### Theorem: Euclid’s Lemma

Let a, b ∈ ℤp|a p|b and let p ∈ ℕ be a prime number. If p is a divisor of ab, i.e., if p|ab applies,

then or also applies.

Proof:

Let (spb + tabps, t ∈ ℤ be a divider of gcd(p, a) = pp gcd(p, a) = sp + ta = 1ab. Since pp is a prime number, either p|spbb a p|a gcd(p, a) = pp gcd(p, a) = 1 or gcd(p, a) = 1p|tabp|b

applies. If , then is a divisor of and applies. If , we can

show that is in this case a divisor of . According to the Bézout’s identity there are num-

bers with . We multiply both sides of the equation by

and get spb + tab = b. Obviously holds and according to the precondition

). Since pp|b thus divides the □ left side of the equation, also divides the right side also holds. With the lemma about divisors of sums and differences it also applies that of the equation and follows.