Stockholms matematiska cirkel
Datorernas matematik

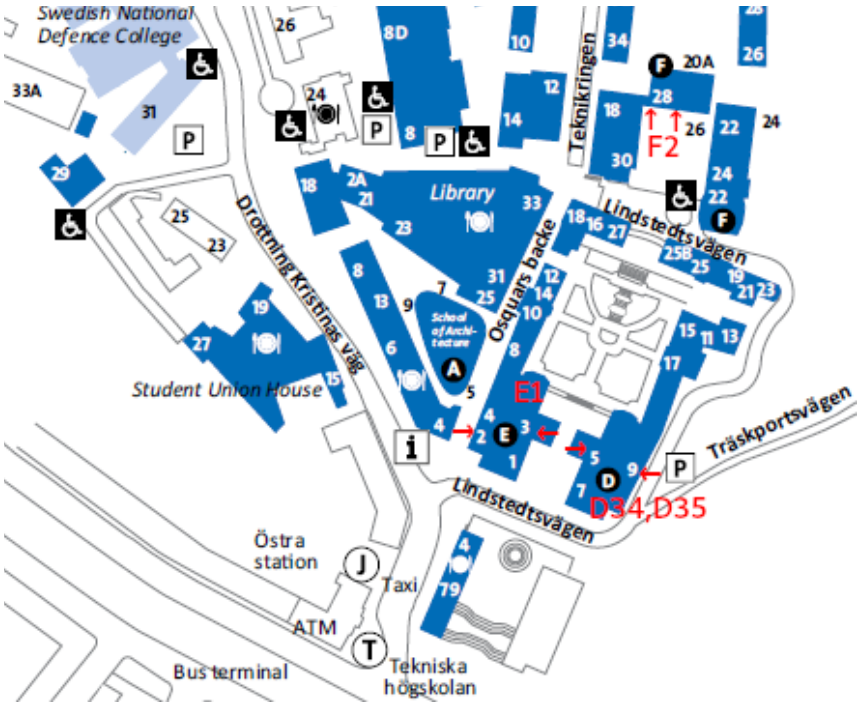
www.math-stockholm.se/cirkel

16.00–16.15: Fika
16.15–17.15: Föreläsning om kapitel 4
17.15–17.30: Rast
17.30–18.00: Gästföreläsning av Gustav Zickert:
Oändliga mängder

Översikt

1. Vad är matematik, egentligen?
2. Hur kan en dator räkna?
3. Tal med decimaler
4. **Tärningen är kastad**
5. Formella språk
6. Tillståndsmaskiner
7. Tillståndsmaskinernas språk

- Nästa **övning** är **23 jan** i salarna **D34, D35**
- Nästa **föreläsning** är **6 feb** i sal **F2**



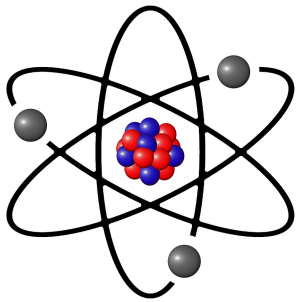
Kapitel 4 – Tärningen är kastad

Äkta slumptal

Kapitel 4 – Tärningen är kastad

Äkta slumptal



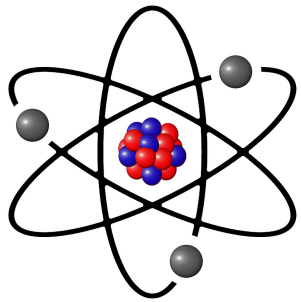


- www.random.org – atmosfäriskt brus

Kapitel 4 – Tärningen är kastad

Äkta slumptal





- www.random.org – atmosfäriskt brus

Upprepade tärningskast:

$$4, \quad 1, \quad 6, \quad 2, \quad 3, \quad 5, \quad 4, \quad 6, \quad 3, \quad 3, \quad \ldots$$

- Inget mönster – ingen förutsägbarhet

Kapitel 4 – Tärningen är kastad

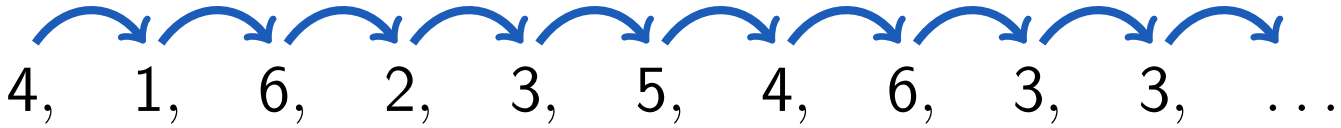
- Äkta slumptal går oftast långsamt att generera, eller kräver dyr utrustning

Kapitel 4 – Tärningen är kastad

- Äkta slumptal går oftast långsamt att generera, eller kräver dyr utrustning

Pseudoslumptal – ”falska” slumptal

- Använd en **funktion** för att **räkna ut** en följd av tal som **”ser ut”** att vara slumpmässig



Kapitel 4 – Tärningen är kastad

"Anyone who considers arithmetical methods
of producing random digits is,
of course, in a state of sin."

— John von Neumann (1951)

Kapitel 4.1 – Pseudoslumptal

På tavlan!

Hjälpsats 4.1.8: Låt m vara ett positivt heltal, och låt x, y och z vara heltal. Om

$$x \equiv y \pmod{m}$$

så är

$$xz \equiv yz \pmod{m}.$$

Hjälpsats 4.1.8: Låt m vara ett positivt heltal, och låt x, y och z vara heltal. Om

$$x \equiv y \pmod{m}$$

så är

$$xz \equiv yz \pmod{m}.$$

Hjälpsats 4.1.9: Låt m vara ett primtal, och låt x, y och z vara heltal. Antag $0 < z < m$. Om

$$xz \equiv yz \pmod{m}$$

så är

$$x \equiv y \pmod{m}.$$

Hjälpsats 4.1.10: Låt $P = L(m, a, b)$ med $b = 0$ och $a > 0$. Då är

$$x_n \equiv a^n x_0 \pmod{m}, \qquad n = 0, 1, 2, \ldots$$

En användbar linjär kongruensgenerator $L(m, a, b)$:

- $S = \{0, 1, 2, \ldots, m-1\}$
- $f(x) = \mathrm{Mod}_m(ax + b)$

En användbar linjär kongruensgenerator $L(m, a, b)$:

- $S = \{0, 1, 2, \ldots, m-1\}$
- $f(x) = \mathrm{Mod}_m(ax + b)$

Välj $m = 2^{31} - 1 = 2\,147\,483\,647$, $a = 7^5 = 16\,807$ och $b = 0$.

En användbar linjär kongruensgenerator $L(m, a, b)$:

- $S = \{0, 1, 2, \ldots, m-1\}$
- $f(x) = \mathrm{Mod}_m(ax + b)$

Välj $m = 2^{31} - 1 = 2\,147\,483\,647$, $a = 7^5 = 16\,807$ och $b = 0$.

Eftersom m är ett primtal
och a är ett primitivt element modulo m
så är enligt Sats 4.1.5 generatorns period $2^{31} - 2$
för alla positiva $x_0 \in S$.

En användbar linjär kongruensgenerator $L(m, a, b)$:

- $S = \{0, 1, 2, \ldots, m-1\}$
- $f(x) = \mathrm{Mod}_m(ax + b)$

Välj $m = 2^{31} - 1 = 2\,147\,483\,647$, $a = 7^5 = 16\,807$ och $b = 0$.

Eftersom m är ett primtal
och a är ett primitivt element modulo m
så är enligt Sats 4.1.5 generatorns period $2^{31} - 2$
för alla positiva $x_0 \in S$.

Slumptalen x_n är heltal i S.

En användbar linjär kongruensgenerator $L(m, a, b)$:

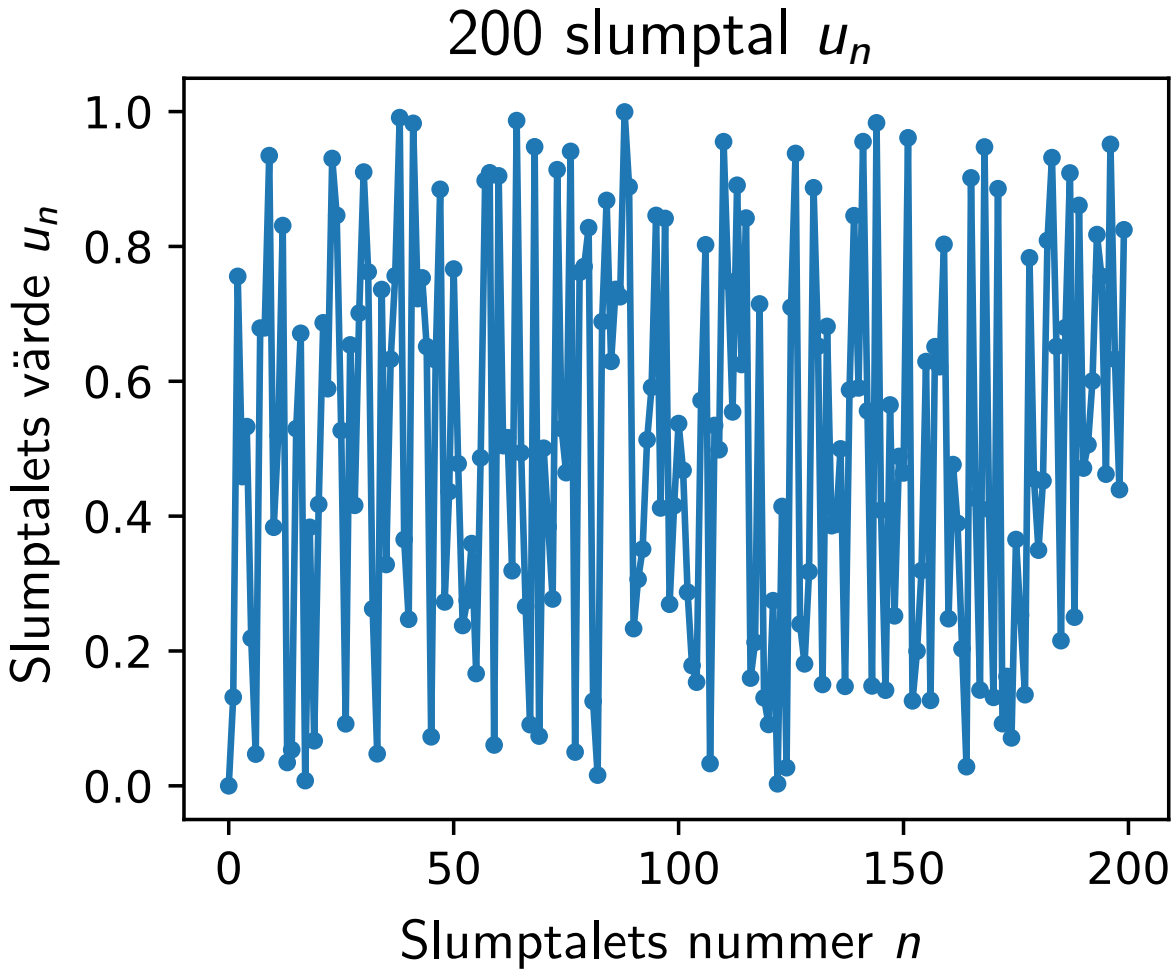
- $S = \{0, 1, 2, \ldots, m-1\}$
- $f(x) = \mathrm{Mod}_m(ax + b)$

Välj $m = 2^{31} - 1 = 2\,147\,483\,647$, $a = 7^5 = 16\,807$ och $b = 0$.

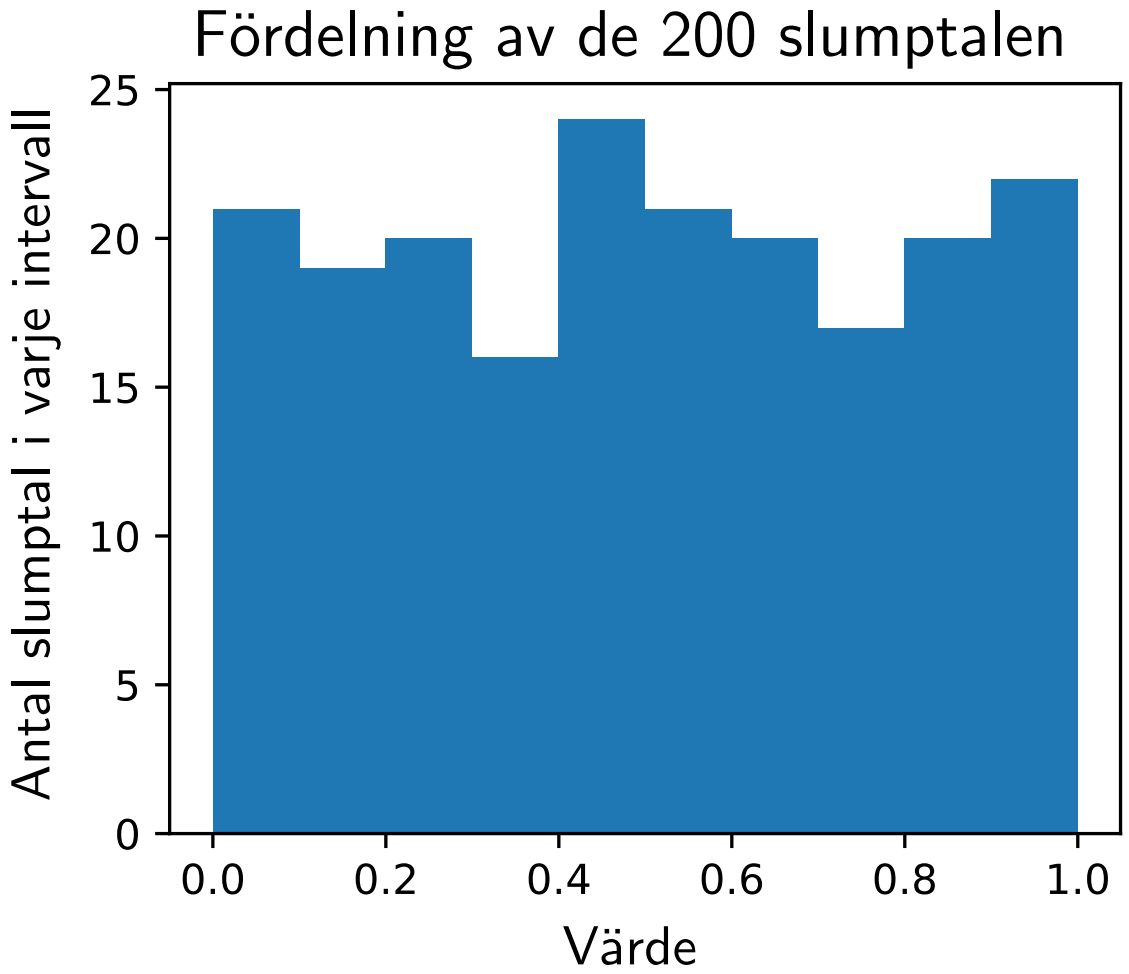
Eftersom m är ett primtal
och a är ett primitivt element modulo m
så är enligt Sats 4.1.5 generatorns period $2^{31} - 2$
för alla positiva $x_0 \in S$.

Slumptalen x_n är heltal i S.
Om vi vill ha slumptal mellan 0 och 1, sätt $u_n = x_n/m$.

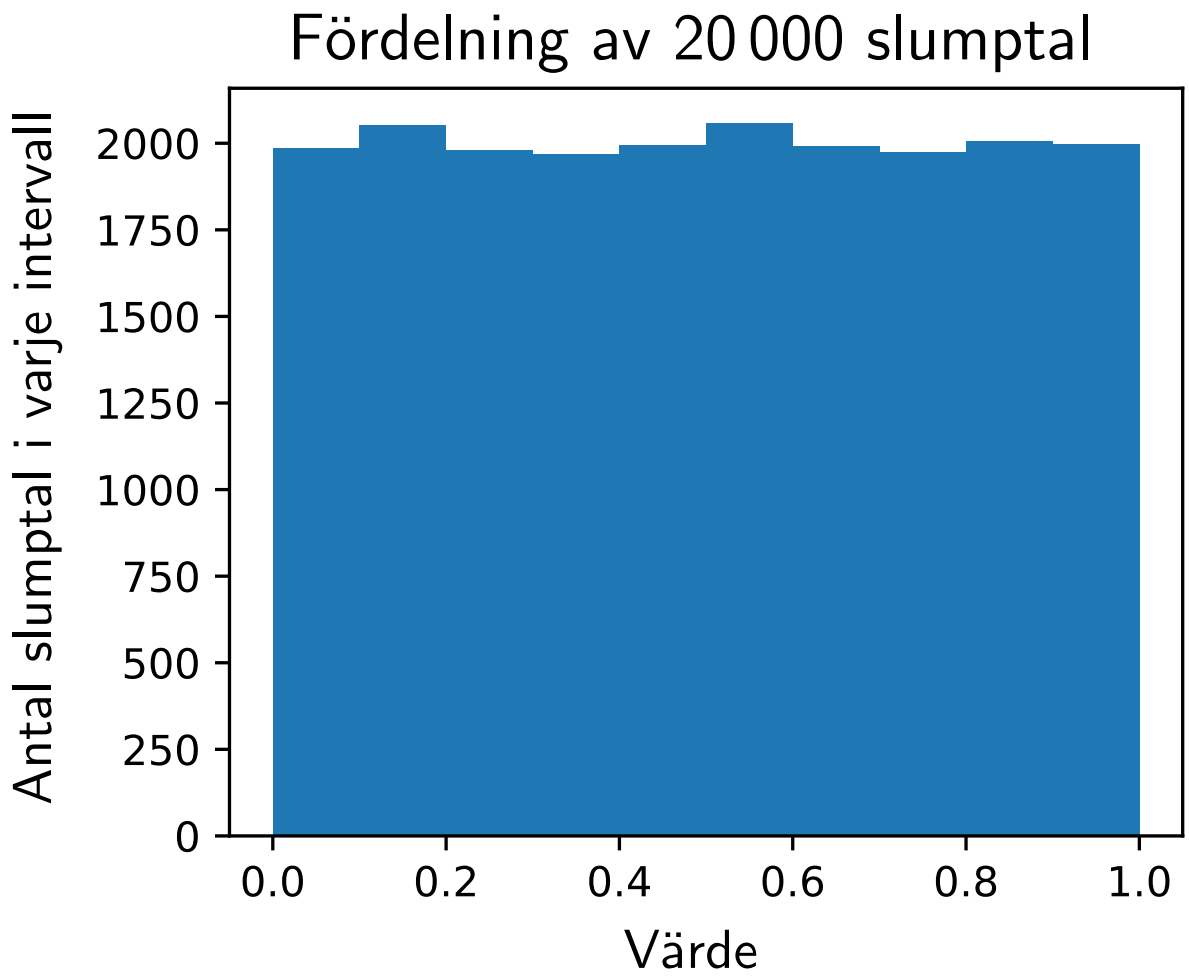
En användbar linjär kongruensgenerator $L(m, a, b)$: $x_0 = 1$



En användbar linjär kongruensgenerator $L(m, a, b)$



En användbar linjär kongruensgenerator $L(m, a, b)$



Exempel 4.1.12: En tärning

Sätt

$$t_n = \lfloor 6u_n \rfloor + 1$$

Exempel 4.1.12: En tärning

Sätt

$$t_n = \lfloor 6u_n \rfloor + 1$$

Med $x_0 = 1$ blir de första t_n

$$1, \quad 1, \quad 5, \quad 3, \quad 4, \quad 2, \quad 1, \quad 5, \quad 5, \quad 6, \quad 3, \quad 4, \quad 5, \quad \ldots$$

Kapitel 4.2 – Tillämpningar av slumptal

Egen läsning i kompendiet

- Kryptering
- Slumpvandring
- Monte Carlo-beräkningar