### Theorem: Fundamental Theorem of Arithmetic

Every natural number the prime factorization of prime numbers p1, ..., px ∈ ℕn, i.e., in the form x. can be written in a unique way as a product of finitely manyx = p1 · . · pn. We call the product p1 · . · pn

Proof:

In this proof we have to show two things: firstly, the existence of the prime factorization and secondly its uniqueness.

Let us begin with the proof of existence:

We assign the empty product to 1. Furthermore, each prime number itself represents its factorization, there must therefore be prime factorizations of and This contradicts the assumption that =and p1zb = q1 · < b < z. · p1 · i · q. · q. Since 1 · j with prime numbers . · qz was chosen as the smallest natural number that has no primej the product of these prime numbers is a prime factorization of z does not have a prime factorization. Thus the exis-p1z, ..., pa, b ∈ ℕi, q1, ..., qj. Then, however, because aab = z and b, i.e., a = p11 < a < z · z = abz > 1. · pz.i own prime factorization. Thus, it remains to be shown that all remaining natural numbers have a prime factorization. Suppose there were natural numbers that could not be represented as products of prime numbers. Let be the smallest of these numbers. Since and is not a prime number, there are numbers with as well as

tence follows.

Now we prove the uniqueness:

Suppose there are natural numbers for which several factorizations of Let z again be the smallest of these numbers. Then z cannot contain a common prime factor z cannot be a prime number and thedifferentp, because otherwise prime factorizations exist.pz would also have different prime factorization, which contradicts the assumption that z is minimal. It can thus be concluded that different factorizations of z cannot have common facpLet pa and q, p ≠ qqb be differenta, b ∈ ℕp p|b prime factorizations of a ≠ b p q z, so z = pa = qbz b , with prime numbersq qb tors.

and , and with . is a divisor of and thus a divisor of . With the lemma of Euclid, is thus also a divisor of or a divisor of . Since is a prime number, only the possibility remains. It follows that the prime factorizations always have a common prime factor. But with this the prime factorizations cannot be different, as we have seen before. Thus, uniqueness follows.

#### STUDY GOALS

On completion of this unit, you will have learned...

how the Caesar cipher works.

what symmetric and asymmetric cryptosystems are.

the advantages and disadvantages of symmetrical and asymmetrical cryptosystems. – what the Eulerian φ function is.

what is meant by the Gaussian bracket.

how to calculate the modulo function. – how the RSA cryptosystem works.

Cipher

In cryptography, a cipher is an algorithm for performing encryption or decryption.