Übung 2

Look at the following sequence:

16, 3, 26, 2, 23, 24, 27, 5, …

Assume the numbers were generated with

s{i+1} = A · s + B mod m, m=31

Find A and B

Calculate the next 3 (pseudo)random numbers

$s_1 = 16$
$s_2 = 3$
$s_3 = 26$
$s_4 = 2$
$s_5 = 23$
$s_6 = 24$
$s_7 = 27$
$s_8 = 5$

$s_{\{i+1\}} = A \cdot s + B$

$s_2 = A \cdot s_1 + B$
$s_3 = A \cdot s_2 + B \Rightarrow B = s_3 - A \cdot s_2$

$s_2 = A \cdot s_1 + B$
$s_2 = A \cdot s_1 + s_3 - A \cdot s_2$
$s_2 - s_3 = A(s_1 - s_2)$
$\boxed{A = \frac{s_2 - s_3}{s_1 - s_2}}$

$A = \frac{s_2 - s_3}{s_1 - s_2} \mod 31$
$A = \frac{3 - 26}{16 - 3} \mod 31$
$A = \frac{-23}{13} \mod 31$
$A = \frac{8}{13} \mod 31$
$A \cdot 13 = 8 \mod 31$
$\frac{A \cdot 13}{31} = 8 \mod 31$
$A \cdot \frac{13}{31} = \mod 31$
$\frac{3 \cdot 13}{31} = 8 \mod 31$
$\Downarrow$
$A = 13$

$s_2 = A \cdot s_1 + B \mod 31$
$3 = 3 \cdot 16 + B \mod 31$
$3 = 48 + B \mod 31$
$B = 3 - 48 \mod 31$
$B = -45 \mod 31$
$B = 14 \mod 31$
$B = 17$

nächste Zahlen

$s_9 = A \cdot s_8 + B \mod 31$
$s_9 = 3 \cdot 5 + 17 \mod 31$
$s_9 = 15 + 17 \mod 31$
$s_9 = 32 \mod 31$
$s_9 = 1$

$s_{10} = A \cdot s_9 + B \mod 31$
$s_{10} = 3 \cdot 1 + 17 \mod 31$
$s_{10} = 3 + 17 \mod 31$
$s_{10} = 20 \mod 31$
$s_{10} = 20$

$s_{11} = A \cdot s_{10} + B \mod 31$
$s_{11} = 3 \cdot 20 + 17 \mod 31$
$s_{11} = 60 + 17 \mod 31$
$s_{11} = 77 \mod 31$
$s_{11} = 15$