# Zufallsgeneratoren - eine visuell orientierte Analyse

## Allgemeines

Die Rekursionsgleichung $\mathbf{x_{n+1} = a \cdot x_n + b \text{ modulo } M}$ erzeugt Pseudozufallszahlen. Man erhält „zirkuläre zyklische Folgen“ bestimmter Länge. Die Qualität eines solchen Generators hängt entscheident von der Wahl der Parameter a, b und M ab. Ein von IBM programmierter Generator benutzte beispielsweise $M = 2^{29}$ und a = 65539.

Ein solcher Generator erzeugt natürlich **bestenfalls eine zyklische Folge der Länge M**.
Für M = 7, a = 2 und b = 0 erhält man mit dem Startwert 3 z. B. die Folge 3 - 6 - 5 - 3 ...
Für M = 7, a = 3 und b = 0 erhält man mit dem Startwert 3 die Folge 3 - 2 - 6 - 4 - 5 -1

Man sollte **M also groß wählen**. Falls b=0 gewählt wird, erhält man als Spezialfall einen einfachen Generator. Wenn dieser möglichst lange Zyklen erzeugen soll, muß **ggT(a, M) = 1** gelten. Falls M prim ist, ist das für alle 0 < a < M der Fall. Diese Bedingung ist allerdings nicht hinreichend um eine Zyklenläge von M-1 zu erzeugen, denn nicht jeder Rest der multiplikativen Restgruppe hat die Ordnung M-1 (allerdings ist die Ordnung der so erzeugten Untergruppen ein Teiler der Gruppengröße, im obigen Beispiel erzeugen die Potenzen von a = 3 alle Reste.

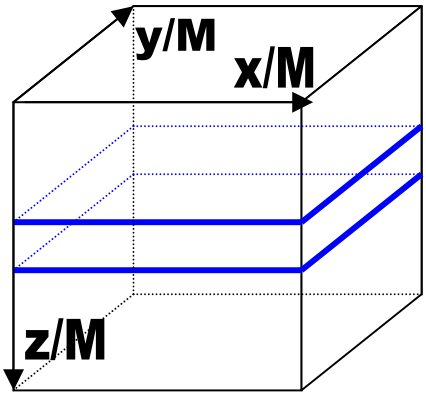
**Man wird sich also einen Rest mit maximaler Ordnung** suchen. Einen Rest, dessen Potenzen alle zum Modul teilerfremden Reste durchlaufen nennt man auch Primitivwurzel (die multiplikative Gruppe ist zyklisch). Wenn es verschiedene Reste maximaler Ordnung gibt, erzeugen diese allerdings nicht automatisch gleichgute Zufallszahlen. Es **spricht auch einiges dafür, die größte auf dem Rechner darstellbare Zahl** (Integer-Format) als Modul zu wählen. **Je nach der Wahl der Parameter erhält man Pseudozufallszahlen unterschiedlicher „statistischer Qualität“** (gleichmäßige Verteilung der einzelnen Zahlen, der Tupel, Tripel usw., gute Werte in Abweichungstests, im Pokertest etc. pp. Die Optimierung dieser Generatoren ist ein Feld für „experimentelle numerische Mathematik“. Mit zahlentheoretischen Methoden allein kann „der beste Generator in einem vorgegebenen Größenbereich nicht bestimmt werden!

## Zu diesem Programm

Mit diesem Programm kann experimentiert werden. Man untersucht selbstdefinierte Generatoren oder den System-Zufallsgenerator. Die besondere Stärke zum Aufspüren „verborgener Muster“ liegt dabei in der Visualisierung. Dazu wird die erzeugte Zufallsfolge als Koordinatenfolge im Raum gedeutet:

x1, x2, x3, x4, x5,... → (x1, x2, x3), (x2, x3, x4), (x3, x4, x5), ...

Dividiert man alle Koordinaten durch M, so erhält man Punkte in einem Einheitswürfel. Das Programm zeigt nun für beliebige Teilquader mit zu den Würfelflächen parallelen Flächen die Projektionen dieser Punkte auf das Einheitsquadrat in der x-y-Ebene.




z.B. können die Häufigkeiten mit statistischen Methoden analysiert werden. Die „heuristische Stärke“ der Visualisierung liegt jedoch in der Möglichkeit, auch **subtile Muster durch einen eher ganzheitlich gestaltorientierten Ansatz aufzudecken**.