Monte-Carlo-Algorithmen für innermathematische Fragestellungen

Katharina Klembalski

Humboldt-Universität Berlin

30. August 2012

Warum Monte-Carlo-Algorithmen im Mathematikunterricht?

schriftl. Addieren
Scheitelpunktsform
Euklidischer Algorithmus
Punktspiegelung
Schnittpunktbestimmung
Distributivgesetz
Newtonverfahren
...

schriftl. Division
Polynomdivsion
Parallelverschiebung
p-q-Formel
Kurvendiskusion
Division von Brüchen
2-Tafelprojektion
...

nützlich, führen zu einem eindeutigen Ergebnis, **deterministisch**

Randomisierte Algorithmen

Randomisierte Algorithmen enthalten Schritte, die durch zufällige Eingaben bestimmt werden.

- Teilweise können falsche Ergebnisse (einseitige bzw. zweiseitige Fehler) auftreten bzw. der Algorithmus versagen. Daher werden Erwartungswert der Rechenzeit bzw. die Fehler- bzw. Versagenswahrscheinlichkeit angegeben.
- Es werden Entscheidungsprobleme bzw. Probleme der Berechenbarkeit gelöst, die deterministisch nicht oder nur schwer zugänglich sind.

Besondere Chance für den Mathematikunterricht

- Schüler beschäftigen sich mit nichtdeterministischen Algorithmen.
- Schüler erfahren Stochastik als (hier durch den Computer zugängliche) Denkweise zum Problemlösen.
- Schüler verbinden Wissen (bis dahin) unabhängiger, mathematischer Teildisziplinen zur Lösung des Problems.

Beispiel 1: Miller-Rabin-Test

Einbettung in den Unterricht

Bereitzustellendes Hintergrundwissen

- Zahlentheorie
  - Rechnen mit Kongruenzen
  - Kleiner Satz von Fermat
  - Satz von Rabin (1980)
- Wahrscheinlichkeitsrechnung
  - mehrstufige Zufallsexperimente, Pfadregeln
  - Simulationen

Möglicher Zeitpunkt des Unterrichtens

- Wahlpflichtunterricht, 9/10, Kryptologie oder Zahlentheorie
- Mathematik, 9/10, Daten und Zufall, Pfadregeln
- als Projekt in Vertiefungs-, Seminarkursen, SEK II

Unterricht: Das Problem

Rekordwurm aus 9,8 Millionen Ziffern

9.808.358 Ziffern, Punkt nicht mitgezählt: Das ist die neueste größte Primzahl. Zwei US-amerikanische Mathematiker haben "M32582657" entdeckt - mit Hilfe von 700 Computern, die neun Monate lang gerechnet haben.

Aufgabe

- Finde alle Primzahlen kleiner 400.
- Finde eine möglichst große Primzahl.

Unterricht: Das Problem

Experimentieren mit Mathematica[1]

- $p = 942876191136657658379477430933277830167219$
  `FactorInteger[p]` in 2,3 s sowie `PrimeQ[p]` in 1/1000 s.
- $p = 213598703592091008239502318434121854383503406330042754837222169102469970110453736043901583\ldots 9606479$
  `FactorInteger[p]` in s sowie `PrimeQ[p]` in 3/1000 s.

[1] kostenfrei auf www.wolframalpha.com oder mit dem CAS Maxima (OpenSource). In GeoGebra heißt der entsprechende Befehl `Faktoren[<Zahl>]`.

Schülervortrag: Miller-Rabin-Test

Eigenschaften von (Pseudo-)Primzahlen

Kleiner Satz von Fermat
Sei p eine Primzahl und a eine natürliche Zahl mit $ggT(a, p) = 1$. Dann gilt:

$$a^{p-1} \equiv 1 \bmod p.$$

Beispiel

- $p = 3$: $5^{3-1} \equiv 1 \bmod 3$
- $p = 5$: $2^{5-1} \equiv 1 \bmod 5$
- $p = 101$: $6^{101-1} \equiv 1 \bmod 101$

Eigenschaften von (Pseudo-)Primzahlen

weitere Beispiele

- $p^* = 341$: $2^{341-1} \equiv 1 \bmod 341$ aber $341 = 11 \cdot 31$
  $\Rightarrow$ 341 heißt *Pseudoprimzahl zur Basis* 2.
- $p^* = 341$: $3^{341-1} \equiv 56 \bmod 341$
  $\Rightarrow$ 341 ist *keine* Pseudoprimzahl zur Basis 3.
- $p^* = 561$: $2^{561-1} \equiv 1 \bmod 561$ und $561 = 3 \cdot 11 \cdot 17$.
  Leider gilt auch $5^{561-1} \equiv 1 \bmod 561$ sowie
  $a^{561-1} \equiv 1 \bmod 561$ für alle $(a, 561) = 1$.
  561 ist eine *Carmichaelzahl*.

  Es gibt unendlich viele Carmichaelzahlen.

Aus dem Satz von Fermat folgt ...

Es sei $p > 2$ prim und $\mathrm{ggT}(a, p) = 1$, dann gilt:

$$
\begin{aligned}
a^{p-1} &\equiv 1 \bmod p \quad \Longleftrightarrow \\
a^{p-1} - 1 &\equiv 0 \bmod p \quad \Longleftrightarrow \\
(a^{\frac{p-1}{2}} - 1)(a^{\frac{p-1}{2}} + 1) &\equiv 0 \bmod p \quad \Longleftrightarrow \\
(a^{\frac{p-1}{4}} - 1)(a^{\frac{p-1}{4}} + 1)(a^{\frac{p-1}{2}} + 1) &\equiv 0 \bmod p \quad \Longleftrightarrow \\
&\dots \\
(a^{\frac{p-1}{2^k}} - 1)(a^{\frac{p-1}{2^k}} + 1)(a^{\frac{p-1}{2^{k-1}}} + 1) \dots (a^{\frac{p-1}{2}} + 1) &\equiv 0 \bmod p.
\end{aligned}
$$

k sei die höchste Potenz, die $p - 1$ teilt.

Aus dem Satz von Fermat folgt ...

$$(a^{\frac{p-1}{2^k}} - 1)(a^{\frac{p-1}{2^k}} + 1)(a^{\frac{p-1}{2^{k-1}}} + 1) \ldots (a^{\frac{p-1}{2}} + 1) \equiv 0 \bmod p$$

Da p eine Primzahl ist, muss gelten

$$a^{\frac{p-1}{2^k}} \equiv 1 \bmod p \text{ oder}$$

$$a^{\frac{p-1}{2^k}} \equiv -1 \bmod p \text{ oder}$$

$$a^{\frac{p-1}{2^{k-1}}} \equiv -1 \bmod p \text{ oder}$$

$$\ldots$$

$$a^{\frac{p-1}{2}} \equiv -1 \bmod p.$$

Test auf Primalität von p^*

Berechnen der Folge $a^{\frac{p^*-1}{2^k}}, a^{\frac{p^*-1}{2^{k-1}}} \ldots, a^{p^*-1} \pmod{p^*}$

$$a^{p^*-1} \equiv (((\underbrace{a^{\frac{p^*-1}{2^k}}}_{\equiv \pm 1 \text{ oder } \equiv -1})^2 \ldots)^2)^2 \bmod p^* \quad \text{oder} \equiv -1$$

p^* besteht den Test, wenn die Folge die folgende Gestalt besitzt:

- $(\pm 1, 1, \ldots, 1)$ oder
- $(X, \ldots, X, -1, 1, \ldots, 1)$ und $X \neq \pm 1$

Beispiele – Aufgaben während des Vortrages

- $p = 101$: $6^{101-1} \equiv ((\underbrace{6^{25}}_{\equiv -1})^2)^2) \bmod 101$

  $\underbrace{\underbrace{\equiv 1}_{\equiv 1}}_{\equiv 1}$

  $\Longrightarrow$ 101 ist ein Primzahlkandidat.

- $p^* = 561$: $2^{561-1} \equiv (((\underbrace{2^{70}}_{\equiv 166})^2)^2)^2 \bmod 561$

  $\underbrace{\underbrace{\underbrace{\equiv 67}_{\equiv 1}}_{\equiv 1}}_{\equiv 1}$

  $\Longrightarrow$ 561 ist zusammengesetzt; 2 heißt *Zeuge* für die Zusammengesetztheit von 561.

Beispiele – Aufgaben während des Vortrages

- $p^* = 781$:

$$5^{781-1} \equiv ((\underbrace{5^{195}}_{\equiv 1})^2)^2 \bmod 781$$

$$\underbrace{\qquad\qquad}_{\equiv 1}$$

$$\underbrace{\qquad\qquad\qquad}_{\equiv 1}$$

aber

$$781 = 11 \cdot 71$$

781 heißt *starke Pseudoprimzahl zur Basis* 5.

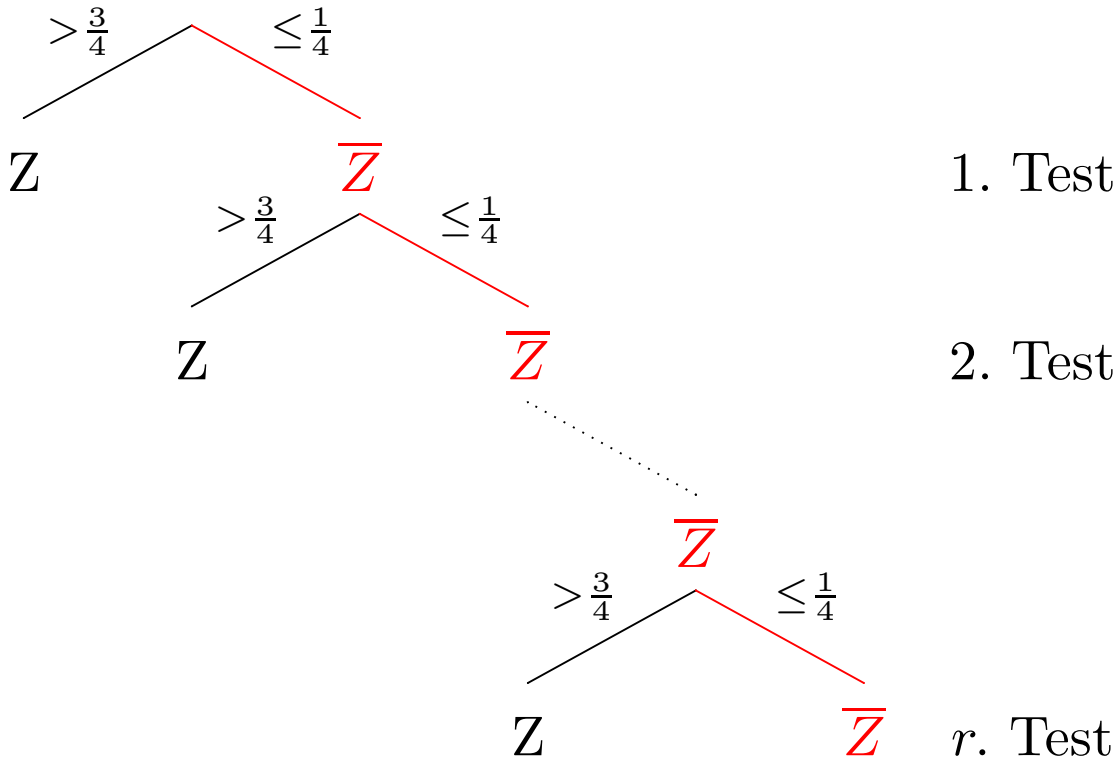
Besteht ein Kandidat p^* den Test?

- nein – Dann ist p^* sicher zusammengesetzt. Wegen des kleinen Fermats ist ausgeschlossen, dass Primzahlen als zusammengesetzt erkannt werden.
- ja – Dann ist p^* vielleicht eine Primzahl. Die Aussage ist nicht sicher, da zusammengesetzte Zahlen fälschlich als prim identifiziert werden können. Die Fehlerwahrscheinlichkeit kann jedoch nach oben abgeschätzt werden:

Satz von Rabin
Sei p^* zusammengesetzt. Dann sind höchstens ein Viertel aller Basen kleiner p^* keine Zeugen für die Zusammengesetztheit von p^*.

Konstruktion des probabilistischen Tests

Sei p^* zusammengesetzt und
$Z := a$ sei Zeuge für die Zusammengesetztheit von p^*.



Es gilt: $P(p^* \text{ besteht den Test} \mid p^* \text{ ist zusammengesetzt}) \leq \left(\frac{1}{4}\right)^r$.

Der Algorithmus

Sei p^* ein Kandidat für eine Primzahl.
Für $i = 1, \ldots r$ tue das Folgende:

- Wähle ein zufälliges $a < p^*$.
- Prüfe, ob $\mathrm{ggT}(a, p^*) = 1$.
- Falls $\mathrm{ggT}(a, p^*) \neq 1$,so antworte: p^* ist zusammengesetzt.
  Sonst teste auf Primalität:
  Gilt nicht $a^{p^*-1} \equiv (((\underbrace{a^{\frac{p^*-1}{2^k}}}_{\equiv \pm 1})^2 \ldots)^2)^2 \bmod p^*$,
  $\underbrace{\underbrace{\text{oder } \equiv -1}}_{\text{oder } \equiv -1}$
  so antworte: p^* ist zusammengesetzt.

Sonst antworte: p^* ist (fast sicher) eine Primzahl.

Der Algorithmus

Sei p^* ein Kandidat für eine Primzahl.
Für $i = 1, \ldots r$ tue das Folgende:

- Wähle ein zufälliges $a < p^*$.
- Prüfe, ob $\mathrm{ggT}(a, p^*) = 1$.
- Falls $\mathrm{ggT}(a, p^*) \neq 1$,so antworte: p^* ist zusammengesetzt.
  Sonst teste auf Primalität:
  Gilt nicht $a^{p^*-1} \equiv (((\underbrace{a^{\frac{p^*-1}{2^k}}}_{\equiv \pm 1})^2 \ldots)^2)^2 \bmod p^*$,
  $\underbrace{\underbrace{\text{oder } \equiv -1}}_{\text{oder } \equiv -1}$
  so antworte: p^* ist zusammengesetzt.

Sonst antworte: p^* ist (fast sicher) eine Primzahl.

Monte-Carlo-Algorithmus – sicher?

. . . Nur *fast sicher* nicht zusammengesetzt!

Aufgabe

Welche Größenordnung verbirgt sich hinter $(1/4)^{30} \approx 9 \cdot 10^{-19}$?
Veranschauliche den Zahlenwert anhand geeigneter Wahrscheinlichkeiten.

Die Chance auf einen 6er im Lotto (mit Superzahl) zwei Wochen hintereinander ist 100mal größer.

Monte-Carlo-Algorithmus – Probabilistik vs. Exaktheit

Aufgabe

Überprüfe die oben bestimmten Primzahlen jeweils auch mit dem anderen Verfahren auf Primalität. Welches Verfahren ist besser? Nach welchen Kriterien entscheidest Du?

theoretisch vs. praktisch
exakt vs. unsicher
langsam vs. schnell (effizient)

Ausblick / Einbettung

Anknüpfungen Zahlentheorie

- Beweis des Satzes von Fermat
- Prüfe, ob $\mathrm{ggT}(a, p) = 1$ (Euklidischer Algorithmus)
- Bestimme $a^{\frac{p-1}{2^k}}, a^{\frac{p-1}{2^{k-1}}} \ldots, a^{p-1} (\mathrm{mod}\, p)$ (Square & Multiply-Algorithmus)
- Abschätzung der falschen Zeugen gegen Zusammengesetztheit
- Wieviele Primzahlen gibt es in einem bestimmten Intervall? $(\pi(n) \to \frac{n}{\ln(n)})$
- Wie sind Primzahlen verteilt? (Primzahllücken, -zwillinge)
- Wie erkenne ich Primzahlen?

Anknüpfungen Stochastik

- Pfadregeln für eine nach oben abgeschätzte Wahrscheinlichkeit
- Wähle zufälliges $a < p$ mit ...
- Abschätzung der falschen Zeugen gegen Zusammengesetztheit
- Was heißt fast sicher?

Anknüpfungen Monte-Carlo-Algorithmen (für Entscheidungsprobleme)

- Zero-Knowledge-Protokolle
- Interaktive Beweise

Beispiel 2: – Bestimmung von π

Einbettung in den Unterricht

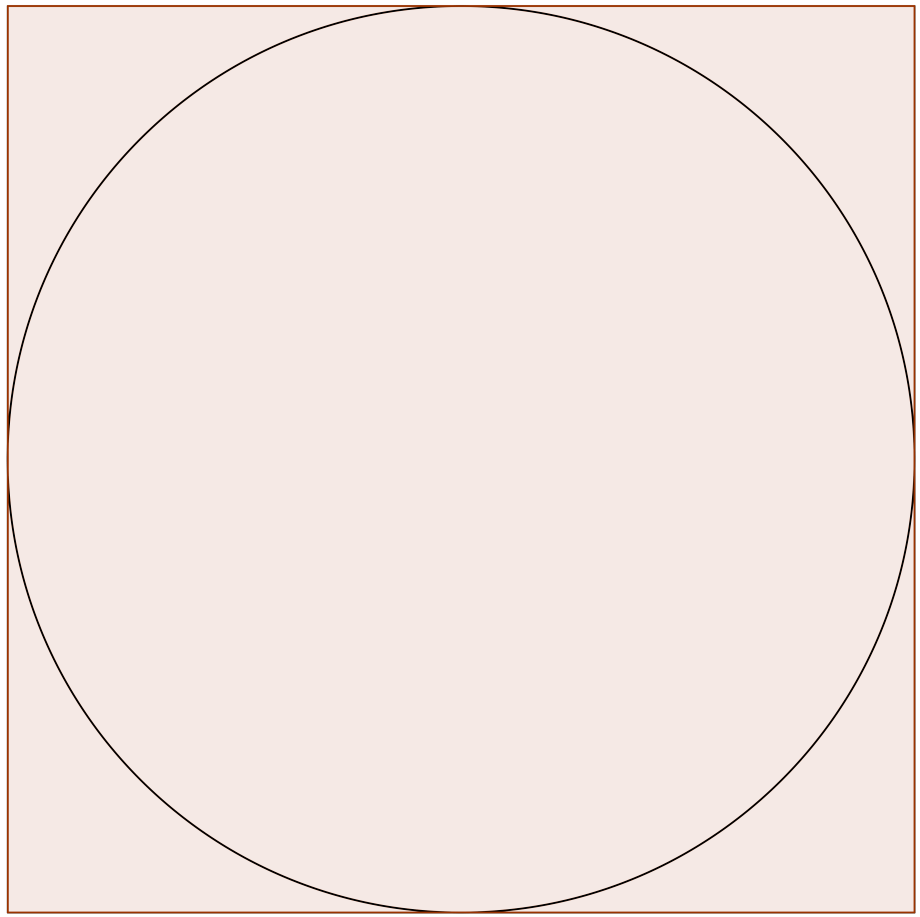
Bereitzustellendes Hintergrundwissen

- Flächeninhalt Kreis und Quadrat
- Abstand zweier Punkte
- Tabellenkalkulation (einfache Formeln)
- Erwartungswert und Varianz von verknüpften Zufallsgrößen / Mittelwert von Zufallsgrößen

Möglicher Zeitpunkt des Unterrichtens : SEK II

Unterricht: Ziel Bestimmung von π

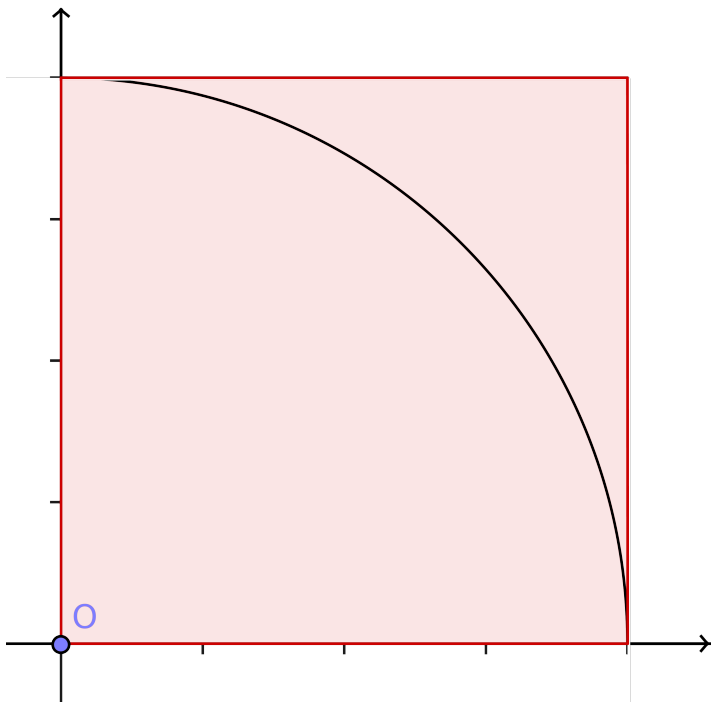
Ansatz: Definition von π mit Hilfe des Verhältnisses von Kreisfläche und Quadratfläche



$$\Longrightarrow \quad \frac{A_K}{A_Q} = \frac{\pi}{4} \text{ also } \pi := 4 \cdot \frac{A_K}{A_Q}.$$

Wie messen wir den Flächeninhalt?[2]

1. „Werfen von Reiskörnern“ auf „gut Glück“.
2. Die Wahrscheinlichkeit für einen Treffer im Kreis ist durch $\frac{A_K}{A_Q}$ gegeben.
3. Die Wahrscheinlichkeit wird näherungsweise durch die relative Trefferhäufigkeit bestimmt.
4. $r = 1$



[2] Jan Hendrik Müller: Reis im Kreis. mathematik lehren 138 (2006), S.23-43

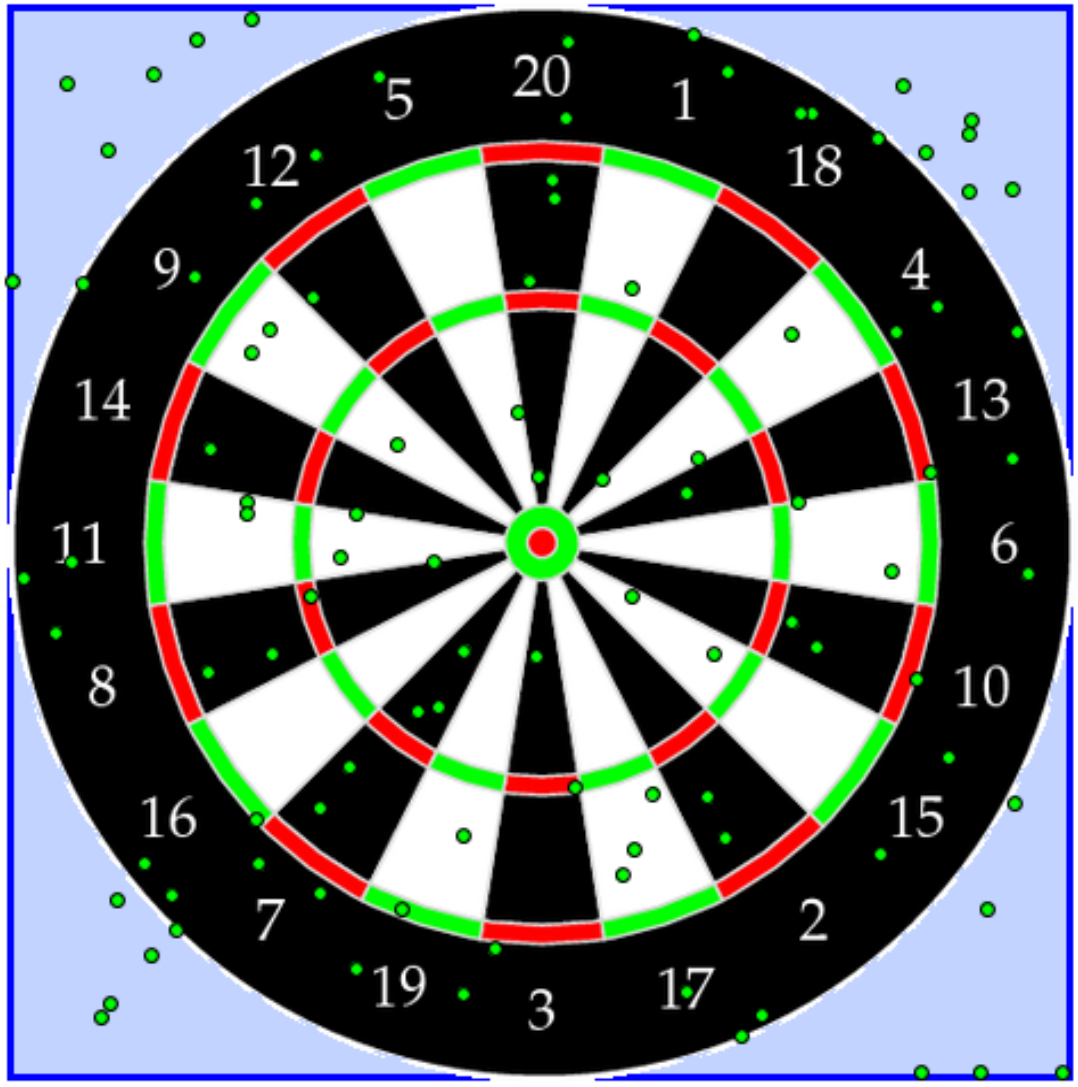
Wie messen wir den Flächeninhalt?

Simulation

Reiskorn	x-Wert	y-Wert	Abstand zum Koord.ursprung	im Kreis? ja = 1, nein = 0	Treffersumm	Flächenanteil x4
1	0,8185	0,1003	0,82	1	1	4,000000
2	0,9803	0,9645	1,38	0	1	2,000000
3	0,2688	0,1969	0,33	1	2	2,666667
4	0,9919	0,0955	1,00	1	3	3,000000
5	0,7116	0,4722	0,85	1	4	3,200000
6	0,4234	0,9358	1,03	0	4	2,666667

Koordinaten	`=ZUFALLSZAHL()`
Abstand	`=WURZEL(ZelleLinks^2+ZelleLinksLinks^2)`
Kreis?	`=WENN(ZelleLinks<=1;1;0)`
Treffersumme	`=ZelleObendrüber+ZelleLinks`
Flächenteil	`=Treffersumme/"Reiskornzahl"`

Wie messen wir den Flächeninhalt? II



http://www.ph-ludwigsburg.de/wp/fest/iamath/files/dartpi.php unter „Andreas Fest & interaktive Mathematik“

Beobachtung – bis zu 1000 Würfe

Wurf	Näherung π	Wurf	Näherung π
10	3,20000	100	3,40000
20	3,60000	200	3,28000
30	3,73333	300	3,24000
40	3,50000	400	3,21000
50	3,28000	500	3,18400
60	3,33333	600	3,16667
70	3,31429	700	3,19429
80	3,35000	800	3,14500
90	3,37778	900	3,17333
100	3,40000	1000	3,18000

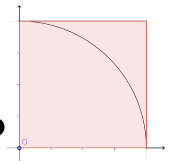
Beobachtung – bis zu 100.000

Wurf	Näherung π	Wurf	Näherung π
1000	3,18000	10000	3,16680
2000	3,17200	20000	3,15380
3000	3,18667	30000	3,14280
4000	3,19500	40000	3,13780
5000	3,18240	50000	3,13784
6000	3,17400	60000	3,13693
7000	3,16457	70000	3,13817
8000	3,16450	80000	3,13940
9000	3,16311	90000	3,13827
10000	3,16680	100000	3,13696

Wie können wir die Näherungswerte verbessern?

Wie können wir die Genauigkeit verbessern?

1. Häufigeres Werfen – Was bedeutet *genau*?



Es sei $r = 1$ und X die Zufallsgröße mit den Werten 1 (im Kreis) und 0 (außerhalb des Kreises).

$$P(X = 1) = \frac{A_{VK}}{A_Q} = \frac{A_{VK}}{1} = A_{VK}$$

$$P(X = 0) = \frac{A_Q - A_{VK}}{A_Q} = 1 - A_{VK}$$

$$E(X) = 0 \cdot (1 - A_{VK}) + 1 \cdot A_{VK} = A_{VK}$$

$$\begin{aligned} \sigma^2 &= (1 - A_{VK})^2 \cdot (A_{VK}) + (0 - A_{VK})^2 \cdot (1 - A_{VK}) \\ &= A_{VK} \cdot (1 - A_{VK}) \end{aligned}$$

Wie können wir die Genauigkeit verbessern?

Einfacher Wurf: X
$E(X) = A_{VK}$, $\sigma^2 = A_{VK} \cdot (1 - A_{VK})$

Mehrfaches Werfen: Zufallsgröße $\bar{X} = \frac{1}{n} \sum_{i=1}^{n} X_i$

- $E(\bar{X}) = E\left(\frac{1}{n} \sum_{i=1}^{n} X_i\right) = \frac{1}{n} \left(\sum_{i=1}^{n} E(X_i)\right) = \frac{1}{n} \cdot n \cdot E(X_i) = A_{VK}$
- $E(\bar{X})$ schätzen wir durch die relative Häufigkeit.
- $Var(\bar{X}) = Var\left(\frac{1}{n} \sum_{i=1}^{n} X_i\right) = \frac{1}{n^2} \sum_{i=1}^{n} Var(X_i) = \frac{1}{n^2} \sum_{i=1}^{n} \sigma^2 = \frac{1}{n} \cdot \sigma^2$
- $\sigma(\bar{X}) = \frac{1}{\sqrt{n}} \cdot \sigma$

Genau genug?

$$
\begin{array}{lll}
n = 10.000 & 4 \cdot \sigma(\bar{X}) = 0,04 & \Rightarrow \pi^* - 0,04 \leq \pi \leq \pi^* + 0,04 \\
n = 100.000 & 4 \cdot \sigma(\bar{X}) = 0,012 & \Rightarrow \pi^* - 0,012 \leq \pi \leq \pi^* + 0,012 \\
n = 1.000.000 & 4 \cdot \sigma(\bar{X}) = 0,004 & \Rightarrow \pi^* - 0,004 \leq \pi \leq \pi^* + 0,004
\end{array}
$$

Ausblick

Anknüpfungen Monte-Carlo-Algorithmen (für Suchprobleme)

- direkt anschlussfähig: Integration von Funktionen (statt Viertelkreis)
- Sortieralgorithmen (Informatik)
- diskrete Optimierung

Monte-Carlo-Algorithmen für innermathematische Probleme

	p^* prim?	Dezimaldarstellung von π
Beispiel für	Entscheidungsproblem	Suchproblem
Fehler / Laufzeit	Fehler beliebig klein	Genauigkeit $\sim 1/\sqrt{n}$
Gegenüberstellung determ. Agorithmus	besser!	besser?

Warum Monte-Carlo-Algorithmen im Mathematikunterricht?

schriftl. Addieren
Scheitelpunktsform
Euklidischer Algorithmus
Punktspiegelung
Schnittpunktbestimmung
Distributivgesetz
Newtonverfahren
Miller-Rabin-Test
...

schriftl. Division
Polynomdivsion
Parallelverschiebung
p-q-Formel
Kurvendiskusion
Division von Brüchen
2-Tafelprojektion
Bestimmung von π
...

nützlich, führen zu einem eindeutigen Ergebnis, **oft** deterministisch