### Definition: Coprime

and have no common factor.

The prime factorization of 6 is 6 = 2 · 3. The prime factorization of 9 is 9 = 3 · 3. the Example: Coprime

The prime factorization of 8 is 8 = 2 · 2 · 2. the prime factorization of 15 is 15 = 3 · 5. numbers 6 and 9 are therefore not coprime, because they have the 3 as a common prime factor.

the numbers 8 and 15 are therefore coprime, because they have no common prime factor.

The property that every natural number can be uniquely represented as the product of finitely many prime numbers makes prime numbers extremely important for mathematics. Prime numbers also play a decisive role in cryptography. In many crypto-procedures randomly selected prime numbers are needed. But how can you determine such a random prime number? In practice, a “random” odd number is often chosen first and then it is checked whether this number is a prime number. There are two problems here: For one thing, the chosen number is of course not really random, since you cannot reproduce real randomness with a computer. Rather, they are pseudo-random numbers calculated according to certain procedures. On the other hand, one faces the problem of having to decide whether the chosen number is actually a prime number or not. Finding an answer to this question is more difficult than it may at first appear. One could try to find possible

Eratosthenes

The ancient Greek scientist, poet, writer, and geographer Eratosthenes of Cyrene developed this procedure by which one might work out whether or not a number is prime.

divisors of this number by successive methodical trial and error. This may still work for smaller numbers but is no longer efficiently affordable for larger numbers. Since cryptography works in particular with very large prime numbers, one therefore needs other possibilities to efficiently decide whether a given number is a prime number. There are various test procedures for this purpose, known as primality tests; we will introduce two of these in the following section. However, we will largely dispense with proof here, as its complexity would go beyond the scope of this course.