

# Schüler-SimuLab

# Kurs 2

**Kursreihe stochastische Simulationen**

**Eine Alternative zum Linearen-Kongruenz-Generator:**

**Der Inverse Kongruenz-Generator**

Stefan Hartmann

Forschungszentrum caesar

## Der Lineare Kongruenz-Generator:

### 1. Schritt: Wähle

- einen **Modul**  $m$  mit  $m > 0$ ,
- einen **Multiplikator**  $a$  mit  $0 \leq a < m$ ,
- eine **Verschiebung**  $c$  mit  $0 \leq c < m$ ,
- einen **Startwert**  $X_0$  mit  $0 \leq X_0 < m$ .

### 2. Schritt: Berechne für $i \geq 0$ :

$$X_{i+1} = \text{Rest}_m(a \cdot X_i + c).$$

### 3. Schritt: Breche ab, sobald eine Periode eintritt.

## Der Inverse Kongruenz-Generator:

### 1. Schritt: Wähle

- einen **(Primzahl)-Modul**  $p$  mit  $p > 0$ , wobei  $p$  eine Primzahl ist,
- einen **Multiplikator**  $a$  mit  $0 \leq a < p$ ,
- eine **Verschiebung**  $c$  mit  $0 \leq c < p$ ,
- einen **Startwert**  $X_0$  mit  $0 \leq X_0 < p$ .

### 2. Schritt: Berechne für $i \geq 0$ :

$$X_{i+1} = \text{Rest}_p (a \cdot X_i^{-1} + c).$$

### 3. Schritt: Breche ab, sobald eine Periode eintritt.

Soviel ändert sich also (scheinbar) nicht!

Doch die Auswirkungen sind enorm,  
wie wir noch sehen werden!

Frage: Was ist  $X_i^{-1}$ ?

Antwort: später!

**Definition 1 (kongruent modulo  $m$ )** *Es sei  $m > 0$  beliebig vorgegeben. Dann nennen wir zwei ganze Zahlen  $a$  und  $b$  **kongruent modulo  $m$** , wenn sie bei der Division durch  $m$  den gleichen Rest lassen.*

*Hier die Schreibweise für „ $a$  ist kongruent zu  $b$  modulo  $m$ “:*

$$a \equiv b \pmod{m}.$$

**Satz 2** *Es gilt genau dann  $a \equiv b \pmod{m}$ , wenn  $m$  ein Teiler von  $a - b$  ist.*

Wie rechnet man nun mit Kongruenzen?

## Beispiele:

Zum Beispiel gilt:

$$8 + 5 = 13 \equiv 2 \pmod{11}$$

und

$$8 + 3 + 12 \equiv 11 + 1 \equiv 1 \pmod{11}.$$

Klar?

Die Gleichung

$$8 + x \equiv 0 \pmod{11}$$

hat die Lösung:  $x \equiv 3 \pmod{11}$ , d.h. es gilt:

$$-8 \equiv 3 \pmod{11}.$$

Allgemeiner gilt:

**Satz 3** *Es seien  $m \in \mathbb{N}$  und  $a \in \mathbb{Z}$  beliebig gewählt. Dann ist die Gleichung*

$$a + x \equiv 0 \pmod{m}$$

*immer lösbar.*

Es gibt zu jedem  $a \in \mathbb{Z}$  ein **Inverses bezüglich der Addition**  $-a$  mit

$$a + (-a) \equiv 0 \pmod{m}.$$

Hierbei ist 0 das sogenannte **neutrale Element bezüglich der Addition**, d.h. für alle  $b \in \mathbb{Z}$  gilt:

$$b + 0 \equiv b \pmod{m}.$$

Das **neutrale Element bezüglich der Multiplikation** ist 1, d.h. für alle  $b \in \mathbb{Z}$  gilt:

$$b \cdot 1 \equiv b \pmod{m}.$$

Die Frage ist jetzt: Gibt es auch zu jedem  $a \in \mathbb{Z}$ ,  $a \neq k \cdot m$  ( $k \in \mathbb{Z}$ ), ein **Inverses bezüglich der Multiplikation**, also ein  $a^{-1} \in \mathbb{Z}$ , für das

$$a \cdot a^{-1} \equiv 1 \pmod{m}$$

gilt?

Es stellt sich also die folgende Frage:

**Es seien  $m \in \mathbb{N}$  und  $a \in \mathbb{Z}$ ,  $a \not\equiv 0 \pmod{m}$ , beliebig gewählt. Ist dann die Gleichung**

$$a \cdot x \equiv 1 \pmod{m}$$

**immer lösbar?**

Testet das doch einfach mal:

**Gruppenaufgabe:**

Ist die Gleichung

$$3 \cdot x \equiv 1 \pmod{15}$$

lösbar?

Man kann zeigen, dass die Gleichung

$$a \cdot x \equiv 1 \pmod{m}$$

genau dann lösbar ist, wenn  $m$  und  $a$  teilerfremd sind.

**Satz 4** *Es sei  $p$  eine Primzahl. Dann ist für alle  $a \in \mathbb{Z}$  mit  $0 < a < p$  die Gleichung*

$$a \cdot x \equiv 1 \pmod{p}$$

*immer lösbar.*

## Bezeichnung 5 ( $a^{-1} \pmod{p}$ )

Es sei  $a \in \mathbb{Z}$  vorgegeben. Man schreibt für  $x \in \mathbb{Z}$ :

$$x \equiv a^{-1} \pmod{p},$$

wenn

$$a \cdot x \equiv 1 \pmod{p}$$

gilt. Im Falle  $a \equiv 0 \pmod{p}$  existiert kein solches  $x \in \mathbb{Z}$ . In diesem Fall setzen wir vereinbarungsgemäß:  $a^{-1} := 0$ .

## Gruppenaufgabe

- (a) Überlege dir, dass  $a^{-1} \pmod{p}$  in  $\mathbb{Z}$  (außer im Fall  $a = 0$  nach Vereinbarung) nicht eindeutig bestimmt ist, wenn es existiert. Nenne mindestens zwei Zahlen  $x \in \mathbb{Z}$ , für die

$$x \cdot 5 \equiv 1 \pmod{11}$$

gilt.

- (b) Nehmen wir einmal an, wir haben ein  $x \in \mathbb{Z}$  mit der Eigenschaft  $a \cdot x \equiv 1 \pmod{p}$  gefunden. Wie bekommen wir dann alle anderen?
- (c) Durch welche zusätzliche Forderung können wir erreichen, dass  $a^{-1} \pmod{p}$  eindeutig bestimmt ist?

Man setzt:

$$a : b \stackrel{\text{def}}{=} \frac{a}{b} \stackrel{\text{def}}{=} a \cdot b^{-1}.$$

Es ist klar, dass dieser Ausdruck nur für  $b \neq k \cdot p$  ( $k \in \mathbb{Z}$ ) sinnvoll ist, also nur für  $b \not\equiv 0 \pmod{p}$ .

Dies entspricht unserer gewohnten Regel, dass man „nicht durch 0 teilen darf“.

⇒ *Arbeitsblatt 1*

**Beispiel:**

Wir berechnen  $4 : 5 \pmod{7}$ .

## Aufgabe 1:

Berechne:

$$5 : 6 \pmod{11},$$

$$5 : 2 \pmod{7},$$

$$\frac{6}{3} \pmod{13},$$

$$\frac{2}{3} \pmod{13}.$$

Die Frage, die sich jetzt natürlich aufdrängt, ist die folgende:

**Wie berechnet man allgemein  $a^{-1} \pmod{p}$ ?**

Für kleine Primzahlen  $p$  kann man  $a^{-1} \pmod{p}$  erraten (siehe oben).

Für große Primzahlen ist das nicht mehr so einfach. Da müsste man alle Zahlen bis  $p$  durchprobieren und das könnte unter Umständen ziemlich lange dauern.

## Bezeichnung 6 ( $ggT(a, b)$ )

Der **größte gemeinsame Teiler** zweier ganzer Zahlen  $a$  und  $b$  (wobei nicht beide Zahlen gleich 0 sind) ist die größte natürliche Zahl, die  $a$  und  $b$  ohne Rest teilt. Man verwendet dafür die Bezeichnung  $ggT(a, b)$ .

Aus technischen Gründen setzen wir zudem  $ggT(0, 0) := 0$ .

Wir nennen  $a$  und  $b$  **relativ prim**, wenn  $ggT(a, b) = 1$  gilt.

Beispiele:

$$ggT(12, 18) =$$

$$ggT(-4, 14) =$$

$$ggT(5, 0) =$$

**Satz 7** *Es gilt für zwei ganze Zahlen  $a$  und  $b$  die folgende Beziehung:*

$$\text{ggT}(a, b) = \text{ggT}(b, a - b),$$

*d.h. man kann  $\text{ggT}(a, b)$  sukzessive ausrechnen, indem man wiederholt von der größeren der beiden Zahlen die kleinere abzieht und dann jeweils den größten gemeinsamen Teiler von der kleineren der beiden Zahlen und der Differenz der beiden Zahlen bildet.*

Beispiel:

Es gilt:

$$\begin{aligned} ggT(48, 30) &= ggT(30, 18) \\ &= ggT(18, 12) \\ &= ggT(12, 6) \\ &= ggT(6, 6) \\ &= 6. \end{aligned}$$

## „Speed-Version“ mit dem Euklidischen Algorithmus:

Haben wir eine Division mit Rest durchgeführt:

$$a = bq + r,$$

so gilt nach dem obigen Satz:

$$\text{ggT}(a, b) = \text{ggT}(b, a-b) = \text{ggT}(b, a-2b) = \dots = \text{ggT}(b, a-qb) = \text{ggT}(b, r).$$



### Gruppenaufgabe:

Überlege dir, dass der Euklidische Algorithmus in jedem Fall irgendwann abbricht, egal wie man  $b_0$  und  $a_0 \neq 0$  auch immer wählt. Tipp: Betrachte mal die Folge  $(r_n)_{n \in \mathbb{N}_0}$  der Reste. Was kannst du über diese Folge aussagen?

## Beispiel:

Wir möchten mit Hilfe des Euklidischen Algorithmus  $ggT(84, 315)$  bestimmen.

Führen wir den Euklidischen Algorithmus für  $b_0 = 315$  und  $a_0 = 84$  durch, so erhalten wir das folgende Schema:

$$315 = 3 \cdot 84 + 63$$

$$84 = 1 \cdot 63 + 21$$

$$63 = 3 \cdot 21 + 0.$$

Wie wir uns gerade in der Aufgabe überlegt haben, gilt also:

$$ggT(315, 84) = 21.$$

## Aufgabe 2:

Berechne mit Hilfe des Euklidischen Algorithmus den größten gemeinsamen Teiler von

(a) 308 und 70 ,

(b) 396 und 210 .

**Satz 8** Der größte gemeinsame Teiler  $ggT(a, b)$  von zwei ganzen Zahlen  $a$  und  $b$  kann als Linearkombination von  $a$  und  $b$  mit ganzzahligen Koeffizienten dargestellt werden, d.h. es gibt  $c, d \in \mathbb{Z}$  mit

$$ggT(a, b) = ca + db.$$

Insbesondere gilt: Wenn  $a$  und  $b$  relativ prim sind, dann hat die Gleichung

$$1 = xa + yb$$

eine ganzzahlige Lösung  $(x, y)$ .

Man beachte, dass die  $c, d \in \mathbb{Z}$  mit

$$\text{ggT}(a, b) = ca + db$$

nicht eindeutig bestimmt sind. Erfüllt das Paar  $(c, d)$  diese Gleichung, so auch alle Paare  $(c', d')$  mit

$$c' = c + kb \quad \text{und} \quad d' = d - ka$$

mit einem beliebigen  $k \in \mathbb{Z}$ .

Die Frage ist jetzt natürlich:

Wie berechne ich  $c$  und  $d$ ?

Antwort: später!

Wir wollen uns erst vom Nutzen überzeugen!

⇒ *am Smart-Notebook vorrechnen*

Wie kommt man auf die ganzzahlige Linearkombination?

Ziel:

Finde  $c \in \mathbb{Z}$  und  $d \in \mathbb{Z}$  mit

$$c \cdot b + d \cdot a = \text{ggT}(a, b).$$

⇒ *am Smart-Notebook vorrechnen*

⇒ *Arbeitsblatt 3*

**Beispiel:** Wir möchten  $ggT(3370, 315)$  bestimmen und  $ggT(3370, 315)$  als ganzzahlige Linearkombination von 3370 und 315 darstellen.

$$\begin{aligned} 3370 &= 10 \cdot 315 + 220 & , & & 0 \leq 220 < 315 & , \\ 315 &= 1 \cdot 220 + 95 & , & & 0 \leq 95 < 220 & , \\ 220 &= 2 \cdot 95 + 30 & , & & 0 \leq 30 < 95 & , \\ 95 &= 3 \cdot 30 + 5 & , & & 0 \leq 5 < 30 & , \\ 30 &= 6 \cdot 5 & . & & & \end{aligned}$$

Zur Kontrolle der gerade am Smartboard vorgeführten Rechnung:

$$\begin{aligned}5 &= 95 - 3 \cdot 30 \\ &= 95 - 3 \cdot (220 - 2 \cdot 95) \\ &= 7 \cdot 95 - 3 \cdot 220 \\ &= 7 \cdot (315 - 1 \cdot 220) - 3 \cdot 220 \\ &= (-10) \cdot 220 + 7 \cdot 315 \\ &= (-10) \cdot (3370 - 10 \cdot 315) + 7 \cdot 315 \\ &= 107 \cdot 315 - 10 \cdot 3370.\end{aligned}$$

### Aufgabe 3:

Bestimme mit der soeben dargestellten Methode den größten gemeinsamen Teiler  $ggT(32174, 6418)$  und stelle  $ggT(32174, 6418)$  als ganzzahlige Linearkombination von 32174 und 6418 dar!

Zur Erinnerung:

Da  $X_i$  und  $p$  teilerfremd sind, gibt es ganze Zahlen  $c$  und  $d$  mit

$$1 = \text{ggT}(X_i, p) = c \cdot X_i + d \cdot p.$$

Rechnet man modulo  $p$ , so erhält man:

$$1 \equiv c \cdot X_i \pmod{p},$$

und es gilt in der Tat:

$$c \equiv X_i^{-1} \pmod{p}.$$

### Gruppenaufgabe:

Es sei ein Primzahlmodul  $p = 647$  gewählt.

Berechne  $20^{-1} \pmod{647}$ .

# Die Eigenschaften des Inversen Kongruenz-Generators

**I.** Frage nach der Verbesserung der bisherigen Nachteile:

**II.** Frage nach dem Erhalt der bisherigen Vorteile:

⇒ *Arbeitsblatt 4*

**Satz 9 (Eichenauer/Lehn, 1986)** *Es seien  $a, c$  und  $p$  die Parameter des Inversen Kongruenz-Generators. Dann gilt für die Periodenlänge  $\lambda$  (beginnend bei  $X_0 = 0$ ) folgendes:*

- (i) Wenn es eine ganze Zahl  $q$  mit  $q^2 \equiv 4a + c^2 \not\equiv 0 \pmod{p}$  gibt, dann ist die um eins vermehrte Periodenlänge  $\lambda + 1$  ein Teiler von  $p - 1$ .*
- (ii) Wenn  $4a + c^2 \equiv 0 \pmod{p}$  gilt, dann ist die Periodenlänge  $\lambda$  gleich  $p - 1$ .*
- (iii) Wenn es keine ganze Zahl  $q$  mit  $q^2 \equiv 4a + c^2 \pmod{p}$  gibt, dann ist die um eins vermehrte Periodenlänge  $\lambda + 1$  ein Teiler von  $p + 1$ .*

#### Aufgabe 4:

Prüfe nach, dass der Inverse Kongruenz-Generator mit  $a = 1$ ,  $c = 2$  und  $p = 11$  der obigen Bedingung (iii) von Satz 3.1 genügt und maximale Periodenlänge hat, indem du für  $X_0 = 0$  die Folgenglieder  $X_1, \dots, X_{10}$  berechnest und verifizierst, dass sie alle Zahlen zwischen 1 und 10 annehmen.

⇒ *Arbeitsblatt 5*

**Satz 10 (Eichenauer-Herrmann, 1991)** *Gegeben sei ein Inverser Kongruenz-Generator mit maximaler Periodenlänge. Für ein beliebiges  $k \geq 2$  betrachten wir  $k$  aufeinanderfolgende Zufallszahlen dieses Generators und fassen diese als Punkte im  $\mathbb{R}^k$  auf. Dann enthält keine Hyperebene im  $\mathbb{R}^k$  mehr als  $k$  Punkte.*

Sprich: In der zweidimensionalen Darstellung enthält keine Gerade mehr als zwei Punkte, in der dreidimensionalen Darstellung enthält keine Ebene mehr als drei Punkte, etc.

Toll! Das ist ein Verhalten, was man sich von Pseudo-Zufallszahlen wünscht!

### Aufgabe 5:

Erzeuge mit dem bereits programmierten Inversen Kongruenz-Generator 2500 Zufallszahlen mit den Parametern  $a = 66$ ,  $p = 2027$  und  $c = 1$ . Lasse dir die Zufallszahlen als Paare in der Ebene darstellen, wie wir das beim Linearen Kongruenz-Generator gemacht haben. Was fällt dir auf? Bestätigen sich die obigen Ergebnisse auch optisch?