### . Conse-

quently, a is a divisor of r′ − r. This also makes a divisor of . However, this is a q′a + rcontradiction, as we have previously shown that r′ ≠ r q′ = q r′ = r □ |a| > r′ − r > 0. Consequently, theb = qa + r =

assumption is wrong and must apply. From this it follows that and therefore must apply. Let a = 5a = 42a = 14a = 15 and b = 17b = 1029b = 98b = 11, then 179811 = 3 · 5+ = 7 · 14 + 1029 = = 0 · 15 + 24 · 42 + 2, so 011q = 3q = 721q = 0 and q = 24r = 2r = 0r = 11. r = 21

#### Example: Division with remainder

Let and , then , so and .

Let and , then , so and .

Let and , then , so and .

We will encounter the division with remainder again later when we perform the Euclidean algorithm. First we want to define what we mean by the greatest common divisor of two numbers.

Definition: Greatest Common Divisor of a and (written as ), if the following holds: divisorThe largest positive intem|n ger that divides each of

Let 2. a, b ∈ ℤand n|a and b n|b for each with a ≠ 0gcd(a, b)m ∈ ℕ. A natural number with (gcdm|a) and m|bn ∈ ℕ is called the greatest common divisor Greatest commontwo or more integers is

1. called the greatest common divisor of those integers.

The greatest common divisor of two numbers a and b thus divides these two numbers on the one hand, and on the other hand it is itself divided by any integer number that also divides these two numbers. It should be noted that the greatest common divisor of two numbers is by definition always a natural number, i.e., in particular always positive. Let a := 1071 and b := 1029. Without using the Euclidean algorithm we could determinea a bbb|a 21|b

#### Example: Greatest Common Divisor

the greatest common divisor, for example, by comparing the divisor sets. To do this, we first determine those natural numbers that divide both and . These are 1, 3, 7 and 21, 3, and 7 cannot each be the greatest common divisors of a and 21 , because they are not and there are other numbers that divide either only or only . However, since we are looking for the greatest common divisor, these numbers are not relevant. The numbers 1, divided by 21. The greatest common divisor is thus 21, because and and 21 itself namely in this example 3 and 7, and their frequencies in the prime factorizations. TheAnother possibility to determine the greatest common divisor of 7prime factorization. It applies that · 7 = 3 · 73. We now look at the prime factors that occur in both decompositions,1071 = 3 · 3 · 7 · 17 = 32 · 7 · 17a and and b1029 = would be the 3 · 7 · is divided by 1, 3 and 7 respectively.

greatest common divisor is then calculated as the product of these factors, with the

factorization of 1029, the corresponding exponent for this factor is 1, and the same applies21to factor 7, which occurs only once in 1071. The greatest common divisor is thus . 31 · 71 = smaller of the two frequencies as exponent. Since factor 3 occurs only once in the prime

Although these procedures can in principle be used to determine the greatest common

for all integers ℤ is much more efficient. divisor of two numbers, both procedures are very time-consuming, especially for large numbers. With the Euclidean algorithm the determination of the greatest common divisor

Before we present this algorithm in detail, we will first briefly explain why it is correct to speak of “the” greatest divisor of two numbers.

Let a, b ∈ ℤ with a, b ≠ 0. Then the greatest common divisor of a and b is uniquely deterLemma: Uniqueness of the Greatest Common Divisor

mined.

Proof:

the generality we can assume that number. This is followed by Assuming that it would be Let nb1 andn2 be the greatest common divisors of nn ≠ nn = n|n applies (because n. Then either > n applies. However, according to the definition ofan and > nnb is the greatest common divisor of . We must show that then or n > n . Without limitation ofa n1 = nb 2.a

and the greatest common divisor, and is therefore shared by any other integer number that also divides 1 1 22 1 2 1 2 2 2 1 and ). But sor is proven. this is a contradiction, because a larger natural number cannot divide a smaller natural□ 1 2 and thus the uniqueness of the greatest common divi-

The greatest common divisor of two numbers is therefore unique. Therefore it is indeed correct to speak of “the” greatest common divisor (instead of “a”).

#### Theorem: Coprimality and the Greatest Common Divisor

Let a, b ∈ ℕ. Then a and b are coprime, if gcd(a, b) = 1.

gcd(a, b) = 1⇒ : Let b a and b be coprime. Then, according to the fundamental theorem of algebra, n ∈ ℕ n > 1 n|a n|b a Proof:

and can be written unambiguously as the product of prime numbers which have not a single factor in common. Accordingly, there is no , with and . Thus

.

=← : Be p gcd(a, b) = 1a m ∈ ℤ. Assume that b p m ≥ pa and b are not coprime. Then according to the funda-gcd(a, b) = mp p|a agcd(a, b) = 1p|b b pgcd(a, b)□

mental theorem of algebra there is a prime number with and . Thus is a common divisor of and . Either is the greatest common divisor of and , then

. Or there is an with and . In both cases this leads to a contradiction, because according to the precondition it applies that .

The following auxiliary theorem is used in the execution of the Euclidean algorithm and provides a rationale for why it actually works correctly. Let 0 ≤ r < |a| be the

#### Theorem: Auxiliary Theorem for the Euclidean Algorithm

and , i.e., is also the greatest com-

Proof:

∈ ℤquently Let x = gcd(a, r) with be a divisor of x|bz x = a y|raa and z x = rx□bbx y|ar = b − qay|b x a apply. So there are r y|x )x and conse-z1, zxaa2

Let yr gcd(a, b) = x , so and . Then it also follows with the same argumentacommon divisor for and

tion as above, that , because . Because is the greatest common divisor of

and and this is by definition shared by every other divisor of and , follows. Thus also fulfills the second condition from the definition of the greatest common divisor for

and b and .

Let a, b ∈ ℤ with a ≠ 0. Then the greatest common divisor of a and b can be uniquely Theorem: Euclidean Algorithm

gcd(a, 0) = |a|If rr1 ≠ = 0, then 0)b = gcd(r, we divide a|a| = gcd(a, 0). with remainder and get a r, 0) with remainder and get . with remainder and continue the procedure in this way until and with the preceding lemma and with the preceding lemma b = q a + ra = q with r0 + r ≤ rgcd(a, b) = gcd(a, rgcd(a, b) = gcd(a, r with ≤ |a|0 ≤ r < r 1)) == determined as follows:

We divide by 1 1 1 .

If 1 1 2 1 2 2 1.

1 1 1

the remainder is 0 at some point.2 r1 by r2

0form:This gives us a descending sequence of residual values procedure will terminate at some point. In this way we obtain a series of equations of the. Since there are only finitely many integers between |a||a| > r and 0, it is guaranteed that the1 > r2 > . > rn > rn+1 =

Example: Euclidean algorithmWith the preceding lemma rrnnr−−nr = gcd(rb=qa=q112===q⋮qqn+131n2ra+rrr21n++−nr, 0) = gcd(rn1rr132+, mit0 < r, mit0 < r, mit0 < rrn, mit0 < rn−1123<<<, rnarrn)21< = rn−. =gcd(a, r1 1) = gcd(a, b).

the greatest common divisor of the two numbers using the Euclidean algorithm.Let a := 1071 and b := 1029 as in the previous example. This time we want to calculate Another example, which also shows that the order of the numbers does not matter, so youThe greatest common divisor of 1071 and 1029 is therefore 1071=1·1029+421029=24·42+2142=2·21+0 gcd(1071, 1029) = 21. that you have to do an additional calculation step): Let can also divide the smaller of the two numbers by the larger one (which, however, meansthat: c = 64 and d = 310. It follows

With the Euclidean algorithm we can determine the greatest common divisor even if oneThe greatest common divisor of 64 and 310 is therefore 310=4·64+5464=0·310+6464=1·54+1054=5·10+410=2·4+24=2·2+0 gcd(64, 310) = 2. or both numbers are negative. For example, if −2002=210=2·98+1498=7·14+0−10·210+98e := −2002 and f := 210. Then it is:

Thus gcd(−2002, 210) = 14.

In cases where negative numbers are involved, please remember that the remainder must , but the remainder would have been and thus a negative number.

210 + (−112)always be a non-negative number! We could have represented −112 −2002 as −2002 = −9 ·

This calculation method would not have led to a correct result. bers do not have a common prime divisor. For example, for and

The greatest common divisor of two numbers can also be gcd(78, 35) = 1 78=2·35+835=4·8+38=2·3+23=1·2+12=2·1+0 1g := 78. This is the case if both num-h := 35

so .