Monte Carlo meetodid, loeng 1

Raul Kangro

4. september 2019

Sissejuhatus

Praktikas pakuvad huvi mitmesugused juhuslike suuruste käitumisega seotud küsimused

- Kui suur on tõenäosus, et 25-st tudengist moodustatud rühmas on vähemalt kolmel sünnipäev samal päeval?
- Kui suur on tõenäosus, et kindlustusfirma läheb pankrotti lähema 10 aasta jooksul?
- Milline on täielikult automatiseeritud kauplemisalgoritmi poolt aasta jooksul teenitava tulu tõenäosusjaotus?
- mis on integraali

$$\iint_{\Omega} e^{-x^2-xy+y^3}\,dxdy$$

ligikaudne väärtus juhul, kui Ω on ühikruut?
- Millega võrdub võrratusega $(x^2+y^2-1)^2-4(x^2+(y-1)^2)\leq 0$ defineeritud kujundi pindala?

Sissejuhatus(jätk)

Kuidas leida vastuseid?

- Teha eeldused juhuslikkuse kohta (mudel), või luua juhuslikkust sisaldav mudel, millega saab siduda huvipakkuva küsimuse
- Edasi erinevad võimalused
  - Kasutada tõenäosusteooria vahendeid, et mudeli põhjal huvipakkuvad suurused välja arvutada
  - sooritada katseid ja teha arvutusi katsetulemuste põhja
- Viimane võimalus ongi Monte-Carlo meetodi rakendamine

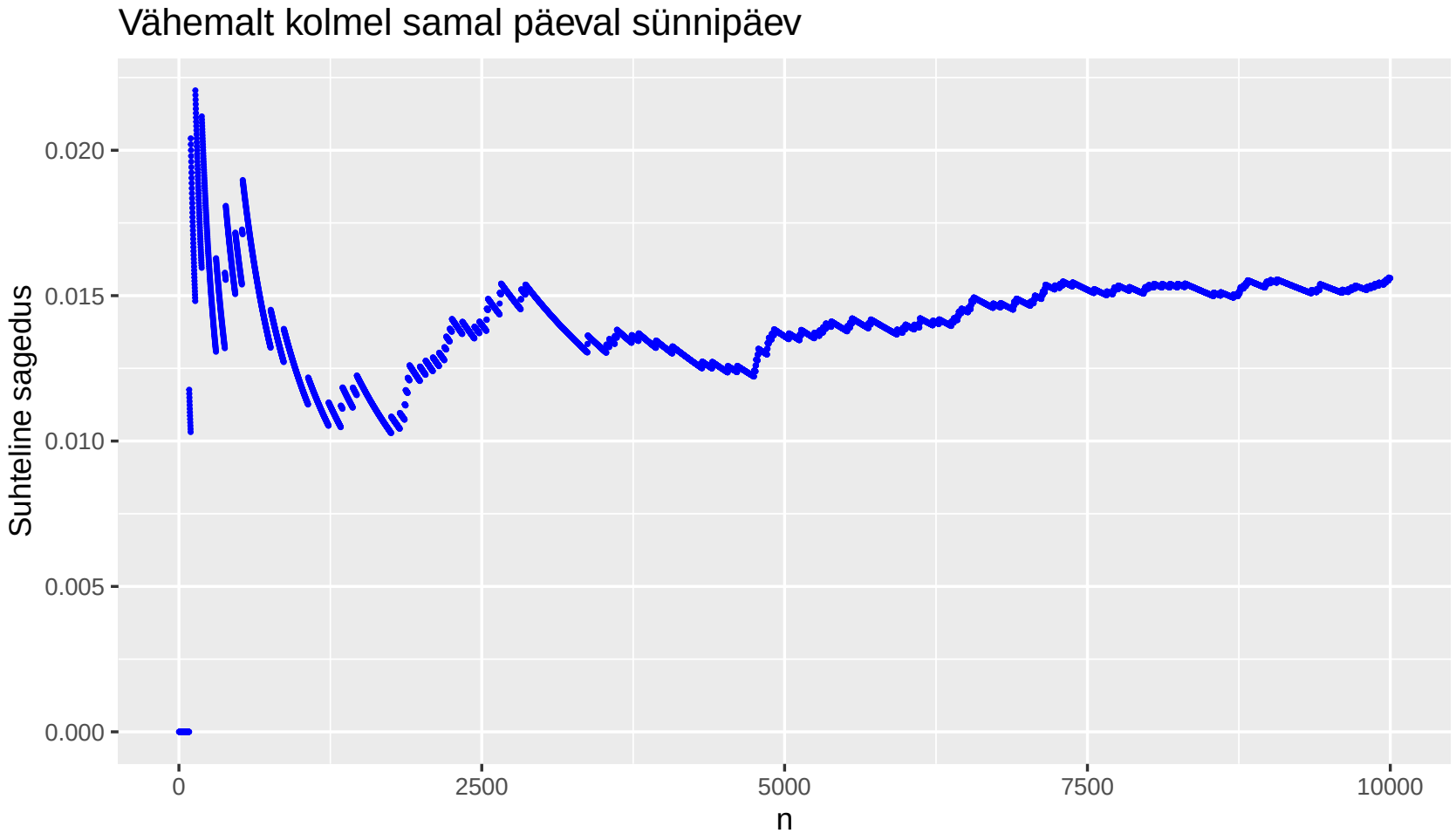
Näide 1

- Kui suur on tõenäosus, et 25-st tudengist moodustatud rühmas on vähemalt kolmel sünnipäev samal päeval?
- Mudel: moodustatud rühmas on sünnipäevad sõltumatud, kõik kuupäevad sama tõenäosusega (v.a. 29 veebruar, mille tõenäosuse loeme nulliks)
- Katse: valime juhuslikult arve 1-st 365-ni (25 arvu)

```
##  [1] 123  70 357  55 332 238 207 361 276 106  75  98 209 160 317 241   2
## [18] 211 291 218 282  19 258 266  40
```

- kordame katset n korda, loeme kokku, mitmel korral oli vähemalt 3 arvu võrdsed

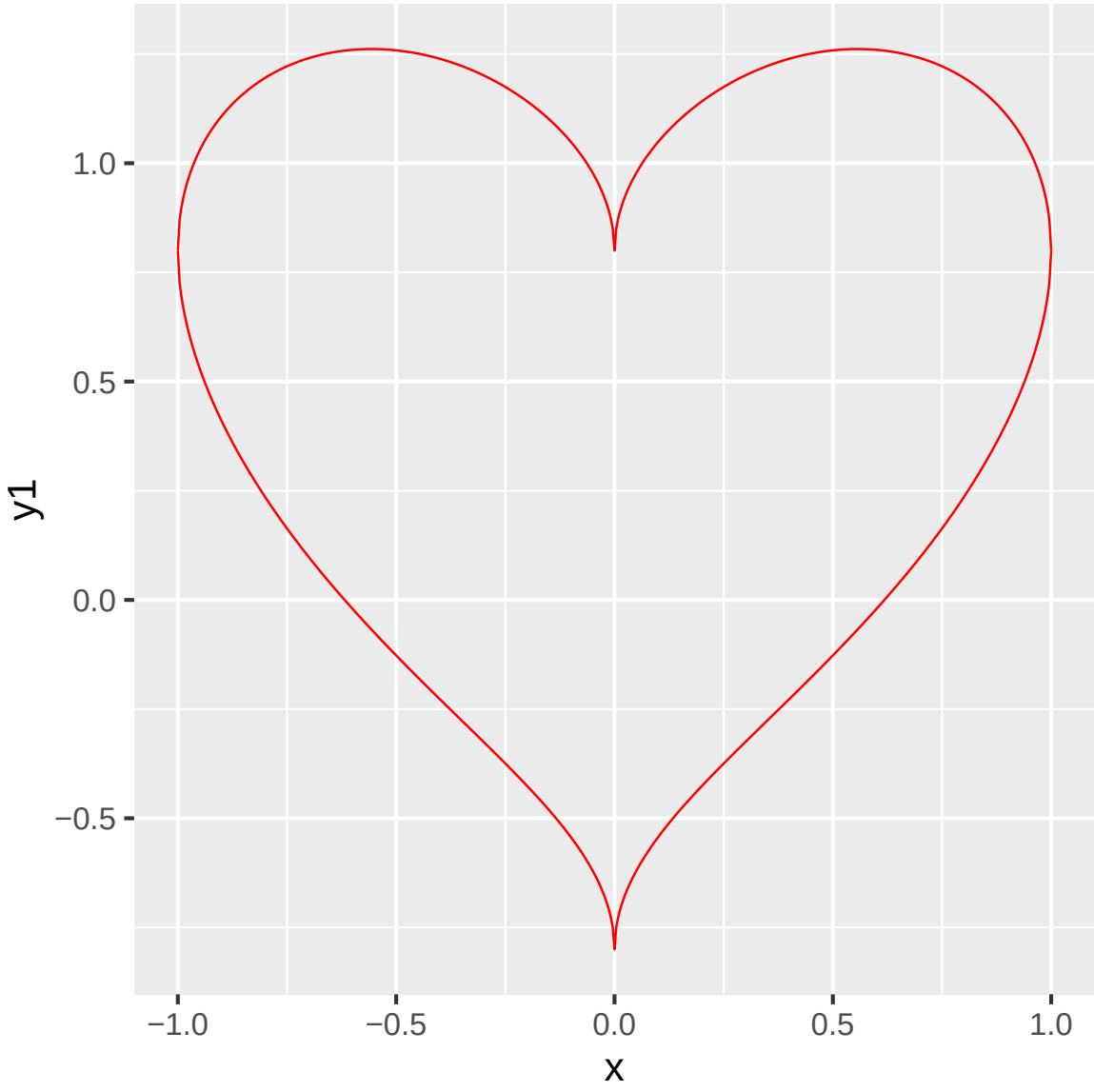
Näide 1 (jätkub)




```
## [1] 0.0156
```

Keerulise objekti pindala

Leida võrratusega $x^2 + (\frac{5}{4}y - \sqrt{|x|})^2 \leq 1$ määratud kujundi pindala



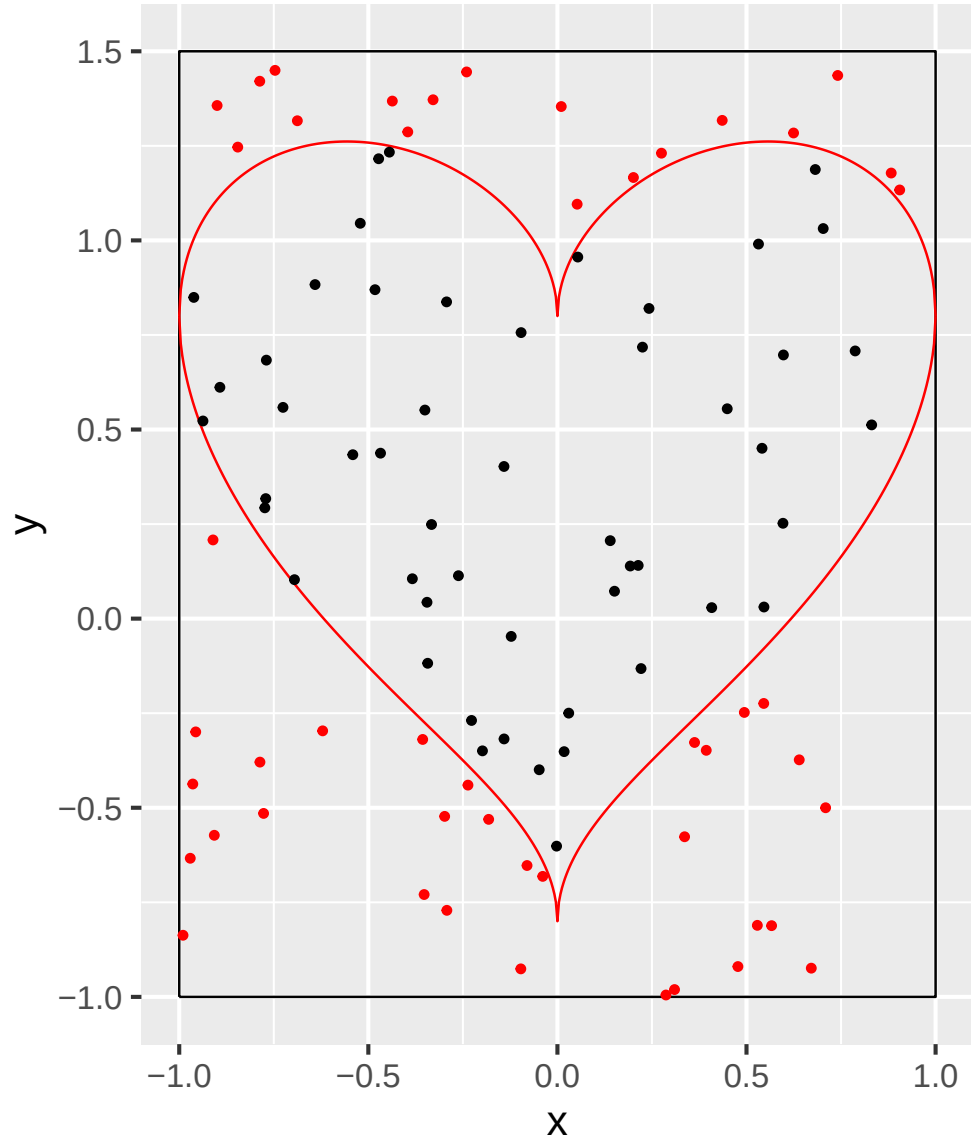
Pindala leidmine (jätk)

Lahendus: Paneme kujundi "kasti" $-1 \leq x \leq 1,\ -1 \leq y \leq 1.5$

"Pommitame" ristkülikut selle seest juhuslikult valitud punktidega

Leiame kujundi sisse sattunud punktide arvu jagatise kõikide punktide arvuga ja korrutame ristküliku pindalaga

Pindala leidmine (jätk)



Piirkonna sees 49, kokku 100 punkti, pindala ligikaudu 2.45

Kuidas saada juhuslikke arve?

- Füüsikalised katsed
  - Mündivise
  - Täringuvise
  - Rulett
  - Atmosfääriline müra
  - Radioaktiivne lagunemine
- Kustkohast tuleb neis katsetes juhuslikkus?
- Kas me võime olla kindlad, et katsetulemused on sõltumatud?

Juhuslikkus arvuti abil

- arvutiprogramm täidab täpselt käske
- päris juhuslikkus saab tulla ainult mingist sisendväljundseadmest
  - hiireklikid
  - klahvivajutused
  - võrguliiklus
  - spetsiaalne lisaseade (hardware random number generator)
- simulatsioonide läbiviimiseks on vaja saada kiiresti ja palju juhuslikke arve
  - füüsilised generaatorid ei ole piisavalt kiired/on liiga kallid
  - Paljude ülesannete jaoks ei ole vahet, kas arvud on “päris juhuslikud” või käituvad piisavalt sarnaselt juhuslikele arvudele
  - Programmide kontrollimiseks on vajadus “fikseerida juhuslikkus”

Juhuslikud arvud

Definitsioon. Arve $x_1, \ldots, x_n$ nimetatakse juhuslikule suurusele X vastavateks juhuslikeks arvudeks, kui nad on saadud juhusliku suuruse X väärtustena juhusliku katse sõltumatul kordamisel.

Matemaatiliselt tähendab eelnev definitsioon, et katsete sooritamisele vastavad juhuslikud suurused $X_1, \ldots, X_n$ on sõltumatud sama jaotusega juhuslikud suurused ning juhuslikud arvud on nende juhuslike suuruste realiseerunud väärtused

Pseudojuhuslikud arvud

Definitsioon. Arve $x_1, \ldots, x_n$ nimetatakse juhuslikule suurusele X vastavateks *pseudojuhuslikeks arvudeks*, kui nad on saadud mingi algoritmi või eeskirja kohaselt ja neid ei õnnestu eristada juhuslikule suurusele X vastavatest juhuslikest arvudest teatud komplekti statistiliste testide abil.

Seda algoritmi või eeskirja, millega pseudojuhuslikke arve $x_1, \ldots, x_n$ saadakse, nimetatakse *pseudojuhuslike arvude generaatoriks* (PJAG)

Testide nimekiri muutub ajas, tuntud on nt *Diehard tests* ja *TestU01* testikomplekt (vt nt Google abil)

Esimene PJAG

- J. von Neumann (1946) - ruudu keskosa meetod
- Võtta k-kohaline arv a (nt $k = 4,\ a = 4793$)
- Leida a^2, vaatleme seda kui $2k$ kohalist arvu (saame $a^2 = 22972849$)
- uueks a väärtuseks võtame selle keskmised k numbrit (saame $a = 9728$, juhuslikuks arvuks võtame 0.9728)
- edasi saame jada 0.6339 -> 0.1829 -> 0.3452 -> 0.9163 -> 0.9605 -> 0.256 -> 0.5536-> . . .
- Ei ole hea generaator, mõne algväärtuse korral väga halb
- 0.9001 -> 0.018 -> 0.0324 -> 0.1049 -> 0.1004 -> 0.008 -> 0.0064-> 0.004 -> 0.0016->0.0002 -> 0->. . .

Kursuse kava

- Õpime tundma PJAG põhimõtteid ja omadusi
- Õpime testima PJAG headust
- Õpime tekitama sobivate omadustega (pseudo)juhuslikke arve (st vastavalt etteantud jaotusele)
- Õpime kastama arvutisimulatsioone mitmesuguste ülesannete lahendamisel (integreerimine, usaldusintervallide leidmine, hinnangu nihke vähendamine jms)

Väike hoiatus

- Arvutisimulatsioonid on sageli hea vahend, et saada aimu keeruliste süsteemide võimalikust käitumisest
- Hea PJAG kasutamisel võib olla üsna kindel, et saadav tulemus on korrektne
- Päris kindel alati olla ei saa. PJAG poolt tekitatud arvudel ei pruugi olla sellist juhuslike arvude omadust, mida konkreetse ülesande puhul vaja läheb
- Näide - leida tõenäosus, et lõigust [0, 1] juhuslikult valitud arv on irratsionaalarv.

Aine läbimine

- 20 punkti I kontrolltöö (kodune). Lävend 10
- 20 punkti II kontrolltöö (praktikum). Lävend 10
- 15 punkti kodutööd
- 45 punkti eksam (kirjalik)

Pseudojuhuslike arvude generaatorid

- Tavalähenemine:
  - Genereerime (pseudo)juhuslikke arve ühtlasest jaotusest $U(0,1)$
  - teisendame neid nii, et tulemus oleks soovitud jaotusest

Millised on juhuslikud arvud lõigust (0, 1)?

- Pikemas seerias peaks mõistliku pikkusega osalõikudesse $[a, b]$ sattuvate punktide osakaal olema lähedane selle lõigu pikkusele $b - a$
- tekitatud arvude jadas ei tohiks olla selgeid, silmaga nähtavaid seaduspärasusi
- ja veel palju omadusi, mis tulenevad kasutamise eesmärgist

Lineaarsed kongruentsed generaatorid (LKG)

$$x_{i+1} = a\,x_i + b \mod m,\ i \geq 0, x_0, a, b \geq 0$$

Pseudojuhuslikud arvud kujul $u_i = \frac{x_i}{m}$

Näide

$a = 5,\ b = 1,\ m = 8$

- $x_0 = 3$
- $x_1 = 0,\ u_1 = 0$
- $x_2 = 1,\ u_2 = 0.125$
- $x_3 = 6,\ u_3 = 0.75$
- $x_4 = 7,\ x_5 = 4, x_6 = 5,\ x_7 = 2,\ x_8 = 3,\ x_9 = 0,\ \ldots$
- Periood on 8

PJAG perioodilisus

Kõik PJAG-d on perioodilised, küsimus on ainult perioodi pikkuses

PJAG üldine tööprintsiip:

1. Lähtesta generaator algseisundisse S_0, $i = 1$
2. Leia uus seisund $S_i = f(S_{i-1})$
3. Väljasta juhuslik suurus $U_i = g(S_i)$
4. Suurenda i väärtust: $i \leftarrow i + 1$ ja jätka punktist 2.

Seisundi salvestamiseks lõplik mälumaht, seega maksimaalse tsükli pikkus on erinevate seisundite arv

Näide:

$a = 5,\ b = 1,\ m = 9$

- $x_0 = 5$
- $x_1 = 8,\ u_1 = 0.8888889$
- $x_2 = 5,\ u_2 = 0.5555556$
- $x_3 = 8,\ u_3 = 0.8888889$
- $x_4 = 5,\ x_5 = 8, x_6 = 5,\ x_7 = 8,\ x_8 = 5,\ x_9 = 8,\ \ldots$
- Periood on 2

Maksimaalse perioodiga LKG-d

Teoreem. Lineaarse kongruentse meetodi korral saavutatakse tsükli maksimaalne pikkus m parajasti siis, kui on täidetud järgmised tingimused:

1. suurim ühistegur $\mathrm{SYT}(b, m) = 1$
2. kui m jagub algarvuga p, siis $(a - 1)$ jagub p-ga
3. kui m jagub 4-ga, siis $(a - 1)$ jagub 4-ga

Eelduste kontroll

- $a = 5,\ b = 1,\ m = 8$
  - eeldused täidetud
- $a = 5,\ b = 1,\ m = 9$
  - teine eeldus ei ole $p = 3$ korral täidetud
- Kuidas saaks parandada teist generaatorit?

Näide

$a = 4,\ b = 1,\ m = 9$

- $x_0 = 5$
- $x_1 = 3,\ u_1 = 0.3333333$
- $x_2 = 4,\ u_2 = 0.4444444$
- $x_3 = 8,\ u_3 = 0.8888889$
- $x_4 = 6,\ x_5 = 7, x_6 = 2,\ x_7 = 0,\ x_8 = 1,\ x_9 = 5,\ \ldots$
- Periood on 9

Multiplikatiivne generaator

- LKG, kus $b = 0$
- Maksimaalne tsükli pikkus $m - 1$. Tingimused:
  - *malgarv*
  - a on algjuur, st iga $m - 1$ algteguri p korral $a^{(m-1)/p}$ ei jagu arvuga m

Tsükli pikkus ja PJAG headus

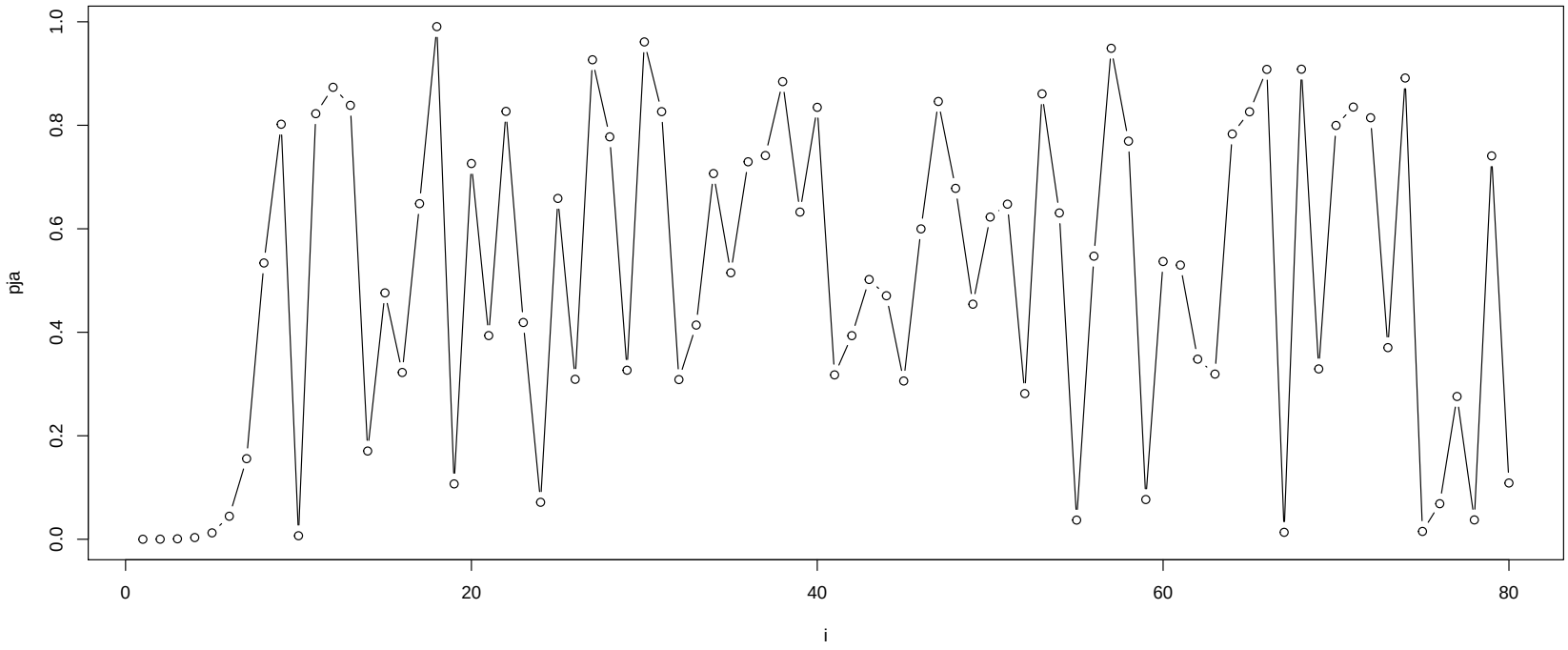
Pikk tsükkel ei tähenda, et generaator oleks hea

$a = 1,\ b = 1,\ m$ kuitahes suur ...

Näited LKG-dest

Nimi	a	b	m
RANDU	65539	0	2^{31}
MinSTD	7^5	0	2^{31} -1
SAS (UNIFORM)	397204094	0	2^{31} -1
Visual Basic (ver $<=$ 6)	1140671485	12820163	2^{24}
MMIX	6364136223846793005	1442695040888963407	2^{64}

Näide pseudojuhuslikest arvudest (RANDU)



Alternatiivid, täiendused

I Kombineeritud LKG-d

Perioodi pikkus oluline, kui simulatioonid kasutavad palju juhuarve

Kasutame mitut generaatorit koos, et tekitada juhuarve

Näiteks LKG(5,1,8) ja LKG(4,1,9), seemneks 1

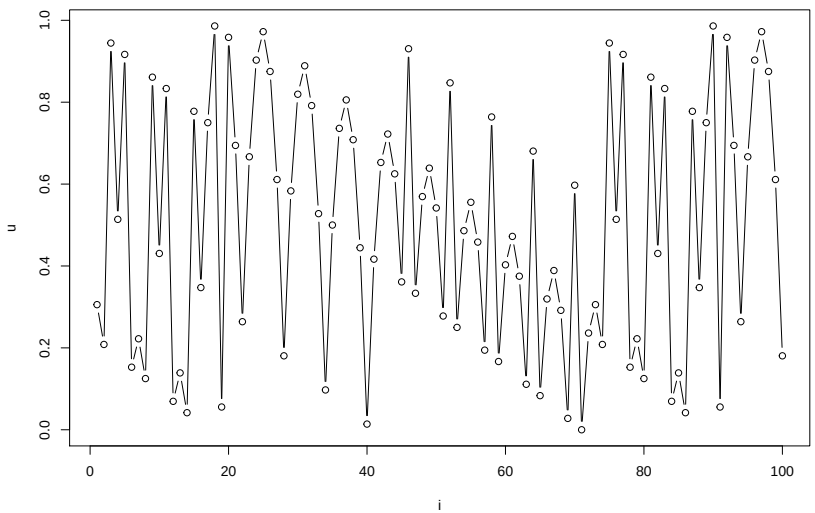
$$x_i = (5 \cdot x_{i-1} + 1) \mod 8$$

$$y_i = (4 \cdot y_{i-1} + 1) \mod 9$$

$$u_i = \left(\frac{x_i}{8} + \frac{y_i}{9}\right) \mod 1$$

Tulemus

```
n=100
x=LKG(n,seeme=1,a=5,b=1,m=8)
y=LKG(n,seeme=1,a=4,b=1,m=9)
u=(x+y) %% 1
i=1:n
plot(i,u,type="b")
```



Periood on $8 \cdot 9 = 72$

Whichman-Hill generaator

$$x_i = (171 \cdot x_{i-1}) \mod 30269$$

$$y_i = (172 \cdot y_{i-1}) \mod 30307$$

$$z_i = (170 \cdot z_{i-1}) \mod 30323$$

$$u_i = \left(\frac{x_i}{30269} + \frac{y_i}{30307} + \frac{z_i}{30323} \right) \mod 1$$

Tegelikult samaväärne LKG-ga juhul $a = 16555425264690$, $b = 0$, $m = 27817185604309$, aga lihtsam korrektselt tööle saada.

II Multirekursiivsed generaatorid (MRG)

Multiple-Recursive Generators

$$x_i = (a_1 x_{i-1} + \ldots + a_k x_{i-k}) \mod m, \; i \geq k$$

kus

$$0 \leq x_0, \ldots, x_{k-1}, a_1, \ldots, a_k < m$$

Pseudojuhuslikud arvud vahemikus 0..1 saadakse valemiga

$$u_i = \frac{x_i}{m}$$

Võimalikke erinevaid seisundeid m^k.

Saab ka kombineerida (vt L'Ecuyer generaator MRG32k3a)

Viivisega Fibonacci generaatorid

Fibonacci arvud

$$f_i = f_{i-1} + f_{i-2},\ i \geq 2,\ f_0 = f_1 = 1$$

Vähe arvutusi (üks tehe)

Sarnane kuju, erinevad nihked: $X_i = (x_{i-p} + x_{i-q}) \mod m$

Näide: Knuth-TAOCP-2002

$$x_i = (x_{i-37} + x_{i-100}) \mod 2^{30}$$

Periood umbes 2^{129}

Välistava või tehe

Arvutid armastavad kahendsüsteemi

Iga täisarvu võib esitada kahendsüsteemis

$$69_{10} = 1000101_2$$

Välistava või tehe (*eXclusive or*, ehk Xor)

X\ Y	True	False
True	False	True
False	True	False

Kui asendada True=1, False=0, siis saab kirjutada

$$a \text{ xor } b = (a + b) \mod 2$$

Bitiviisiline välistav või

Kui vaadelda arve bittide vektorina ja leida kahest arvust uus arv, võttes komponentide haaval xor tehte, saame uue tehte täisarvude vahel

Tähistame $\oplus$

$$69_{10} \oplus 7_{10} = 1000101_2 \oplus 0000111_2 = 1000010_2 = 66_{10}$$

Mersenne Twister

R vaikegeneraator

$$x_i = x_{i-m} \oplus (g(x_{i-n}, x_{i-n+1})A),$$

kus g paneb kokku uue w-bitise arvu kahe varem genereeritud sama pika arvu erinevatest osadest ning (tulemust vaatleme reavektorina) ning A on spetsiaalse struktuuriga maatriks (ehk lineaarteisendus)

Täpsemalt saab uurida nt Wikipedia vastavast artiklist https://en.wikipedia.org/wiki/Mersenne_Twister

PJAG salakirjade jaoks

Tugevamad nõuded: Kui teame teatud arvu genereeritud väärtuseid ja generaatori algoritmi, ei tohi olla võimalik leida järgmisi väärtuseid

Blum-Blum-Shub generaator:

$$x_i = x_{i-1}^2 \mod m$$

kus $m = p \cdot q$, p ja q on suured raskestiaimatavad algarvud, mille jääk jagamisel 4-ga on 3 (nn Blum'i algarvud)

näiteks: p = 126765060022822940149670398151 9, q = 126765060022822940149670431835 9

Väljastatakse $u_i = x_i \mod 2$, st bitijada.