

1 Numbers

This chapter serves as an introduction to the modern theory of algebra through the natural numbers $0, 1, 2, \dots$. The list of natural numbers never ends and most of them are far beyond everyday use. Gigantic numbers of more than 100 digits are used to protect information transmitted over the internet.

Suppose Alice has to send a message to Bob over the internet and it must be kept secret. Alice and Bob live far apart and many intermediate computers will see the message on its way. Alice will have to scramble (encrypt) the message and send it, but at the same time Bob will have to know how to unscramble (decrypt) it. How does Alice get this information through to him? She could call and tell him. But then again someone could be listening in on their phone call. Is there a way out of this problem?

The answer is an amazing “yes” and it builds on a current paradox of mathematics: the existence of so-called one-way functions $f(X)$. These are functions easy to compute given the input X . Once they are computed and only $f(X)$ is known, it appears to be exceedingly difficult to recover X unless some secret information is known.

Here is an example of a one-way function. Fix a natural number N and let $f(X) = [X^3]$, where $[Y]$ denotes the remainder of Y after division by N . This is a function $f : M \rightarrow M$, where $M = \{0, 1, 2, \dots, N - 1\}$. When $N = 15$, f can be tabulated as

X	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
$f(X)$	0	1	8	12	4	5	6	13	2	9	10	11	3	7	14

Of course we can easily find X given $f(X)$ by using the above table. But in general, as N grows the difficulty of finding X given $f(X)$ seems insurmountable unless you know some secret information. In the above example the secret information is that $f(f(X)) = X$ (you can see this using the table). In a sense we are raising a number to the third power and then scrambling things up by

taking the remainder. So far nobody has found effective methods for finding cube roots in this setting. In the above example Alice sends the encrypted message $f(X)$ to Bob and Bob decrypts it using f . This is the basic principle behind the RSA cryptosystem [22], which was the first cryptosystem based on the groundbreaking idea [8] of using one-way functions (with a trapdoor).

On a more detailed level Bob computes two gigantic prime numbers (usually 100 digits or more) p and q and forms $N = pq$. He then uses p and q to compute a number e (for encryption) and a number d (for decryption). He makes the numbers N and e public so that people wishing to write secret messages to him can use the function $f(X) = [X^e]$ for encryption, where $[Y]$ denotes the remainder of Y after division by N . He keeps the function $g(X) = [X^d]$ secret (the point being that $g(f(X)) = X$). In the example above we have $p = 3, q = 5, N = 15, e = 3, d = 3$. One way of systematically finding the secret decryption function g in the RSA system is to find the prime factors p and q of N (N being available to the general public). The straightforward method of trial division (dividing with successive primes $2, 3, 5, \dots$) is much too slow. Mathematicians have tried at least since Gauss's time (1777–1855) to find faster methods for factoring numbers. In fact Gauss writes in ([11], Art. 329)

The problem of distinguishing prime numbers from composite numbers and of resolving the latter into their prime factors is known to be one of the most important and useful in arithmetic. It has engaged the industry and wisdom of ancient and modern geometers to such an extent that it would be superfluous to discuss the problem at length. Nevertheless we must confess that all methods that have been proposed thus far are either restricted to very special cases or are so laborious and prolix that even for numbers that do not exceed the limits of tables constructed by estimable men, i.e., for numbers that do not yield to artificial methods, they try the patience of even the practiced calculator. And these methods do not apply at all to larger numbers.

RSA Labs has put forward several factoring challenges. The hardest unsolved challenge is called RSA-2048. This is the 2048-bit number (617 digits) N on the cover of this book. It is known to be the product of two prime numbers p and q . A computer was instructed to forget p and q after forming $N = pq$. Given two candidates p' and q' , it is easy to multiply them to see if their product equals N . This can be done in a small fraction of a second on any modern computer. Nevertheless, finding p and q knowing only N seems to be a painstakingly slow process not within the limits of modern computers and algorithms. If you can find p and q you will be able to claim the \$200 000 prize by submitting your factorization via <http://www.rsasecurity.com/go/factorization.html>. Alternatively, you could settle for the less ambitious RSA factoring challenges presented at

<http://www.rsasecurity.com/rsalabs/challenges/factoring/numbers.html>. It has not been proved mathematically that factoring a number is a difficult problem in a precise sense, so a fast algorithm may exist waiting to be discovered. In a sense this would disrupt the pillars of the modern information age. The algebraic reasoning behind the RSA cryptosystem is founded on basic results (more than 300 years old) about the natural numbers.

1.1 The natural numbers and the integers

The natural numbers $1, 2, 3, \dots$ were handed over to mankind by God (in the words of Kronecker (1823–91)). Mankind later added the important natural number 0 . We will reserve the symbol \mathbb{N} for the natural numbers $\{0, 1, 2, 3, \dots\}$. The need for negative numbers leads us to introduce the set of integers $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$ containing the natural numbers \mathbb{N} . We have deliberately cut through the red tape of formally defining \mathbb{N} and \mathbb{Z} here. We will also take the addition (and subtraction) and multiplication of integers for granted. This will be the starting point of our study of numbers.

1.1.1 Well ordering and mathematical induction

For $X, Y \in \mathbb{Z}$ we define $X \leq Y$ if $Y - X \in \mathbb{N}$ and $X < Y$ if $X \neq Y$ and $X \leq Y$. This leads to the usual way of ordering the integers,

$$\dots < -3 < -2 < -1 < 0 < 1 < 2 < 3 < \dots$$

An element s in a subset $S \subseteq \mathbb{Z}$ is said to be a first element in S if $s \leq x$ for every $x \in S$. There are many subsets of \mathbb{Z} that do not have a first element. If a subset of \mathbb{Z} has a first element then the latter has to be unique (see Exercise 1.1 at the end of the chapter). The basic axiom for starting our investigation of numbers says that *every non-empty subset of \mathbb{N} has a first element*. We also say that the set of natural numbers is *well ordered*.

The property that \mathbb{N} is well ordered is equivalent to mathematical induction. Recall that mathematical induction says that if we are given statements $P(n)$ for every integer $n \geq 1$ such that

- (i) $P(1)$ is true and
- (ii) $P(n)$ is true implies that $P(n + 1)$ is true

then $P(n)$ is true for every $n \geq 1$.

Example 1.1.1 Let us prove the formula

$$1 + 2 + \cdots + n = \frac{n(n+1)}{2} \quad (1.1)$$

for $n \in \mathbb{N}$ using mathematical induction. This means that we consider (1.1) as a statement $P(n)$. Clearly $P(1)$ is true, since $1 \cdot (1+1) = 2$. Suppose now that $P(n)$ is true. Then

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

The right hand side can be rewritten as

$$\begin{aligned} \frac{n(n+1)}{2} + (n+1) &= \frac{n(n+1) + 2(n+1)}{2} \\ &= \frac{(n+1)(n+2)}{2}. \end{aligned}$$

This is the formula for $n+1$. So we have proved that $P(n)$ implies $P(n+1)$. By mathematical induction we have proved $P(n)$ for every $n \geq 1$.

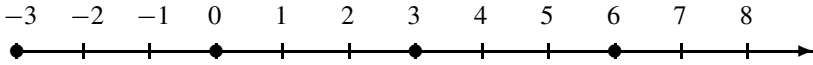
Of course, having the formal machinery for constructing a proof like this does not necessarily provide the beauty of a really ingenious mathematical argument. When Gauss was in school (at the age of seven) his mathematics teacher asked the class to sum up all numbers from 1 to 100. The students worked furiously with their small slates. Gauss was the first to give his slate with the number 5050 to the teacher. The teacher replied “Oh, I see, you probably knew the answer.” “No, no! I just realized that

$$\begin{aligned} 1 + 100 &= 101, \\ 2 + 99 &= 101, \\ 3 + 98 &= 101, \\ &\vdots \\ 100 + 1 &= 101. \end{aligned}$$

Therefore $1 + 2 + \cdots + 100 = (100 \cdot 101)/2 = 5050$,” Gauss replied.

1.2 Division with remainder

Suppose that you mark all multiples of 3 on the axis of the integers:



An integer is uniquely given by the closest multiple of 3 to its left and the remainder you have to walk to the right. Examples are $5 = 3 + 2 = 1 \cdot 3 + 2$, $7 = 6 + 1 = 2 \cdot 3 + 1$, $-2 = -3 + 1 = -1 \cdot 3 + 1$ and $6 = 6 + 0 = 2 \cdot 3 + 0$. Division with remainder is the generalization of this simple fact.

Theorem 1.2.1 *Let $d \in \mathbb{Z}$, where $d > 0$. For every $x \in \mathbb{Z}$ there is a unique remainder $r \in \mathbb{N}$ such that*

$$x = qd + r,$$

where $q \in \mathbb{Z}$ and $0 \leq r < d$.

Proof. To prove the uniqueness of r assume that $x = q_1d + r_1$ and $x = q_2d + r_2$, where $q_1, q_2, r_1, r_2 \in \mathbb{Z}$ and $0 \leq r_1, r_2 < d$. Then

$$(q_1 - q_2)d = r_2 - r_1.$$

If $r_1 \neq r_2$ we may assume that $r_2 > r_1$. This implies that $r_2 - r_1 = md$, where $m \geq 1$. But this contradicts the fact that $r_2 - r_1 \leq r_2 < d$. To prove the existence of r , let $M = \{x - qd \mid q \in \mathbb{Z}\}$. Then $M \cap \mathbb{N} \neq \emptyset$ (see Exercise 1.2) and we let r be the first element in the subset $M \cap \mathbb{N}$ of \mathbb{N} . Now $r = x - qd$ for some q and we claim that $0 \leq r < d$. If $r \geq d$ then $r > r - d \geq 0$ and $r - d = x - (q + 1)d \in M \cap \mathbb{N}$. This contradicts that r is the first element in $M \cap \mathbb{N}$. \square

Definition 1.2.2 Suppose that $a = bc$ where $a, b, c \in \mathbb{Z}$. Then we say that c is a *divisor* of a (it *divides* a). We write this as $c \mid a$.

Notice that 1 and -1 divide every integer and that 0 only divides 0.

Definition 1.2.3 If $x, d \in \mathbb{Z}$, where $d > 0$, we let $[x]_d$ denote the unique remainder r in Theorem 1.2.1. Sometimes we use the notation $[x]$ when it is clear which d we are using.

1.3 Congruences

Gauss published his monumental work [11] on numbers when he was 24 years old. He had begun his deep studies in the theory of numbers at age 18. At the

start of [11] he introduced the theory of congruences, which turned out to be of fundamental importance. Congruences form an elegant way of organizing the integers according to their remainders with respect to a fixed number.

Definition 1.3.1 Let $a, b, c \in \mathbb{Z}$. Then a and b are called *congruent modulo c* if c divides $b - a$. This is denoted

$$a \equiv b \pmod{c}.$$

This may seem strange at first, but using remainders the definition (for $c > 0$) just states that a and b are congruent modulo c if and only if a and b have the same remainder when divided by c . This is the content of the following:

Proposition 1.3.2 Let $c \in \mathbb{Z}$, where $c > 0$. Then

- (i) $a \equiv [a]_c \pmod{c}$,
- (ii) $a \equiv b \pmod{c}$ if and only if $[a]_c = [b]_c$,

for $a, b \in \mathbb{Z}$.

Proof. We may write $a = qc + [a]_c$ for some $q \in \mathbb{Z}$, by Theorem 1.2.1. Therefore $c \mid a - [a]_c = qc$. This proves (i). Now write $b = q'c + [b]_c$ for some $q' \in \mathbb{Z}$. Then $a - b = (q - q')c + [a]_c - [b]_c$. Therefore $c \mid a - b$ if and only if $c \mid [a]_c - [b]_c$. But $c \mid [a]_c - [b]_c$ if and only if $[a]_c = [b]_c$, since $0 \leq [a]_c, [b]_c < c$. This proves (ii). \square

Example 1.3.3 The integers 24 and 14 can be written $24 = 4 \cdot 5 + 4$ and $14 = 2 \cdot 5 + 4$. So $[24]_5 = [14]_5 = 4$. This means that $24 \equiv 14 \pmod{5}$. Of course this could just as easily have been observed from the fact that $5 \mid 24 - 14$.

Proposition 1.3.4 Suppose that $x_1 \equiv x_2 \pmod{d}$ and $y_1 \equiv y_2 \pmod{d}$. Then

- (i) $x_1 + y_1 \equiv x_2 + y_2 \pmod{d}$,
- (ii) $x_1 y_1 \equiv x_2 y_2 \pmod{d}$

for $x_1, x_2, y_1, y_2, d \in \mathbb{Z}$.

Proof. If d divides $x_1 - x_2$ and $y_1 - y_2$ then it also divides $x_1 - x_2 + y_1 - y_2 = x_1 + y_1 - (x_2 + y_2)$. This proves (i). Rearranging, we also get that d divides $x_1 y_1 - x_2 y_2 = x_1(y_1 - y_2) + y_2(x_1 - x_2)$. This proves (ii). \square

Proposition 1.3.4 may look innocuous at first. It is surprisingly useful. For one thing, when you combine it with Proposition 1.3.2, you get (see Exercise 1.3)

$$[xy] = [[x][y]]. \quad (1.2)$$

Using (1.2) you can tell in a flash that the remainder of 13^{2003} divided by 4 has to be 1 (how?). Take a look at the following example.

1.3.1 Repeated squaring – an example

How does one find the remainder of 12^{11} divided by 21 efficiently? This problem confronts a sender of a secret message in the RSA cryptosystem, where the encryption exponent is the number $e = 11$ and the possible messages are the natural numbers less than $N = 21$. As you may have guessed the trick is to avoid computing the integer 12^{11} , divide by 21 and find the remainder. First we write 11 in the binary expansion (11 can be expressed as 1011 in the binary positional system) as

$$2^3 + 2 + 1.$$

Then using (1.2) twice we see that

$$[12^{11}] = [12^{2^3} 12^{2^1} 12^1] = [[12^{2^3}][12^2][12^1]].$$

Again using (1.2) we build a table of remainders for use in the calculation

$$\begin{aligned} [12^1] &= 12, \\ [12^2] &= 18, \\ [12^{2^2}] &= [(12^2)^2] = [[12^2][12^2]] = [18 \cdot 18] = 9, \\ [12^{2^3}] &= [(12^{2^2})^2] = [[12^{2^2}][12^{2^2}]] = [9 \cdot 9] = 18. \end{aligned}$$

Picking out the relevant numbers we get

$$\begin{aligned} [12^{11}] &= [[18 \cdot 18] \cdot 12] \\ &= [9 \cdot 12] \\ &= 3. \end{aligned}$$

We have reduced the horrendous procedure of computing the remainder of $12^{11} = 743008370688$ divided by 21 to computing the remainders of numbers less than $21^2 = 441$. The algorithm above is called *repeated squaring*, because we constantly use the following consequence of (1.2):

$$[a^{2^n}] = [(a^{2^{n-1}})^2] = [[a^{2^{n-1}}][a^{2^{n-1}}]],$$

for $a, n \in \mathbb{Z}$ where $n \geq 0$ (recall that $(a^b)^c = a^{bc}$, where $a, b, c \in \mathbb{Z}$ with $b, c \geq 0$).

1.4 Greatest common divisor

Let

$$\text{div}(n) = \{d \in \mathbb{N} \mid d \mid n\}$$

denote the set of natural divisors in $n \in \mathbb{Z}$. Notice that $\text{div}(0) = \mathbb{N}$ and $\text{div}(n) = \text{div}(-n)$ for every $n \in \mathbb{Z}$.

Example 1.4.1 Let us list a few examples:

- (i) $\text{div}(18) = \{1, 2, 3, 6, 9, 18\}$,
- (ii) $\text{div}(24) = \{1, 2, 3, 4, 6, 8, 12, 24\}$,
- (iii) $\text{div}(36) = \{1, 2, 3, 4, 6, 9, 12, 18, 36\}$.

From this example we have

$$\text{div}(24) \cap \text{div}(18) = \{1, 2, 3, 6\} = \text{div}(6)$$

$$\text{div}(24) \cap \text{div}(36) = \{1, 2, 3, 4, 6, 12\} = \text{div}(12).$$

This indicates a striking fact. Given two integers m, n it seems that the common divisors $\text{div}(m) \cap \text{div}(n)$ of m and n are exactly the divisors $\text{div}(d)$ of some third number. This is not a coincidence. It was discovered by the Greek mathematician Euclid of Alexandria (325–265BC) and is contained in book seven of his masterpiece, the *Elements*.

Lemma 1.4.2 (Euclid) *Let $m, n \in \mathbb{Z}$. There exists a unique natural number $d \in \mathbb{N}$ such that*

$$\text{div}(m) \cap \text{div}(n) = \text{div}(d).$$

Proof. The uniqueness follows from the fact that $\text{div}(d_1) = \text{div}(d_2)$ if and only if $d_1 = d_2$ assuming that $d_1, d_2 \in \mathbb{N}$. When proving the existence of d we may assume that $m, n \in \mathbb{N}$, since $\text{div}(x) = \text{div}(-x)$ for $x \in \mathbb{Z}$. We proceed using induction on $\min(m, n)$, where $\min(m, n) = m$ if $m \leq n$ and $\min(m, n) = n$ if $m > n$. If $\min(m, n) = 0$ we may assume that $n = 0$. Therefore $\text{div}(m) \cap \text{div}(n) = \text{div}(m)$. This settles the initial step $\min(m, n) = 0$ of the induction.

Now assume that we have proved $\text{div}(m) \cap \text{div}(n) = \text{div}(d)$ for every $m, n \in \mathbb{N}$ with $\min(m, n) < N$, where $N > 0$. Suppose for the induction step that we are given $m, n \in \mathbb{N}$ with $\min(m, n) = N$ and that $m \geq n = N$. Then we may write $m = qn + r$, where $0 \leq r < n$ by Theorem 1.2.1. But (this is the clever step)

$$\text{div}(m) \cap \text{div}(n) = \text{div}(m - qn) \cap \text{div}(n) = \text{div}(r) \cap \text{div}(n),$$

since a number divides m and n if and only if it divides $m - qn$ and n . By induction we know that $\text{div}(r) \cap \text{div}(n) = \text{div}(d)$ for some $d \in \mathbb{N}$, since $\min(r, n) = r < n = N$. This completes the proof. \square

Definition 1.4.3 The unique number $d \in \mathbb{N}$ satisfying $\text{div}(d) = \text{div}(m) \cap \text{div}(n)$ is called the *greatest common divisor* of m and n . It is denoted $\text{gcd}(m, n)$.

If one of m and n is non-zero there is a finite number of common natural divisors. The greatest common divisor is really the greatest among these with respect to the usual ordering of \mathbb{Z} (see Exercise 1.9). Notice that $\text{gcd}(0, 0) = 0$.

1.5 The Euclidean algorithm

As already hinted in the inductive proof of Lemma 1.4.2, there is an algorithm for finding the greatest common divisor. The inductive step in the proof of Lemma 1.4.2 can be found in Euclid's *Elements* (around 300 BC) even though Euclid did not have the concept of induction and the rigor of a modern mathematical proof. The idea behind the modern version of Euclid's algorithm is the same.

Proposition 1.5.1 *Let $m, n \in \mathbb{Z}$. Then*

- (i) $\text{gcd}(m, 0) = m$ if $m \in \mathbb{N}$.
- (ii) $\text{gcd}(m, n) = \text{gcd}(m - qn, n)$ for every $q \in \mathbb{Z}$.

Proof. Since $\text{div}(0) = \mathbb{N}$, (i) follows. We get (ii) from the fact that

$$\text{div}(m) \cap \text{div}(n) = \text{div}(m - qn) \cap \text{div}(n).$$

This is a way of saying that a natural number d divides m and n if and only if d divides $m - qn$ and n , so that $\text{gcd}(m, n) = \text{gcd}(m - qn, n)$. \square

Suppose that we wish to find the greatest common divisor of $m, n \in \mathbb{Z}$. We may assume that $m \geq n \geq 0$. If $n = 0$, we are done since $\gcd(m, 0) = m$ by Proposition 1.5.1(i). Assume that $n > 0$. The basic observation is that if we divide m by n and write $m = qn + r$ according to Theorem 1.2.1, then

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

and $n > r$. This follows from Proposition 1.5.1(ii). An example shows how this works.

Example 1.5.2 Let $m = 34$ and $n = 13$. Then

$$\begin{aligned}\gcd(34, 13) &= \gcd(13, 8) = \gcd(8, 5) \\ &= \gcd(5, 3) = \gcd(3, 2) = \gcd(2, 1) \\ &= \gcd(1, 0) = 1.\end{aligned}$$

This can also be illustrated as a sequence of divisions with remainders:

$$\begin{aligned}34 &= 2 \cdot 13 + 8, \\ 13 &= 1 \cdot 8 + 5, \\ 8 &= 1 \cdot 5 + 3, \\ 5 &= 1 \cdot 3 + 2, \\ 3 &= 1 \cdot 2 + 1, \\ 2 &= 2 \cdot 1 + 0.\end{aligned}$$

Now return to the general case $m \geq n \geq 0$. Put $r_{-1} = m$ and $r_0 = n$. If $r_0 = 0$ then $\gcd(r_{-1}, r_0) = r_{-1}$. Otherwise define r_1 to be the remainder of r_{-1} divided by r_0 , so that $r_1 = r_{-1} - q_1 r_0$ for some integer q_1 . Then we have

$$\gcd(r_{-1}, r_0) = \gcd(r_0, r_1)$$

and $r_{-1} > r_0 > r_1$. Proceeding in this way (if $r_1 \neq 0$) we let $r_2 = r_0 - q_2 r_1$ be the remainder of r_0 divided by r_1 . Again we have

$$\gcd(r_0, r_1) = \gcd(r_1, r_2)$$

and $r_{-1} > r_0 > r_1 > r_2$. Eventually we are forced to the situation $r_N = 0$, for some step $N > 0$. This means that $\gcd(m, n) = \gcd(r_{N-1}, 0) = r_{N-1}$. The point is that the Euclidean algorithm gives rise to a strictly decreasing sequence of natural numbers $r_{-1} > r_0 > r_1 > \dots$. If we consider the subset $R = \{r_{-1}, r_0, r_1, \dots\}$ as a subset of \mathbb{N} , it has a first element $r_N \in R$ since \mathbb{N} is well ordered. If $r_N \neq 0$ we may continue division with remainder and get

$r_N > r_{N+1} \geq 0$, contradicting the fact that r_N is the first element in R . Therefore $r_N = 0$ and the Euclidean algorithm terminates in a finite number of steps.

A very important fact is hidden in the Euclidean algorithm: the greatest common divisor $\gcd(m, n)$ can be written as a \mathbb{Z} -linear combination of m and n . There exist integers λ and μ such that

$$\lambda m + \mu n = \gcd(m, n).$$

Let us go through the steps in the Euclidean algorithm once more and make a few adjustments.

Example 1.5.3 We know that $\gcd(34, 13) = 1$. The claim above says that one can find integers x and y such that $34x + 13y = 1$. This is not obvious. We need an algorithm for computing x and y . The trick is to adjust x and y for each remainder in the steps of the Euclidean algorithm:

$$\begin{aligned} 34 &= 1 \cdot 34 + 0 \cdot 13, \\ 13 &= 0 \cdot 34 + 1 \cdot 13, \\ 8 &= 34 - 2 \cdot 13 = (1 \cdot 34 + 0 \cdot 13) - 2 \cdot (0 \cdot 34 + 1 \cdot 13), \\ &= 1 \cdot 34 - 2 \cdot 13, \\ 5 &= 13 - 8 = (0 \cdot 34 + 1 \cdot 13) - (1 \cdot 34 - 2 \cdot 13) \\ &= -1 \cdot 34 + 3 \cdot 13, \\ 3 &= 8 - 5 = (1 \cdot 34 - 2 \cdot 13) - (-1 \cdot 34 + 3 \cdot 13) \\ &= 2 \cdot 34 - 5 \cdot 13, \\ 2 &= 5 - 3 = (-1 \cdot 34 + 3 \cdot 13) - (2 \cdot 34 - 5 \cdot 13) \\ &= -3 \cdot 34 + 8 \cdot 13, \\ 1 &= 3 - 2 = (2 \cdot 34 - 5 \cdot 13) - (-3 \cdot 34 + 8 \cdot 13) \\ &= 5 \cdot 34 - 13 \cdot 13. \end{aligned}$$

Attaching these small updates to the Euclidean algorithm we have produced the identity

$$5 \cdot 34 - 13 \cdot 13 = 1,$$

which would have been hard to guess initially.

Definition 1.5.4 The Euclidean algorithm with the above attachment for computing x and y is called the *extended Euclidean algorithm*.

Let us be a little more formal in the description of the extended Euclidean algorithm. Define at each step of the algorithm integers a_i and b_i with the

property that $a_i m + b_i n = r_i$. One can start by putting $a_{-1} = 1$, $b_{-1} = 0$ and $a_0 = 0$, $b_0 = 1$. The first step of the algorithm is $r_1 = r_{-1} - q_1 r_0$. The definition of a_1 and b_1 leaves no choice: $a_1 = a_{-1} - q_1 a_0$, $b_1 = b_{-1} - q_1 b_0$. The i th step proceeds similarly, as $r_i = r_{i-2} - q_i r_{i-1}$ (where $r_{i-2} = q_i r_{i-1} + r_i$ according to Theorem 1.2.1). This means that for $i \geq 1$ we put

$$\begin{aligned} a_i &= a_{i-2} - q_i a_{i-1}, \\ b_i &= b_{i-2} - q_i b_{i-1}. \end{aligned}$$

Assuming that $a_{i-1} m + b_{i-1} n = r_{i-1}$ and $a_{i-2} m + b_{i-2} n = r_{i-2}$ this ensures that

$$\begin{aligned} a_i m + b_i n &= (a_{i-2} - q_i a_{i-1}) m + (b_{i-2} - q_i b_{i-1}) n \\ &= a_{i-2} m + b_{i-2} n - q_i (a_{i-1} m + b_{i-1} n) \\ &= r_{i-2} - q_i r_{i-1} \\ &= r_i. \end{aligned}$$

The extended Euclidean algorithm is conveniently carried out using the table in the example below.

Example 1.5.5 The greatest common divisor of 13 and 8 is 1. Illustrated in the table below is the extended Euclidean algorithm, giving $-3 \cdot 13 + 5 \cdot 8 = 1$.

i	-1	0	1	2	3	4
r_i	13	8	5	3	2	1
q_i			1	1	1	1
a_i	1	0	1	-1	2	-3
b_i	0	1	-1	2	-3	5

Remark 1.5.6 Which numbers less than a given number result in the maximum number of steps in the Euclidean algorithm? To answer this question we need to define the Fibonacci numbers F_n . They are given by $F_0 = 1$, $F_1 = 1$ and $F_n = F_{n-1} + F_{n-2}$ for $n \geq 2$. The first few Fibonacci numbers are 1, 1, 2, 3, 5, 8, 13, 21, These numbers have a surprising relation ([16], subsection 4.5.3) to the complexity of the Euclidean algorithm: if $u > v > 0$ are integers, and u is the smallest number such that the Euclidean algorithm for u and v needs exactly n steps, then $u = F_{n+1}$ and $v = F_n$.

This result dates back to 1845 and is due to Lamé. Knuth [16] writes that it has the historical claim of being the first practical application of Fibonacci numbers.

Let us reiterate the very important fact contained in the extended Euclidean algorithm. It is the basis of almost all the results in the rest of this chapter.

Lemma 1.5.7 *Let $m, n \in \mathbb{Z}$. Then there are integers $\lambda, \mu \in \mathbb{Z}$ such that*

$$\lambda m + \mu n = \gcd(m, n).$$

Proof. Let $d = \gcd(m, n)$. The extended Euclidean algorithm gives this result if $m, n \in \mathbb{N}$. In this case we can find $\lambda, \mu \in \mathbb{Z}$ such that $\lambda m + \mu n = d$. Notice that $(-\lambda)(-m) + \mu n = \lambda m + (-\mu)(-n) = (-\lambda)(-m) + (-\mu)(-n) = d$. So it is easy to get the result for $m, n \in \mathbb{Z}$. \square

Definition 1.5.8 Two integers $a, b \in \mathbb{Z}$ are called *relatively prime* if

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

Remark 1.5.9 Notice that if there are $\lambda, \mu \in \mathbb{Z}$ such that $\lambda a + \mu b = 1$ then a and b are relatively prime (see Exercise 1.14).

Corollary 1.5.10 *Suppose that $a \mid bc$, where $a, b, c \in \mathbb{Z}$ and a and b are relatively prime. Then $a \mid c$.*

Proof. According to Lemma 1.5.7, we may find $\lambda, \mu \in \mathbb{Z}$ such that $\lambda a + \mu b = 1$. Multiply this equation by c and get $\lambda ac + \mu bc = c$. Now a divides the left hand side, since a divides bc . Therefore a divides c . \square

Corollary 1.5.11 *Let $a, b, c \in \mathbb{Z}$.*

- (i) *If a and b are relatively prime, $a \mid c$ and $b \mid c$ then $ab \mid c$.*
- (ii) *If a and b are relatively prime and a and c are relatively prime then a and bc are relatively prime.*

Proof. Since $\gcd(a, b) = 1$ we get $\lambda a + \mu b = 1$ for suitable $\lambda, \mu \in \mathbb{Z}$ by Lemma 1.5.7. Both a and b divide c , so we may write $c = ax = by$ for suitable $x, y \in \mathbb{Z}$. Then

$$c = c(\lambda a + \mu b) = c\lambda a + c\mu b = by\lambda a + ax\mu b = ab(y\lambda + x\mu).$$

This proves (i). To prove (ii), we again use Lemma 1.5.7. This time we get two identities $\lambda a + \mu b = 1$ and $\lambda_1 a + \mu_1 c = 1$ for suitable $\lambda, \mu, \lambda_1, \mu_1 \in \mathbb{Z}$.

Multiplying these we get

$$(\lambda\lambda_1a + \lambda\mu_1c + \lambda_1\mu b)a + \mu\mu_1bc = 1.$$

This shows that $\gcd(a, bc) = 1$, so that a and bc must be relatively prime. \square

In trying to grasp statements as Corollaries 1.5.10 and 1.5.11, it often pays to play with small numbers to find counter-examples, such as the simple fact that $4 \mid 2 \cdot 2$ but $4 \nmid 2$. Also, $6 \mid 12$ and $3 \mid 12$ but $6 \cdot 3 = 18 \nmid 12$.

1.6 The Chinese remainder theorem

Think of a natural number x less than 30. Let a, b, c respectively denote the rows (numbered upwards from zero) in the three tables below, in which the number is located.

0	2	4	6	8	10	12	14	16	18	20	22	24	26	28
1	3	5	7	9	11	13	15	17	19	21	23	25	27	29

0	3	6	9	12	15	18	21	24	27
1	4	7	10	13	16	19	22	25	28
2	5	8	11	14	17	20	23	26	29

0	5	10	15	20	25
1	6	11	16	21	26
2	7	12	17	22	27
3	8	13	18	23	28
4	9	14	19	24	29

For example, if $x = 14$ then $a = 0, b = 2$ and $c = 4$. The real surprise is that one needs only to know these three row numbers in order to determine the original number. This is called the 30-riddle. It has impressed many souls unspoiled by abstract algebra and number theory. The most hard-core algebraists will say it is trivial, referring to the fundamental isomorphism $\mathbb{Z}/30 \cong \mathbb{Z}/2 \times \mathbb{Z}/3 \times \mathbb{Z}/5$. Let us expand a little on this theme.

Definition 1.6.1 Define

$$\mathbb{Z}/N = \{X \in \mathbb{N} \mid 0 \leq X < N\},$$

for $N \in \mathbb{N}$. If $N = n_1 \cdots n_t \neq 0$ is the product of $n_1, \dots, n_t \in \mathbb{N}$ we let

$$r : \mathbb{Z}/N \rightarrow \mathbb{Z}/n_1 \times \cdots \times \mathbb{Z}/n_t$$

be the map given by $r(X) = ([X]_{n_1}, \dots, [X]_{n_t})$. We call r the *remainder map*.

Example 1.6.2 Let $N = 2 \cdot 3 \cdot 5 = 30$ and $x = 14$. Then

$$r(x) = (0, 2, 4).$$

This corresponds to the fact that 14 is in row 0 of the first table, row 1 of the second table and row 4 of the third table.

The secret to unlocking the 30-riddle is contained in the following lemma.

Lemma 1.6.3 Suppose that $N = n_1 \cdots n_t$, where $n_1, \dots, n_t \in \mathbb{N} \setminus \{0\}$ and $\gcd(n_i, n_j) = 1$ if $i \neq j$. Then the remainder map

$$r : \mathbb{Z}/N \rightarrow \mathbb{Z}/n_1 \times \cdots \times \mathbb{Z}/n_t$$

is bijective.

Proof. If $r(X) = r(Y)$ then $n_1 \mid X - Y, \dots, n_t \mid X - Y$ by Proposition 1.3.2(i). Repeated application of Corollary 1.5.11 gives $N = n_1 \cdots n_t \mid X - Y$. Since $0 \leq X, Y < N$, the only way that this is possible is if $X = Y$, so r must be injective. This implies that r is bijective, since it is an injective map between two sets with the same number of elements. \square

Lemma 1.6.3 explains the 30-riddle in the sense that a natural number less than 30 is uniquely given by its remainders by division with 2, 3 and 5. The only practical problem is to find a way to compute the inverse map r^{-1} . This is the map you need in order to impress your friends by practicing magic with the 30-riddle. We move on to state and prove the more classical version of Lemma 1.6.3 known as the Chinese remainder theorem (the theorem can be traced back to the Chinese mathematicians Sun-Tsu (around 280–473) and Chin Chiu Shao (1247)). At the end of the proof you will see how to compute the map r^{-1} .

Theorem 1.6.4 (Chinese remainder theorem) Suppose that $N = n_1 \cdots n_t$, where $n_1, \dots, n_t \in \mathbb{Z} \setminus \{0\}$ and $\gcd(n_i, n_j) = 1$ for $i \neq j$. Consider the system

$$\begin{aligned} X &\equiv a_1 \pmod{n_1}, \\ X &\equiv a_2 \pmod{n_2}, \\ &\vdots \\ X &\equiv a_t \pmod{n_t} \end{aligned} \tag{1.3}$$

of congruences for $a_1, \dots, a_t \in \mathbb{Z}$. Then

- (i) (1.3) has a solution $X \in \mathbb{Z}$.
- (ii) If $X, Y \in \mathbb{Z}$ are solutions of (1.3) then $X \equiv Y \pmod{N}$. If X is a solution of (1.3) and $Y \equiv X \pmod{N}$ then Y is a solution of (1.3).

Proof. We will prove (ii) first. If X, Y are two solutions of (1.3) then $X \equiv a_j \pmod{n_j}$ and $Y \equiv a_j \pmod{n_j}$ for $j = 1, \dots, t$. Therefore $X \equiv Y \pmod{n_j}$ (see Exercise 1.11). So $n_j \mid X - Y$, $j = 1, \dots, t$ and since the n_j are relatively prime, we get (by repeated application of Corollary 1.5.11) that $N = n_1 \cdots n_t$ divides $X - Y$ or $X \equiv Y \pmod{N}$. However, if $Y \equiv X \pmod{N}$ then $Y \equiv X \pmod{n_j}$ for $j = 1, \dots, t$. In this case, Y also solves (1.3). This proves (ii).

The proof of (i) comes from the extended Euclidean algorithm (Lemma 1.5.7) and the fact that n_j and N/n_j are relatively prime (by repeated application of Corollary 1.5.11): we can find integers λ_j, μ_j such that

$$\begin{aligned} \lambda_1 n_1 + \mu_1 N/n_1 &= 1, \\ \lambda_2 n_2 + \mu_2 N/n_2 &= 1, \\ &\vdots \\ \lambda_t n_t + \mu_t N/n_t &= 1. \end{aligned}$$

These identities give the useful numbers $A_j = \mu_j(N/n_j)$ for $j = 1, \dots, t$. Notice that $A_j \equiv 1 \pmod{n_j}$ and $A_j \equiv 0 \pmod{n_i}$ if $i \neq j$. We can build a solution from these by putting

$$X = a_1 A_1 + \cdots + a_t A_t.$$

You can check immediately that X solves (1.3). □

The following example shows how the map r^{-1} is computed using the proof of Theorem 1.6.4(i).

Example 1.6.5 Let us test our knowledge on the 30-riddle itself. Here $n_1 = 2$, $n_2 = 3$ and $n_3 = 5$. The first step is to find $\lambda_i, \mu_i \in \mathbb{Z}$ such that

$$\lambda_1 n_1 + \mu_1 N / n_1 = 2\lambda_1 + 15\mu_1 = 1,$$

$$\lambda_2 n_2 + \mu_2 N / n_2 = 3\lambda_2 + 10\mu_2 = 1,$$

$$\lambda_3 n_3 + \mu_3 N / n_3 = 5\lambda_3 + 6\mu_3 = 1.$$

Here we can take $\lambda_1 = -7, \mu_1 = 1, \lambda_2 = -3, \mu_2 = 1, \lambda_3 = -1, \mu_3 = 1$. Therefore we get $A_1 = 15, A_2 = 10, A_3 = 6$ and

$$X = 15a_1 + 10a_2 + 6a_3$$

as a solution to the system

$$X \equiv a_1 \pmod{2},$$

$$X \equiv a_2 \pmod{3},$$

$$X \equiv a_3 \pmod{5}$$

of congruences. By taking the remainder of X after division by 30 we get the number $X', 0 \leq X' < 30$, solving the 30-riddle. If $a_1 = 0, a_2 = 2, a_3 = 4$, we get $X = 20 + 24 = 44$. This gives $X' = [X]_{30} = 14$ as expected.

1.7 Euler's theorem

Let

$$(\mathbb{Z}/N)^* = \{X \in \mathbb{Z}/N \mid \gcd(X, N) = 1\}$$

for $N \in \mathbb{N}$ and define the function $\varphi(N) = |(\mathbb{Z}/N)^*|$. This function is the famous Euler φ -function. It counts the numbers relatively prime to and smaller than a given natural number. The beginning of the table of values looks like

n	0	1	2	3	4	5	6	7	8	9	10	11	12	13
$\varphi(n)$	0	1	1	2	2	4	2	6	4	6	4	10	4	12

If you can come up with an effective way of computing φ you will have broken the RSA cryptosystem. The above table was constructed by listing the numbers less than n and counting the ones relatively prime to n . This is a terribly slow way of computing φ . There is a better way, which is still not good enough. It is based on factoring the number n and use of the Chinese remainder theorem. From the table above it is clear that one cannot expect $\varphi(mn) = \varphi(m)\varphi(n)$ for

general numbers m and n . Once again the key notion is that of relatively prime numbers.

Proposition 1.7.1 *Let m and n be relatively prime natural numbers. Then*

$$\varphi(mn) = \varphi(m)\varphi(n).$$

Proof. Put $N = mn$ and let $r : \mathbb{Z}/N \rightarrow \mathbb{Z}/m \times \mathbb{Z}/n$ be the remainder map. We know that r is a bijective map by Lemma 1.6.3. If we can prove that

$$r((\mathbb{Z}/N)^*) = (\mathbb{Z}/m)^* \times (\mathbb{Z}/n)^*$$

then we are done, since r then restricts to give a bijective map from $(\mathbb{Z}/N)^*$ to $(\mathbb{Z}/m)^* \times (\mathbb{Z}/n)^*$. Thus we need to prove that $\gcd(X, N) = 1$ if and only if $\gcd([X]_m, m) = 1$ and $\gcd([X]_n, n) = 1$.

Recall that $\gcd(a, c) = \gcd(c, [a]_c)$ for $a, c \in \mathbb{Z}$ with $c > 0$, by Proposition 1.5.1(ii). So $\gcd([X]_m, m) = 1$ and $\gcd([X]_n, n) = 1$ if and only if $\gcd(X, m) = 1$ and $\gcd(X, n) = 1$. It follows by Corollary 1.5.11 that $\gcd(X, m) = 1$ and $\gcd(X, n) = 1$ if and only if $\gcd(X, mn) = 1$. This proves that $\gcd(X, N) = 1$ if and only if $\gcd([X]_m, m) = 1$ and $\gcd([X]_n, n) = 1$. \square

Let us state and prove the main theorem, which is due to Euler (1707–83).

Theorem 1.7.2 (Euler) *Let $a, n \in \mathbb{Z}$ be relatively prime integers, where $n \in \mathbb{N}$. Then*

$$a^{\varphi(n)} \equiv 1 \pmod{n}.$$

Proof. First list the $\varphi(n)$ numbers less than and relatively prime to n :

$$0 \leq a_1 < a_2 < \cdots < a_{\varphi(n)} < n.$$

As a key point we will prove that

$$\{[aa_1], \dots, [aa_{\varphi(n)}]\} = \{a_1, \dots, a_{\varphi(n)}\}, \quad (1.4)$$

where we consider remainders with respect to n . Now, $[aa_i] = [aa_j]$ implies that $aa_i \equiv aa_j \pmod{n}$ by Proposition 1.3.2. Therefore $n \mid a(a_i - a_j)$. Since $\gcd(n, a) = 1$ we have $n \mid a_i - a_j$ by Corollary 1.5.10. This is only possible when $a_i = a_j$ or $i = j$. Thus $[aa_i] \neq [aa_j]$ when $i \neq j$. Notice that $\gcd(n, aa_i) = 1$ by Corollary 1.5.11. This implies that $\gcd(n, aa_i) = \gcd(n, [aa_i]) = 1$ by Proposition 1.5.1(ii). To sum up, we have $\varphi(n)$ different numbers $[aa_1], \dots, [aa_{\varphi(n)}] \in \mathbb{Z}/n$ all having greatest common divisor 1

with n . The only way this is possible is by having the identity in (1.4). This identity gives

$$[aa_1][aa_2] \cdots [aa_{\varphi(n)}] = a_1 a_2 \cdots a_{\varphi(n)}.$$

Since $aa_i \equiv [aa_i] \pmod{n}$ by Proposition 1.3.2(i), we get

$$a^{\varphi(n)} a_1 a_2 \cdots a_{\varphi(n)} \equiv a_1 a_2 \cdots a_{\varphi(n)} \pmod{n},$$

so that

$$n \mid a_1 \cdots a_{\varphi(n)} (a^{\varphi(n)} - 1).$$

By repeated application of Corollary 1.5.11 we get $\gcd(n, a_1 \cdots a_{\varphi(n)}) = 1$. This shows that $n \mid a^{\varphi(n)} - 1$ by Corollary 1.5.10. Therefore $a^{\varphi(n)} \equiv 1 \pmod{n}$. \square

After having learned a little group theory we will be able to give a really elegant proof of Euler's theorem. This will be a prime example of how things become easier once you find the right (abstract) framework.

1.8 Prime numbers

A prime number is a natural number $p > 1$ that cannot be expressed as a product of natural numbers strictly less than p . In our notation this means that $\text{div}(p) = \{1, p\}$. This is a fundamental definition. The natural number 1 is of a different nature, since it divides every integer. It is easy to decide whether a given number x is relatively prime to a prime number p : it happens if and only if $p \nmid x$ (why?). This implies that $\varphi(p) = p - 1$. We will compute φ for powers of a prime number in subsection 1.8.3. The list of prime numbers begins

$$2, 3, 5, 7, 11, 13, 17, 19, 23, \dots$$

and can be generated by a beautiful classical method known as the sieve of Eratosthenes, as follows. List the natural numbers > 1 :

$$2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, \dots$$

Begin by crossing out all the numbers divisible by 2 (except 2). Move on to the next available number, which is not crossed out (3), cross out all numbers divisible by 3 (except 3) and so on. This leads to the sequence

$$2, 3, \times, 5, \times, 7, \times, \times, \times, 11, \times, 13, \times, \times, \times, 17, \times, 19, \times, \times, \times, 23, \dots,$$

where the numbers left have to be prime numbers. The number

$$2^{24\,036\,583} - 1,$$

discovered on May 15, 2004 is currently the largest prime number known to man. This is a number with over four million digits. Without the use of a computer, Lucas (1842–91) proved in 1876 that

$$2^{127} - 1 = 170141183460469231731687303715884105727$$

is a prime number. This was referred to as having a huge number of digits, 39 [18], in 1948. A prime number of the form $M_n = 2^n - 1$ is called a Mersenne prime number (named after the French monk Marin Mersenne (1588–1648)). There is hectic activity on the internet searching for new Mersenne prime numbers (this project is called GIMPS — the Great Internet Mersenne Prime Search). Skilled programmers developed the settings for the project, in which you can participate using the idle CPU-seconds on your personal computer. Currently a \$100 000 prize (from the Electronic Frontier Foundation) is offered to the person(s) discovering the first ten-million-digit prime number. Using the URL <http://www.Mersenne.org/> you may catch up with the current status of GIMPS.

1.8.1 There are infinitely many prime numbers

It is not known whether there are infinitely many Mersenne prime numbers. Euclid proved that there are infinitely many prime numbers. This proof is more than 2000 years old and still breathtaking. First we need a lemma.

Lemma 1.8.1 *Every non-zero natural number n is a product of prime numbers.*

Proof. The natural number 1 is the empty product of prime numbers by definition. We prove the general statement by induction. Assume that every natural number $m < n$ is a product of prime numbers. Then we have to prove that n is a product of prime numbers. If n is a prime number then it is a product of prime numbers (with one factor). If n is not a prime number then

$$n = n_1 n_2$$

where n_1 and n_2 are natural numbers strictly less than n . By induction, n_1 and n_2 are products of prime numbers. Therefore n is a product of prime numbers. \square

Theorem 1.8.2 (Euclid) *There are infinitely many prime numbers.*

Proof. Suppose that there are only finitely many prime numbers, listed as

$$p_1, p_2, \dots, p_n.$$

Now form the integer $N = p_1 \cdot \dots \cdot p_n + 1$. By Lemma 1.8.1 we know that there is a prime number p dividing N (this may or may not be N itself). But p cannot be on our list above (a prime number on our list does not divide N – it leaves a remainder of 1 by Theorem 1.2.1). This means that from any finite list of prime numbers, we can prove the existence of a prime number not on the list: so, there are infinitely many prime numbers. \square

One may even prove that the sum

$$\frac{1}{2} + \frac{1}{3} + \frac{1}{5} + \frac{1}{7} + \frac{1}{11} + \dots$$

of reciprocal prime numbers is infinite (this is one of the many proofs that there are infinitely many prime numbers). A twin prime is a prime number p such that $p + 2$ (or $p - 2$) is a prime number. Here is a list of the first few twin primes:

$$3, 5, 7, 11, 13, 17, 19, 29, 31, \dots$$

A long-standing conjecture is that there are infinitely many twin primes. In this connection the Norwegian mathematician V. Brun (1885–1978) proved that the sum

$$B = \frac{1}{3} + \frac{1}{5} + \frac{1}{5} + \frac{1}{7} + \frac{1}{11} + \frac{1}{13} + \dots$$

of reciprocals of the twin primes is finite! The number $B (= 1.90216 \dots)$ is called Brun's constant. It has been computed to a high degree of accuracy by the American mathematician T. Nicely. In the latter half of 1994 Nicely discovered a disagreement between a computed and a published value of $\pi(20 \cdot 10^{12})$, where $\pi(x)$ is the number of prime numbers $\leq x$. After a long-winded process eliminating all kinds of errors, this led to the discovery¹ of the infamous FDIV bug in Intel's initial launch of their Pentium processor.

A crucial property of prime numbers (even though it looks strange at the beginning) is the following lemma.

¹ See <http://www.trnicely.net/pentbug/pentbug.html>

Lemma 1.8.3 *Let p be a prime number and suppose that $p \mid ab$, where $a, b \in \mathbb{Z}$. Then $p \mid a$ or $p \mid b$.*

Proof. If $p \nmid a$ then $\gcd(p, a) = 1$ and therefore $p \mid b$ by Corollary 1.5.10. Similarly if $p \nmid b$ then $p \mid a$. This shows that $p \mid a$ or $p \mid b$. \square

Remark 1.8.4 Lemma 1.8.3 extends to products with more than two factors: if p is a prime number and $p \mid a_1 a_2 \cdots a_n$ then $p \mid a_1$ or $p \mid a_2$ or \dots or $p \mid a_n$. Can you prove this?

1.8.2 Unique factorization

We know that every number can be written as a product of prime numbers. Gauss was the first to see a potential problem hidden in this statement. Can one have two different collections

$$p_1 \leq p_2 \leq \cdots \leq p_r \quad \text{and} \quad q_1 \leq q_2 \leq \cdots \leq q_s$$

of prime numbers such that $p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s$? A bit of experimentation shows that one seems to get different numbers given different collections of prime numbers (for example $2 \cdot 3 \cdot 11 \neq 5 \cdot 13$). This is a mathematical statement crying out for a rigorous proof. Many mathematicians before Gauss took “unique factorization” for granted. Commenting on this Gauss wrote ([11], Section II)

However, we did not wish to omit it (*the proof of unique factorization*) because many modern authors have offered up feeble arguments in place of proof or have neglected the theorem completely . . .

The idea behind the proof of unique factorization is quite easy. Suppose we wish to prove that $2 \cdot 3 \cdot 11 \neq 5 \cdot 13$ without multiplying. Assume that $2 \cdot 3 \cdot 11 = 5 \cdot 13$. Then $2 \mid 5 \cdot 13$. Lemma 1.8.3 implies that $2 \mid 5$ or $2 \mid 13$. This is a contradiction.

Theorem 1.8.5 *Every non-zero natural number n can be factored uniquely into a product of prime numbers (up to changing the order of the factors):*

$$n = p_1 \cdots p_r.$$

Proof. We may assume that $n > 1$ (since 1 factors uniquely into the empty product of prime numbers). Suppose that

$$n = p_1 \cdots p_r = q_1 \cdots q_s$$

are prime factorizations. If a prime factor p_j appears on the right hand side among q_1, \dots, q_s , then we divide both sides by p_j . We can therefore assume from the beginning that the left and right hand sides of the above equation have no prime factors in common. Furthermore, we may assume that $r \geq 1$ and $s > 1$. But we know that $p_1 \mid n$ and, so by Lemma 1.8.3 (applied $s - 1$ times), we get $p_1 \mid q_1$ or $p_1 \mid q_2$ or \dots or $p_1 \mid q_s$. Assume that $p_1 \mid q_j$. The only way this can happen is if $p_1 = q_j$, and this contradicts the fact that every common prime factor has been cancelled. \square

There is a very nice and short proof of unique factorization using that \mathbb{N} is well ordered (see Exercise 1.31). The above proof, however, seems to be the “natural” one as it carries over to more general settings.

Remark 1.8.6 Suppose that $n > 1$ is a natural number with the prime factorization

$$n = p_1^{e_1} \cdots p_r^{e_r},$$

where $e_1, \dots, e_r \geq 0$. Then Theorem 1.8.5 shows that

$$\operatorname{div}(n) = \{p_1^{k_1} \cdots p_r^{k_r} \mid 0 \leq k_1 \leq e_1, \dots, 0 \leq k_r \leq e_r\}.$$

Suppose that

$$m = p_1^{f_1} \cdots p_r^{f_r},$$

where $f_1, \dots, f_r \geq 0$. Then

$$\operatorname{div}(m) = \{p_1^{k_1} \cdots p_r^{k_r} \mid 0 \leq k_1 \leq f_1, \dots, 0 \leq k_r \leq f_r\}$$

and $\operatorname{div}(m) \cap \operatorname{div}(n)$ is

$$\begin{aligned} & \{p_1^{l_1} \cdots p_r^{l_r} \mid 0 \leq l_1 \leq e_1, 0 \leq l_1 \leq f_1, \dots, 0 \leq l_r \leq e_r, 0 \leq l_r \leq f_r\} \\ &= \{p_1^{l_1} \cdots p_r^{l_r} \mid 0 \leq l_1 \leq \min(e_1, f_1), \dots, 0 \leq l_r \leq \min(e_r, f_r)\}. \end{aligned}$$

Therefore

$$\gcd(m, n) = p_1^{\min(e_1, f_1)} \cdots p_r^{\min(e_r, f_r)}.$$

Similarly, the smallest natural number having both m and n as divisors must be

$$p_1^{\max(e_1, f_1)} \cdots p_r^{\max(e_r, f_r)}.$$

This number is denoted $\operatorname{lcm}(m, n)$ and is called the *least common multiple* of m and n . So if you have access to the prime factorizations of m and n it is easy

to read off the greatest common divisor and the least common multiple. Take $n = 140$ and $m = 154$. Here

$$n = 2^2 \cdot 5^1 \cdot 7^1 \cdot 11^0,$$

$$m = 2^1 \cdot 5^0 \cdot 7^1 \cdot 11^1$$

Therefore $\gcd(140, 154) = 2^1 \cdot 7^1 = 14$ and $\text{lcm}(140, 154) = 2^2 \cdot 5^1 \cdot 7^1 \cdot 11^1 = 1540$.

1.8.3 How to compute $\varphi(n)$

So far the most effective way known of computing $\varphi(n)$ for a natural number n is by way of its prime factorization. By Proposition 1.7.1

$$\varphi(n) = \varphi(p_1^{r_1}) \cdots \varphi(p_s^{r_s})$$

where $n = p_1^{r_1} \cdots p_s^{r_s}$ is the prime factorization ($p_i \neq p_j$ for $i \neq j$) of n . So we need to know how to compute $\varphi(p^m)$ for a power p^m of a prime number p . Fortunately this is easy. First observe that a number x is relatively prime to p^m if and only if $p \nmid x$ (why?). So the natural numbers less than p^m that are not relatively prime to p^m are simply the multiples of p . We list them below:

$$0, p, 2p, \dots, (p-1)p, p^2, \dots, (p^2-1)p, p^3, \dots, (p^{m-1}-1)p.$$

There are p^{m-1} natural multiples of p less than p^m . This implies that $\varphi(p^m) = p^m - p^{m-1}$. Therefore

$$\varphi(n) = (p_1^{r_1} - p_1^{r_1-1}) \cdots (p_s^{r_s} - p_s^{r_s-1}) = n \left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_s}\right).$$

The fact that this is the only efficient way known of computing φ gives the security underlying the RSA cryptosystem.

1.9 RSA explained

Let us return to the setting of the introduction to this chapter, where the RSA cryptosystem was described. Recall that a person wishing to receive an encrypted message must make two natural numbers e and N public. The number N (the public key) is the product of two distinct prime numbers p and q . A person wishing to send the number X ($0 \leq X < N$) sends the encrypted number $[X^e]$. Now the receiver can read this message because he knows a secret number d such that $[[X^e]^d] = X$. Here remainders are with respect to N .

We will now see how to construct the numbers e and d . By earlier results (Proposition 1.3.2 and (1.2)) we know that $[[X^e]^d] = [X^{ed}] = X$ if and only if $X \equiv X^{ed} \pmod{N}$. We also know that $\varphi(N) = \varphi(p)\varphi(q) = (p-1)(q-1)$ by subsection 1.8.3. The following proposition captures the algebraic essence of the RSA cryptosystem.

Proposition 1.9.1 *Let X be any integer and k a natural number. Then*

$$X^{k(p-1)(q-1)+1} \equiv X \pmod{N}.$$

Proof. By Corollary 1.5.11(i) it is enough to prove that

$$X^{k(p-1)(q-1)+1} \equiv X \pmod{p},$$

$$X^{k(p-1)(q-1)+1} \equiv X \pmod{q}.$$

We will prove the congruence for p (the proof for q is similar). If $p \mid X$ then $X \equiv 0 \pmod{p}$. Therefore $X^{k(p-1)(q-1)+1} \equiv 0 \pmod{p}$ and $X^{k(p-1)(q-1)+1} \equiv X \pmod{p}$. However, if $p \nmid X$, then $\gcd(X, p) = 1$. Therefore Theorem 1.7.2 gives $X^{\varphi(p)} = X^{p-1} \equiv 1 \pmod{p}$, and then we compute with congruences:

$$X^{k(p-1)(q-1)} \equiv (X^{p-1})^{k(q-1)} \equiv 1 \pmod{p}.$$

Multiplying the congruence with X , we get the desired result $X^{k(p-1)(q-1)+1} \equiv X \pmod{p}$. \square

1.9.1 Encryption and decryption exponents

Now we come to the selection of the encryption exponent. This exponent e is chosen as a natural number relatively prime to $\varphi(N) = (p-1)(q-1)$. Once e is chosen the decryption exponent d may be computed as follows. According to Lemma 1.5.7 we can find integers λ and μ , such that

$$\lambda(p-1)(q-1) + \mu e = 1,$$

where we may assume that $0 < \mu < (p-1)(q-1)$ (see Exercise 1.13) and therefore that $\lambda < 0$. The decryption exponent is $d = \mu$. This gives the existence of natural numbers k and d ($k = -\lambda$ and $d = \mu$) such that $k(p-1)(q-1) + 1 = de$. By (1.2) we get

$$[[X^e]^d] = [X^{ed}] = [X^{k(p-1)(q-1)+1}] = X$$

for every natural number $0 \leq X < N$, where the last equality comes from Propositions 1.9.1 and 1.3.2. This is exactly the statement that the decryption of the encrypted text recaptures the text.

Notice the secret buried in $\varphi(N) = (p-1)(q-1)$. If we can compute $\varphi(N)$, we may compute a decryption key, given a public encryption key, using the Euclidean algorithm as above. Finding $\varphi(N)$ in this case is just as hard as factoring N (see Exercise 1.38). Knowledge of N and the exponents e and d is enough to “guess” the prime numbers p and q . It is therefore not safe to let different people share the same public key N (see Exercise 1.40 (HOF)).

One very practical question remains. The public key N must be the product of two enormous prime numbers p and q (more than 100 digits each). How do we find huge prime numbers with more than 100 digits without factoring numbers? The answer lies in an old result of Fermat dating back to 1640.

1.9.2 Finding astronomical prime numbers

A corollary of Euler’s theorem (Theorem 1.7.2) says that a prime number p divides $a^p - a$ for all integers a . This result is due to Fermat (1601–65). In a letter dated 18 October 1640 to Frénicle de Bessy, Fermat writes

It seems to me after this that I should tell you the foundation on which I support the demonstrations of all which concerns geometric progressions, namely: Every prime number measures infallibly one of the powers minus unity in any progression, and the exponent of this power is a divisor of the given prime number minus one; and after one has found the first power which satisfies the condition, all those whose exponents are multiples of the first satisfy the condition.

Fermat writes in his letter “... I would send you the demonstration, if I did not fear its being too long.” The first known proof of Fermat’s result dates back to Euler in 1736. Later, in 1760, Euler gave his general result, which we proved in Theorem 1.7.2.

Corollary 1.9.2 (Fermat’s little theorem) *Let p be a prime number and a an integer with $\gcd(a, p) = 1$. Then*

$$a^{p-1} \equiv 1 \pmod{p}.$$

Proof. This is a consequence of Theorem 1.7.2 since $\varphi(p) = p - 1$. □

You may wonder what Fermat’s big theorem is. This is known by the name “Fermat’s last theorem” and goes back to 1647. It says that the equation

$$X^n + Y^n = Z^n$$

has no solutions $X, Y, Z \in \mathbb{Z}$ for $n > 2$ apart from the trivial ones where one of X, Y, Z is zero (when $n = 2$ there are infinitely many non trivial solutions). Fermat conjectured this in his notes in the margin of his copy of Diophantus's *Arithmetica* with the famous remark "For this I have discovered a truly wonderful proof, but the margin is too small to contain it." As you may know Fermat's last theorem haunted mathematicians for more than 300 years before it was finally proved by A. Wiles in 1994.

It is unlikely that Fermat could have foreseen that his little theorem would play a crucial role in generating large prime numbers for use in the modern information age. By using congruences it is easy to see (since $5 \equiv -1 \pmod{6}$) that

$$5^5 \equiv 5 \not\equiv 1 \pmod{6}.$$

Thus by Corollary 1.9.2, 6 is not a prime number. This is of course a complicated way of proving the latter, but in fact it contains the idea for some beautiful algorithms for deciding whether a number is composite without ever trying to factor it. However,

$$8^8 \equiv (-1)^8 = 1 \pmod{9}.$$

Here Corollary 1.9.2 does not tell us that 9 is composite. We are led to the following definition.

Definition 1.9.3 Let N be a composite natural number and a an integer. Then N is called a *pseudoprime* relative to the base a if $a^{N-1} \equiv 1 \pmod{N}$.

Notice that if the base a is not relatively prime to N then N cannot be a pseudoprime relative to a (see Exercise 1.41). A natural question is whether there exist numbers pseudoprime to every relatively prime base. The answer is yes, and the smallest example is $N = 561 = 3 \cdot 11 \cdot 17$ (see Exercise 1.45). Numbers having this property are called Carmichael numbers (or pseudoprimes). It was proved recently [1] that there are infinitely many Carmichael numbers.

We are left with the fact that there are composite numbers that are not distinguished from prime numbers by Corollary 1.9.2. There is a surprisingly simple way to improve this situation. The key point is the following lemma.

Lemma 1.9.4 Let p be a prime number and $x \in \mathbb{Z}$. If $x^2 \equiv 1 \pmod{p}$ then $x \equiv \pm 1 \pmod{p}$.

Proof. By assumption, $p \mid x^2 - 1 = (x + 1)(x - 1)$. Thus, by Lemma 1.8.3, $p \mid x + 1$ or $p \mid x - 1$. This completes the proof. \square

Consider, say, $N = 341$. Using repeated squaring we compute

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

From this we cannot deduce that 341 is composite. But using Lemma 1.9.4 we can drag 2 through some more questioning that tell us whether 341 really is composite. Assuming, then, that 341 is a prime number, Lemma 1.9.4 gives that

$$2^{170} \equiv \pm 1 \pmod{341},$$

since $(2^{170})^2 = 2^{340}$. Again one computes that $2^{170} \equiv 1 \pmod{341}$. Now we reach the crucial question. Since $2^{170} = (2^{85})^2$, Lemma 1.9.4 implies that $2^{85} \equiv \pm 1 \pmod{341}$. In this step, 2 breaks down and tells us that

$$2^{85} \equiv 32 \pmod{341}$$

and therefore that 341 cannot be a prime number. From this example we get the following definition.

Definition 1.9.5 An odd composite number N is called a *strong pseudoprime* relative to the base a if either $a^q \equiv 1 \pmod{N}$ or there exists $i = 0, \dots, k-1$ such that

$$a^{2^i q} \equiv -1 \pmod{N},$$

where $N-1 = 2^k q$ and $2 \nmid q$.

The strong pseudoprimes are precisely the composite numbers, which pass both tests (Corollary 1.9.2 and Lemma 1.9.4) without getting caught. The following result shows that a number that fails repeated application of Lemma 1.9.4 (as for $N = 341$ and $a = 2$) must be a composite number.

Proposition 1.9.6 Let p be an odd prime number and suppose that

$$p-1 = 2^k q,$$

where $2 \nmid q$. If $a \in \mathbb{Z}$ and $\gcd(a, p) = 1$ then either $a^q \equiv 1 \pmod{p}$ or there exists $i = 0, \dots, k-1$ such that

$$a^{2^i q} \equiv -1 \pmod{p}.$$

Proof. Let $a_i = a^{2^i q}$, $i = 0, \dots, k$. Observe that $a_k \equiv 1 \pmod{p}$ by Corollary 1.9.2 and that $a_{i+1} = a_i^2$ for $i = 0, \dots, k-1$. Therefore $a_0 \equiv 1 \pmod{p}$ if and only if $a_i \equiv 1 \pmod{p}$ for every $i = 0, \dots, k$. So, if $a_0 \not\equiv 1 \pmod{p}$ then

there exists a_i , $i \geq 0$, such that $a_i \not\equiv 1 \pmod{p}$. Let j be the largest index with this property. Since $j < k$ and $a_j^2 \equiv a_{j+1} \equiv 1 \pmod{p}$ we get $a_j \equiv -1 \pmod{p}$ by Lemma 1.9.4. \square

The reason strong pseudoprimes are extremely useful in real-life primality testing is the following theorem, due to M. Rabin [20].

Theorem 1.9.7 (Rabin) *Suppose that $N > 4$ is an odd composite integer and let B be the number of bases a ($1 < a < N$) such that N is a strong pseudoprime relative to a . Then*

$$B < \varphi(N)/4 \leq (N-1)/4.$$

Theorem 1.9.7 shows the strong contrast between a strong pseudoprime and a pseudoprime to a base a . There are true pseudoprimes (composite numbers pseudoprime to every relatively prime base). Theorem 1.9.7 states that we can find many bases revealing that a given composite number is not a prime number!

Suppose that we are given a natural number N and a randomly chosen a , $1 < a < N$. If N is composite then the probability that N is a strong pseudoprime relative to a is $< 1/4$ by Theorem 1.9.7. If we have a good method of generating (uniformly distributed) random numbers,² then we can try out a sequence of random bases $1 < a_1, \dots, a_m < N$. The upshot is that if N is a strong pseudoprime relative to the m random bases a_1, \dots, a_m then the probability that N is composite is less than

$$(1/4)^m.$$

In fact the probability is usually much smaller. For example, if a number p of around 180 digits (600 bits) is tested and p is a strong pseudoprime to just one base then the probability that p is composite is less than $(1/2)^{76}$. Already for $m \geq 30$ the rough estimate $(1/4)^m$ is comparable to the probability of a hardware error in your computer caused by cosmic radiation (quoting Knuth). So if a number is a strong pseudoprime relative to more than 30 random bases then the number tested is a prime number for all practical purposes. This is basically how one builds huge prime numbers for use in cryptography. Starting with a random integer x (with more than 100 digits), one searches for the first probable prime number $\geq x$.

² The best sources of randomness are atmospheric noise from a radio (<http://www.random.org>) or radioactive decay (<http://www.fourmilab.ch/hotbits/>).

1.10 Algorithms for prime factorization

One way of breaking the RSA encryption is by having effective algorithms for prime factorization. So far these work only up to 155 digits, and the largest number took six months to factor using distributed supercomputing over the internet. In August 1999 RSA-155 was factored. Here is part of the press release from RSA Labs:

Factoring the 512-binary-bit key, equivalent to 155 decimal digits and called RSA-155, took the team a total elapsed time of 5.2 months, not including nine weeks needed for preliminary computations, and was accomplished using 292 individual computers located at 11 different sites in The Netherlands, Canada, the United Kingdom, France, Australia and the United States. Prior to this, the largest RSA key length to be factored was 140 decimal digits long in February of this year. RSA's recommended key lengths are 230 digits or more. . . . These latest results were achieved using about 160 175-400-MHz SGI and Sun workstations, eight 250-MHz SGI Origin 2000 processors, 120 300-450-MHz Pentium II PCs and four 500-MHz Digital/Compaq CPUs, and required approximately 8000 MIPS-years of CPU effort. The specific approach used to determine the prime factors was based on the work done to solve the RSA-140 Challenge earlier this year.

The statement that every integer can be written as a product of prime numbers is a typical mathematical statement with a simple proof. Things become much more complicated when you (inspired by Gauss) ask for a good algorithm for factoring a given integer N . In a non-trivial factorization $N = ab$ one of the factors a and b must be $\leq \sqrt{N}$. If N is even, 2 divides it and we have found a factor. If N is odd we may find a factor of N by starting with 3 and trying division by odd numbers up to \sqrt{N} . This procedure is called *trial division*. The number of steps in trial division is proportional to the size of the smallest prime factor. This is extremely slow. If you want to factor a 100-digit number that is the product of two 50-digit prime numbers, you must carry out approximately 10^{50} steps of trial division. If every step takes 10^{-10} seconds, you will have to wait for 10^{40} seconds (or approximately 10^{32} years). It is not clear, though, that there are better algorithms. In fact the three faster algorithms we will describe each contain an ingenious idea. They are all tied to the Euclidean algorithm. The object is to hunt down a number $a \in \mathbb{N}$ such that $1 < \gcd(a, N) < N$, where N is the composite number we wish to factor.

1.10.1 The birthday problem

Suppose that N people are gathered in an auditorium. What is the probability that two of them share the same birthday? This is a problem easily solved by elementary probability theory. Consider the “inverse” problem: what is the

probability, $P(N)$, that none of them share a birthday? We get, for example, that

$$P(2) = \frac{364}{365}$$

since there are 364 possible dates left when one is taken. Similarly,

$$P(3) = \frac{364}{365} \cdot \frac{363}{365}.$$

In general,

$$P(N) = \frac{365 \cdot 364 \cdots (365 - N + 1)}{365^N}.$$

At $N = 23$, $P(N)$ is already less than 0.5. So if there are more than 23 people present there is more than a 50% chance that two share the same birthday. If there are 50 people present there is more than a 97% chance that two share the same birthday.

The mathematical abstraction is sampling with replacement from a sample space consisting of N objects. The average number of samplings before a repetition occurs can be computed as the mean value of a stochastic variable. When N is big this mean value is close to

$$\sqrt{\frac{\pi N}{2}}.$$

1.10.2 Pollard's ρ -algorithm

How does the birthday problem relate to the factoring of a composite integer N ? Suppose that p is a prime number dividing N and that we are given two numbers $0 \leq a, b < N$ with $a \equiv b \pmod{p}$. Then $p \mid a - b$. Therefore $1 < \gcd(a - b, N) \leq N$ and, if $a \not\equiv b \pmod{N}$, $\gcd(a - b, N)$ is a non-trivial factor in N . This innocent observation contains the idea for a much faster factoring algorithm than trial division. Suppose we have a way of generating random integers X_1, X_2, \dots with $0 \leq X_i < N$. We know by subsection 1.10.1 that on average we see $\sqrt{(\pi N)/2}$ random numbers before a repetition occurs. For factoring purposes it suffices to have a repetition modulo p , where p is the smallest prime dividing N : if $X_i \equiv X_j \pmod{p}$ then $1 < \gcd(X_i - X_j, N) \leq N$. So it is sufficient to look at the random integers X_1, X_2, \dots modulo p . Here we only see $\sqrt{(\pi p)/2}$ random numbers, on average, before a repetition occurs.

It is not easy to generate true random numbers in mathematics. Let us rely on a function that generates a sequence of numbers conjectured to be sufficiently

random. Consider the function from \mathbb{Z}/N to \mathbb{Z}/N given by

$$f(X) = [X^2 + 1]_N. \quad (1.5)$$

Start out with $X_0 = 0$ and let $X_{i+1} = f(X_i)$ in each successive step. This sequence will contain repetitions modulo p (there are only p remainders so there will be a repetition when $i \geq p$). How do we check for repetitions modulo p ? The following lemma gives the crux of the algorithm.

Lemma 1.10.1 *Let $f : M \rightarrow M$ be a function where M is a finite set. Pick $x_0 \in M$ and generate the sequence x_0, x_1, x_2, \dots , where $x_{i+1} = f(x_i)$ for $i \geq 0$. There exist $i, j \in \mathbb{N}$ such that $i \neq j$ and $x_i = x_j$. Furthermore there exists $n > 0$ such that $x_n = x_{2n}$. The sequence y_0, y_1, y_2, \dots given by $y_0 = x_0$ and $y_{i+1} = f(f(y_i))$ for $i \geq 0$ equals the sequence x_0, x_2, x_4, \dots .*

Proof. We have a map $g : \mathbb{N} \rightarrow M$ given by $g(n) = f^n(x_0)$. Since M is a finite set, g cannot be injective. Thus there exist $i, j \in \mathbb{N}$ with $i \neq j$ such that $g(i) = g(j)$. This shows that $x_i = x_j$ for $i \neq j$.

Suppose that $x_i = x_j$ for $j > i$. If $n \geq i$ and $2n = n + k(j - i)$ with $k \geq 0$ we must have $x_n = x_{2n}$. So choosing $k \geq 0$ such that $n = k(j - i) \geq i$ gives the desired n . As $x_{m+2} = f(f(x_m))$ it follows that $y_m = x_{2m}$. \square

Now we have all the tools for building a factoring algorithm based on recognizing repetitions modulo p . The key point is the existence of a repetition modulo p of the form $X_n \equiv X_{2n} \pmod{p}$, as pointed out in Lemma 1.10.1.

We start out by putting $X_0 = Y_0 = 0$. At each step we iterate $X_{i+1} = f(X_i)$ and $Y_{i+1} = f(f(Y_i))$ using the function f in (1.5). Then we compute $d = \gcd(Y_{i+1} - X_{i+1}, N)$ using the Euclidean algorithm. If d equals 1 or N we repeat the process. If not, d must be a non-trivial factor in N and we are done. An example is given below.

Example 1.10.2 Let $N = 11 \cdot 13 = 143$. Then

i	0	1	2	3	4	5	6	7	8	9
X_i	0	1	2	5	26	105	15	83	26	105
Y_i	0	2	26	15	26	15	26	15	26	15

The X_i -sequence turns into the sequence 0, 1, 2, 5, 4, 6, 4, 6, 4, ... viewed modulo 11. At the sixth step above $Y_6 - X_6 = 11$ and the factor 11 is found.

Of course there is a problem with this algorithm if repetition modulo N coincides with repetition modulo p . This is rather unlikely for large N since the sequence modulo N repeats after $\sqrt{(\pi N)/2}$ steps on average compared with $\sqrt{(\pi p)/2}$ steps modulo p on average.

This algorithm for factoring is called Pollard's ρ -algorithm (because ρ represents the shape of the sequence repeating itself). It was invented in 1975 by J. M. Pollard. The Pollard ρ -algorithm needs $\sqrt[4]{N}$ steps on average for factoring an integer N as compared with \sqrt{N} steps for trial division. We move on to describe another factoring algorithm due to Pollard.

1.10.3 Pollard's $(p - 1)$ -algorithm

Suppose we wish to factor a composite number N divisible by a prime number p . If a is an integer and $p \nmid a$ then

$$a^{p-1} \equiv 1 \pmod{p}$$

by Corollary 1.9.2. If m is a natural number such that $p - 1 \mid m$ then

$$a^m \equiv 1 \pmod{p}. \quad (1.6)$$

So if we have a and m such that (1.6) holds, we may conclude that $\gcd(N, a^m - 1) > 1$ since $p \mid a^m - 1$. This suggests that a good strategy for finding a non-trivial factor of N proceeds by systematically trying out a and m in the hope that they fit (1.6). We can use the Euclidean algorithm to compute

$$d = \gcd(N, a^m - 1) = \gcd(N, [a^m - 1]_N).$$

Computing $[a^m - 1]_N$ can be done using repeated squaring, first evaluating $[a^m]_N$. If $1 < d < N$ we have found a non-trivial factor of N . If $d = 1$ then we try with a different (bigger) m . If $d = N$ then m might work with a different a . This is the idea behind Pollard's $(p - 1)$ -algorithm. This algorithm is very successful if N contains a prime factor p such that $p - 1$ is a product of small primes. In fact one builds up m as a product of primes of increasing size. The jackpot in the algorithm occurs when we hit an m that is divisible by $p - 1$, where p is a prime factor of N .

How do we search systematically through the m -values for a specific a ? A good strategy is to decide on a bound B , considering only the prime numbers $< B$ dividing m . One then takes the powers of the prime number $q < B$ entering m as the least integer greater than or equal to $\log_q \sqrt{N}$ ([5], Section 4.3). Again we will do a toy example that fully explains the basic idea.

Example 1.10.3 Consider $N = 143 = 11 \cdot 13$ and $a = 2$. We consider primes $< B = 5$. Thus in this case $m = 2^4 3^3 = 432$. Using repeated squaring we find that

$$[2^{432}]_{143} = 92.$$

Therefore

$$\gcd(143, 2^{432} - 1) = \gcd(143, 91) = 13.$$

We have found the factor 13 in 143.

To protect a public RSA-key from the Pollard $(p - 1)$ -algorithm one should choose (secret) prime numbers p and q such that $p - 1$ and $q - 1$ are not products of small prime numbers.

The (hidden group theoretic) idea behind the $(p - 1)$ -algorithm can be used to construct a much stronger factoring algorithm using arithmetic on elliptic curves (this was done by Lenstra in 1985).

1.10.4 The Fermat–Kraitchik algorithm

Currently the most effective algorithms for factoring difficult RSA integers originate in the historic fact that if an integer N can be written as the difference $x^2 - y^2$ between two squares, we have the factorization $N = x^2 - y^2 = (x + y)(x - y)$. However, if an odd number $N = uv$ is composite then

$$N = \left(\frac{u+v}{2}\right)^2 - \left(\frac{u-v}{2}\right)^2.$$

This method of factoring goes back to Fermat. Suppose we wish to factor N . Fermat's method uses the function

$$S(x) = x^2 - N$$

and a search for x such that $S(x)$ is a square. Usually one runs through $x = [\sqrt{N}]$, $[\sqrt{N}] + 1, \dots$, where $[\sqrt{N}]$ denotes the largest integer $\leq \sqrt{N}$. Putting $N = 2491$, one finds $S(49) = -90$, $S(50) = 9 = 3^2$. This means that $2491 = (50 + 3)(50 - 3) = 53 \cdot 47$. Of course, using this method on a composite number such as 2^{1000} works just as poorly as trial division. There is a beautiful variation of Fermat's method, due to M. Kraitchik (1882–1957), using congruences. The insight is that to find a factor of N it usually suffices that N divides $x^2 - y^2$. If

$$N \mid x^2 - y^2 = (x + y)(x - y)$$

and N does not divide either $x + y$ or $x - y$ then we may conclude that $\gcd(x + y, N) > 1$ by Corollary 1.5.10 and use the Euclidean algorithm to find $\gcd(N, x + y)$, which is a non-trivial factor of N . So one should look for integers x, y such that

$$\begin{aligned}x^2 &\equiv y^2 \pmod{N}, \\x &\not\equiv \pm y \pmod{N}.\end{aligned}$$

Suppose that we have collected x_1, \dots, x_n along with the congruences

$$x_1^2 \equiv a_1 \pmod{N}, \quad \dots, \quad x_n^2 \equiv a_n \pmod{N}$$

for some integers a_1, \dots, a_n . If a subset a_{i_1}, \dots, a_{i_r} of a_1, a_2, \dots, a_n satisfies that $a_{i_1} \cdots a_{i_r}$ is a square then

$$(x_{i_1} \cdots x_{i_r})^2 \equiv a_{i_1} \cdots a_{i_r} \pmod{N}$$

by Proposition 1.3.4 and we have our congruence $x^2 \equiv y^2 \pmod{N}$. This congruence may or may not satisfy $x \not\equiv \pm y \pmod{N}$. To tell whether a number n is square we factor it,

$$n = p_1^{m_1} \cdots p_r^{m_r},$$

using some predefined factor basis $P = \{p_1, \dots, p_r\}$ of (small) prime numbers. In this context, n is a square if and only if all the exponents m_1, \dots, m_r are even. Using linear algebra there is a method of systematically finding a subset $\{i_1, \dots, i_r\}$ such that $a_{i_1} \cdots a_{i_r}$ is a square (see Exercise 1.49).

Let us apply this algorithm to the numbers we get from the function $S(x) = x^2 - N$. Notice that $x^2 \equiv S(x) \pmod{N}$. For $N = 2041$ (this example is from [19]) we illustrate this in the table below. The marked entries together indicate the subset whose product is a square.

x	$S(x)$	Factorization	Marked
46	75	$3 \cdot 5^2$	✓
47	168	$2^3 \cdot 3 \cdot 7$	✓
48	263	263	
49	360	$2^3 \cdot 3^2 \cdot 5$	✓
50	459	$3^3 \cdot 17$	
51	560	$2^4 \cdot 5 \cdot 7$	✓

The above table shows that $S(46)S(47)S(49)S(51) = 75 \cdot 168 \cdot 360 \cdot 560 = (2^5 \cdot 3^2 \cdot 5^2 \cdot 7)^2$ is a square. Putting $u = 2^5 \cdot 3^2 \cdot 5^2 \cdot 7$, we get

$$u^2 = 50400^2 \equiv 1416^2 \pmod{2041}.$$

Now we know that $u^2 \equiv v^2 \pmod{2041}$ where $v = 46 \cdot 47 \cdot 49 \cdot 51 = 5402838 \equiv 311 \pmod{2041}$. Using the Euclidean algorithm one finds the greatest common divisor of $u - v = 1416 - 311 = 1105$ and 2041, which is 13. We have found the factorization $2041 = 13 \cdot 157$. Using the original method of Fermat we would have to wait until $x = 85$ before $S(x)$ is a square. The heavy part of the algorithm is factoring $S(x) = x^2 - N$. Around 1982, Pomerance discovered a nice trick that avoids this. His observation was that a prime power p^r divides $S(x)$ if and only if it divides $S(x + kp^r)$, where $k \in \mathbb{Z}$. So if we can locate a number x such that $p^r \mid S(x)$ then we know in advance that $p^r \mid S(x + p^r)$, $S(x + 2p^r)$, \dots . This is a so-called sieving procedure (like the sieve of Eratosthenes, which eliminates multiples of prime numbers). It leads to a factorization algorithm called the quadratic sieve. In [19] you can find a nice description of this and more advanced sieving methods for factoring. These are currently the most effective algorithms for the challenges issued by RSA Labs. In fact RSA-155 was factored using sieving.

1.11 Quadratic residues

In this section we introduce the fundamentals of quadratic residues modulo a prime number p . Gauss originally developed this theory, starting with the question whether a number a has a square root modulo p : can one find an integer x such that $x^2 \equiv a \pmod{p}$? This question led Gauss to exceptionally beautiful mathematics (see “Congruences of the second degree,” Section IV in [11] and be sure to enjoy the clarity of the exposition).

Later, we will use quadratic residues when writing prime numbers $\equiv 1 \pmod{4}$ as a sum of two squares.

Definition 1.11.1 Let p be a prime number. If $p \nmid a$ then a is called a *quadratic residue modulo p* if it is congruent to a square modulo p (i.e. there exists $x \in \mathbb{Z}$ such that $a \equiv x^2 \pmod{p}$). Otherwise a is called a *quadratic non-residue modulo p* . If $p \mid a$ then a is considered neither a quadratic residue nor a quadratic non-residue. This definition is contained in the Legendre symbol

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{if } p \mid a, \\ 1 & \text{if } a \text{ is a quadratic residue modulo } p, \\ -1 & \text{if } a \text{ is a quadratic non-residue modulo } p. \end{cases}$$

If $a \equiv x^2 \pmod{p}$ for some integer $x \in \mathbb{Z}$, we may find a y such that $0 \leq y < p$ and $a \equiv y^2 \pmod{p}$. We simply put $y = [x]_p$. Then $y \equiv x \pmod{p}$ and

therefore $y^2 \equiv x^2 \pmod{p}$. Thus the quadratic residues among the numbers $1, 2, \dots, p-1$ are the numbers

$$[1^2], [2^2], [3^2], \dots, [(p-1)^2],$$

where the remainder is with respect to p . This is reflected in the Legendre symbol:

$$\left(\frac{a}{p}\right) = \left(\frac{a+kp}{p}\right)$$

where $k \in \mathbb{Z}$.

Example 1.11.2 Let $p = 7$. Since a non-zero square x^2 modulo p is always congruent to one of the squares $1^2, 2^2, 3^2, 4^2, 5^2, 6^2$, we may list the quadratic residues among $1, 2, 3, 4, 5, 6$ as

$$\begin{aligned} [1^2] &= 1, \\ [2^2] &= 4, \\ [3^2] &= 2, \\ [4^2] &= 2, \\ [5^2] &= 4, \\ [6^2] &= 1 \end{aligned}$$

by taking the remainder after division by 7. Notice the symmetry above: $[3^2] = [4^2]$, $[2^2] = [5^2]$, $[1^2] = [6^2]$. This is a consequence of the fact that $x^2 \equiv (7-x)^2 \pmod{7}$. There are an equal number of quadratic residues, $\{1, 2, 4\}$, and quadratic non-residues, $\{3, 5, 6\}$.

Proposition 1.11.3 Let p denote an odd prime. Half the numbers $1, 2, 3, \dots, p-1$ are quadratic residues; the other half are quadratic non-residues modulo p .³

Proof. We already know that the quadratic residues are $[1^2], [2^2], \dots, [(p-1)^2]$. But since $x^2 \equiv (p-x)^2 \pmod{p}$, we see that the quadratic residues are given by the first $(p-1)/2$ numbers $[1^2], [2^2], \dots, [(p-1)/2]^2$. These numbers really are different. If $[i^2] = [j^2]$ then $i^2 \equiv j^2 \pmod{p}$ and $p \mid i^2 - j^2 = (i+j)(i-j)$. Therefore $p \mid i+j$ or $p \mid i-j$. This is only possible if $i = j$, because $0 \leq i, j \leq (p-1)/2$. So there are $(p-1)/2$ quadratic residues

³ An interesting problem is how the quadratic non-residues are distributed among $1, 2, \dots, p-1$. In particular, how big is the smallest quadratic non-residue a ? If a generalization of the famous Riemann hypothesis is true one can prove that $a < 2(\log p)^2$, where \log denotes the natural logarithm.

and therefore $(p-1) - (p-1)/2 = (p-1)/2$ quadratic non-residues among the numbers $1, 2, \dots, p-1$. \square

The following important theorem is due to Euler.

Theorem 1.11.4 (Euler) *Let p be an odd prime and let a be an integer not divisible by p . Then*

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

Proof. If a is a quadratic residue then $a \equiv x^2 \pmod{p}$, where $p \nmid x$ for some $x \in \mathbb{Z}$. Therefore

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

by Corollary 1.9.2. Therefore we have at least $(p-1)/2$ incongruent solutions to the congruence

$$X^{(p-1)/2} - 1 \equiv 0 \pmod{p}. \quad (1.7)$$

What is shown in Exercise 1.50 implies that (1.7) can have at most $(p-1)/2$ incongruent solutions. Therefore a quadratic non-residue a cannot be a solution to (1.7). Thus $a^{(p-1)/2} \not\equiv 1 \pmod{p}$ and therefore $a^{(p-1)/2} \equiv -1 \pmod{p}$ by Lemma 1.9.4. This finishes the proof of Lemma 1.9.4. \square

Corollary 1.11.5 *Let p be an odd prime. Then the Legendre symbol satisfies*

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \left(\frac{b}{p}\right).$$

Another very nice consequence of Theorem 1.7.2 is the following.

Proposition 1.11.6 *Let p be an odd prime. Then -1 is a quadratic residue modulo p if $p \equiv 1 \pmod{4}$ and a quadratic non-residue if $p \equiv 3 \pmod{4}$.*

Proof. From Theorem 1.7.2 we get

$$\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}.$$

Now the result follows, since $(p-1)/2$ is even if $p \equiv 1 \pmod{4}$ and odd if $p \equiv 3 \pmod{4}$. \square

We move on to a celebrated lemma due to Gauss. We give the proof because it is very similar to the proof of Theorem 1.7.2. First we need some notation. Let p be an odd prime number. Then every integer $a \in \mathbb{Z}$ such that $p \nmid a$ is congruent to precisely one number (its remainder) from

$$M = \{1, 2, 3, \dots, p-1\}.$$

The clever thing is to break M into two and flip the right hand part below zero. We do this by replacing x by $x - p$ if $x > (p-1)/2$. This means that every number from M is congruent to precisely one number in the set

$$S = \left\{ -\frac{p-1}{2}, -\frac{p-3}{2}, \dots, -2, -1, 1, 2, \dots, \frac{p-3}{2}, \frac{p-1}{2} \right\}.$$

Consider the list

$$a, 2a, 3a, \dots, \frac{p-1}{2}a,$$

where $p \nmid a$. None of these numbers is divisible by p (why not?). Also, they satisfy $ia \not\equiv \pm ja \pmod{p}$, since $p \nmid i - j$ and $p \nmid i + j$ when $i \neq j$ and $0 \leq i, j \leq (p-1)/2$. This means that ia is congruent to a unique number in $\{1, 2, \dots, (p-1)/2\}$, up to a sign.

Definition 1.11.7 Let $\mu(a)$ denote the number of elements from the list

$$a, 2a, 3a, \dots, \frac{p-1}{2}a$$

congruent to a negative number in S .

Example 1.11.8 Let $p = 11$. Then

$$S = \{-5, -4, -3, -2, -1, 1, 2, 3, 4, 5\}.$$

If $a = 6$ then $6 \equiv -5$, $12 \equiv 1$, $18 \equiv -4$, $24 \equiv 2$, $30 \equiv -3$ modulo 11. This means that $\mu(a) = 3$ in this case.

Remark 1.11.9 Notice that $\mu(a)$ also is the number of elements in

$$\{[a], [2a], \dots, [a(p-1)/2]\} \cap \{(p+1)/2, \dots, p-1\}.$$

Here we count the remainders $> (p-1)/2$.

Lemma 1.11.10 (Gauss) *Keep the above notation. Then*

$$\left(\frac{a}{p}\right) = (-1)^{\mu(a)}.$$

Proof. An element ja , where $j = 1, \dots, (p-1)/2$, is congruent to $\pm m_j$, where $1 \leq m_j \leq (p-1)/2$. Since ia cannot be congruent to $\pm ja$ modulo p , when $i \neq j$ and $1 \leq i, j \leq (p-1)/2$ (this amounts to the same argument as in the proof of Theorem 1.7.2), it follows that

$$a^{(p-1)/2} \left(\frac{p-1}{2}\right)! \equiv (-1)^\mu \left(\frac{p-1}{2}\right)! \pmod{p}.$$

Since $p \nmid ((p-1)/2)!$ we get

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

and Theorem 1.11.4 finishes the proof. \square

Corollary 1.11.11 *Let p be an odd prime. Then 2 is a quadratic residue modulo p if $p \equiv 1, 7 \pmod{8}$ and a quadratic non-residue if $p \equiv 3, 5 \pmod{8}$.*

Proof. The number $\mu = \mu(2)$ in Lemma 1.11.10 is the number of elements in the list

$$1 \cdot 2, 2 \cdot 2, 3 \cdot 2, \dots, \frac{p-1}{2} \cdot 2$$

that are greater than $(p-1)/2$. To compute μ we consider two cases. If $p \equiv 1 \pmod{4}$ then

$$\mu = \frac{p-1}{2} - \frac{p-1}{4} = \frac{p-1}{4}.$$

If $p \equiv 3 \pmod{4}$ then

$$\mu = \frac{p-1}{2} - \frac{p-3}{4} = \frac{p+1}{4}.$$

Using Lemma 1.11.10 we conclude that

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod{8}, \\ -1 & \text{if } p \equiv 3 \pmod{8}, \\ -1 & \text{if } p \equiv 5 \pmod{8}, \\ 1 & \text{if } p \equiv 7 \pmod{8}, \end{cases}$$

since $(p-1)/4$ is even when $p \equiv 1 \pmod{8}$ and odd when $p \equiv 5 \pmod{8}$ and $(p+1)/4$ is even when $p \equiv 7 \pmod{8}$ and odd when $p \equiv 3 \pmod{8}$. \square

Now we know how to compute $\left(\frac{-1}{p}\right)$ and $\left(\frac{2}{p}\right)$, but we are missing the crucial insight needed to get our hands on $\left(\frac{a}{p}\right)$ in general. This insight is one of the most beautiful results in the history of mathematics. It is known as the law of quadratic reciprocity (due to Gauss, of course). It states that

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{(p-1)(q-1)/4},$$

where p and q are odd primes. Put another way,

$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right) (-1)^{(p-1)(q-1)/4} = \begin{cases} -\left(\frac{q}{p}\right) & \text{if } p \equiv q \equiv 3 \pmod{4}, \\ \left(\frac{q}{p}\right) & \text{otherwise.} \end{cases}$$

Think about it. If you have two odd primes p and q , it is totally unexpected that the two congruences

$$x^2 \equiv q \pmod{p} \quad \text{and} \quad x^2 \equiv p \pmod{q}$$

should have any connection. We will give a proof of quadratic reciprocity in Section 4.7, when we will have access to some more abstract algebra. Let us give an example showing how the Legendre symbol is computed using these rules.

Example 1.11.12

$$\left(\frac{19}{43}\right) = -\left(\frac{43}{19}\right) = -\left(\frac{5}{19}\right) = -\left(\frac{19}{5}\right) = -\left(\frac{4}{5}\right) = -\left(\frac{2}{5}\right)\left(\frac{2}{5}\right) = -1.$$

By the magic of the law of quadratic reciprocity we have proved that $x^2 \equiv 19 \pmod{43}$ has no solutions.

1.12 Exercises

1. Prove that if a subset $S \subseteq \mathbb{Z}$ has a first element then the latter has to be unique.
2. Let $x, d \in \mathbb{Z}$, where $d > 0$. Prove that $M \cap \mathbb{N} \neq \emptyset$, where $M = \{x - qd \mid q \in \mathbb{Z}\}$.

3. Let $a, b, N \in \mathbb{Z}$, where $N > 0$. Prove that $[ab] = [[a][b]]$, where $[x]$ denotes the remainder of x after division by N .
4. Verify that the remainder of 2^{340} after division by 341 is 1, using the repeated squaring algorithm.
5. Let τ be a natural number > 1 . A τ -adic expansion of a number $x \in \mathbb{N}$ is the expression

$$x = a_0 + a_1\tau + \cdots + a_r\tau^r,$$

where $r \in \mathbb{N}$, $a_i \in \mathbb{N}$ and $0 \leq a_i < \tau$.

- (i) Compute a 3-adic expansion of 17.
- (ii) Prove that every $x \in \mathbb{N} \setminus \{0\}$ can be written as

$$x = a\tau^r + b,$$

where $0 \leq a < \tau$, $0 \leq b < \tau^r$ and $r = \max\{s \in \mathbb{N} \mid \tau^s \leq x\}$.

- (iii) Prove that every natural number has a unique τ -adic expansion.
6. Let a be a number written (in base 10) as

$$a_0 \cdot 10^0 + a_1 \cdot 10^1 + a_2 \cdot 10^2 + \cdots + a_n \cdot 10^n$$

where $0 \leq a_i < 10$.

- (i) Prove that 2 divides a if and only if 2 divides a_0 .
- (ii) Prove that 4 divides a if and only if 4 divides $a_0 + 2a_1$.
- (iii) Prove that 8 divides a if and only if 8 divides $a_0 + 2a_1 + 4a_2$.
- (iv) Prove that 5 divides a if and only if 5 divides a_0 .
- (v) Prove that 9 divides a if and only if 9 divides the sum $a_0 + a_1 + \cdots + a_n$ of its digits.
- (vi) Prove that 3 divides a if and only if 3 divides the sum of its digits.
- (vii) Prove that 11 divides a if and only if 11 divides

$$a_0 - a_1 + a_2 - \cdots.$$

- (viii) What is the rule for divisibility by 7?
7. Suppose that someone tricks you into believing that $233 \cdot 577 = 135441$. Use congruences to prove in a flash that this is wrong. Is there a smart way of using congruences to double-check computations such as $a + b$ and ab for integers a and b ? Give a few examples.
8. Prove that $3 \mid 4^n - 1$, where $n \in \mathbb{N}$.
9. Let $m, n \in \mathbb{Z}$ not both equal zero. Prove that

$$\gcd(m, n) = \max \operatorname{div}(m) \cap \operatorname{div}(n),$$

where $\max(m, n) = m$ if $m \geq n$ and $\max(m, n) = n$ if $m < n$.

10. Let $u, v \in \mathbb{Z}$. Show that
- (i) $2 \mid u, v \Rightarrow \gcd(u, v) = 2 \gcd(u/2, v/2)$.
 - (ii) $2 \mid u, 2 \nmid v \Rightarrow \gcd(u, v) = \gcd(u/2, v)$.
 - (iii) Use (i) and (ii) to construct a “new” Euclidean algorithm, where you also apply the fact that $\gcd(u, v) = \gcd(u - v, v)$. Give a few examples.
- The “new” Euclidean algorithm alluded to in this exercise is called the binary Euclidean algorithm. It was discovered in 1961.
11. Let $x, y, z, d \in \mathbb{Z}$. Prove the following statements.
- (i) $x \equiv x \pmod{d}$.
 - (ii) If $x \equiv y \pmod{d}$ then $y \equiv x \pmod{d}$.
 - (iii) If $x \equiv y \pmod{d}$ and $y \equiv z \pmod{d}$ then $x \equiv z \pmod{d}$.
12. Compute $\lambda, \mu \in \mathbb{Z}$ such that $89\lambda + 55\mu = 1$ and find all solutions $x \in \mathbb{Z}$ to

$$89x \equiv 7 \pmod{55}.$$

13. Suppose that $\lambda N + \mu M = d$, where $\lambda, \mu, M, N \in \mathbb{Z}$ and $N > 0$. Prove that one may find $\lambda', \mu' \in \mathbb{Z}$ such that

$$\lambda' N + \mu' M = d,$$

where $0 \leq \mu' < N$.

14. Let $m, n \in \mathbb{Z}$ and suppose that there exist $\lambda, \mu \in \mathbb{Z}$ such that $\lambda m + \mu n = 1$. Prove that m and n are relatively prime.
15. Suppose that $a, b \in \mathbb{Z}$ and $\gcd(a, b) = 1$. Prove that $\gcd(a^m, b^n) = 1$ for $m, n \in \mathbb{N}$.
16. Let $m, n \in \mathbb{N}$ and let $S = \{xm + yn \mid x, y \in \mathbb{Z}\} \subseteq \mathbb{Z}$. Prove that
- (i) $q \in \mathbb{Z}$ and $s, t \in S \Rightarrow qs \in S$ and $s + t \in S$.
 - (ii) Assume that $S \neq \{0\}$. Use (i) to prove that $S = \{ad \mid a \in \mathbb{Z}\}$, where d is the first element > 0 in $S \cap \mathbb{N}$.
 - (iii) Prove that $d = \gcd(m, n)$ (again assuming that $S \neq \{0\}$).
- This gives another proof of Lemma 1.5.7.
17. What is the smallest odd natural number that leaves a remainder of 2 when divided by 3 and a remainder of 3 when divided by 5?
18. Solve the system ([11][18])

$$X \equiv 17 \pmod{504},$$

$$X \equiv -4 \pmod{35},$$

$$X \equiv 33 \pmod{16},$$

of congruences in X .

19. Why does the following number game work?

Ask anyone to select a number less than 60. Request him to perform the following operations. (i) Divide it by 3 and mention the remainder; suppose it to be a . (ii) Divide it by 4, and mention the remainder; suppose it to be b . (iii) Divide it by 5 and mention the remainder; suppose it to be c . Then the number selected is the remainder obtained by dividing $40a + 45b + 36c$ by 60.

20. (Quoted from [18]) An old woman goes to market and a horse steps on her basket and crushes her eggs. The rider offers to pay for the damages and asks her how many eggs she had brought. She does not remember the exact number, but when she had taken them out two at a time, there was one egg left. The same had happened when she picked them out three, four, five and six at a time, but when she took them out seven at a time they came out even (no eggs left). What is the smallest number of eggs she could have had?
21. On a desert island, five men and a monkey gather coconuts all day, then they go to sleep. The first man wakes up and takes his share. He divides the coconuts into five equal shares and gives the monkey the one coconut left over, hides his share and goes back to sleep. The second man wakes up, takes his fifth from the remaining pile; he too finds one extra and gives it to the monkey. Each of the remaining three men does likewise in turn. Find the minimum number of coconuts that must have been originally present.
22. Prove that $\varphi(n) = \varphi(2n)$ if n is odd.
23. It seems that $\varphi(n)$ is even when $n > 2$. Can you prove this without using the formula in subsection 1.8.3?
24. Suppose that p_1, \dots, p_N are the first N prime numbers. Is $p_1 \cdots p_N + 1$ a prime number? (hint: $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \equiv -1 \pmod{19}$).
25. Prove that n has to be a prime number if the Mersenne number $M_n = 2^n - 1$ is a prime number. Is M_n a prime number if n is a prime number?
26. Prove that if $2^n + 1$ is a prime then n is a power of 2 (hint: if $n = ab$, where b is odd, then $2^a + 1$ divides $2^n + 1$). The n th Fermat number F_n is defined as $2^{2^n} + 1$. Prove that F_0, F_1, F_2, F_3, F_4 are prime numbers.
27. Prove that F_m and F_n (see the previous exercise) are relatively prime if $m \neq n$ (hint: prove and use that $\prod_{i=0}^{n-1} F_i = F_n - 2$). Use this to prove that there are infinitely many prime numbers.
28. Find a prime factorization of 2419 in less than 3 minutes.
29. (i) Let $p > 3$ be a prime number. Prove that for every a , $1 < a < p - 1$, there is a unique $b \neq a$, $1 < b < p - 1$, such that $ab \equiv 1 \pmod{p}$.

(ii) Let p be a prime number. Prove that $(p-1)! \equiv -1 \pmod{p}$ (hint: think in pairs and apply (i)).

(iii) Suppose that $(n-1)! \equiv -1 \pmod{n}$, where $n \geq 2$. Is n a prime number?

The result in (ii) is called Wilson's theorem.

30. (i) Let p be a prime number. Prove that

$$p \mid \binom{p}{i} \quad \text{for } 1 \leq i \leq p-1$$

using Lemma 1.8.3.

(ii) Prove that

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

for integers a, b and a prime number p (hint: use (i) or Corollary 1.9.2).

(iii) Suppose that

$$n \mid \binom{n}{i} \quad \text{for } 1 \leq i \leq n-1.$$

Is n a prime number?

31. Prove unique factorization using that \mathbb{N} is well ordered, by assuming that

$$M = \{n \in \mathbb{N} \setminus \{0\} \mid n \text{ does not have a unique factorization}\}$$

is a non-empty subset of \mathbb{N} . Let m denote the first element in M . Consider two different prime factorizations

$$m = p_1 \cdots p_r,$$

$$m = q_1 \cdots q_s$$

of m .

(i) Prove that

$$\{p_1, \dots, p_r\} \cap \{q_1, \dots, q_s\} = \emptyset.$$

(ii) Assume that $p_1 < q_1$. Use the fact that the number

$$\begin{aligned} n &= p_1 \cdots p_r - p_1 q_2 \cdots q_s \\ &= (q_1 - p_1) q_2 \cdots q_s \end{aligned}$$

has a unique factorization to reach a contradiction.

This proof of unique factorization is from the classic text by Courant and Robbins [4].

32. What is the product of the greatest common divisor and the least common multiple?

33. Let $n \in \mathbb{N} \setminus \{0\}$ have the prime factorization

$$n = p_1^{e_1} \cdots p_m^{e_m},$$

where $p_i \neq p_j$ for $i \neq j$. Let $d(n) = |\text{div}(n)|$ and

$$\sigma(n) = \sum_{d \in \text{div}(n)} d$$

be respectively the number of natural divisors in n and the sum of the natural divisors in n .

(i) Prove that $d(n) = (e_1 + 1) \cdots (e_m + 1)$.

(ii) Prove that

$$\sigma(n) = \frac{p_1^{e_1+1} - 1}{p_1 - 1} \cdots \frac{p_m^{e_m+1} - 1}{p_m - 1}.$$

34. A number $n \in \mathbb{N}$ is called perfect if $\sigma(n) = 2n$. So, a number is perfect if it is the sum of its natural divisors except itself. Prove that if $2^{n+1} - 1$ is a prime number then $2^n(2^{n+1} - 1)$ is perfect.
35. Use GIMPS and a computer to find a perfect number with more than one million digits.
36. Let $n = p_1^{s_1} p_2^{s_2}$, where $p_1 \neq p_2$ are prime numbers. Prove that $\varphi(n) = (p_1^{s_1} - p_1^{s_1-1})(p_2^{s_2} - p_2^{s_2-1})$ by counting explicitly the number of natural numbers less than n that are relatively prime to n . If you like counting and combinatorics you may generalize this to give a proof of the formula for computing φ in subsection 1.8.3.
37. Prove that the fifth Fermat number (see Exercise 1.26) $F_5 = 2^{32} + 1$ is composite (this was first proved by Euler in 1739, thereby demolishing the conjecture that every F_n is prime) by using the following hints: $5^4 + 2^4 = 1 + 2^7 \cdot 5$ and

$$F_5 = (5^4 + 2^4)(2^7)^4 - 5^4(2^7)^4 + 1.$$

It is not known whether there is a Fermat number F_n that is prime for $n > 4$.

38. Suppose that $N = pq$ is the product of two different prime numbers p and q . Show that p and q are solutions to the equation

$$X^2 + (\varphi(N) - N - 1)X + N = 0.$$

This shows that (given $N = pq$) finding p and q is just as “difficult” as finding $\varphi(N)$.

39. **(HOF)** Around 1994 the following email circulated (partially quoted):

We are happy to announce that

```
RSA-129 = 114381625757888676692357799761466120102182967212423625625618429 \
          35706935245733897830597123563958705058989075147599290026879543541
          = 3490529510847650949147849619903898133417764638493387843990820577 *
          32769132993266709549961988190834461413177642967992942539798288533
```

The encoded message published was

```
968696137546220614771409222543558829057599911245743198746951209308162 \
98225145708356931476622883989628013391990551829945157815154
```

This number came from an RSA encryption of the ‘secret’ message using the public exponent 9007.

The symbol \ indicates that the number is continued on the next line. This email announced that the original 1977 RSA challenge from Martin Gardner’s Scientific American column had been factored. It also gives the encoded message using the following encoding: space = 00, A = 01, B = 02, . . . What was the secret message encrypted in 1977?

The factorization of RSA-129 was a real challenge, involving participants in every corner of the world:

To find the factorization of RSA-129, we used the double large prime variation of the multiple polynomial quadratic sieve factoring method. The sieving step took approximately 5000 mips years, and was carried out in 8 months by about 600 volunteers from more than 20 countries, on all continents except Antarctica. Combining the partial relations produced a sparse matrix of 569466 rows and 524338 columns. This matrix was reduced to a dense matrix of 188614 rows and 188160 columns using structured Gaussian elimination. Ordinary Gaussian elimination on this matrix, consisting of 35489610240 bits (4.13 gigabyte), took 45 hours on a 16K MasPar MP-1 massively parallel computer. The first three dependencies all turned out to be ‘unlucky’ and produced the trivial factor RSA-129. The fourth dependency produced the above factorization.

We would like to thank everyone who contributed their time and effort to this project. Without your help this would not have been possible.

Derek Atkins
Michael Graff
Arjen Lenstra
Paul Leyland

40. **(HOF)** Suppose that you are given e , d and N in the context of the RSA cryptosystem. The purpose of this exercise is to show that one can deduce the prime factorization $N = pq$ from this.
- Show that the congruence $x^2 \equiv 1 \pmod{N}$ has four solutions modulo N (there are two more apart from the obvious $x = \pm 1$).
 - Show that one of these solutions x satisfies $x \equiv -1 \pmod{p}$ and $x \equiv 1 \pmod{q}$. How can this be used to find p effectively?

- (iii) Using that $\varphi(N)$ is even, deduce an effective probabilistic algorithm for finding p and q given e, d and N (you already know that $\varphi(N) \mid ed - 1$ and that $a^{\varphi(N)} \equiv 1 \pmod{N}$ for $\gcd(a, N) = 1$).
- (iv) Why is it not secure to use the same N for different people in the RSA system?
- 41. Prove that $a^{N-1} \not\equiv 1 \pmod{N}$ if $\gcd(a, N) > 1$, where $a, N \in \mathbb{Z}$ and $N \geq 1$.
- 42. Prove that 899 is composite using only Corollary 1.9.2.
- 43. Prove that 15 is not a strong pseudoprime relative to 11.
- 44. Prove that 25 is a strong pseudoprime relative to 7.
- 45. Let $n = p_1 \cdots p_r$ be a product of primes, where $p_i \neq p_j, 1 \leq i < j \leq r$. Suppose that $p_i - 1 \mid n - 1$ for $i = 1, \dots, r$.
 - (i) Prove that $a^{n-1} \equiv 1 \pmod{n}$ if $\gcd(a, n) = 1$.
 - (ii) Prove that 561 is a Carmichael number.
 - (iii) Give an example of a Carmichael number $\neq 561$.
- 46. Use Pollard's ρ -algorithm to factor $N = 10403$.
- 47. **(HOF)** Implement Pollard's ρ -algorithm using a computer language with infinite-precision integer arithmetic. Use the polynomial $f(X) = X^{2048} + 1$ and $X_0 = Y_0 = 3$ instead of $f(X) = X^2 + 1$ and $X_0 = 0$ to factor the eighth Fermat number

$$F_8 = 2^{2^8} + 1.$$

This is a number with 78 digits.

- 48. Use Pollard's $(p - 1)$ -algorithm to factor $N = 295927$.
- 49. Part (ii) of this exercise uses linear algebra over the finite field \mathbb{F}_2 with two elements, which is detailed later in the book (see Chapter 3 and Appendix B).
 - (i) Let $x = p_1^{m_1} \cdots p_r^{m_r}$ be a prime factorization of a positive natural number. Prove that x is a square if and only if all the exponents m_1, \dots, m_r are even.
 - (ii) Suppose that the prime factorizations of a_1, \dots, a_n over the factor basis $P = \{p_1, \dots, p_r\}$ (assume that all the a factor completely using primes from P) are

$$\begin{aligned} a_1 &= p_1^{m_{11}} \cdots p_r^{m_{1r}}, \\ a_2 &= p_1^{m_{21}} \cdots p_r^{m_{2r}}, \\ &\vdots \\ a_n &= p_1^{m_{n1}} \cdots p_r^{m_{nr}}. \end{aligned}$$

Translate the problem of finding a subset $\{i_1, \dots, i_s\}$ of $\{1, 2, \dots, n\}$ such that $a_{i_1} \cdots a_{i_s}$ is a square into linear algebra over \mathbb{F}_2 .

50. Let $f(X) = a_n X^n + \cdots + a_1 X + a_0$, where $a_i \in \mathbb{Z}$, $n \in \mathbb{N}$ and X is a variable. The degree of f is said to be n modulo $N \in \mathbb{Z}$ if $N \nmid a_n$.
- (i) Show that $X - a \mid X^n - a^n$, where $X, a \in \mathbb{Z}$ and $n \in \mathbb{N}$.
 - (ii) Let $a, N \in \mathbb{Z}$. Show that if f has degree n modulo N and $f(a) \equiv 0 \pmod{N}$ then $f(X) \equiv (X - a)g(X) \pmod{N}$, where g has degree $n - 1$ modulo N (use (i) and $f(X) \equiv f(X) - f(a) \pmod{N}$).
 - (iii) Show that the congruence $f(X) \equiv 0 \pmod{p}$ has at most n incongruent solutions modulo p , if p is a prime and f has degree n modulo p . What if p is not a prime?
51. Let p be an odd prime.
- (i) Prove that the product of two quadratic residues modulo p is a quadratic residue modulo p .
 - (ii) Prove that the product of two quadratic non-residues modulo p is a quadratic residue modulo p .
 - (iii) Prove that the product of a quadratic residue modulo p and a quadratic non-residue modulo p is a quadratic non-residue modulo p .
52. Determine the quadratic residues and non-residues modulo 13.
53. Show that 3 is a quadratic residue modulo the prime p if $p \equiv 1 \pmod{12}$.
54. Compute

$$\left(\frac{7}{17}\right).$$