d \mid n$.

4) If $d \mid m$ and $d \mid n$, then $d \mid (am + bn)$ for any integers a and b.

Proof. The first two statements follow immediately from the definition of divisibility. For (3) we simply observe that if m/d and n/m are integers, then so is $n/d = n/m \times m/d$. Similarly for (4), the number

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

is an integer when $d \mid m$ and $d \mid n$. ▽

The sum of any multiples of m and n, i.e., $am + bn$, is commonly called a *linear combination* of m and n. Proposition 1.1(4) states, in other words, that a common divisor of two numbers divides their linear combinations too.

EXERCISE 1.2. Investigate true or false.

a) If $d \mid m$ then $d \leq m$.
b) If $m \mid n$ and $n \mid m$, then $m = n$.
c) If $c \mid m$ and $d \mid n$, then $cd \mid mn$.
d) If $d \mid mn$, then either $d \mid m$ or $d \mid n$.
e) If $dn \mid mn$ then $d \mid m$.

EXERCISE 1.3. Prove that $n^2 + 2$ is not divisible by 4 for any integer n.

[2] The number 19392 is a zip code earlier seen in this book!

Definition. For any real number x, the notation $\lfloor x \rfloor$ denotes the greatest integer no more than x. For example, $\lfloor 3.14 \rfloor = 3$ and $\lfloor 2 \rfloor = 2$. The function $f(x) = \lfloor x \rfloor$ is known as the *floor function,* and $\lfloor x \rfloor$ reads *the floor of* x. It is useful to note the inequalities $\lfloor x \rfloor \leq x < \lfloor x \rfloor + 1$.

Exercise 1.4. Evaluate $\lfloor 19392/7 \rfloor$.

Exercise 1.5. The *ceiling function* $\lceil x \rceil$, a companion to the floor function, returns the least integer value no less than x. Prove the chain of inequalities $\lceil x \rceil - 1 \leq \lfloor x \rfloor \leq x \leq \lceil x \rceil \leq \lfloor x \rfloor + 1$.

Definition. With $n > 0$, we define the *residue* of m *mod* n,

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

Here, the symbol % is used to stand for the word *mod.*[3] For example, since $\lfloor 18/5 \rfloor = 3$, then $18 \,\%\, 5 = 18 - 3 \times 5 = 3$. Similarly, $18 \,\%\, 3 = 18 - 6 \times 3 = 0$. Refering to the operation $m \,\%\, n$, we at times say that m is *reduced mod* n.

Exercise 1.6. Find these residues.

a) $369 \,\%\, 5$
b) $24 \,\%\, 8$
c) $123456789 \,\%\, 10$
d) $19392 \,\%\, 7$
e) $7 \,\%\, 11$

Exercise 1.7. Suppose the time is now 11 o'clock in the morning. What time will it be after 100 hours? How does this problem relate to residues?

Note that $m \,\%\, n$ is really the remainder upon dividing m by n, using the *long division* technique taught in grade school, and that it lies in the range $0 \leq m \,\%\, n \leq n - 1$. In particular, $m \,\%\, n = 0$ if and only if $n \mid m$. These claims, though seemingly obvious, need to be stated and proved carefully.

Theorem 1.2. Suppose m and n are integers, with $n > 0$. Then

1) $0 \leq m \,\%\, n \leq n - 1$

2) $m \,\%\, n = 0$ if and only if $n \mid m$

3) if $m = qn + r$ with $0 \leq r \leq n - 1$, then $q = \lfloor \frac{m}{n} \rfloor$ and $r = m \,\%\, n$.

[3] Adopted from Java programming language, the notation $m \,\%\, n$ is a personal preference to the usual m mod n. The latter is sometimes confused with the mod in a congruence relation, (Chapter 3) which is very closely related to residue mod.

Proof. Let $Q = \lfloor \frac{m}{n} \rfloor$ and $R = m \,\%\, n$. By definition, we have $Q \leq \frac{m}{n}$, hence $R = m - Qn \geq m - \frac{m}{n} \times n = 0$. But we also have $Q + 1 > \frac{m}{n}$, and so $R = m - Qn < m - (\frac{m}{n} - 1)n = n$. It follows that $0 \leq R < n$, proving (1).

For (2), if $\frac{m}{n}$ is an integer then clearly $R = m - \frac{m}{n} \times n = 0$. Conversely, if $0 = R = m - Qn$ then $Q = \frac{m}{n}$. Since Q is an integer, we then have $n \mid m$.

Lastly, suppose that $m = qn + r$ with $0 \leq r \leq n - 1$. Then $\frac{m}{n} = q + \frac{r}{n}$ with $0 \leq \frac{r}{n} < 1$. It can only mean, by the definition of the floor function, that $\lfloor \frac{m}{n} \rfloor = q$, from which $r = m \,\%\, n$ follows as well. $\bigtriangledown$

Example. Let $n = 2$. Since $m \,\%\, 2 = 0$ or 1, we find that the set of integers can be partitioned in two groups, i.e., the even numbers, of the form $2k$, and the odd numbers, of the form $2k + 1$. Similarly with $n = 3$, there are three classes of integers, of the forms $3k$, $3k + 1$, and $3k + 2$.

Exercise 1.8. Define the *absolute residue* of m *mod* n to be

$$m \,\%\%\, n = \begin{cases} m \,\%\, n & \text{if } m \,\%\, n \leq \frac{n}{2} \\ m \,\%\, n - n & \text{if } m \,\%\, n > \frac{n}{2} \end{cases}$$

For lack of a better notation, we use %% to read *absolute mod*.

a) Show that $0 \leq |m \,\%\%\, n| \leq n/2$.
b) Show that $m \,\%\%\, n = 0$ if and only if $n \mid m$.
c) Suppose $m = qn + m \,\%\%\, n$. Find the relation between q and $\lfloor m/n \rfloor$.
d) Redo Exercise 1.6, replacing % by %%.

Concluding this first section, the following fact, simple but useful, can be proved using the concept of residues.

Proposition 1.3. One in every k consecutive integers is divisible by k.

Proof. Let m be the first integer, and let $r = m \,\%\, k$. If $r = 0$ then $k \mid m$. Otherwise $1 \leq r \leq k - 1$, and our consecutive integers can be written as

$$m = \lfloor \tfrac{m}{k} \rfloor k + r,\ \lfloor \tfrac{m}{k} \rfloor k + r + 1,\ \lfloor \tfrac{m}{k} \rfloor k + r + 2,\ \ldots\ ,\ \lfloor \tfrac{m}{k} \rfloor k + r + k - 1$$

with $r + k - 1 \geq k$. Then one of these numbers is $\lfloor \frac{m}{k} \rfloor k + k$, which is a multiple of k. $\bigtriangledown$

Exercise 1.9. Prove the following statements.

a) A number in the form $n^2 \pm n$ is always even.
b) A number in the form $n^3 - n$ is divisible by 3.
c) The number $n^2 - 1$ is divisible by 8 when n is odd.
d) The number $n^5 - n$ is a multiple of 5 for every integer n.

1.2 Greatest Common Divisors

Given two integers m and n, we can always find a common divisor, e.g., $d = 1$. Moreover, every nonzero integer can have only a finite number of divisors, since $d \mid m$ implies $|d| \le |m|$. We are then interested in finding the greatest of all divisors common to m and n, for this quantity is of central importance in the theory of divisibility.

Definition. The *greatest common divisor* of two integers m and n, not both zero, is the largest integer which divides both. This number is denoted by $\gcd(m, n)$. For example, $\gcd(18, 24) = 6$ because 6 is the largest integer with the property $6 \mid 18$ and $6 \mid 24$.

Exercise 1.10. Evaluate $\gcd(m, n)$.

a) $\gcd(28, 42)$
b) $\gcd(36, -48)$
c) $\gcd(24, 0)$
d) $\gcd(1, 99)$
e) $\gcd(123, 100)$

Exercise 1.11. Find all integers n from 1 to 12 such that $\gcd(n, 12) = 1$.

Exercise 1.12. Investigate true or false.

a) $\gcd(m, n) > 0$
b) $\gcd(m, n) = \gcd(m - n, n)$
c) $\gcd(m, mn) = m$
d) $\gcd(m, m + 1) = 1$
e) $\gcd(m, m + 2) = 2$

Now there is an algorithm to evaluate $\gcd(m, n)$ which is very time-efficient, even for large values of m and n; and that is the well-known *Euclidean algorithm*, which is essentially an iterative application of the following theorem.

Theorem 1.4. For any integers m and $n > 0$, we have

$$\gcd(m, n) = \gcd(n, m \,\%\, n)$$

Proof. It suffices to show that the two pairs (m, n) and $(n, m \,\%\, n)$ have identical sets of common divisors. This is achieved entirely using Proposition 1.1(4) upon observing that, from its definition, $m \,\%\, n$ is a linear combination of m and n, as is m of n and $m \,\%\, n$. $\triangledown$

Example (Euclidean Algorithm). Suppose we wish to evaluate $\gcd(486, 171)$. Upon computing $486 \,\%\, 171 = 486 - 2 \times 171 = 144$, the theorem gives us $\gcd(486, 171) = \gcd(171, 144)$. We may then iterate this process another time by computing $171 \,\%\, 144$, and on as follows.

$$\begin{aligned}
486 - (2)\ 171 &= 144 & \rightarrow \quad \gcd(486,171) &= \gcd(171,144)\\
171 - (1)\ 144 &= 27 & &= \gcd(144,27)\\
144 - (5)\ 27 &= 9 & &= \gcd(27,9)\\
27 - (3)\ 9 &= 0 & &= \gcd(9,0)
\end{aligned}$$

We arrive in the end at the result $\gcd(486, 171) = \gcd(9, 0) = 9$. In general, the answer will be the last residue before we reach $m \,\%\, n = 0$.

EXERCISE 1.13. Use the Euclidean algorithm to evaluate $\gcd(m, n)$.

a) $\gcd(456, 144)$
b) $\gcd(999, 503)$
c) $\gcd(1000, 725)$
d) $\gcd(12345, 67890)$
e) $\gcd(19392, 29391)$

EXERCISE 1.14. Show that $\gcd(m, n) = \gcd(n, m \,\%\%\, n)$, and use this to reevaluate $\gcd(m, n)$ given in Exercise 1.13. (See Exercise 1.8 for the definition of absolute residue.) This makes the algorithm even faster as each subsequent residue, in absolute value, is no more than half its predecessor.

Next, an extremely important property about greatest common divisors is the fact that $\gcd(m, n)$ is actually a linear combination[4] of m and n.

Theorem 1.5 (Bezout's Lemma). There exist integers a and b such that

$$\gcd(m, n) = am + bn$$

Proof. Since $\gcd(m, n) = \gcd(m, -n)$, we may just assume that $n > 0$. Now the sequence of residues in applying the Euclidean algorithm consists of strictly decreasing positive integers, thus says Theorem 1.2(1):

$$\begin{array}{ccccccc}
\gcd(m,n) & = & \gcd(n, m \,\%\, n) & = & \gcd(m \,\%\, n, n \,\%\, (m \,\%\, n)) & = & \cdots \\
n & > & m \,\%\, n & > & n \,\%\, (m \,\%\, n) & > & \cdots
\end{array}$$

Hence this algorithm must terminate with a zero residue, say $\gcd(m, n) = \cdots = \gcd(d, 0) = d$. Since each of these residues is a linear combination of the previous pair of integers, by going through a finite number of steps, we may express d as a linear combination of m and n. ▽

[4] Remember, gcd is a linear combination!

Exercise 1.15. Prove that if $d \mid m$ and $d \mid n$, then $d \mid \gcd(m, n)$.

Exercise 1.16. If $\gcd(m, n) = am + bn$, show that $\gcd(a, b) = 1$.

The algorithm involved in actually finding the integers a and b given in Bezout's lemma is called the *extended Euclidean algorithm.* It is suggested in the proof of Theorem 1.5 that we perform repeated backward substitutions upon completing the Euclidean algorithm. This could be very messy. Let us illustrate, instead, a neat tabular version of the extended Euclidean algorithm, due to W. A. Blankinship (1963).

Example (Extended Euclidean Algorithm). Let us reconsider $\gcd(486, 171)$, this time expressing it as a linear combination of 486 and 171. We form rows of three numbers, beginning with

486	1	0
171	0	1

Since $\lfloor 486/171 \rfloor = 2$, we subtract 2 times the second row from the first. This gives the next row,

144	1	−2

Next, as $\lfloor 171/144 \rfloor = 1$, we subtract this third row from the second in order to get the fourth row,

27	−1	3

Continue in this manner until we get 0 in the first column:

d	a	b
486	1	0
171	0	1
144	1	−2
27	−1	3
9	6	−17
0	−19	54

We claim that, for each row, the triple (d, a, b) satisfies the equality $d = 486a + 171b$. In particular, the row before the last gives the desired linear combination, $\gcd(486, 171) = 9 = 486(6) + 171(-17)$.

Exercise 1.17. Justify these claims, proving that the algorithm is valid for any pair (m, n) of nonzero integers.

Exercise 1.18. Continue with Exercise 1.13 and find integers a and b, for which $\gcd(m, n) = am + bn$.

Exercise 1.19. Repeat Exercise 1.18, using absolute mod in performing the Euclidean algorithm. Do we get the same values of a and b?

Bezout's lemma further leads to a number of ready consequences, blending together the properties of divisibility and those of gcd. Upon presenting these, we will be ready to move on to the next section.

Proposition 1.6. Let L be the set of all linear combinations of m and n.

1) L is equal to the set of all multiples of $\gcd(m, n)$.

2) $\gcd(m, n)$ is the least[5] positive element of L.

3) $\gcd(m, n) = 1$ if and only if the number 1 belongs to L.

4) $\gcd(m, n) = 1$ if and only if L is the set of all integers.

Proof. All multiples of $\gcd(m, n)$ belong to L, according to Bezout's lemma. Conversely, $\gcd(m, n)$ divides every element in L, by Proposition 1.1(4). This proves the first statement, from which follows the rest. $\triangledown$

Corollary 1.7. If $d \mid m$ and $d \mid n$, then $\gcd(m/d, n/d) = \gcd(m, n)/d$. In particular, if $d = \gcd(m, n)$ then $\gcd(m/d, n/d) = 1$.

Proof. By Proposition 1.6(2) $\gcd(m/d, n/d)$ is the least positive linear combination of m/d and n/d, which is $1/d$ times the least positive linear combination of m and n, which is $\gcd(m, n)/d$. $\triangledown$

Exercise 1.20. Prove that if $k > 0$ then $\gcd(km, kn) = k \gcd(m, n)$.

Definition. Two integers m and n are said to be *relatively prime* or *coprime* to each other when $\gcd(m, n) = 1$. This is to say that the two have no common factor larger than 1. Proposition 1.6(4) says that a pair of relatively prime integers can represent any number as their linear combination.

Theorem 1.8. The following statements hold.

1) If $d \mid mn$ and $\gcd(d, m) = 1$, then $d \mid n$. (Euclid's Lemma)

2) If $c \mid m$ and $d \mid m$, with $\gcd(c, d) = 1$, then $cd \mid m$.

3) If $\gcd(m, n) = 1$ and $\gcd(m, N) = 1$, then $\gcd(m, nN) = 1$.

Proof. 1) Recall that gcd is a linear combination. If $\gcd(d, m) = 1$, then $1 = ad + bm$ for some integers a and b. Multiplying this by n/d yields $n/d = an + b(mn/d)$, which is an integer if $d \mid mn$.

[5] So the least shall be the greatest!

2) Again, $\gcd(c, d) = 1$ implies $1 = ac + bd$. This time multiply by $m/(cd)$ to get $m/(cd) = a(m/d) + b(m/c)$, which is an integer if $c \mid m$ and $d \mid m$.

3) Write $1 = am + bn$ and $1 = Am + BN$, and multiply the two together:

$$1 = (aAm + aBN + bAn)m + (bB)nN$$

This last equation displays the number 1 as a linear combination of m and nN. Hence, $\gcd(m, nN) = 1$ by Proposition 1.6(4). $\bigtriangledown$

Euclid's lemma, namely Theorem 1.8(1), is another simple yet very useful divisibility fact. Note that the relatively prime condition, $\gcd(d, m) = 1$, cannot be omitted. Consider for example, $6 \mid 72 = 8 \times 9$, where 6 divides neither 8 nor 9. The same can be said of Theorem 1.8(2) where, for instance, $4 \mid 60$ and $6 \mid 60$, but $4 \times 6 = 24 \nmid 60$.

Exercise 1.21. Prove the following statements.

a) Every number in the form $n^3 - n$ is divisible by 6.
b) If n is odd then $n^3 - n$ is divisible by 24.
c) The number 30 divides $n^5 - n$ for all integers n.
d) The product of five consecutive integers is a multiple of 120.

1.3 Linear Diophantine Equations

We are now in a position to describe the general solutions of linear equations in two variables x and y, in the form $mx + ny = c$. By a solution, of course, we mean integer solution; and that is the only reason an equation is called *diophantine*.

Being a linear combination of m and n, says Proposition 1.6(1), c is required to be a multiple of $\gcd(m, n)$, or else there can be no solution. Assume therefore, $\gcd(m, n) \mid c$. We then know how to find a and b, for which $ma + nb = \gcd(m, n)$. This equation, multiplied through by $c/\gcd(m, n)$, will produce at least one solution for x and y. We give first an example before proceeding to finding the general solution.

Example. Let us find (x, y) such that $486x + 171y = 36$. From the earlier example on the extended Euclidean algorithm, we have $\gcd(486, 171) = 9 = 486(6) + 171(-17)$. We multiply through this equation by 4 to get $486(24) + 171(-68) = 36$, thus one solution pair, $x = 24$ and $y = -68$.

Exercise 1.22. Find a solution of $34x + 55y = 11$.

Theorem 1.9 (Linear Equation Theorem)**.** The linear equation $mx+ny=c$ has a solution if and only if $d = \gcd(m,n) \mid c$, in which case all its solutions are given by the pairs (x,y) satisfying

$$x = x_0 - \frac{kn}{d} \quad \text{and} \quad y = y_0 + \frac{km}{d}$$

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

Proof. The necessary and sufficient divisibility condition has already been explained. Now suppose we have a particular solution (x_0, y_0). We consider first the case $d = 1$. All solutions to the linear equation must lie on the line passing through (x_0, y_0) with a slope of $-m/n$. Another point on this line will be given by $(x_0 - t,\ y_0 + tm/n)$ for any real number t. If the coordinates are to be integers, then by Euclid's lemma we must have $t = kn$ for some integer k. Thus the general solution $(x_0 - kn,\ y_0 + km)$.

If now $d > 1$, replace the linear equation by $(m/d)x + (n/d)y = c/d$. Doing so will not alter its solution set. But then Corollary 1.7 implies that $\gcd(m/d, n/d) = 1$ and, repeating the argument for $d = 1$, we arrive at the general solution $(x_0 - kn/d,\ y_0 + km/d)$. ▽

Exercise 1.23. Prove that $\gcd(m,n) = 1$ if and only if the linear equation $mx + ny = 1$ has a solution.

Example. The previous example continues. We have found a particular solution $(x,y) = (24, -68)$ to the equation $486x + 171y = 36$. The general solution is then given by $(24 - 171k/9,\ -68 + 486k/9) = (24 - 19k,\ -68 + 54k)$ for any integer k. For instance, $k = 1$ corresponds to a solution $(5, -14)$ and $k = 2$ gives $(-14, 40)$.

Exercise 1.24. Find all the solutions, if any, for each linear equation.

a) $34x + 55y = 11$
b) $12x + 25y = 1$
c) $24x + 18y = 9$
d) $25x + 65y = -5$
e) $42x - 28y = 70$

Exercise 1.25. Arun made two calls using his Orange$^{\text{TM}}$mobile—one local call to a Zain network user, for 7 piasters per minute, and an international call to Indonesia, for 13 piasters a minute. The total charge was 1 dinar and 54 piasters. For how long did Arun talk in each call?[6]

[6] The peculiar company names in this problem are relevant in the kingdom of Jordan, where 1 dinar is equivalent to 100 piasters.

1.4 Divisibility Criteria [Project 1]

Without using a calculator, there are relatively quick tests we can perform to find small factors of a given number. Let's say, $n = 1234567890123456$. The following criteria apply.

1) The number n is divisible by 2, or 5, if and only if its *unit digit* is, respectively. In this example, 6 is the unit digit. Hence, $2 \mid n$ and $5 \nmid n$.

2) The number n is divisible by 3, or 9, if and only if its *iterative digit sum* is. In this case, $1+2+3+4+5+6+7+8+9+0+1+2+3+4+5+6 = 66$. Then, $6+6 = 12$, and $1+2 = 3$. Thus $3 \mid n$, while $9 \nmid n$.

3) For divisibility by 11, similarly, we may replace n by its alternating digit sum. Here, $1-2+3-4+5-6+7-8+9-0+1-2+3-4+5-6 = 2$. Since $11 \nmid 2$, then $11 \nmid n$.

4) For divisibility by 7 or 13, we work with the alternating sum of consecutive 3-digit blocks. For this example, $1 - 234 + 567 - 890 + 123 - 456 = -889$, divisible by 7 but not 13. We conclude, $7 \mid n$ and $13 \nmid n$.

Project 1.4.1. Write the proof for each item above, for arbitrary n. Then try to find similar criteria for divisibility by 4, 8, 10, 25, 37, and 101.

And here is a divisibility-by-17 test. Write $n = 10t + u$, where u is the unit digit in n. For instance, if $n = 125443$ then $t = 12544$ and $u = 3$. We claim that $17 \mid n$ if and only if $17 \mid (t - 5u)$. With $n = 125443$, we have

$$12544 - 5 \times 3 = 12529 \rightarrow 1252 - 5 \times 9 = 1207 \rightarrow 120 - 5 \times 7 = 85$$

Since $17 \mid 85$, we conclude that $17 \mid 125443$. Indeed, $125443 = 17 \times 7379$.

Project 1.4.2. Prove the divisibility criteria below, where $n = 10t + u$ as before. Illustrate each one with some fairly large numbers of your choice.

a) $17 \mid n$ if and only if $17 \mid (t - 5u)$
b) $19 \mid n$ if and only if $19 \mid (t + 2u)$
c) $13 \mid n$ if and only if $13 \mid (t + 4u)$
d) $7 \mid n$ if and only if $7 \mid (t - 2u)$

Finding a factor of a given integer n will be a recurring theme of this book. For large and arbitrary n, this problem is not an easy one, even with the help of modern computing machines. We will encounter more about factoring methods in the next chapter, including a coming project (Section 2.4) on this topic.