### Primality Test: Fermat Test

Let site number.p ∈ ℕ, p > 10 < x < p be the number that you want to test for primeness. We randomly selectp d 1 < d ≤ x < p p

an .

If has a divisor with . Consequently, is a compo-

If If If xgcd(x, p) = 1 mod p ≠ 1mod p = 1x p , we consider , , pp is a composite number. is a prime number or xp−1 mod p. p is a Carmichael number or p p is a compositex p−1 number. If xp−1 is composite and is not a Carmichael number, the probability of choosing such an was at most one out of two.

a) p is a composite number. The Fermat test can obviously give two different results depending on and : b) p is a prime number, a Carmichael number or a composite number.p

If the test produces output a, is composite with absolute certainty and not a prime numIf, on the other hand, the test produces output b, we have no certainty at first: p can then ber.

be a prime number, a Carmichael number or a composite (and not a Carmichael number). The probability of the latter is at most one out of two.

could simply run the test several times in a row − each time with a k different x, of course. Ifp If there were no Carmichael number, we would have found a very good primality test: We

the test result is b. every time, we can theoretically minimize the probability that is actually a composite number. Performing the test times reduces the probability to at most 12 · 12 ·⋯· 12 = 21k

Unfortunately, Alford, Granville and Pommerance (1994) showed that there are infinite Carmichael numbers. A closer examination of these figures may lead to an optimization of the Fermat test, but this would go beyond the scope of this course. We therefore leave it at

and then checking for case b. Whether the considered number p occurs in this list, one the above description of the Fermat test and instead mention a simpler, but also more limited solution: By creating a list of all Carmichael numbers up to a certain upper limit

obtains an efficient and practical test. The list of Carmichael numbers remains manageably small, even for large numbers.

#### STUDY GOALS

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

how and why division with remainder works.

what is meant by the greatest common divisor of two numbers.

how to calculate this divisor using the Euclidean algorithm.

how the extended Euclidean algorithm works.

why every natural number can be written uniquely as the product of prime numbers.