7 Number Theory

7.1 Introduction

The basic arithmetic operations we have learned in primary school are addition, subtraction, multiplication, and division on natural numbers. These operations are meaningful, not only for numbers, but also for more general objects, like functions and, in particular, polynomials. Some properties of the arithmetic operations remain valid in these more general structures, whereas other properties lose their validity.

In this chapter we study some of the properties of integer numbers, which are the numbers $\cdots, -2, -1, 0, 1, 2, 3, \cdots$. The set of these numbers is called $\mathbb{Z}$; it has the set $\mathbb{N}$ of the natural numbers $0, 1, 2, 3, \cdots$ as a subset. So, $\mathbb{N}$ includes 0. In the earlier days of mathematics 0 was not considered a natural number, but if we "define" the natural numbers as the numbers used for *counting* then 0 is a very natural number: at the moment I write this, for instance, I have 0 coins in my pocket. (As a child I have learned that "zero is nothing", but this is not true, of course: although I have 0 coins in my pocket, it is not empty: it contains 0 coins but 1 handkerchief and 1 keyring holding 5 keys.) Also, at any given moment my wallet may contain 3 Euros and 0 U.S. dollars. Moreover, 0 has the, very important, algebraic property that it is the identity element of addition: $x+0 = x$, for all $x \in \mathbb{N}$ (and also for x in $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$, of course). In addition, the natural numbers have the property that every natural number is equal to the number of its *predecessors*, where the predecessors of x are all natural numbers less than x: for every $x \in \mathbb{N}$, we have that x is equal to the number of elements of the set $\{ y \in \mathbb{N} \mid y < x \}$, and this is also true if $x = 0$.

The set of *positive naturals* is denoted by $\mathbb{N}^+$; it equals $\mathbb{N}$ but without 0, so we have $\mathbb{N}^+ = \mathbb{N} \setminus \{0\}$. When we discuss the *prime numbers* we will have need of the set of all natural numbers that are at least 2, so this is $\mathbb{N}$ without 0 and 1. We will call such numbers "multiples" and denote its set as $\mathbb{N}^{+2}$. So, $\mathbb{N}^{+2} = \mathbb{N} \setminus \{0, 1\}$.

7.2 Divisibility

We start our subject with an exploration of *divisibility* and its, hopefully well-known, properties.

7.1 Definition. For $a, d \in \mathbb{Z}$ we say that "a is *divisible by* d" or, equivalently, that "a is a *multiple of* d" or, equivalently, "d is a *divisor of* a" if and only if:

$$(\exists q : q \in \mathbb{Z} : a = q * d) \quad .$$

□

By this definition, every integer is a divisor of 0, even 0 itself, although $0/0$ is not defined! If, however, $d \neq 0$, then for every $a \in \mathbb{Z}$ the value q, if it exists, for which $a = q * d$ is *unique*, and we write it as a/d, called the "quotient of" a and d. So, note that a/d is well-defined *if and only if* both a is divisible by d and $d \neq 0$.

Other simple properties are that every integer is divisible by 1 and by itself, and, as a consequence, 1 is a divisor of every integer.

The relation "is a divisor of" is often denoted by the (infix) symbol $|$. That is, we write $d\,|\,a$ for the proposition "d is a *divisor of* a". Then, as we have seen earlier, $(\mathbb{N}^+, |)$ is a poset: the relation $|$ is reflexive, anti-symmetric, and transitive.

7.2 Lemma. $(\forall a, d : a, d \in \mathbb{N}^+ : d\,|\,a \Rightarrow d \leq a)$.

Proof. If $d\,|\,a$ for $d, a \in \mathbb{N}^+$, then $a = q * d$ for some integer q. Since $d, a \in \mathbb{N}^+$ this is only possible for $q \geq 1$, so $a - d = q * d - d = (q-1) * d \geq 0$. □

A direct consequence of Lemma 7.2 is that the set of all (positive) divisors of a positive natural number is *finite*: the set of divisors of $a \in \mathbb{N}^+$ is a subset of the (finite) interval $[\,1\,,\,a\,]$. Because $1\,|\,a$ the set of divisors of a is non-empty, for every $a \in \mathbb{N}^+$.
Another important property of divisibility (by d) is that it is invariant under addition of multiples (of d). We call this a *translation property*.

7.3 Lemma. $(\forall a, d, x : a, d \in \mathbb{N}^+ \wedge x \in \mathbb{Z} : d\,|\,a \;\Leftrightarrow\; d\,|\,(a + x * d))$.

Proof. If $d\,|\,a$ then $a = q * d$ for some integer q. Hence $a + x * d = q * d + x * d = (q + x) * d$. Since both q and x are integer, so is $q + x$, hence $d\,|\,(a + x * d)$.

Conversely, assume $d\,|\,(a + x * d)$. Then $a + x * d = q * d$ for some integer q. Hence $a = q * d - x * d = (q - x) * d$. Since both q and x are integer, so is $q - x$, hence $d\,|\,a$. □

* * *

We have seen that not every number is divisible by every other number: a/d is not defined for all a, d, even if $d \neq 0$. Division can, however, be defined more generally, if only we allow the possibility of a, so-called, *remainder*. For the sake of this discussion we restrict ourselves to *positive* d, so $d \in \mathbb{N}^+$.

The equation, with $q \in \mathbb{Z}$ as the unknown, $a = q * d$ may not have a solution, but we can weaken the equation in such a way that it has a solution, and then the solution still happens to be unique.

7.4 Theorem. For all $a \in \mathbb{Z}$ and $d \in \mathbb{N}^+$ unique integers q, r exist satisfying:

$$a \;=\; q * d + r \;\;\wedge\;\; 0 \leq r < d \;\;.$$

Proof. We prove existence of the solution and its uniqueness separately.

Existence. We distinguish the cases $0 \leq a$ and $a < 0$. For the first case we prove, for all $a \in \mathbb{N}$, existence of a solution by Mathematical Induction on a. Firstly, if $a < d$, then $q = 0$ and $r = a$ are a solution. Secondly, if $d \leq a$ then $a - d \in \mathbb{N}$ and, because $1 \leq d$, we have $a - d < a$. Now, we assume, by Induction Hypothesis, that q and r satisfy:

$$a-d \;=\; q*d+r \;\;\wedge\;\; 0\leq r<d \;\;.$$

Then we also have:

$$a \;=\; (q+1)*d+r \;\;\wedge\;\; 0\leq r<d \;\;,$$

hence, $q+1$ and r are a solution for a and d.

The proof for the case $a<0$ is very similar, but now by Mathematical Induction on $-a$. Firstly, if $-d\leq a$ then $q=-1$ and $r=a+d$ are a solution. Secondly, if $a\leq -d$ then we have $a+d<0$ and $-(a+d)<-a$. So let, again by Induction Hypothesis, q and r satisfy:

$$a+d \;=\; q*d+r \;\;\wedge\;\; 0\leq r<d \;\;.$$

Then we also have:

$$a \;=\; (q-1)*d+r \;\;\wedge\;\; 0\leq r<d \;\;,$$

hence, now $q-1$ and r are a solution for a and d.

Uniqueness. Assume that q_0 and r_0 satisfy: $a \;=\; q_0*d+r_0 \;\;\wedge\;\; 0\leq r_0<d$, and, similarly, assume that q_1 and r_1 satisfy: $a \;=\; q_1*d+r_1 \;\;\wedge\;\; 0\leq r_1<d$. To prove uniqueness of the solution, then, we must prove $q_0=q_1$ and $r_0=r_1$. We now derive:

$$\begin{array}{ll} & a \;=\; q_0*d+r_0 \;\;\wedge\;\; a \;=\; q_1*d+r_1 \\ \Rightarrow & \qquad \{\text{ transitivity of } =\ \} \\ & q_0*d+r_0 \;=\; q_1*d+r_1 \\ \Leftrightarrow & \qquad \{\text{ algebra }\} \\ & r_0-r_1 \;=\; (q_1-q_0)*d \;\;, \end{array}$$

from which we conclude that r_0-r_1 is a multiple of d. From the restrictions on r_0 and r_1, in the above equations, however, it follows that $-d<r_0-r_1<+d$, and the only multiple of d in this range is 0. So, we conclude that $r_0-r_1=0$, which is equivalent to $r_0=r_1$. But now we also have $(q_1-q_0)*d=0$, which, because $d\neq 0$, is equivalent to $q_0=q_1$, as required.

□

7.5 Definition. The unique value q mentioned in the theorem is called the "quotient of" a and d, and is denoted as $a\,\mathsf{div}\,d$. The unique value r mentioned in the theorem is called the "remainder of" a and d, and is denoted as $a\,\mathsf{mod}\,d$. As a result we obtain the following relation for div and mod, which we consider their definition, albeit an implicit one:

$$a \;=\; (a\,\mathsf{div}\,d)*d+a\,\mathsf{mod}\,d \;\;\wedge\;\; 0\leq a\,\mathsf{mod}\,d<d \;\;.$$

□

warning: Most programming languages have operators for quotient and remainder, even for negative values of d. The definitions of these operators not always are consistent with the definition given here. They do, however, always yield values q and r that satisfy $a \;=\; q*d+r$, but differences may

arise in the additional restrictions imposed upon r. If both a and d are natural, however, so $0 \leq a$ and $1 \leq d$, then the operators for quotient and remainder yield the same values as $a \operatorname{div} d$ and $a \bmod d$ as defined here. Be careful, though, in cases where either a or d may be negative. In particular, for negative a or d, the operations in several programming languages do *not* have the translation properties in Lemma 7.7

□

Operators div and mod are a true generalization of division, as they have the following properties that are immediate from the definitions.

7.6 Lemma. For all $a \in \mathbb{Z}$ and $d \in \mathbb{N}^+$ we have:

$$a \bmod d = 0 \;\Leftrightarrow\; d \mid a \quad \text{, and:}$$
$$a \bmod d = 0 \;\Rightarrow\; a \operatorname{div} d = a / d \quad .$$

□

Operators div and mod have many other useful properties, such as the following, so-called, *translation properties*. For more properties we refer the reader to the exercises.

7.7 Lemma. For all $a \in \mathbb{Z}$ and $d \in \mathbb{N}^+$, and for all $x \in \mathbb{Z}$ we have:

$$(a + x * d) \operatorname{div} d = a \operatorname{div} d + x \quad \text{, and:}$$
$$(a + x * d) \bmod d = a \bmod d$$

Proof. $a + x * d = (a \operatorname{div} d) * d + a \bmod d + x * d = ((a \operatorname{div} d) + x) * d + a \bmod d$, due to $0 \leq a \bmod d < d$ and unicity as stated in Theorem 7.4 we conclude the lemma. □

7.3 Greatest common divisors

In this section we consider positive natural numbers only. Throughout this chapter we use names a, b, c, d for variables of type $\mathbb{N}^+$ and variables x, y, z to denote variables of type $\mathbb{Z}$.

As we have seen already in Lemma 7.2 the set of (positive) divisors of $a \in \mathbb{N}^+$ is non-empty, as it contains 1 and a, and it is finite. We denote this set as $\mathcal{D}(a)$.

7.8 Definition. For $a \in \mathbb{N}^+$ the set $\mathcal{D}(a)$ of (positive) divisors of a is defined by:

$$\mathcal{D}(a) \;=\; \{\, d \in \mathbb{N}^+ \mid d \mid a \,\} \quad .$$

□

For all $a, b \in \mathbb{N}^+$ their respective sets $\mathcal{D}(a)$ and $\mathcal{D}(b)$ have a non-empty intersection, because both contain 1, and this intersection is finite as well. The elements of the set $\mathcal{D}(a) \cap \mathcal{D}(b)$ are called *common divisors* of a and b. As an abbreviation we also denote this intersection as $\mathcal{D}(a, b)$. So, by definition $\mathcal{D}(a, b)$ satisfies:

$$\mathcal{D}(a,b) \;=\; \{\, d{\in}\mathbb{N}^+ \mid d|a \wedge d|b \,\} \quad .$$

Because $\mathcal{D}(a,b)$ is non-empty and finite it has a maximum. This maximum is called the *greatest common divisor* of a and b. This depends on a and b, of course, so it is a function, which we call gcd.

7.9 Definition. Function gcd, of type $\mathbb{N}^+ \times \mathbb{N}^+ \to \mathbb{N}^+$, is defined by, for all $a,b \in \mathbb{N}^+$:

$$gcd(a,b) \;=\; \mathsf{max}\, \mathcal{D}(a,b) \quad ,$$

or, stated in words, $gcd(a,b)$ is the greatest number of which both a and b is a divisor.
□

The common divisors of a and a itself just are the divisors of a, that is, we have $\mathcal{D}(a,a) = \mathcal{D}(a)$; hence the greatest common divisor of a and a itself just is the greatest divisor of a, which is a. If $b<a$ then $a-b \in \mathbb{N}^+$, and on account of translation Lemma 7.3, we conclude that $\mathcal{D}(a,b) = \mathcal{D}(a-b\,,b)$. In words: if $b<a$ then a and b have the same common divisors as $a-b$ and b; hence, their greatest common divisors are equal as well. Similarly, if $a<b$ then $\mathcal{D}(a,b) = \mathcal{D}(a\,,b-a)$ and the greatest common divisor of a and b is equal to the greatest common divisor of b and $b-a$. Thus we obtain the following lemma.

7.10 Lemma. For all $a,b \in \mathbb{N}^+$:

$$\begin{array}{lcll} gcd(a,a) & = & a & \\ gcd(a,b) & = & gcd(a-b\,,b) & \text{, if } b<a \\ gcd(a,b) & = & gcd(a\,,b-a) & \text{, if } a<b \end{array}$$

□

Greatest common divisors also have the following, quite surprising, property that the common divisors of a and b are the divisors of $gcd(a,b)$.

7.11 Lemma. For all $a,b,c \in \mathbb{N}^+$ with $c = gcd(a,b)$:

$$\mathcal{D}(a,b) \;=\; \mathcal{D}(c) \quad .$$

Proof. By Mathematical Induction on the value $a+b$. Firstly, if $a=b$ then, as we have seen, $\mathcal{D}(a,b) = \mathcal{D}(a)$ and, by Lemma 7.10, we have $c=a$, so also $\mathcal{D}(c) = \mathcal{D}(a)$; hence, $\mathcal{D}(a,b) = \mathcal{D}(c)$. Secondly, if $b<a$ then, as we have seen, $\mathcal{D}(a,b) = \mathcal{D}(a-b\,,b)$, and, by Lemma 7.10, we have $c = gcd(a-b\,,b)$; now we assume, by Induction Hypothesis – because $(a-b)+b < a+b$ – that $\mathcal{D}(a-b\,,b) = \mathcal{D}(c)$; then it also follows that $\mathcal{D}(a,b) = \mathcal{D}(c)$. Thirdly, the case $a<b$ is similar to the previous case, because the situation is symmetric in a and b.
□

A direct consequence of translation Lemma 7.3 is that every common divisor of a and b also is divisor of any linear combination of a and b.

7.12 Lemma. For all $a, b, d \in \mathbb{N}^+$ and for all $x, y \in \mathbb{Z}$:

$$d \,|\, a \wedge d \,|\, b \;\Rightarrow\; d \,|\, (x*a + y*b) \quad .$$

□

In particular, $gcd(a,b)$ is a common divisor of a and b; hence, $gcd(a,b)$ also is a divisor of every linear combination of a and b. There is more to this, however, as the following theorem shows.

7.13 Theorem. For all $a, b \in \mathbb{N}^+$, integers $x, y \in \mathbb{Z}$ exist satisfying:

$$gcd(a,b) \;=\; x*a \,+\, y*b$$

Proof. A constructive proof is given in the next section, in the form of Euclid's extended algorithm, which shows how suitable numbers x and y can be calculated.
□

A consequence of this theorem is that $gcd(a,b)$ is the *smallest* of all positive linear combinations of a and b.

7.14 Theorem. For all $a, b \in \mathbb{N}^+$ we have:

$$gcd(a,b) \;=\; \mathsf{min}\,\{\, x*a + y*b \mid x, y \in \mathbb{Z} \wedge 1 \leq x*a + y*b \,\} \quad .$$

Proof. Let xm and ym be integers for which $xm*a + ym*b$ is positive and minimal. Let $c = gcd(a,b)$ and let xc and yc be integers for which $c = xc*a + yc*b$; on account of Theorem 7.13 such numbers exist. Now we must prove: $c = xm*a + ym*b$, which we do by proving $c \leq xm*a + ym*b$ and $xm*a + ym*b \leq c$ separately:

$$\begin{array}{ll} & c \leq xm*a + ym*b \\ \Leftarrow & \quad \{\text{ Lemma 7.2, using that both } c \text{ and } xm*a+ym*b \text{ are positive } \} \\ & c \mid (xm*a + ym*b) \\ \Leftarrow & \quad \{\text{ Lemma 7.12 } \} \\ & c \,|\, a \;\wedge\; c \,|\, b \\ \Leftrightarrow & \quad \{\; c = gcd(a,b) \;\} \\ & \mathsf{true} \quad , \end{array}$$

and:

$$\begin{array}{ll} & xm*a + ym*b \leq c \\ \Leftrightarrow & \quad \{\text{ definition of } xc \text{ and } yc \;\} \\ & xm*a + ym*b \;\leq\; xc*a + yc*b \\ \Leftrightarrow & \quad \{\text{ both sides of the inequality are positive, and the LHS is minimal } \} \\ & \mathsf{true} \end{array}$$

□

* * *

Numbers of which the greatest common divisor equals 1 are called *relatively prime* or also *co-prime*. As we have seen – Theorem 7.13 –, for all $a, b \in \mathbb{N}^+$ integers x, y exist such that

$$gcd(a,b) \;=\; x*a + y*b \quad .$$

If $gcd(a,b) = 1$ this amounts to the existence of integers x and y satisfying:

$$x*a + y*b \;=\; 1 \quad .$$

The following two lemmas are useful consequences of this property.

7.15 Lemma. For all $a, b, c \in \mathbb{N}^+$: $\quad gcd(a,b) = 1 \;\wedge\; a \,|\, (b*c) \;\Rightarrow\; a \,|\, c$.

Proof. Let $gcd(a,b) = 1$ and let $a \,|\, (b*c)$; that is, assume that $x, y, z \in \mathbb{Z}$ satisfy:

(15) $\quad x*a + y*b = 1$

(16) $\quad b*c = z*a$

Now we derive:

$$\begin{array}{ll}
 & \mathsf{true} \\
\Leftrightarrow & \quad \{\ (15)\ \} \\
 & x*a + y*b = 1 \\
\Rightarrow & \quad \{\ \text{Leibniz}\ \} \\
 & x*a*c + y*b*c = c \\
\Leftrightarrow & \quad \{\ (16)\ \} \\
 & x*a*c + y*z*a = c \\
\Leftrightarrow & \quad \{\ \text{algebra}\ \} \\
 & (x*c + y*z)*a = c \\
\Rightarrow & \quad \{\ \exists\text{-introduction, with } q := x*c + y*z\ \} \\
 & (\exists q : q \in \mathbb{Z} : c = q*a) \\
\Leftrightarrow & \quad \{\ \text{Definition of } |\ \} \\
 & a \,|\, c
\end{array}$$

□

7.16 Lemma. For all $a, b, c \in \mathbb{N}^+$: $\quad gcd(a,b) = c \;\Rightarrow\; gcd(a/c\,,\, b/c) = 1$.

□

7.4 Euclid's algorithm and its extension

The relations in Lemma 7.10 can be considered as a recursive definition of function gcd; that, thus, function gcd is well-defined is, again, proved by Mathematical Induction on the value $a+b$. So, the following recursive definition actually constitutes an algorithm for the computation of the greatest common divisor of two positive naturals. This is known as "Euclid's algorithm". For all $a, b \in \mathbb{N}^+$:

$$\begin{array}{lcl} gcd(a,b) & = & \mathsf{if}\ \ a=b \ \rightarrow\ \ a \\ & & []\ \ a>b \ \rightarrow\ \ gcd(a-b\,,b) \\ & & []\ \ a<b \ \rightarrow\ \ gcd(a\,,b-a) \\ & & \mathsf{fi} \end{array}$$

This version of the algorithm is not particularly *efficient*, but it is the simplest possible. If, for instance, a is very much larger than b the calculation of $gcd(a,b)$ gives rise to the repeated subtraction $a-b$, until a does not exceed b anymore. Therefore, a more efficient algorithm can be constructed by means of div and mod operations.

* * *

According to Theorem 7.13 we have that $gcd(a,b)$ is a *linear combination* of a and b; this means that, for every $a, b \in \mathbb{N}^+$, integers x, y exist satisfying:

(17) $\quad gcd(a,b) \ = \ x*a \ + \ y*b \ .$

In what follows we call such integers "matching numbers" for $gcd(a,b)$. Matching numbers are not *unique*: if, for instance, x and y are matching numbers for $gcd(a,b)$ then so are $x+b$ and $y-a$.

Because Theorem 7.13 is about *existence* of integers, we can try to prove it constructively by showing how these numbers can be computed. It so happens that Euclid's algorithm can be *extended* in such a way that, in addition to $gcd(a,b)$, integers x and y are calculated that satisfy (17) as well. As a result, provided we have proved the correctness of the extended algorithm, we not only have a proof of the theorem but we also obtain an algorithm to compute these numbers. (And, from the point of view of proving the theorem, efficiency is of no concern and the simplest possible algorithm yields the simplest possible proof.)

As was the case with function gcd we present Euclid's extended algorithm in the form of a recursively defined function. For this purpose we simply call this function F here; it maps a pair of positive naturals to a *triple* consisting of a positive natural and two integers, namely the GCD of the pair together with matching numbers. We denote such a triple as $\langle\, c\,, x\,, y\,\rangle$, in which c, x, and y are the elements of the triple. This means that function F is required to satisfy the following *specification*.

specification: Function F has type $\mathbb{N}^+ \times \mathbb{N}^+ \rightarrow \mathbb{N}^+ \times \mathbb{Z} \times \mathbb{Z}$, and for all $a, b, c \in \mathbb{N}^+$ and for all $x, y \in \mathbb{Z}$, function F satisfies:

$$F(a,b) = \langle\, c\,, x\,, y\,\rangle \ \Rightarrow \ c = gcd(a,b) \ \wedge \ c = x*a + y*b$$

□

Notice that this specification does not specify F uniquely: because, as we have seen, matching numbers are not unique, several different functions F will satisfy this specification. This specification only states, firstly, that for every pair of positive naturals a and b its value $F(a,b)$ is a triple consisting of a positive natural and two integers, and, secondly, that for every such triple its first element is equal to $gcd(a,b)$ and its second and third elements are matching numbers for $gcd(a,b)$.

A simple recursive definition for F can now be constructed, based on the following considerations, using Mathematical Induction on $a+b$ again. Firstly, if $a=b$ then $gcd(a,b)=a$, and $a = 1*a+0*b$: hence, in this case $x=1$ and $y=0$ is an acceptable solution for x and y. Because $a=b$ we also have $gcd(a,b)=b$; therefore, $x=0$ and $y=1$ is an acceptable solution too: this illustrates once more that the numbers x and y are not unique.

Secondly, if $a>b$ then we have $gcd(a,b) = gcd(a-b,b)$. Now suppose, by Induction Hypothesis, that x,y are integers satisfying:

$$gcd(a-b,b) \;=\; x*(a-b) + y*b \quad .$$

The right-hand side of this equality can be rewritten to:

$$gcd(a-b,b) \;=\; x*a + (y-x)*b \quad ,$$

and because $gcd(a,b) = gcd(a-b,b)$ this is equivalent to:

$$gcd(a,b) \;=\; x*a + (y-x)*b \quad .$$

From this we conclude that if x and y are matching numbers for $gcd(a-b,b)$ then x and $y-x$ are matching numbers for $gcd(a,b)$.

Finally and similarly, for the case $a<b$ we can show that if x and y are matching numbers for $gcd(a,b-a)$ then $x-y$ and y are matching numbers for $gcd(a,b)$.

We now combine these results into the following recursive definition for F; this we call *Euclid's extended algorithm*:

$$\begin{array}{lcll} F(a,b) & = & \mathsf{if}\ \ a=b & \rightarrow\ \ \langle\, a\,,1\,,0\,\rangle \\ & & []\ \ a>b & \rightarrow\ \ \langle\, c\,,x\,,y-x\,\rangle \\ & & & \quad \mathsf{where}\ \langle\, c\,,x\,,y\,\rangle \;=\; F(a-b,b) \\ & & []\ \ a<b & \rightarrow\ \ \langle\, c\,,x-y\,,y\,\rangle \\ & & & \quad \mathsf{where}\ \langle\, c\,,x\,,y\,\rangle \;=\; F(a\,,b-a) \\ & & \mathsf{fi} & \end{array}$$

This recursive definition is an example of a, so-called, *functional program*, but it is not difficult to encode this as a recursive function in languages like PASCAL or JAVA. As was the case with Euclid's algorithm proper, this algorithm is not very efficient, but it can be transformed into a more efficient one by means of division and remainder operations.

When applying this version of Euclid's algorithm or its extension to compute the gcd of, for instance, 1 and one million, the number one will be subtracted from the other number nearly one million times. As this example already shows, the complexity of the algorithm will not be better than linear in the arguments, which is not acceptable for applications in which the argument may be very large, as e.g. in cryptography. Now we present an improvement for which the complexity is improved to be logarithmic in the size of the arguments, by which it is suitable for using it for arguments in the order of magnitude of 10^{1000}. This improved version is one of the building blocks of modern public key cryptography.

The key ingredient of Euclid's algorithm as presented is that $gcd(a,b) = gcd(a, b-a)$, for $b > a > 0$. However, we also have $gcd(a,b) = gcd(a, b - c * a)$ for any choice for c we like, satisfying $c * a \leq b$. In the above version $c = 1$ was chosen, while the improved version takes $c = b \,\mathsf{div}\, a$. A first attempt looks as follows:

$$\begin{array}{lcll} gcd(a,b) & = & \mathsf{if} & a = b \;\rightarrow\; a \\ & & [\!] & a > b \;\rightarrow\; \cdots \\ & & [\!] & a < b \;\rightarrow\; gcd(a\,, b - (b \,\mathsf{div}\, a) * a) \\ & & \mathsf{fi} & \end{array}$$

This we will work out further. Note that $b-(b \,\mathsf{div}\, a) * a = b \,\mathsf{mod}\, a$. A further difference with our first version is that in case a is a divisor of b, we obtain $b-(b \,\mathsf{div}\, a) * a = 0$, and the resulting $b-(b \,\mathsf{div}\, a) * a = b \,\mathsf{mod}\, a$ is always $< a$. By keeping the first argument always less than the second argument, we now may further polish our algorithm without case analysis on $a > b$ and $a < b$. The resulting algorithm for $gcd(a,b)$ for $0 \leq a < b$ reads:

$$\begin{array}{lcll} gcd(a,b) & = & \mathsf{if} & a = 0 \;\rightarrow\; b \\ & & [\!] & a > 0 \;\rightarrow\; gcd(b \,\mathsf{mod}\, a, a) \\ & & \mathsf{fi} & \end{array}$$

This version correctly computes $gcd(a,b)$ for $a < b$ by construction, while now the worst case complexity can be shown to be logarithmic in the largest argument b.

Also the extended version can be modified in this way:

$$\begin{array}{lcll} F(a,b) & = & \mathsf{if} & a = 0 \;\rightarrow\; \langle\, b\,, 0\,, 1\,\rangle \\ & & [\!] & a > 0 \;\rightarrow\; \langle\, c\,, y - x * (b \,\mathsf{div}\, a)\,, x\,\rangle \\ & & & \quad \mathsf{where}\ \langle\, c\,, x\,, y\,\rangle = F(b \,\mathsf{mod}\, a\,, a) \\ & & \mathsf{fi} & \end{array}$$

Here for $0 \leq a < b$ the result of $F(a,b)$ is a triple (c,x,y) in which $c = gcd(a,b)$ and $x*a+y*b = c$. Also this algorithm can be shown to be logarithmic in the largest argument b since the number of steps is the same as for the basic gcd algorithm. Correctness follows since from $c = x * (b \,\mathsf{mod}\, a) + y * a$ one concludes $c = (y - x * (b \,\mathsf{div}\, a)) * a + x * b$. This is the version of the algorithm that is extensively used in practice.

To get a feeling how the algorithm works we apply it by hand to compute values x, y satisfying $73x + 87y = 1 = gcd(73, 87)$. In order to compute $F(73, 87)$ by the algorithm we have to compute $F(14, 73)$ since $87 \,\mathsf{mod}\, 73 = 14$, for which we have to compute $F(3, 14)$, and so on, until we arrive at $F(0, 1) = (1, 0, 1)$. In fact executing the algorithm corresponds to filling the following table:

a	b	x	y	$c = x * a + y * b$
73	87	31	-26	1
14	73	-26	5	1
3	14	5	-1	1
2	3	-1	1	1
1	2	1	0	1
0	1	0	1	1

Here first the columns for a and b are filled from top to bottom. Then in the last line $x = 0$ and $y = 1$ is filled, yielding $c = x * a + y * b = 1$. Next the values for x and y are filled from bottom to top in such a way that for every line $x * a + y * b = 1$ holds: according to the algorithm this is done by giving y the value of x from the line below, and giving x the value $y - x * (b \,\mathsf{div}\, a)$. At the end we fill the first line by $x = 31$ and $y = -26$, indeed satisfying the required property $73 * 31 + 87 * (-26) = 1 = gcd(73, 87)$.

7.5 The prime numbers

In this section we study the set $\mathbb{N}^{+2}$ of *multiples*, which are the natural numbers from 2 onwards. As we have seen, every integer, and, hence, also every multiple is divisible by 1 and by itself. A multiple with the property that it is *not* divisible by any other number is called a *prime (number)*.

7.17 Definition. A *prime* is a multiple that is divisible by 1 and itself only.

□

If we would not restrict ourselves to multiples but to positive naturals instead, 1 would be a prime too, according to this definition. There are sound, technical reasons, however, not to consider 1 as a prime, which is why we define the primes as a subset of the multiples. So, the smallest prime is 2.

7.18 Example. The primes less than 100 are: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97. Notice that 2 is even and that it is the *only* even prime.

□

The following lemma expresses that every multiple is divisible by at least one prime. If we would have allowed 1 as a prime number this lemma would have been void.

7.19 Lemma. For every $a \in \mathbb{N}^{+2}$ a prime p exists such that $p \,|\, a$.

Proof. By Mathematical Induction on a. Firstly, if a is a prime then a is a prime

and $a \mid a$. Secondly, if a is not prime then a multiple $b \in \mathbb{N}^{+2}$ exists satisfying $b \neq a$, and $b \mid a$. From Lemma 7.2, using $b \mid a$, we conclude that $b \leq a$, but because $b \neq a$ this amounts to $b < a$. So, by Induction Hypothesis, we may assume that p is a prime such that $p \mid b$. Because $b \mid a$, by the transitivity of divisibility, we then conclude $p \mid a$, as required.

□

The following theorem is important; it has been proved already by Euclides.

7.20 Theorem. The set of all primes is infinite.

Proof. One way to prove that a set is infinite is to prove that every *finite subset* of it differs from the whole set; that is, for every finite subset the whole set contains an element not in that subset. So, let V be a finite subset of the primes. Now we define multiple a by:

$$a \;=\; (\Pi p : p \in V : p) + 1 \quad .$$

Because the product $(\Pi p : p \in V : p)$ is divisible by every $p \in V$, the number a is *not* divisible by p, for every $p \in V$. On account of Lemma 7.19, however, a is divisible by at least one prime, which therefore, is not an element of V.

□

* * *

A very old algorithm to compute "all" primes is known as *Eratosthenes's sieve*. This involves infinite enumerations of infinite subsets of the multiples, which is unfeasible, of course, but for the purpose of computing any finite number of primes, finite prefixes of these infinite enumerations will do. To compute all, infinitely many, primes would, of course, take an infinite amount of time. Yet, we call it an algorithm to compute "all" primes because it can be used to compute as many primes as desired in a finite amount of time.

Informally, the algorithm is presented as follows. One starts with writing down all – that is: sufficiently many – multiples in increasing order:

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

The first number of this sequence, 2, is the first prime number, and we now construct a new sequence from the first one by eliminating all multiples of 2 from it:

$$3\,,\ 5\,,\ 7\,,\ 9\,,\ 11\,,\ 13\,,\ 15\,,\ 17\,,\ 19\,,\ 21\,,\ 23\,,\ \cdots \quad .$$

This second sequence is an enumeration, again in increasing order, of all multiples that are not divisible by the first prime, 2. The first number, 3, of this second sequence is the second prime, and, again, we construct a third sequence from this second one, this time by eliminating all multiples of 3:

$5\,,\ 7\,,\ 11\,,\ 13\,,\ 17\,,\ 19\,,\ 23\,,\ \cdots\ .$

This sequence contains all multiples that are not divisible by either 2 or 3; its first element, 5, is the *next* prime number, which is the smallest prime that is larger than 2 and 3. And so on...

The general properties on account of which this algorithm is correct are easily formulated. After n steps, for some $n\in\mathbb{N}$, a sequence is obtained that contains, in increasing order, all multiples that are *not* divisible by the smallest n prime numbers. The first number of this sequence then, because the sequence is increasing, is its minimum, and it can be proved that this minimum is the *next* prime, that is, the smallest prime number exceeding the smallest n prime numbers. By eliminating all multiples of this next prime the next sequence is obtained, containing all multiples not divisible by the first $n+1$ primes.

* * *

We have seen that the set of primes is infinite, but we may still ask for the *density* of the primes; that is, for any given multiple n we may ask *how many* primes are less than n. Because the number of potential divisors of n increases with n, the likelihood – not in the mathematical meaning of the word – that an arbitrary number is prime may be expected to decrease with increasing numbers.

The, so-called, *Prime Number Theorem* states that the number of primes less than n is approximately $n/\ln(n)$. This formula really gives an approximation only; for example, the number of primes less than 10^9 equals $50\,847\,534$, whereas $10^9/\ln(10^9)$ is $48\,254\,942$ (rounded). An elementary proof of the Prime Number Theorem has been constructed by the famous Hungarian mathematician Pál Erdös.

The greatest common divisor of a prime p and a positive natural a can have only one out of two possible values: either $p\,|\,a$ and then $gcd(p,a)=p$, or $\neg\,(p\,|\,a)$ and then $gcd(p,a)=1$. An important consequence of this is the following lemma.

7.21 Lemma. For every prime p and for all $a,b\in\mathbb{N}^+:\ p\,|\,(a*b)\ \Rightarrow\ p\,|\,a\ \vee\ p\,|\,b$.

Proof. By distinguishing the cases $p\,|\,a$ and $\neg\,(p\,|\,a)$ and, for the latter case, using Lemma 7.15 and $gcd(a,p)=1$ if $\neg\,(p\,|\,a)$.

□

7.22 Lemma. If p,q are distinct prime numbers and $k\geq 0$, then q is not a divisor of p^k.

Proof. Induction on k. For $k=0$ clearly q is not a divisor of $p^k=p^0=1$. For $k>0$ we write $p^k=p*p^{k-1}$. If $q\,|\,p*p^{k-1}$ then by Lemma 7.15 and $gcd(p,q)=1$ we conclude $q\,|\,p^{k-1}$, contradicting the induction hypothesis. □

The following theorem is known as the Unique Prime Factorization Theorem. Just like we write Σ for summation, we write Π for product. We even take infinite

products over all prime numbers as long as all but finitely many are equal to 1: then the meaning of the product is the product of the remaining finitely many arguments.

7.23 Theorem. Every positive natural $a \in \mathbb{N}^+$ satisfies

$$a = \prod_{p \text{ prime}} p^{k(p,a)}$$

in which $k(p,a)$ is the largest number k such that $p^k \,|\, a$, for every prime number p.

Proof. We apply induction on a. For $a = 1$ we have $k(p,a) = 0$ for all prime numbers, indeed yielding $1 = \Pi_{p \text{ prime}} p^{k(p,1)}$.

For $a > 1$ by Lemma 7.19 a prime q exists such that $q \,|\, a$. We will apply the induction hypothesis on a/q, yielding $a/q = \Pi_{p \text{ prime}} p^{k(p,a/q)}$, and we will compare $k(p,a/q)$ with $k(p,a)$ for all primes p. Since $q^{k(q,a/q)} \,|\, a/q$ but not $q^{k(q,a/q)+1} \,|\, a/q$, we obtain $q^{k(q,a/q)+1} \,|\, a$ but not $q^{k(q,a/q)+2} \,|\, a$, so $k(q,a) = k(q,a/q) + 1$.

Next let p be any prime number unequal to q and k any number > 0. We will prove $p^k \,|\, a$ if and only if $p^k \,|\, a/q$. If $p^k \,|\, a/q$ then $a/q = b * p^k$ for some b, yielding $a = p^k * (b * q)$, so $p^k \,|\, a$. Conversely let $p^k \,|\, a$. Then $a = b * p^k$ for some b. Since $q \,|\, a$ but not $q \,|\, p^k$ (by Lemma 7.22), by Lemma 7.21 we conclude $q \,|\, b$, so $b = q * c$ for some c. From $a = b * p^k = q * c * p^k$ we conclude $a/q = c * p^k$, so $p^k \,|\, a/q$. So we have proved $p^k \,|\, a$ if and only if $p^k \,|\, a/q$, so $k(p,a) = k(p,a/q)$.

Combining these results yields

$$\begin{array}{rcll} a & = & q * (a/q) & \\ & = & q * \prod_{p \text{ prime}} p^{k(p,a/q)} & \text{(induction hypothesis)} \\ & = & q * q^{k(q,a/q)} * \prod_{p \text{ prime}, p \neq q} p^{k(p,a/q)} & \text{(splitting product)} \\ & = & q^{k(q,a)} * \prod_{p \text{ prime}, p \neq q} p^{k(p,a)} & \text{(above observations)} \\ & = & \prod_{p \text{ prime}} p^{k(p,a)} & \text{(combine product),} \end{array}$$

concluding the proof. □

If $a = \prod_{p \text{ prime}} p^{k(p,a)}$ and $b = \prod_{p \text{ prime}} p^{k(p,b)}$, then it is easily checked that $a \,|\, b$ if and only if $k(p,a) \leq k(p,b$ for all prime numbers p. As a consequence we obtain

$$gcd(a,b) \;=\; \prod_{p \text{ prime}} p^{\min(k(p,a),k(p,b))}.$$

For instance, $6! = 2 * 3 * 4 * 5 * 6 = 2^4 * 3^2 * 5^1 * 7^0$ and $\binom{8}{3} = 6 * 7 * 8/(3!) = 2^3 * 3^0 * 5^0 * 7^1$, so $gcd(6!, \binom{8}{3}) = 2^3 * 3^0 * 5^0 * 7^0 = 8$.

Apart from the Greatest Common Divisor (*gcd*) of two numbers $a, b > 0$ one may also consider the Least Common Multiple (*lcm*): $lcm(a,b)$ is defined to be the

least number n such that $a \,|\, n$ and $b \,|\, n$. Such a number n with $a \,|\, n$ and $b \,|\, n$ always exists since $a * b$ satisfies the requirements, but $a * b$ does not need to be the smallest one. In fact, from the above observations one easily checks

$$lcm(a,b) \;=\; \prod_{p \text{ prime}} p^{\max(k(p,a),k(p,b))}.$$

Since for any two numbers k, k' we have $\max(k,k') + \min(k,k') = k + k'$, we obtain

$$gcd(a,b) * lcm(a,b) \;=\; \prod_{p \text{ prime}} p^{\min(k(p,a),k(p,b))+\max(k(p,a),k(p,b))}$$

$$= \prod_{p \text{ prime}} p^{k(p,a)+k(p,b)} \;=\; a * b$$

for all $a, b > 0$.

From these characterizations of *gcd* and *lcm* one easily derives that

$$c \,|\, a \wedge c \,|\, b \;\Leftrightarrow\; c \,|\, gcd(a,b)$$

and

$$a \,|\, c \wedge b \,|\, c \;\Leftrightarrow\; gcd(a,b) \,|\, c$$

for all numbers $a, b, c > 0$. As a consequence, we obtain that $(\mathbb{N}^+, |)$ is a *lattice*, in which *gcd* corresponds to the infimum and *lcm* corresponds to the supremum.

7.6 Modular Arithmetic

7.6.1 Congruence relations

Almost everybody probably knows that the product of two *even* integers is even, and that the product of two *odd* integers is odd. Also, the sum of two even integers is even too, and even the sum of two odd numbers is even. The point is that, apparently, whether the result of an operation, like addition or multiplication, is even or odd *only* depends on whether the arguments of the operation are even or odd.

The proposition that integer "x is even" is equivalent to "x is divisible by 2", which in turn is equivalent to $x \,\mathsf{mod}\, 2 = 0$; similarly, the proposition "x is odd" is equivalent to $x \,\mathsf{mod}\, 2 = 1$. That the property "being even" of the sum of two integers only depends on the "being even" of these two numbers know means that $(x+y) \,\mathsf{mod}\, 2$ only depends on $x \,\mathsf{mod}\, 2$ and $y \,\mathsf{mod}\, 2$ (and not on $x \,\mathsf{div}\, 2$ or $y \,\mathsf{div}\, 2$). In formula this is rendered as:

$$(18) \qquad (x+y) \,\mathsf{mod}\, 2 \;=\; (x \,\mathsf{mod}\, 2 + y \,\mathsf{mod}\, 2) \,\mathsf{mod}\, 2 \quad \text{, for all } x, y \in \mathbb{Z} \;.$$

Properties like these are not specific for 2 as a divisor: similar properties hold for all positive divisors. From the chapter on relations we recall that, for every function of type $B \to V$, the relation, on its domain B, "having the same function value"

is an equivalence relation. For any fixed $d \in \mathbb{N}^+$, the function $(\mathsf{mod}\, d)$ that maps every $x \in \mathbb{Z}$ to $x \,\mathsf{mod}\, d$ has type $\mathbb{Z} \to [\,0\,..\,d\,)$. This function induces an equivalence relation, on $\mathbb{Z}$, of "having the same remainder when divided by d". This relation partitions $\mathbb{Z}$ into d different (and, as always, disjoint) equivalence classes, namely one for every value of the function $(\mathsf{mod}\, d)$: the equivalence class corresponding to $a \in [\,0\,..\,d\,)$ is the set

$$\{\, x \in \mathbb{Z} \mid x \,\mathsf{mod}\, d = a \,\} \quad ,$$

which can also be formulated as:

$$\{\, q * d + a \mid q \in \mathbb{Z} \,\} \quad .$$

In particular, of course, $a \in \{\, x \in \mathbb{Z} \mid x \,\mathsf{mod}\, d = a \,\}$, because $a \,\mathsf{mod}\, d = a$, for every $a \in [\,0\,..\,d\,)$.

Now properties similar to (18) also hold in this case; that is, we now have:

$$(19) \qquad (x+y) \,\mathsf{mod}\, d \;=\; (x \,\mathsf{mod}\, d + y \,\mathsf{mod}\, d) \,\mathsf{mod}\, d \quad \text{, for all } x, y \in \mathbb{Z} \quad .$$

A similar property holds for subtraction and multiplication:

$$(20) \qquad (x * y) \,\mathsf{mod}\, d \;=\; (x \,\mathsf{mod}\, d * y \,\mathsf{mod}\, d) \,\mathsf{mod}\, d \quad \text{, for all } x, y \in \mathbb{Z} \quad .$$

A consequence of propositions like (19) and (20) is that equivalence is *preserved under* arithmetic operations like addition and multiplication. Using (19), for instance, we can now derive, for all $x, y, z \in \mathbb{Z}$:

$$(21) \qquad x \,\mathsf{mod}\, d \;=\; y \,\mathsf{mod}\, d \;\Rightarrow\; (x+z) \,\mathsf{mod}\, d \;=\; (y+z) \,\mathsf{mod}\, d \quad .$$

An equivalence relation that is preserved under a given set of operations is called a *congruence relation*. In our case, the relation "having the same remainder when divided by d" is congruent with the operations addition, subtraction, and multiplication. Conversely, we also say that the operations addition, subtraction, and multiplication are *compatible with* the relation.

Notation: According to mathematical tradition, the fact that x and y are congruent modulo d is often denoted as:

$$x \;=\; y \,(\mathrm{mod}\, d) \quad .$$

This notation is somewhat awkward, though, because it is not very clear what the *scope* is of the suffix "$(\mathrm{mod}\, d)$". Apparently, its scope extends over the complete equality textually preceding it; that is, if we would use some sort of brackets to delineate the scope of "$(\mathrm{mod}\, d)$" more explicitly, we should write something like:

$$[\![\; x \;=\; y \,(\mathrm{mod}\, d) \;]\!] \quad .$$

Because the relation is a congruence relation and because it is not the same as sheer equality, although it resembles it, it seems better to denote the relation as an infix symbol resembling but different from "$=$". For example, the

symbol "$=_{\mathrm{mod}\, d}$" would be appropriate, as the subscript explicitly indicates the nature of the congruence. In this text we will abbreviate this to "$=_d$"; so, by definition we now have, for all $d \in \mathbb{N}^+$ and $x, y \in \mathbb{Z}$:

$$x =_d y \;\Leftrightarrow\; x \bmod d = y \bmod d \quad .$$

For example, congruence property (21) can now be rendered as, for all $x, y, z \in \mathbb{Z}$:

$$x =_d y \;\Rightarrow\; x + z =_d y + z \quad .$$

□

Other algebraic properties are compatible with congruence modulo d too. The numbers 0 and 1, for instance, are the identity elements of addition and multiplication, respectively, and this remains so under congruence. In addition, the property that 0 is a zero-element of multiplication – that is: $0 * x = 0$ – is retained. Finally, that multiplication distributes over addition remains true as well.

For any given $d \in \mathbb{N}^+$ we can now define binary operations $\oplus$ and $\otimes$, say, by, for all $x, y \in \mathbb{Z}$:

$$x \oplus y \;=\; (x + y) \bmod d \quad , \text{ and:}$$

$$x \otimes y \;=\; (x * y) \bmod d \quad , \text{ and:}$$

(If we would be very strict we should make the dependence on d explicit by writing $\oplus_d$ and $\otimes_d$.) Now $\oplus$ and $\otimes$ have type $[0\,..\,d) \times [0\,..\,d) \to [0\,..\,d)$ and with these operators various algebraic structures can be formed, which we mention here without further elaboration or proofs.

7.24 Theorem. For all $d \in \mathbb{N}^+$:

(a) $([0\,..\,d), \oplus, 0)$ is a group.

(b) $([0\,..\,d), \otimes, 1)$ is a monoid but not a group.

(c) $([1\,..\,d), \otimes, 1)$ is a group if and only if d is prime.

Proof. Most monoid and group axioms are checked straightforwardly, where 0 is the identity of $\oplus$ and 1 is the identity of $\otimes$.

In (b) it is not a group since 0 has no inverse: there is no $x \in [0\,..\,d)$ such that $x \otimes 0 = 1$.

For (c) we also have to check that $\otimes$ is well-defined, that is, if $a, b \in [1\,..\,d)$ then $a \otimes b$ should be in $[1\,..\,d)$ too, that is, $a * b \bmod d \in [1\,..\,d)$. If d is not a prime, this is not the case since we can write $d = a * b$ for $a, b \in [1\,..\,d)$, by which $a * b \bmod d = 0 \notin [1\,..\,d)$. If d is prime then well-definedness holds since if $a, b \in [1\,..\,d)$ then $a * b \bmod d \neq 0$ due to Lemma 7.21. It remains to prove that every $a \in [1\,..\,d)$ has an inverse. Observe that $gcd(a, d) = 1$. By the extended Euclid's algorithm then there exist x, y such that $x * a + y * d = 1$. Hence $x * a \bmod d = 1$, so x is the inverse of a. □

7.6.2 An application: the nine and eleven tests

A technique that was commonly applied to verify manual calculations is the, so-called, *nine test*. This is based on the property that, in our decimal number representation, the remainder of a number when divided by 9 can be easily calculated: it equals the remainder of the sum of the number's digits modulo 9. As the sum of the digits of a number usually is much smaller than the number itself, the problem has been reduced. This process is repeated until a number is obtained that is less than 10: this last number, then, is the remainder of the original number modulo 9, except when it is 9 in which case the remainder is 0, of course.

For example, the sum of the digits of the number 123456789 equals 45, and the sum of the digits of 45 is 9. Hence, the remainder of 123456789 modulo 9 is 0.

Now to verify a calculation, for instance the addition or multiplication of two large numbers, one calculates the remainders modulo 9 of both numbers and of the result of the calculation, and one performs the same operation, modulo 9, to these remainders. If the results match we can be pretty confident that our calculation was correct, although we do not have certainty, of course. But, if the results do not match we certainly have made an error!

* * *

The property that the remainder modulo 9 of a number equals the remainder modulo 9 of the sum of the digits of that number's decimal representation is based on the observation that $10 \bmod 9 = 1$. Now we have that a number like, for instance, 1437 is equal to $143 * 10 + 7$. Therefore, we have:

$$
\begin{array}{ll}
 & 1437 \bmod 9 \\
= & \quad \{ \text{ above property } \} \\
 & (143 * 10 + 7) \bmod 9 \\
= & \quad \{ \ 10 = 9 + 1 \ \} \\
 & (143 * 9 + 143 * 1 + 7) \bmod 9 \\
= & \quad \{ \ \bmod \text{ over } +\text{; multiples of 9 may be discarded and } 7 \bmod 9 = 7 \ \} \\
 & (143 \bmod 9 + 7) \bmod 9 \quad .
\end{array}
$$

This calculation shows that $1437 \bmod 9$ is equal to $143 \bmod 9$ plus 7, modulo 9; if now, by Induction Hypothesis, $143 \bmod 9$ is equal to the sum, modulo 9, of the digits of 143 then $1437 \bmod 9$ also is equal to the sum of its digits, modulo 9.

* * *

In general, the decimal representation of natural numbers can be defined in a recursive way, as follows. A sequence of n decimal digits "$d_{n-1} \cdots d_2 d_1 d_0$" represents the natural number d_0 if $n = 1$: in this case the sequence just is a single digit, "d_0". If $n \geq 2$, the number represented by the sequence is equal to the number represented by the sequence of $n-1$ digits "$d_{n-1} \cdots d_2 d_1$" times 10 plus d_0.

By means of this recursive definition it can be proved, by Mathematical Induction, of course, that the number represented by a sequence of decimal digits and the sum of these digits are congruent modulo 9. By means of the recursive definition it also is possible to prove that the number represented by the sequence of digits "$d_{n-1} \cdots d_2 d_1 d_0$" is equal to:

$$(\Sigma i : 0 \leq i < n : d_i * 10^i) \quad ,$$

but in most cases the recursive definition is more manageable than this expression.

* * *

In a very similar, albeit slightly more complicated way we observe that 10 is congruent to -1 modulo 11, and that $100 \bmod 11$ is equal to 1. This is the basis of the *eleven test*: the remainder of a natural number modulo 11 is equal to the remainder modulo 11 of the sum of the digits of that number's decimal representation, but here the digits are added with *alternating signs*, starting at the least-significant digit with a positive sign. The number 123456789, for example, is congruent modulo 11 to: $+9-8+7-6+5-4+3-2+1$, which equals 5.

As was the case with the nine test, the eleven test can be used to "verify" the results of calculations.

7.7 Fermat's little theorem

We prove the following theorem which is known as "Fermat's little theorem".

7.25 Theorem. For every prime number p and for every $a \in \mathbb{N}^+$ we have:

$$\neg (p \mid a) \;\Rightarrow\; a^{p-1} \bmod p = 1 \quad .$$

Proof. Let p be a prime and let $a \in \mathbb{N}^+$. Assume $\neg (p \mid a)$; this is equivalent to $a \bmod p \neq 0$, so we have: $1 \leq a \bmod p < p$; that is, $a \bmod p \in [\,1 \,..\, p\,)$. For the sake of brevity, we define $b = a \bmod p$. Now we have that $a^{p-1} \bmod p$ is equal to b^{p-1}, where $b \in [\,1 \,..\, p\,)$ and b^{p-1} is to be interpreted in terms of $\otimes$-operations, instead of $*$. Hence, we also have $b^{p-1} \in [\,1 \,..\, p\,)$.

By Theorem 7.24, part (c), we have that $([\,1 \,..\, p\,), \otimes, 1)$ is a group, because p is prime. The set $\{\, b^i \mid 0 \leq i \,\}$ together with $\otimes$ and 1 is the subgroup of $([\,1 \,..\, p\,), \otimes, 1)$ generated by b. Because the whole group is finite, of size $p-1$, so is this subgroup. Therefore, a number $n \in \mathbb{N}^+$ exists such that $b^n = 1$ and $b^i \neq 1$, for all $i : 1 \leq i < n$. Then we have: $\{\, b^i \mid 0 \leq i \,\} = \{\, b^i \mid 0 \leq i < n \,\}$, and n is the size of this set.

On account of Lagrange's Theorem we conclude $n \mid (p-1)$. So, let $z \in \mathbb{N}$ satisfy $p-1 = z * n$. Now we derive:

$$\begin{array}{ll} & a^{p-1} \bmod p \\ = & \quad \{ \text{ as observed above } \} \\ & b^{p-1} \\ = & \quad \{ \text{ definition of } z \, \} \end{array}$$

$$
\begin{array}{ll}
 & b^{z*n} \\
= & \quad \{ \text{ property of exponentiation } \} \\
 & (b^n)^z \\
= & \quad \{ \text{ definition of } n \} \\
 & 1^z \\
= & \quad \{ \ 1 \text{ is the identity of } \otimes \ \} \\
 & 1
\end{array}
$$

□

7.8 Cryptography: the RSA algorithm

We conclude this chapter with a practical application of the theory, namely in the area of *cryptography*, which is the art of transmitting messages in a secure way, such that these messages cannot be read by anyone else than the intended receiver. For this purpose the messages are *encrypted* in such a way that they become unintelligible, except for the intended receiver who is the only one able to *decipher* the messages.

The algorithms for encryption and decryption themselves usually are not kept secret, but the parameters used in the process are. In cryptography such parameters usually are called *keys*.

Here we discuss the, so-called, RSA-algorithm, named after its inventors: Rivest, Shamir, and Adleman. This is an example of a so-called *public key* system. This means that the keys needed for encryption and decryption are chosen by the receiver of the messages, and the receiver makes the encryption key publicly known: everybody who wishes to send a message to this particular receiver now can use this public encryption key. The security of this arrangement is based on the assumption that it is (virtually) impossible to infer the (secret) decryption key from the (public) encryption key.

In older encryption schemes the encryption and decryption keys used to be chosen by the sender of the messages, and the sender now was faced with the problem how to communicate the decryption key to the intended receiver(s) in a secure way. In a public key system this difficulty is avoided.

The security of the RSA-algorithm rest on the assumption that it is very hard to factorize very large numbers into their prime factors. Here "very large numbers" means: numbers the decimal representation of which comprises several hundreds of digits.

* * *

The RSA-algorithm is based in two very large prime numbers p and q. Let $n = p * q$. Let a be any positive natural number not divisible by p or q. Then, by Fermat's little theorem, we have:

$$a^{p-1} \bmod p = 1 \ \wedge \ a^{q-1} \bmod q = 1 \ .$$

From this it follows that we also have, because 1^{p-1} and 1^{q-1} are equal to 1:

$$a^{(p-1)*(q-1)} \bmod p = 1 \ \wedge \ a^{(p-1)*(q-1)} \bmod q = 1 \ .$$

So $a^{(p-1)*(q-1)} - 1$ is divisible by both p and q, so also by $p * q$ since p and q are prime. So

$$a^{(p-1)*(q-1)} \bmod n = 1 \ . \tag{22}$$

For every $k \geq 0$ we have $1^k = 1$, so

$$a^{k*(p-1)*(q-1)+1} \bmod n = a.$$

Now encryption of a secret message works as follows. Choose an encryption number e with $gcd(e, (p-1)*(q-1)) = 1$. Represent the message by a number M, with $0 < M < n$, not divisible by p or q, for instance, the number of which the binary representation is the sequence of bits of the message. Now the encrypted message is $M^e \bmod n$. By the extended Euclid's algorithm find numbers d, k such that $d * e - k * (p-1) * (q-1) = 1$. Now we obtain

$$(M^e)^d \bmod n = M^{d*e} \bmod n = M^{k*(p-1)*(q-1)+1} \bmod n = M.$$

If some person A wants to receive a secret message from B then A chooses two large prime numbers p, q, computes $n = p * q$, chooses a corresponding value e and sends n, e to B in a non-safe way, by which also intruders may know n, e. Next B takes its secret message M, and computes $M' = M^e \bmod n$ (encryption), and sends M' to A in a non-safe way, by which also intruders may know M'. Now A can decrypt M' to M by computing d as presented above, and computing $M'^d \bmod n = M$. The crucial point is that knowledge of both p and q are required to do this computation, so intruders that may know n, e, M' have no clue how to construct the secret message M. Safety and feasibility of this approach depend on the following assumptions:

- if you know $n = p * q$, there is no feasible way to establish p and q,
- the extended Euclid's algorithm is feasible, even for n having thousands of digits,
- for numbers a, b, n of thousands of digits each, computation of $a^b \bmod n$ is feasible.

For computing $a^b \bmod n$ clearly a^b should not be computed since this number can never be stored: probably the number of digits of this number exceeds the number of atoms in the universe. Also not b times a multiplication with a should be executed, since b is far too large. But by carefully combining squaring and multiplying by a, and reducing all intermediate result modulo n, computing $a^b \bmod n$ is feasible.

Although there is no formal proof that when knowing n, e, M' it is not feasible to compute M, it has turned out to be safe in practice. The RSA algorithm was proposed by Rivest, Shamir and Adleman in 1977. In that time taking prime numbers of 100 digits was safe. However, both to increasing computational power and improved algorithms the approach is currently not safe any more for 100 digits, but for 1000 digits it is.

7.9 Exercises

1. Let $a, d \in \mathbb{Z}$ and $d \neq 0$. Assuming that a is divisible by d, prove that the value q satisfying $a = q * d$ is unique.

2. (a) What are the divisors of 1? Prove the correctness of your answer.
   (b) Prove $(\forall a, d : a \in \mathbb{Z} \wedge d \in \mathbb{N}^{+2} : d \,|\, a \Rightarrow \neg (d \,|\, (a+1)))$.
   (c) Prove $(\forall a, b, d : a, b \in \mathbb{Z} \wedge d \neq 0 : d \,|\, a \vee d \,|\, b \Rightarrow d \,|\, (a * b))$.
   (d) Give a simple counter-example illustrating that Lemma 7.21 does *not* hold if p is *not* prime, for every $p \in \mathbb{N}^{+2}$.

3. Prove the following properties of div and mod, using Definition 7.5; it is given that $d \in \mathbb{N}^{+}$ and that $a, b, x \in \mathbb{Z}$:

   (a) $0 \leq a < d \;\Leftrightarrow\; (a \,\mathsf{mod}\, d) = a$
   (b) $0 \leq a < d \;\Leftrightarrow\; (a \,\mathsf{div}\, d) = 0$
   (c) $0 \leq a \;\Leftrightarrow\; 0 \leq a \,\mathsf{div}\, d$
   (d) $(a+d) \,\mathsf{mod}\, d \;=\; a \,\mathsf{mod}\, d$
   (e) $(a+d) \,\mathsf{div}\, d \;=\; (a \,\mathsf{div}\, d) + 1$
   (f) $(a + x * d) \,\mathsf{mod}\, d \;=\; a \,\mathsf{mod}\, d$
   (g) $(a + x * d) \,\mathsf{div}\, d \;=\; (a \,\mathsf{div}\, d) + x$
   (h) $(a \,\mathsf{mod}\, d) \,\mathsf{mod}\, d \;=\; a \,\mathsf{mod}\, d$
   (i) $(a \,\mathsf{mod}\, d) \,\mathsf{div}\, d \;=\; 0$
   (j) $(a+b) \,\mathsf{mod}\, d \;=\; (a \,\mathsf{mod}\, d + b \,\mathsf{mod}\, d) \,\mathsf{mod}\, d$
   (k) $(a+b) \,\mathsf{div}\, d \;=\; (a \,\mathsf{div}\, d) \;+\; (b \,\mathsf{div}\, d) \;+\; (a \,\mathsf{mod}\, d + b \,\mathsf{mod}\, d) \,\mathsf{div}\, d$
   (l) Give (simple) counter examples illustrating that $(a+b) \,\mathsf{mod}\, d$ is not necessarily equal to $a \,\mathsf{mod}\, d + b \,\mathsf{mod}\, d$, and that $(a+b) \,\mathsf{div}\, d$ is not necessarily equal to $a \,\mathsf{div}\, d + b \,\mathsf{div}\, d$.
   (m) $(a * b) \,\mathsf{mod}\, d \;=\; ((a \,\mathsf{mod}\, d) * (b \,\mathsf{mod}\, d)) \,\mathsf{mod}\, d$
   (n) $a \,\mathsf{mod}\, d = 0 \;\Leftrightarrow\; d \,|\, a$
   (o) $a \,\mathsf{mod}\, d = 0 \;\Leftrightarrow\; a \,\mathsf{div}\, d \;=\; a / d$
   (p) $1 \leq a \;\Leftrightarrow\; a \,\mathsf{div}\, d < a$, provided that $2 \leq d$
   (q) $a \,\mathsf{mod}\, d \;=\; b \,\mathsf{mod}\, d \;\Leftrightarrow\; (a - b) \,\mathsf{mod}\, d \;=\; 0$
   (r) Determine $(-1) \,\mathsf{div}\, d$ en $(-1) \,\mathsf{mod}\, d$

4. Given are $c, d \in \mathbb{N}^{+}$. Prove that for all $a \in \mathbb{Z}$:
   $$(a * d) \,\mathsf{mod}\, (c * d) \;=\; (a \,\mathsf{mod}\, c) * d \;\text{ and:}$$
   $$(a * d) \,\mathsf{div}\, (c * d) \;=\; a \,\mathsf{div}\, c \;\;.$$

5. (a) Determine the *gcd* of the numbers 112 and 280.

(b) Determine numbers x and y satisfying: $x*112 + y*280 = gcd(112, 280)$.

6. Determine, by hand, all prime numbers between 100 and 200.
7. Prove that $x*(x+1)*(x+2)$ is divisible by 6, for all $x \in \mathbb{Z}$.
8. Prove that $(x^2-1) \bmod 8 \in \{0, 3, 7\}$, for all $x \in \mathbb{Z}$.
9. Resolve $8! - 3*7!$ into prime factors.
10. Determine the *lcm* of the numbers 1500000021 and 3000000045.
11. Find integers x, y such that $100 * x + 17 * y = 1$.
12. Find an integer x such that $0 < x < 144$ and $83 * x \bmod 144 = 1$.
13. Find integers x, y such that $111 * x + 27 * y = 5$.
14. We consider the number whose decimal representation consists of 38 digits 1. We call this number X.
    (a) Give a, formally correct, mathematical expression for X.
    (b) What is the remainder of the division of x by 9?
    (c) What is the remainder of the division of x by 11?
    (d) What is the remainder of the division of x by 99?
15. Determine all values $x \in \mathbb{Z}$ satisfying both: $x = 2 \pmod{11}$ and: $x = 3 \pmod{23}$.
16. Resolve $\binom{17}{5}$ into prime factors.
17. Determine the *gcd* and *lcm* of $\binom{17}{5}$ and $\binom{18}{4}$.
18. Prove that $(n+1)*(n+2)*\cdots*(n+k)$ is divisible by $k!$, for all $n, k \in \mathbb{N}$.
19. Prove that a natural number is divisible by 4 if and only if, in the representation of that number in base 17, the sum of the digits is divisible by 4.
20. We know that $37 * 43 = 1591$. Determine $e \in \mathbb{N}$ in such a way that, for all $m \in \mathbb{Z}$, we have: $m^{127*e} =_{1591} m$.
21. Represent the number 1000 in base m, for every $m \in \{2, 3, 4, 5, 6, 7, 8, 9, 10\}$.
22. What is the period of the recurring decimal fraction that represents $1/1001001$?
23. For a natural number $n > 10$ it is given that $2^n \bmod n = 5$. Prove that n is not a prime number.
24. Determine all prime numbers p with the property that $33 * p + 1$ is a square.
25. A given number requires 10 (ternary) digits for its ternary representation. How many digits are needed to represent this number in the decimal system?