Introduction

Most of us encounter *prime numbers* for the first time in secondary school: a number is *prime* if it has exactly two divisors, namely 1 and the number itself. We also learn that every natural number can be written as a product of its prime factors – for example $2013 = 3 \cdot 11 \cdot 61$ and the numbers 3, 11, and 61 are primes. However, it is rarely emphasized in classrooms that this is only the beginning of a long story, in which mathematicians working in the area of "number theory" have been discovering the secrets of prime numbers for thousands of years. Moreover, the story is far from over: many questions remain unsolved, with no solutions currently in sight. (A few open problems can be found in Appendix A.)

Also, many people are unaware that they use prime numbers almost every day. As recently as in the year 1940, the great English mathematician G. H. Hardy wrote in his book *A Mathematician's Apology* [**Har**] that number theory has no conceivable practical applications but that it deserves to be studied for its beauty alone. However, advances in information technology during the second half of the twentieth century led researchers to look for secure methods of electronic transmission of information. In the process, they proved Hardy wrong about the applicability of number theory (though not about its beauty). In 1977, the computer scientists Ronald Rivest, Adi Shamir, and Leonard Adleman developed a procedure, now known as

the **RSA algorithm**, that allows the secure transmission of a message to which no one but the sender and the receiver should have access. This is the foundation of all encryption methods commonly used today, e.g. for online credit card purchases or online banking.

We will study the RSA method more closely in Section 4.2. Its basic idea is the following surprising principle:

> It is (relatively) **easy** to decide whether or not a given number is prime. However, it is **hard** to find the prime divisors of a given composite (i.e. non-prime) number.

Considering our knowledge about prime numbers from school, this is a remarkable claim. For example, we can use an ancient method known as the *Sieve of Eratosthenes* (Section 1.5) to test whether a given number is prime. If it is not, this procedure will also provide us with a list of its prime divisors.

However, numbers routinely used in encryption algorithms today may have several hundreds or even thousands of digits. Anyone who has used the Sieve of Eratosthenes by hand, e.g. to find all prime numbers less than 200 (see Exercise 1.5.1), will find it easy to believe that this method cannot be carried out in practice for numbers of that size – even using the most advanced computer technology. To encourage research in this direction, *RSA Laboratories* (a leading security company) dared experts and puzzlers worldwide from 1991 to 2007 to break the RSA encryption scheme in the **Factoring Challenge**. They published a list of so-called **RSA numbers** (products of two different, extremely large primes), daring the public to find the two prime factors. In some cases, rather large amounts of money were offered for the solution. Although the challenge was officially closed in 2007, many factorizations still remain unknown!

So it is difficult to find prime factors. But why should detecting primality be a simpler problem, as claimed above? The key is to find properties of prime numbers that do not require excluding the presence of divisors and can therefore be checked much more efficiently.

Just such a property of prime numbers was already discovered in 1640 by the French lawyer and mathematician Pierre de Fermat. In

```
RSA-2048 = 25195908475657893494027183240048398571429282126204032027777137836043662020707595556264018525880784406918290641249515082189298559149176184502808489120072844992687392807287776735971418347270261896375014971824691165077613379859095700097330459748808428401797429100642458691817195118746121515172654632282216869987549182422433637259085141865462043576798423387184774447920739934236584823824281198163815010674810451660377306056201619676256133844147603833904414952634432190114657544454178424020924616515723350778707749817125772467962926386356373289912154831438167899885040445364023527381951378636564391212010397122822120720357
```

Until 2007, anyone who found the prime factors of the number "RSA-2048" would have received a prize of US$200,000. No factorization is known to the present day.

the 1970s, computer scientists Gary Miller and Michael Rabin refined this property to obtain a practical primality test. Their test is still used today when encrypting messages using the RSA method, demonstrating that mathematical theories developed without aspirations of real-life applications can turn out to have unexpected and extremely important practical consequences.

Curiously, the Miller-Rabin method of primality testing is **randomized**, meaning that it relies on a random choice of certain parameters. Hence there is a (small) chance that the procedure does not provide a correct answer after a reasonable amount of time. As one can ensure that the probability of error is negligible, this element of chance does not have real disadvantages in practice. However, from a theoretical perspective it is natural to ask whether randomization is really necessary: is there an efficient method for primality testing that is **deterministic**, i.e. does not require the use of random numbers?

This problem remained unsolved for decades, until the Indian computer scientists Agrawal, Kayal, and Saxena proposed an elegant solution in 2002. Due to its fundamental importance and the elementary nature of the methods employed, their result received great attention throughout mathematics. The article was immediately celebrated as a "Breakthrough for Everyone" [**Bo**] and appeared in 2004 in the *Annals of Mathematics*, one of the most prestigious mathematical journals [**AKS**].

The objective of this book is to give a complete presentation of the proof of the theorem of Agrawal, Kayal, and Saxena, without requiring any prior knowledge beyond general computational skills and the ability to think logically. As part of this presentation, we naturally develop the prerequisites from mathematics and computer science that are needed to understand the proof and to appreciate its importance. We hope that, at the same time, the reader will catch a glimpse of the beauty of mathematics and obtain an impression of how many interesting questions still remain open.

About this book. The book is aimed at interested high school pupils and teachers, but also at undergraduate students in mathematics and computer science (to whom it should be accessible from the first year). It can be used as the textbook for a summer school or a reading course.

It is not our intention to primarily give an introduction to the theory of numbers or algorithms. There are already many excellent such books – the reader will find some of them in the references at the end of the relevant chapters. On the other hand, our book is not a work of mathematical research; it is written neither by nor for experts. Research mathematicians and computer scientists might feel that the original article by Agrawal, Kayal, and Saxena or other sources (such as the book *Primality Testing in Polynomial Time* by Dietzfelbinger [**Dtz**] that is written for a more advanced audience) proceed at a more appropriate pace for them.

Instead, we shall focus on one main goal – the treatment of the algorithm of Agrawal, Kayal, and Saxena, henceforth referred to as the "AKS algorithm" – throughout the whole book. Thus we shall cover

precisely those concepts that are part of the required background for this result. At the same time, we gently introduce the reader to the world of mathematical proof. As far as we know, this approach to a complete treatment of a recent mathematical breakthrough separates our text from other books written for the same audience.

The first four chapters are designed mainly to introduce the reader to number theory and algorithm theory, as far as required for the AKS algorithm. We also give a brief historical and mathematical survey of cryptography (the science of encryption). In content and scope, we stay close to the material that was covered in our course at the Deutsche SchülerAkademie.

In the second part of the book, we essentially present the content of the AKS article [**AKS**], referring to the mathematics learned in the first part and developing further "ingredients" when necessary. We take care to both explain the underlying ideas and present the proof correctly and in detail. Readers with solid background knowledge can skip the first part of the book and give the AKS algorithm a try immediately, looking back when necessary.

Numerous exercises and comments are included at the end of each section to provide further background to the reader. The purpose of the exercises is not only to confirm that the new ideas from the section have been understood, but they are also meant as a general invitation to "learning by doing". From our experience, this is the best way to learn mathematics. Also, as a reader, one might appreciate certain ideas – particularly if they seem natural in hindsight – much more after several hours or even days spent thinking about a solution! We intentionally did not order the exercises according to difficulty. Those that require the use of an electronic computer or calculator are marked with "(P)" and those that will be used later in the book with "(!)". At the end of a section, there are usually further (and possibly more difficult) exercises and comments. These are meant to invite the reader to learn more about the corresponding subject but can be omitted at the first reading. Appendix A discusses open problems regarding prime numbers, while Appendix B contains solutions or hints to all exercises marked with "(!)". Complete solutions and our contact details will be provided at the website

`www.ams.org/bookpages/stml70`. We appreciate all comments, corrections of mistakes (including typographical errors), and, of course, all questions or suggestions for improvement.

Proofs. "Proofs" are a central concept in mathematics. They establish the truth of mathematical statements beyond all doubt. In a proof, we usually start with the given **hypothesis** and deduce the desired **conclusion** using a number of logical steps. Sometimes we change perspective and begin with the assumption that the conclusion does *not* hold, deriving a **contradiction** to our hypothesis or to known facts. In school, proofs often receive little attention and can seem mysterious or difficult to understand, so we shall take care to explain our arguments very carefully and in detail.

A proof can also be viewed as an **explanation**, helping the reader to understand why a claim is true. This is precisely what we aim to achieve in our book. Assuming no prior knowledge apart from elementary rules of calculation that are familiar from school, the reader will learn all necessary prerequisites to understand the work of Agrawal, Kayal, and Saxena. We attempt to point out the underlying ideas clearly and to explain the separate logical steps carefully. For this reason, we sometimes refrain from using the shortest or most elegant arguments, in the hope that our treatment can provide the reader with a deeper understanding of the material.

This book will not only familiarize the readers with the principles of mathematical proof but should also enable them to deduce simple results themselves. Thus, in later chapters, we sometimes relegate parts of the arguments to exercises and give generous hints.

Definitions, lemmas, and theorems. In mathematics, it is important that all terms be clearly defined before they are used, i.e. that their meanings be rigorously established. Such an introduction of mathematical notation or of a new concept is called a **definition**. Once a mathematical object or a mathematical property has been defined, we can investigate it and try to prove certain facts about it. We distinguish between more difficult or more significant results and those that may be of a more auxiliary nature (e.g. established on the way to the proof of a more important fact). The former are referred

to as **theorems** whereas the latter will be called **lemmas**. Which of these two categories a given fact is placed in may, however, depend on personal taste! Lemmas and theorems are both formulated in the same manner, beginning with a hypothesis and ending with a conclusion that is claimed to follow from the hypothesis. Therefore all lemmas and theorems require a proof. Results that follow in a simple manner from a previously proved fact are referred to as **corollaries**.

To make references easier to find, theorems, lemmas, definitions, exercises, etc., are labelled consecutively within each section.

If a statement takes the form "A implies B", then the **converse** of this statement is "B implies A". An implication and its converse usually have very different meanings; for example, "if 6 divides n, then 3 divides n" is always true, while its converse, "if 3 divides n, then 6 divides n", is false in general. When both the implication "A implies B" and its converse hold, we also say that A holds **if and only if** B does. For example, 6 divides n if and only if n is even and 3 divides n.

Mathematical notation. In school, we encounter the following collections of numbers:

- the **natural numbers** $\mathbb{N} = \{1, 2, 3, 4, \dots\}$;
- the **integers** $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$;
- the **even integers**, i.e. the set $\{\dots, -4, -2, 0, 2, 4, \dots\}$;
- the **odd integers**, i.e. the set $\{\dots, -3, -1, 1, 3, 5, \dots\}$;
- the **rational numbers** $\mathbb{Q} = \left\{ \frac{p}{q} : p, q \in \mathbb{Z}, q \neq 0 \right\}$;
- the **real numbers** $\mathbb{R}$ (i.e., the full number line).

If a and b are numbers from one of these sets, then $a \leq b$ and $a < b$ stand for "a is less than or equal to b" and "a is strictly less than b", respectively. The notation $a \geq b$ and $a > b$ is defined analogously.

We explicitly note that zero is *not* a natural number according to our definition. (There is no general agreement on this among mathematicians.) Hence we also define

$$(*) \qquad \mathbb{N}_0 := \{a \in \mathbb{Z} : a \geq 0\}.$$

Here the symbol := means "is defined as". It is used to introduce an abbreviation or a new notation (*not* to claim the equality of two previously defined quantities). So we can read (∗) as "$\mathbb{N}_0$ denotes the collection of all non-negative integers".

Collections as above are called **sets** in mathematics. That is, a set is a collection of distinct objects (its **elements**); two sets are equal if they have the same elements. The sets we encounter will almost exclusively consist of numbers, rather than more complicated objects. As the basic notation of set theory – as usually encountered in school – will be used routinely throughout the book, let us briefly review it here. If M is a set, then $x \in M$ means "x is an element of the set M". When y does *not* belong to M, we write $y \notin M$. A set N is called a **subset** of a set M if every element of N is also an element of M. In this case we write $N \subseteq M$. For example,

$$\mathbb{N} \subseteq \mathbb{N}_0 \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R}.$$

Note that, by definition, every set is a subset of itself. If $N \subseteq M$ and $N \neq M$, then N is called a **proper subset** of M, and we write $N \subsetneq M$. The symbol $\varnothing$ denotes the **empty set**: the (unique) set that has no elements. The number of elements of a set M is denoted by $\#M$; for example $\#\{2, 4, 6, 8, 10\} = 5$ and $\#\mathbb{N} = \infty$. (The symbol ∞ stands, as usual, for "infinity".) As already encountered in (∗),

$$\{x \in M : x \text{ has the property } \dots\}$$

denotes the set of all elements of M that have the stated property.

We use the standard notation from school for addition, subtraction, multiplication, and division, as well as for powers. Occasionally we omit the dot for multiplication, writing (for example) $3x$ instead of $3 \cdot x$. Elementary rules of calculation, such as the distributive law $a(b + c) = ab + ac$, are used routinely throughout.

If $x_1, \dots, x_n$ are real numbers, with $n \in \mathbb{N}$, then their sum and product are abbreviated as follows:

$$\sum_{i=1}^{n} x_i = x_1 + x_2 + \cdots + x_n; \quad \prod_{i=1}^{n} x_i = x_1 \cdot x_2 \cdots x_n.$$

For example, $\sum_{i=1}^{n} i = 1 + 2 + \cdots + n$ and $\sum_{i=1}^{n} \frac{1}{i} = \frac{1}{1} + \frac{1}{2} + \cdots + \frac{1}{n}$.

If n is any natural number, then $n!$ denotes the **factorial** of n, defined by

$$n! := \prod_{i=1}^{n} i \quad \Big(= 1 \cdot 2 \cdots (n-1) \cdot n \Big).$$

For example, $1! = 1$, $3! = 6$, and $5! = 120$. We also define $0! := 1$.

Recall the following rules for transforming powers: if a, b, x, y are real numbers with $a, b > 0$, then

$$a^x \cdot a^y = a^{x+y}, \quad (ab)^x = a^x \cdot b^x, \quad \text{and} \quad (a^x)^y = a^{x \cdot y}.$$

Instead of $a^{(x^y)}$ we write a^{x^y}. In general, this is *not* the same as $(a^x)^y$: for example we have $2^{3^2} = 512$, but $(2^3)^2 = 64$. By definition, raising any number to the power zero yields 1: $a^0 := 1$ for all $a \in \mathbb{R}$. We say that a natural number n is a **perfect power** of $a \in \mathbb{N}$ if there is some $b \in \mathbb{N}$ such that $b \geq 2$ and $n = a^b$. For example, 81 is a perfect power of 3, since $81 = 3^4$.

The **logarithm** to base 2 of a real number $x > 0$ is denoted by $\log x$, i.e. $\log x$ is the (unique) real number ℓ that satisfies $2^\ell = x$. For example, $\log 2 = 1$ and $\log 8 = 3$. Once in a while we also use the **natural logarithm** $\ln x$: this is the logarithm to base e, where e is Euler's constant. That is, $\ln x$ is the number $\ell \in \mathbb{R}$ for which $e^\ell = x$.

If N and M are sets, then "$f : N \to M$" is an abbreviation for "f is a function from N to M". This means that f associates to every element $x \in N$ an element of M, usually denoted by $f(x)$. For example, we can define a function f from $\mathbb{N}$ to $\mathbb{R}$ by setting $f(n) := \log n$ for all $n \in \mathbb{N}$.

If $x \in \mathbb{R}$, then $|x|$ denotes the **absolute value** of x. (So $|x| = x$ when $x \geq 0$ and $|x| = -x$ otherwise.) We also write $\lfloor x \rfloor$ to denote the largest integer n with the property that $n \leq x$. Similarly, we write $\lceil x \rceil$ for the smallest integer n satisfying $n \geq x$. (See Exercise 1.1.11.) For example, $\lfloor \frac{3}{2} \rfloor = 1$ and $\lceil \frac{3}{2} \rceil = 2$.

Mathematicians often use Greek letters to refer to certain quantities (for example, angles in elementary geometry). We will utilize the uppercase letter Π ("Pi") and the lowercase letters α ("alpha"), δ ("delta"), ε ("epsilon"), ζ ("zeta"), μ ("mu"), φ ("phi"), and, of course, π ("pi").

All other concepts and notations are introduced at the appropriate time (with many examples). They are also listed in the index and in the list of symbols at the end of the book.