## 8.2 Fundamental Theorem of Arithmetic

The following lemma is from the French mathematician Étienne Bézout (1730—1783). The Lemma

statement of the lemma is extremely important. We will need it for the proof of Euclid’s A lemma is a minor proposition (sometimes referlemma, which we in turn need for the proof of the fundamental theorem of arithmetic. red to as a helping or auxFurthermore, we will later apply the lemma constructively in cryptography. You should iliary theorem) which therefore please work through and internalize the following proof and examples. The serves as a stepping stone

to the establishment of a proof after that, on the other hand, can be passed over at first without any disadvantages greater proposition or

and can be revisited later if necessary. theory. Lemmas can also have standalone signifi-

Theorem: Bézout’s Identity cance.

Let a, b ∈ ℤ with a ≠ 0. Then there are numbers s, t ∈ ℤ with gcd(a, b) = sa + tb.

Proof:

The assertion is derived from the Euclidean algorithm. For this purpose we convert the rr1==ba −q1a rr

equations according to the remainders and obtain:

inserting qInduction step: We now show that the statement is also correct for all following remain-tBase case: for By applying induction, one can now show that there are numbers ti1b := −qq for all 2a = (1 + q1. ≤ i ≤ nr . s1s := −qi, ti ∈ ℤ := 1 + qa) = a − q1 and with tr1 := 1i = s1q22 andib +a +. By

2 2

The validity of the assertion then follows with The proof of the lemma of Bézout thus gives us the constructive answer to how we canapplies to sinsert case the statement is valid for ders. For this purpose, i−1a + tri andi−1rb − qi+1ri−1 with in the equation of i+1ssi+1ia − q := s1 < i < ni−1i+1 − qtrib = (siand . We consider i+1ri+1rsi−1i and i−1 and get and it is − qti+1i+1 := ts := ssrrrii+1 = s = (s = rn ia + ti−1t := t − qa + tib. and i+1n □riib) − qr. According to the base)i−1b. Thus the statement = si+1i−1(a + tsia + ti−1bib) =. We

compute the numbers also called Bézout then apply them successively as in the proof. The final result is role for the RSA algorithm. We would like to illustrate the procedure once again with a fewcoefficients.s and t: we convert the equations according to the remainders and The calculation of these numbers will play an importants and t. These numbers are

examples.

Example: Bézout’s identity1. seen above that that Let the following equations above when performing the Euclidean algorithm:a := 107121 = s · 1071 + t · and gcd(1071, 1029) = 21b := 10291029 as in the example for the Euclidean algorithm. We have. We proceed as in the previous proof. We have formed. Now we want to calculate numbers s and t so

We convert these equations according to the remainders (of course we don’t have to1071=1·1029+421029=24·42+2142=2·21+0 would only give We insert the first equation into the second and get:consider the last equation, because there the remainder is 0 and the conversion0 = 0) and get42=107121=1029: −−102924·42 21=1029=1029=25·1029+−−24·24·11071−071+24·124 −·10711029029

2. dean algorithm we have seen that The sought numbers are therefore We consider the numbers and rearrange them according to the remainders. We get:= s · 64 + t · 310. For this we again consider the equations we have set up above:c := 6464=0·310+6464=1·54+1054=5·10+410=2·4+24=2·2+0gcd(64, 310) = 2s := −24 and d := 310 and t := 25. In the above example of the Eucli-. We now determine . s and t with 2

310=4·64+54

We now successively insert the third equation into the fourth, the second into the54=31010=644=542=10−−−−1·545·102·44·64

OftenThe sought numbers are therefore third and the first into the second equation. This way we get:2=10 Bézout’s identity is combined with the Euclidean algorithm and then the greatest=64=64=5·64=64−−−−2·4 = 101·1·1·310+4·64−−−−51·3101·3101·3101·3103104−−13−2·−−−−−4·64·310542·2·2·122·−·−6·31031031054310+58·64−5·2·−2·−−63105·1044·644·64−−31029·64−s := 631·544·64−−−45·25· and 64−·64+5·3105·645·−t := −135·64−−1·310641·3−. 1·10+4·64310−4·64 =5·64=5·64=5·64=63·64+

common divisor is calculated first, followed by the numbers to as the extended Euclidean algorithm. s and t. This is often referred

The following lemma also comes from the works of Euclid and is found in Book IIX, Proposition 30 of Euclid’s “The Elements” (2003).