

# Schüler-SimuLab

# Kurs 1

**Kursreihe stochastische Simulationen**

**Die Erzeugung von Pseudo-Zufallszahlen:**

**Der Lineare Kongruenz-Generator und Statistische Tests**

Stefan Hartmann

Forschungszentrum caesar

**Ein Computer ist eine deterministische Maschine: Mit ihm lassen sich nur deterministische Prozesse durchführen.**

Ein Prozess heißt **deterministisch**, wenn zu jedem Zeitpunkt während des Prozesses bestimmt ist, wie der weitergeht.

*Any one who considers arithmetical methods of producing random digits is, of course, in a state of sin.*

Zitat von John von Neumann (1951).

**Wann nennen wir eine  
Zahlenfolge „zufällig“?**

*Eine Folge von lauter Nullen und Einsen heißt zufällig, wenn sie sich nicht durch eine kürzere Folge beschreiben lässt.*

Zur Erläuterung: Die Folge 010101... ist in diesem Sinne nicht zufällig.



A. N. Kolmogorov



G.J. Chaitin

- (1) Wie kann man (pseudo-)zufällige Zahlenfolgen erzeugen?
  
- (2) Was kann man mit solchen (pseudo-)zufälligen Zahlenfolgen anfangen?
  
- (3) Wie kann man erkennen, wie „gut“ solche (pseudo-)zufälligen Zahlenfolgen sind?

**Die Schwächen sind nicht immer  
sofort zu erkennen!**

→ *Arbeitsblatt 1*

## Aufgabe 1:

Zufallszahlen zur Simulation eines Würfelexperimentes:

### 1. Beispiel:

1	3	4	2	5	6	6	3	2	1	4	4	5	3	2	1	1	4	3	6
3	2	2	4	5	3	3	1	1	4	1	5	3	2	1	6	6	5	4	3
2	4	1	1	2	4	3	6	6	1	4	5	5	2	3	4	1	1	2	6
4	3	3	2	1	6	6	5	4	1	3	2	2	4	3	2	1	4	6	3
3	2	1	4	6	3	3	2	1	4	6	3	3	2	1	4	6	3	3	2
1	4	6	3	3	2	1	4	6	3	3	2	1	4	6	3	3	2	1	4

## 2. Beispiel:

1	1	2	3	2	4	1	2	5	2	6	3	4	6	3	4	2	4	3	4
6	5	6	3	2	5	6	1	5	1	3	1	4	1	4	6	5	6	6	2
3	4	6	2	4	2	1	5	3	5	4	6	4	5	6	5	3	3	5	6
4	2	6	1	6	1	2	4	3	4	2	5	4	5	3	5	2	3	4	2
3	6	3	1	3	2	4	3	5	3	6	2	2	1	5	1	5	6	3	6
4	5	1	3	1	6	1	3	2	1	6	1	3	4	5	4	5	3	2	5

	1	2	3	4	5	6
1	1	3	5	2	4	3
2	3	1	4	5	4	2
3	3	5	1	7	4	3
4	2	5	3	0	5	5
5	3	2	5	3	0	6
6	5	3	5	3	3	1

## Auf der Suche nach Zufallszahlen

- Der französische Naturforscher G. Buffon (1707-1788) warf eine Münze 4040 mal und erreichte dabei 2048 mal „Kopf“ und 1992 mal „Zahl“.
- Der englische Biologe W. F. R. Weldon zeichnete 26 306 Würfe mit 12 Würfeln auf.
- Der Schweizer Naturwissenschaftler R. Wolf führte 100 000 Würfe mit einem einzigen Würfel durch.
- Der Statistiker K. Pearson analysierte den Ausgang zahlreicher Roulette-spiele und notierte sich die Zahlen.

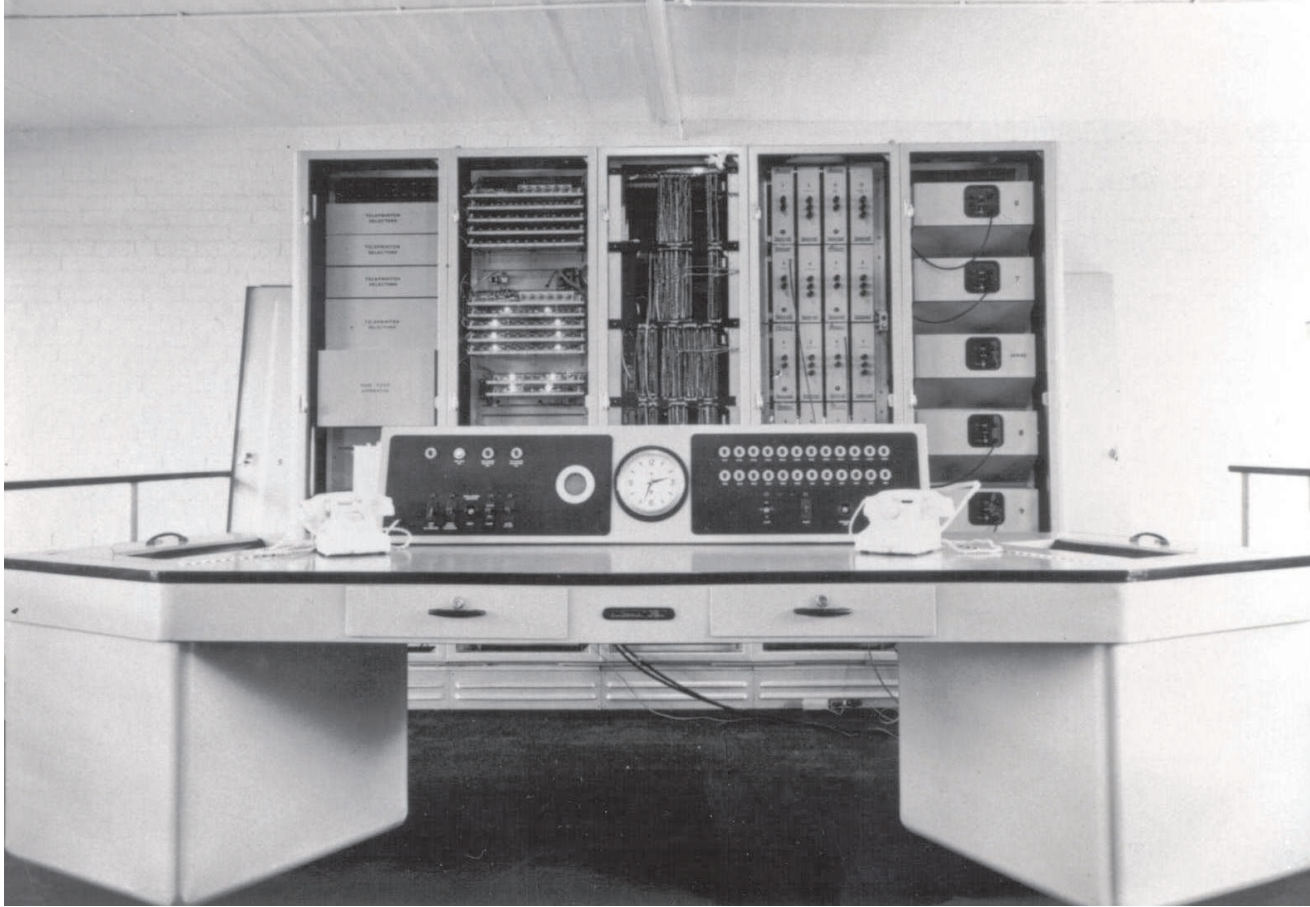
Bei **echten Zufallszahlengeneratoren** handelt es sich um **mechanische oder elektrische Geräte**, die echte zufällige Zahlenfolgen liefern.

Erster kommerziell hergestellter Computer: Ferranti Mark I

echte Zufallszahlen durch einen Rauschgenerator!

Im Jahre 1955 druckte die RAND Cooperation ein Buch mit 1.000.000 Zufallszahlen ab, die durch elektrisches Rauschen erzeugt wurden.

Zeile Nr.	Spalte Nr.									
	1-5	6-10	11-15	16-20	21-25	26-30	31-35	36-40	41-45	46-50
0	10097	12553	76510	15586	54675	14876	80959	09117	59292	74943
1	37542	04803	64894	74296	24805	24057	20636	10402	00822	91665
2	08422	68953	19645	09503	25209	02160	15953	34764	35080	55606
3	99019	02529	09576	70615	38511	51165	88676	74597	04436	27659
4	12807	99970	80157	36147	64032	36613	98951	16877	22171	76853
5	66065	74717	34072	76850	36697	56170	61815	39885	11199	29170
6	31060	10805	45571	82406	55505	42614	86799	07459	25405	09752
7	81269	77602	02051	65692	68665	74818	75055	85247	18625	88579
8	65575	32155	05525	47048	90555	57548	28468	28709	85495	25624
9	75796	41755	05129	64778	35808	34282	60955	20544	55275	88455
10	98520	17767	14905	68607	22109	40558	60970	95455	50500	75998
11	11805	05451	59808	27752	50725	68248	29205	24201	54775	67851
12	85452	99654	06288	98085	15746	70078	18475	40610	68711	77817
13	88685	40200	86507	18401	36766	67951	90564	76495	29609	11062
14	99594	67548	87517	64969	91826	08928	95785	65568	25478	54155
15	65481	17674	17468	50950	58047	76974	75059	57186	40218	16544
16	80124	55655	17727	08015	45518	22574	22115	78255	14585	55765
17	74550	99817	77402	77214	45236	00210	45521	64257	96286	02655
18	69916	26805	66252	29148	56956	87205	76621	15990	94400	56458
19	09893	20505	14225	68514	46427	56788	96297	78822	54582	24598
20	91499	14525	68479	27686	46162	85554	94750	89925	57089	20048
21	80356	94598	26940	56858	70297	54555	55540	55540	42050	82521
22	44104	81949	85557	47954	52979	26575	57600	40881	22222	06455
23	12550	75742	11100	02040	12860	74697	96644	89459	28707	25855
24	65606	49529	16505	34484	40219	52565	45651	77082	07207	51790
25	61196	90446	26457	47774	51924	55729	65594	59595	42582	60527
26	15474	45266	95270	79955	59567	85848	82596	10518	33211	59466
27	94557	28575	67897	54587	54622	44451	91590	42592	92927	45975
28	42481	16215	97544	08721	16868	48767	05071	12059	25701	46670
29	25525	78557	75208	89857	68955	91416	26252	29665	05522	82562
30	04495	52494	75246	55824	45862	51025	61962	79555	65557	12472
31	00540	97654	64051	88559	96159	65896	54692	82591	25287	29529
32	55965	15507	26898	09554	55555	55462	77974	50024	90105	59555
33	59808	08591	45427	26842	83609	49700	15021	24892	78565	20106
34	46058	85236	05590	92286	77281	44077	95950	85647	70617	42941
35	52179	00597	87579	25241	05567	07007	86745	17557	85594	11858
36	69254	61406	20117	45204	55956	60000	18745	92225	97118	96558
37	19565	41430	05758	75579	40419	25585	66674	56806	84962	25207
38	45555	14958	19476	07246	45667	94545	59047	90055	20826	69541
39	94864	55994	56168	10851	54888	85555	05540	55456	05014	55576
40	98086	24826	45240	28404	44999	08896	59094	75407	55441	55880
41	55185	16252	45941	50949	89455	48581	88695	45994	57548	75045
42	80951	00406	96582	70774	20551	25587	25016	25298	24624	65571
43	79752	49540	75961	28296	69861	02591	74852	20559	00587	59579
44	18655	52557	98145	06571	51050	24674	05455	65427	77958	95956
45	74029	45902	75557	52270	97790	17559	52527	58021	80814	55748
46	54578	45651	80995	57145	05555	12969	56527	19255	56040	90524
47	11664	49885	52079	84827	59581	75559	09975	55440	88462	25556
48	48524	77928	55249	64710	02295	56870	52507	57546	15020	09994
49	69074	94558	87657	95976	55584	04401	10518	21655	01848	76958



ERNIE

Was sind die

Vorteile

und was sind die

Nachteile

von „echten“ Zufallszahlengeneratoren im Vergleich zu algorithmischen Zufallszahlengeneratoren?

## Die Vorteile von „echten“ Zufallszahlengeneratoren:

- man bekommt „gute“ Zufallszahlen, mit denen man sehr realistisch simulieren kann
- Perioden oder ähnliches treten nicht auf

## Die Nachteile:

- zeitaufwändige Erstellung der Tafeln
- Beschränkung des Vorrats an Zufallszahlen
- keine Reproduzierbarkeit der Zufallszahlen
- Verschleißerscheinungen der eingesetzten Geräte

→ *Arbeitsblatt 2*

Der älteste algorithmische Zufallszahlengenerator ist der von John von Neumann etwa 1946 vorgeschlagene

## „Mitten-Quadrat-Generator“:

Beispiel:

$$x_0 = 1234 \quad x_0^2 = 01 \underbrace{5227}_{=x_1} 56$$

$$x_1 = 5227 \quad x_1^2 = 27 \underbrace{3215}_{=x_2} 29$$

$$x_2 = 3215 \quad x_2^2 = 10 \underbrace{3362}_{=x_3} 25$$

USW.

## Aufgabe 2:

Beginne mal mit dem Startwert  $x_0 = 5283$  und führe den Algorithmus ein paar Mal durch. Was fällt dir auf? Wie ist dieser Zufallszahlengenerator auf Grund dieses Ergebnisses zu bewerten?

Für eine reelle Zahl  $r$  bezeichnen wir mit  $\text{INT}(r)$  den ganzzahligen Anteil dieser Zahl, d.h. wir „schneiden die Zahl hinter dem Komma ab“.

Beispiele:

$$\text{INT}(3,14159) = 3,$$

$$\text{INT}(0,356) = 0,$$

$$\text{INT}(-36,98) = -36.$$

In excel: `GANZZAHL()`

Nun können wir den Algorithmus angeben:

(1) Wähle vierstelligen Startwert  $x(0)$ .

(2) Setze für  $i = 1, \dots, N$ :

$$x(i) := \text{INT}((x(i-1))^2/100)$$

$$x(i) := x(i) - \text{INT}(x(i)/10000) \cdot 10000$$

$$i := i + 1$$

Und nun programmieren wir ihn!

Wir haben gesehen: Dieser Algorithmus hat **eklatante Schwächen!**

Vielleicht sind wir ja **nicht chaotisch genug** vorgegangen?

Was kann mal also tun? Mehr Chaos veranstalten?

**Je mehr Chaos, desto bessere Zufallszahlen?**

→ *Algorithmus K (der „superzufällige“ Zufallszahlengenerator)*

**Merke: Zufallszahlen sollten niemals mit einer zufälligen Methode erzeugt werden!**

## Division mit Rest

Es sei  $m$  eine beliebig gewählte natürliche Zahl mit  $m > 0$ . Für eine natürliche Zahl  $a$  bezeichnen wir im Folgenden mit

$$\text{Rest}_m(a) = r$$

den Rest, der auftritt, wenn wir  $a$  durch  $m$  mit Rest teilen:

$$a = q \cdot m + r \quad \text{mit} \quad 0 \leq r < m.$$

Beispiele:

•  $a = 20, m = 7:$        $20 = 2 \cdot 7 + 6$        $\Rightarrow$        $\text{Rest}_7(20) = 6,$

•  $a = 3, m = 10:$        $3 = 0 \cdot 10 + 3$        $\Rightarrow$        $\text{Rest}_{10}(3) = 3,$

•  $a = 45, m = 9:$        $45 = 5 \cdot 9 + 0$        $\Rightarrow$        $\text{Rest}_9(45) = 0.$

## Gruppenaufgabe:

Finde für die folgenden Paare die Division mit Rest und gib  $\text{Rest}_m(a)$  an:

(a)  $a = 30, m = 6,$

(b)  $a = 77, m = 8,$

(c)  $a = 0, m = 1000,$

(d)  $a = 100, m = 99.$

## Der Lineare Kongruenz-Generator

wurde 1949 von dem amerikanischen Mathematiker D. H. Lehmer (1905-1991) eingeführt

Der Lineare Kongruenz-Generator ist häufig immer noch ein Bestandteil vieler Zufallszahlengeneratoren.

**Aber: Wir werden später sehen, wo die Schwächen liegen.**

## 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 $i \geq 0$ :

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

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

### Gruppenaufgabe:

Führe den Algorithmus durch für  $m = 10$ ,  $X_0 = 1$ ,  $a = 7$  und  $c = 7$ .

Was fällt dir auf?

„Pech“ gehabt?

Gibt es vielleicht **Regeln** für ein gutes Ergebnis?

Was ist überhaupt ein **gutes Ergebnis**?

### Gruppenaufgabe:

Nehmen wir mal an, wir haben  $m$ ,  $X_0$ ,  $a$  und  $c$  irgendwie gewählt.

Nach wie vielen Schritten tritt allerspätestens wieder eine Wiederholung auf? Was ist also die größtmögliche Periodenlänge?

→ *Arbeitsblatt 3*

Jetzt wissen wir also, was wir bestenfalls erwarten dürfen. Wie aber können wir das erreichen?

*Die durch einen Linearen Kongruenz-Generator erzeugte Zahlenfolge hat genau dann die größtmögliche Periodenlänge, also  $m$ , wenn die folgenden Bedingungen erfüllt sind:*

*(a)  $c$  und  $m$  sind teilerfremd.*

*(b)  $a - 1$  ist durch jede Primzahl teilbar, durch die  $m$  teilbar ist.*

*(c) Wenn  $m$  durch 4 teilbar ist, dann ist auch  $a - 1$  durch 4 teilbar.*

### Aufgabe 3:

Wir betrachten den Linearen Kongruenz-Generator mit  $a = 5$ ,  $m = 8$  und  $c = 1$ . Sind dann die obigen Bedingungen erfüllt? Führe den Algorithmus jetzt mal für ein beliebiges  $X_0$  mit  $0 \leq X_0 < m$  durch und schaue, ob du wirklich eine Periode der maximalen Länge  $m = 8$  erhältst.

→ *Arbeitsblatt 4*

## Aufgabe 4:

Versuche mal mit dem Linearen Kongruenz-Generator in Excel Zufallszahlen zu erzeugen. Mache dir erst einmal klar, was du alles brauchst:

- Felder, wo man  $m$ ,  $a$ ,  $c$  und  $X_0$  eintragen kann
- die Formel  $X_1 = \text{Rest}_m(a \cdot X_0 + c)$
- ganz viele Kopien dieser Formel, nur mit  $X_i$  anstatt  $X_0$  und  $X_{i+1}$  anstatt  $X_1$ .

Jetzt erzeugst du mit deinem Zufallsgenerator 20000 Zufallszahlen mit den Parametern  $a = 313$ ,  $m = 16384$ ,  $c = 3271$  und  $X_0 = 0$ .

## Transformation von Zufallszahlen

Wie kann man aus einer beliebigen Folge natürlicher Zufallszahlen eine Folge reeller Zufallszahlen konstruieren kann, deren Werte zwischen 0 und 1 liegen?

Führe das in deinem Excel-Programm kurz durch!

**Ziel: Wir wollen 100 zufällige Wochentage erzeugen!**

Hierbei gilt:

0	↔	„Sonntag“
1	↔	„Montag“
⋮	⋮	⋯
6	↔	„Samstag“

→ *Excel-Programm (auch: Einerziffern)*

$$X_0, X_1, X_2, \dots, X_{m-1} \in \{0, 1, 2, \dots, m-1\}$$

$$\frac{X_0}{m}, \frac{X_1}{m}, \frac{X_2}{m}, \dots, \frac{X_{m-1}}{m} \in [0, 1)$$

1, 2, 3, 4, 5, 6

→ *Arbeitsblatt 5*

## Simulation eines Würfelexperimentes:

### Aufgabe 5:

Simuliere nun mit dem gerade erlernten Verfahren tausend zufällige Würfe mit einem Würfel. Verwende dazu die entsprechende Spalte des Excel-Arbeitsblattes „Linearer Kongruenz-Generator“. Lass den Computer zählen, wie oft eine „1“, „2“, „3“ usw. vorkam. Verwende dabei den Befehl ZÄHLENWENN (siehe Excel-Hilfe). Versuche das Ergebnis zu interpretieren: Von wievielen Versuchen hast du wie oft eine bestimmte Zahl „gewürfelt“? Bilde die Verhältnisse, also die relativen Häufigkeiten. Überlege nun: Wie groß sind die (theoretischen) Wahrscheinlichkeiten? Vergleiche die Werte. Mache das Gleiche mit zehntausend zufälligen Würfeln. Vergleiche die beiden Ergebnisse und plote alle Werte in geeigneten Balkendiagrammen.

→ *Arbeitsblatt 6*

## Visualisierungen

Die Linearen Kongruenz-Generatoren haben einen systematischen „Fehler“! Welchen?

Wir betrachten eine Folge von Zufallszahlen:

$$X_0, X_1, X_2 \dots, X_i \dots, X_{m-1}$$

Interpretation als Punkte der Ebene:

$$\begin{aligned} P_0 &= (X_0, X_1), \\ P_1 &= (X_1, X_2), \\ P_2 &= (X_2, X_3), \\ &\vdots \quad \vdots \quad \vdots \\ P_{m-2} &= (X_{m-2}, X_{m-1}). \end{aligned}$$

Im Idealfall, also bei echten Zufallszahlen, würden wir folgendes erwarten:

## Aufgabe 6:

Experimentiere selber mal ein bisschen mit den graphischen Darstellungen. Lasse dir für verschiedene Lineare Kongruenz-Generatoren mal die zweidimensionale Visualisierung im Excel-Programm anzeigen. Was stellst du fest? Siehst du irgendwelche Muster? Versuche es zunächst mal mit

$$a = 1229 \quad , \quad m = 2048 \quad , \quad c = 1 \quad \text{und} \quad X_0 = 0.$$

Was beobachtest du?

Wir bilden nun Punkte im Raum aus drei aufeinander folgenden Zufallszahlen:

$$\begin{aligned} P_0 &= (X_0, X_1, X_2), \\ P_1 &= (X_1, X_2, X_3), \\ P_2 &= (X_2, X_3, X_4), \\ &\vdots \quad \vdots \quad \quad \quad \vdots \\ P_{m-3} &= (X_{m-3}, X_{m-2}, X_{m-1}), \end{aligned}$$

Welche Musterbildung erwartet ihr jetzt?

→ *Matlab*

**Kann man diese Eindrücke, die man von den Graphiken her bekommt, auch mathematisch in den Griff bekommen?**

**Wie kann man testen, ob eine zufällige Zahlenfolge „gut“ ist?**

# Der $\chi^2$ -Test

am Beispiel der Augensumme  $s$  zweier Würfel

Beispiel:

1. Würfel: 4

2. Würfel: 3

**Augensumme:** 7

Ausgang $s$	W'keit $p_s$
2	$\frac{1}{36}$
3	$\frac{2}{36}$
4	$\frac{3}{36}$
5	$\frac{4}{36}$
6	$\frac{5}{36}$
7	$\frac{6}{36}$
8	$\frac{5}{36}$
9	$\frac{4}{36}$
10	$\frac{3}{36}$
11	$\frac{2}{36}$
12	$\frac{1}{36}$

Beispiel: Augensumme:  $s = 4$        $p_4 = \frac{3}{36}$

Bei **36 Würfeln** sollte ungefähr

$$36 \cdot \frac{3}{36} = 3$$

mal die Augensumme 4 vorkommen.

Bei **72 Würfeln** sollte ungefähr

$$72 \cdot \frac{3}{36} = 6$$

mal die Augensumme 4 vorkommen.

Bei **144 Würfeln** sollte ungefähr

$$144 \cdot \frac{3}{36} = 12$$

mal die Augensumme 4 vorkommen.

## Allgemein:

Wenn man nun  $n$  mal die beiden Würfel wirft, sollte jede Summe  $s$  ungefähr

$$n \cdot p_s \text{ – mal}$$

vorkommen.

Dies ist der sogenannte **Erwartungswert** für die Anzahl der Würfe mit Augensumme  $s$ .

Tabelle bei 144 Würfeln:

<b>Ausgang <math>s</math></b>	<b>Erwartungswert: <math>144 \cdot p_s</math></b>
2	4
3	8
4	12
5	16
6	20
7	24
8	20
9	16
10	12
11	8
12	4

<b>Ausgang <math>s</math></b>	<b>Erwartungswert: <math>144 \cdot p_s</math></b>	<b>Wert <math>Y_s</math> aus Experiment</b>
2	4	2
3	8	4
4	12	10
5	16	12
6	20	22
7	24	29
8	20	21
9	16	15
10	12	14
11	8	9
12	4	6

Wie können wir nun auf Grund der Beobachtungen ein

## Urteil

darüber abgeben, ob die Würfel „fair“ sind?

Wie können wir sicher sein, dass wir uns nicht irren?

Was ist die

## Entscheidungsgrundlage?

**Wichtig: Wir können auf keinen Fall ein sicheres, endgültiges Urteil abgeben! Wir können anhand statistischer Tests nur sagen, dass wahrscheinlich etwas gilt oder nicht gilt.**

Naheliegend:

Berechne

$$Q = (Y_2 - n \cdot p_2)^2 + (Y_3 - n \cdot p_3)^2 + \dots + (Y_{12} - n \cdot p_{12})^2$$

gezinkte Würfel → hohe Abweichungen → hoher Wert von  $Q$

faire Würfel → kleine Abweichungen → niedriger Wert von  $Q$

Problem?

Man nennt

$$\chi^2 = \frac{(Y_2 - n \cdot p_2)^2}{n \cdot p_2} + \frac{(Y_3 - n \cdot p_3)^2}{n \cdot p_3} + \dots + \frac{(Y_{12} - n \cdot p_{12})^2}{n \cdot p_{12}}$$

die  $\chi^2$ -**Statistik** der Beobachtungen  $Y_2, \dots, Y_{12}$ .

Wert $x$	Wahrscheinlichkeit: $P(\chi^2 \leq x)$
2.558	0.01
3.940	0.05
6.737	0.25
9.342	0.5
12.55	0.75
18.31	0.95
23.21	0.99

Ausgang $s$	Erwartungswert: $144 \cdot p_s$	Wert $Y_{s_1}$ aus Experiment 1	Wert $Y_{s_2}$ aus Experiment 2
2	4	4	3
3	8	10	7
4	12	10	11
5	16	13	15
6	20	20	19
7	24	18	24
8	20	18	21
9	16	11	17
10	12	13	13
11	8	14	9
12	4	13	5

$$\begin{aligned}
\chi_1^2 &= \frac{(4-4)^2}{4} + \frac{(10-8)^2}{8} + \frac{(10-12)^2}{12} + \frac{(13-16)^2}{16} + \frac{(20-20)^2}{20} \\
&\quad + \frac{(18-24)^2}{24} + \frac{(18-20)^2}{20} + \frac{(11-16)^2}{16} + \frac{(13-12)^2}{12} \\
&\quad + \frac{(14-8)^2}{8} + \frac{(13-4)^2}{4} \\
&= 29 \frac{59}{120},
\end{aligned}$$

$$\begin{aligned}\chi^2_2 &= \frac{(3-4)^2}{4} + \frac{(7-8)^2}{8} + \frac{(11-12)^2}{12} + \frac{(15-16)^2}{16} + \frac{(19-20)^2}{20} \\ &\quad + \frac{(24-24)^2}{24} + \frac{(21-20)^2}{20} + \frac{(17-16)^2}{16} + \frac{(13-12)^2}{12} \\ &\quad + \frac{(9-8)^2}{8} + \frac{(5-4)^2}{4} \\ &= 1 \frac{17}{120} .\end{aligned}$$

### Gruppenaufgabe:

Führe den Test jetzt selber einmal mit 72 Würfeln durch. Erstelle eine Tabelle, die die Erwartungswerte und die tatsächlich erwürfelten Anzahlen für alle möglichen Augensummen enthält.

Berechne nun die  $\chi^2$ -Statistik und schaue in der Tabelle nach. Sind die Würfel (wahrscheinlich) fair?

# Statistische Tests für zufällige Zahlenfolgen

## Eindimensionaler Test

Wir zerlegen das Intervall  $[0, 1)$  in  $m$  gleich große Teilintervalle. Nehmen wir mal an, wir wählen  $m = 100$ . Dann zerlegen wir das Intervall  $[0, 1)$  also in die folgenden Teilintervalle:

$$[0; 0.01), [0.01; 0.02), [0.02; 0.03), \dots, [0.99, 1.00].$$

Wie groß ist dann die Wahrscheinlichkeit, in einem bestimmten Teilintervall zu liegen?

Da wir  $m$  Teilintervalle haben, ist die Wahrscheinlichkeit gerade  $p = \frac{1}{m}$ .

In unserem obigen Beispiel

$[0; 0.01), [0.01; 0.02), [0.02; 0.03), \dots, [0.99, 1.00)$

ist  $p = \frac{1}{100}$ .

### Gruppenaufgabe:

Nehmen wir einmal an, wir haben das Intervall in  $m$  Teilintervalle zerlegt und wir haben  $n$  Zufallszahlen erzeugt. Wie viele Zufallszahlen sollten dann erwartungsgemäß in jedem Teilintervall liegen?

Wende  $\chi^2$ -Test an:

$$\chi^2 = \frac{(Y_0 - \frac{n}{m})^2}{\frac{n}{m}} + \frac{(Y_1 - \frac{n}{m})^2}{\frac{n}{m}} + \dots + \frac{(Y_{m-1} - \frac{n}{m})^2}{\frac{n}{m}}.$$

zu hoher Wert von  $\chi^2$

→ die Zahlen scheinen **nicht gleichmäßig verteilt**

zu niedriger Wert von  $\chi^2$

→ die Zahlen scheinen **nicht zufällig**

Beispiel bei Zerlegung in 100 Teilintervalle:

Wert $\chi_p^2$	Wahrscheinlichkeit: $p = P(\chi^2 \leq \chi_p^2)$
63.23	0.01
77.046	0.05
89.181	0.25
98.334	0.5
108.093	0.75
123.225	0.95
134.642	0.99

## Gruppenaufgabe:

Schaue dir das Excel-Arbeitsblatt zum eindimensionalen Test für zufällige Zahlenfolgen an. Versuche zu verstehen, was in dem Excel-Arbeitsblatt genau gemacht wird. Hierbei wird das Intervall  $[0, 1)$  in 100 Teilintervalle zerlegt:

$[0; 0.01), [0.01; 0.02), [0.02; 0.03), \dots, [0.99, 1.00).$

Führe den eindimensionalen Test nun für die von Excel selbst erzeugten Zufallszahlen durch. Die entsprechende  $\chi^2$ -Tabelle ist im Excel-Blatt angegeben.

## Serientest

Zerlege

$$[0, 1) \times [0, 1) = \{ (x, y) : x \in [0, 1), y \in [0, 1) \}$$

in  $m^2$  Teilquadrate:

Wie groß ist die Wahrscheinlichkeit für ein Paar  $(x, y) \in [0, 1) \times [0, 1)$  von Zufallszahlen, in einem bestimmten Teilquadrat zu liegen?

Da wir  $m^2$  Teilquadrate haben, ist die Wahrscheinlichkeit gerade  $p = \frac{1}{m^2}$ .

### Gruppenaufgabe:

Nehmen wir einmal an, wir haben das Quadrat in  $m^2 = 100 \cdot 100 = 10\,000$  Teilquadrate zerlegt und wir haben  $2n = 200\,000$  Zufallszahlen erzeugt. Wie viele Paare von Zufallszahlen sollten dann erwartungsgemäß in jedem Teilquadrat liegen?

Wir betrachten die Größe:

$$\chi^2 = \frac{(Y_0 - \frac{n}{m^2})^2}{\frac{n}{m^2}} + \frac{(Y_1 - \frac{n}{m^2})^2}{\frac{n}{m^2}} + \dots + \frac{(Y_{m-1} - \frac{n}{m^2})^2}{\frac{n}{m^2}}.$$

Wert $\chi_p^2$	Wahrscheinlichkeit: $p = P(\chi^2 \leq \chi_p^2)$
9672.965	0.01
9767.537	0.05
9903.258	0.25
9998.333	0.5
10094.016	0.75
10232.737	0.95
10330.917	0.99

## Gruppenaufgabe:

Schaue dir das Excel-Arbeitsblatt zum Serientest für zufällige Zahlenfolgen an. Versuche zu verstehen, was in dem Excel-Arbeitsblatt genau gemacht wird. Hierbei wird das Quadrat  $[0, 1) \times [0, 1)$  in  $100 \cdot 100 = 10\,000$  Teilquadrate zerlegt.

Führe den Serientest nun für die von deinem eigenen Linearen Kongruenz-Generatoren erzeugten Zufallszahlen und für die von Matlab, C und Excel erzeugten Zufallszahlen durch.

## **Kopplung von Zufallszahlengeneratoren**

Es gibt viele Möglichkeiten die typischen Schwächen des Linearen Kongruenz-Generators, die wir ausführlich kennengelernt haben, zu verringern. Eine Möglichkeit:

**Wir koppeln einfach zwei Zufallszahlengeneratoren!**

einfaches Beispiel:

Wir betrachten die beiden Linearen Kongruenz-Generatoren

$$(1) \quad X_{i+1} = \text{Rest}_7(50 \cdot X_i + 9), \quad X_0 = 5,$$

$$(2) \quad X_{i+1} = \text{Rest}_7(50 \cdot X_i + 9), \quad X_0 = 6.$$

Die erste Folge hat (bis zum Eintreten der Periode) die Gestalt:

5, 0, 2, 4, 6, 1, 3,

die zweite Folge sieht wie folgt aus:

6, 1, 3, 5, 0, 2, 4.

**erste Folge: Zufallszahlen**

**zweite Folge: Position der Zufallszahlen**

Problem: es gibt keine 0-te Position!

Also: erste Folge unverändert:

5, 0, 2, 4, 6, 1, 3,

zweite Folge jetzt:

7, 2, 4, 6, 1, 3, 5.

### Gruppenaufgabe:

Wie lautet also jetzt die vollständige Folge, die wir auf diese Art durch Kopplung der beiden Zufallszahlenfolgen erhalten?

## Gruppenaufgabe

Erinnerst du dich an den Zufallszahlengenerator aus Aufgabe 6? Es war ein Linearer Kongruenz-Generator mit

$$a = 1229 \quad , \quad m = 2048 \quad , \quad c = 1 \quad \text{und} \quad x_0 = 0,$$

bei dem in der zweidimensionalen Darstellung nur wenige, relativ weit voneinander entfernte Linien sehen waren? Betrachte nun das Excel-Arbeitsblatt „Kopplung“ zu dieser Aufgabe. Es werden dort 2048 Zufallszahlen mit diesem (schlechten) Linearen Kongruenz-Generator erzeugt.

Schau dir nun an, was passiert, wenn man diesen Zufallszahlengenerator mit einem anderen Generator koppelt.