



Übung 2

Abgabe bis Mittwoch, 14.5.

Aufgabe 2: [Lineare Kongruenzgeneratoren]

Wir betrachten den linearen Kongruenzgenerator

$$x_{n+1} = (ax_n + b) \pmod{m}$$

zur Erzeugung von gleichverteilten, ganzzahligen Pseudo-Zufallszahlen in $\{0, \dots, m-1\}$.

(a) Überprüfen sie, ob der Generator für die Wahlen von

- $a = 3432, b = 6789, m = 9973$
- $a = 1229, b = 1, m = 2048$
- $a = 1711, b = 0, m = 30269$

maximale Periode besitzt.

(b) Zeigen sie für den Fall $a = 7, b = 6, m = 64$, dass es Startwerte x_0 gibt, zu denen Zyklen der Periodenlänge 1, 2 und 8 gehören.

(c) Zeigen sie für $n, k \in \mathbb{N}_0$:

- $x_n = \left(a^n x_0 + \frac{a^n - 1}{a - 1} b \right) \pmod{m}$
- $x_{n+k} = \left(a^k x_n + \frac{a^k - 1}{a - 1} b \right) \pmod{m}$

(d) Sei $a = 1229, b = 0, m = 2048$ und setze $u_n = x_n/m$. Ermitteln sie (ohne Verwendung des Programms aus Aufgabe (e)), auf wie vielen Geraden in $[0, 1]^2$ die Punkte (u_n, u_{n+1}) liegen.

(e) Schreiben sie ein Computerprogramm in einer Programmiersprache ihrer Wahl zur Erzeugung von jeweils 1000 Pseudozufallszahlen mit dem Generatoren aus Aufgabe (a) und (d) und plotten sie jeweils die Punkte (u_n, u_{n+1}) .