Lineare Kongruenzmethode

Author: Philipp G. Freimann (BBW (Berufsbildungsschule Winterthur) https://www.bbw.ch)

Zum Testen von Software, insbesondere zur Testdatenerzeugung, zur Simulation von Ereignissen, zur Entscheidungsfindung und nicht zuletzt für die Verschlüsselung werden zuverlässige Zufallszahlen benötigt. Jedoch widerspricht sich das Konzept "Algorithmus" mit dem Konzept "Zufall".

In der Praxis hat sich dennoch ein Algorithmus zum Erstellen von sog. Pseudozufallszahlen durchgesetzt: Die **lineare Kongruenzmethode**.

Dazu werden drei Zahlen (a, b und m) fest vorgegeben. Eine Startzahl x_0 wird als sog. *seed* eingetragen. Nun werden "Zufallszahlen" x_1, x_2, x_3, ... nach dem folgenden Algorithmus berechnet:

$x_{i+1} := (a * x_i + b)$ MODULO m

Schreiben Sie ein Programm, das vom Anwender a, b, m und x_0 erfragt und danach x_1 bis x_m auf der Konsole ausgibt.

Diskutieren Sie die folgenden Fälle:
$a = m$
$m = 1$
ggT(a, b, m) > 1