Theoretical Computer Science – Exercise 13

SS 2022
Jochen Schmidt

Technische Hochschule Rosenheim

Please prepare the following exercise at home prior to the tutorial:

Exercise 1

Using the formula $x_{n+1} = (a\ x_n + c) \bmod m$ we can generate pseudo random integers in the range [0; m – 1].

Let: a = 3, c = 9, m = 16

a) Calculate the first three random numbers x_1, x_2, and x_3 starting with the initial value $x_0 = 1$.

b) Does this choice of parameters guarantee the maximum possible period length (which is…?)?

c) Transform x_1, x_2, and x_3 to the integer interval [–6; +1].

d) Transform x_1, x_2, and x_3 to the real number interval [–6; +1].

We will do the following exercise together during the tutorial:

Exercise 2

Use the Fermat test to check if the following numbers are prime:

a) 5; use the numbers 2, 3, and 4 for the test. Can you use more numbers to check whether 5 is prime?

b) 15; use the numbers 2, 3, and 4 for the test. Do you have to use all these numbers to check whether 5 is prime?

What is the result? Is it guaranteed to be correct?

Now perform the prime check using the Miller-Rabin test.