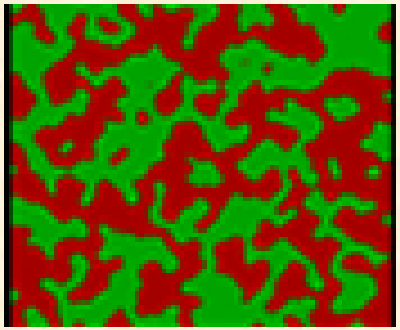
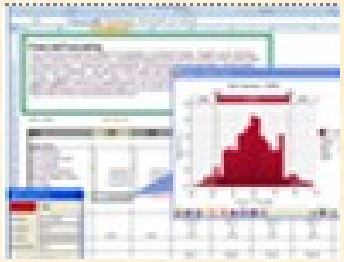
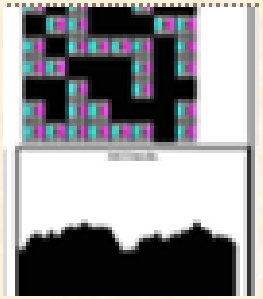
Véletlenszámok

Véletlenszámok



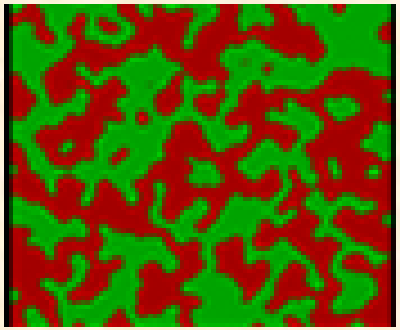


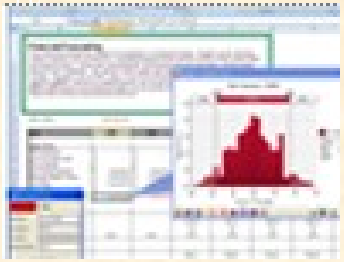


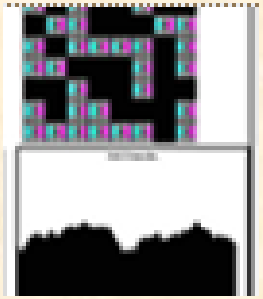
Valószínűség-számítási alapfogalmak:

- Esemény, elemi esemény
- Gyakoriság, relatív gyakoriság, valószínűség
- Eloszlás, eloszlásfüggvény, sűrűségfüggvény, függetlenség
- Várható érték, szórásnégyzet

Véletlenszámok



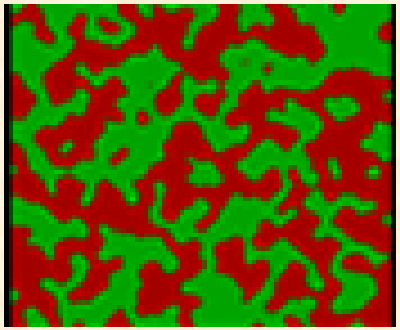


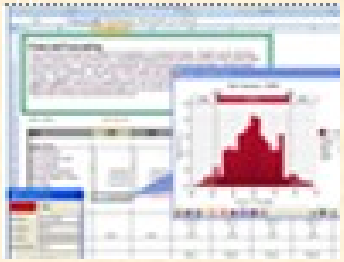


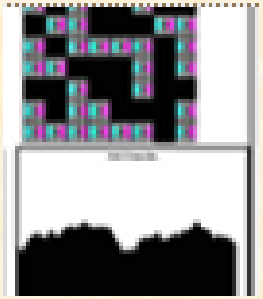
Követelmények:

- minden lehetséges kimenetele előbb-utóbb bekövetkezzen
- az előzőekből ne lehessen következtetni a következőre
- szokásos problémái: periodikus, illetve elfajulhat

Véletlenszámok



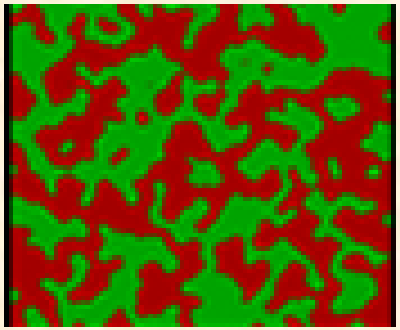


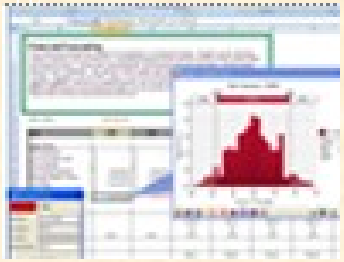


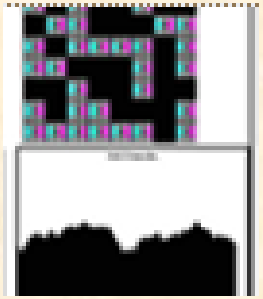
Megvalósítás:

- V_0 kezdőszám választása
- $V_{n+1} := f(V_n)$
- $0 \le V_i < M$ egész számok
- kezdőszám ne legyen megismételhető – belső óra használata
- miért nem jó az óra általában véletlenszám készítésre?

Véletlenszám előállítási módszerek







Négyzetközép módszer

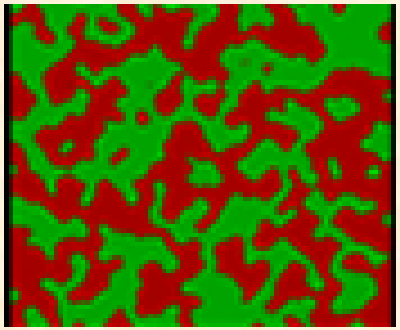
- v_0 :=tetszőleges K jegyű egész szám
- v_{n+1}:=v_n*v_n középső k számjegye

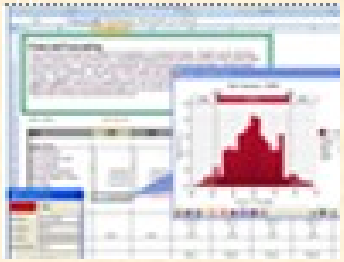
Nem túl gyors; egy ideig véletlenszerűként viselkedik, de utána általában rövid ciklusba áll be: pl. 20 bites számok esetén csak 13 különböző ciklus van, és ezek közül a leghosszabb 142 hosszú. (Zempléni András)

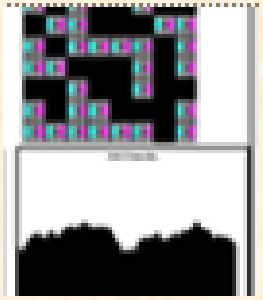
Szorzatközép módszer

- v_0 :=tetszőleges K jegyű egész szám
- v_{n+1}:=A*v_n+B középső k számjegye

Véletlenszám előállítási módszerek







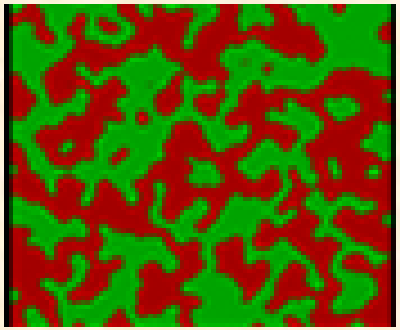
Szorzatközép módszer

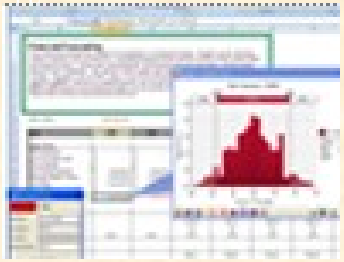
```
Program:
  Be: R0; A:=11; B:=53
  Ciklus amíg szükséges
    Ki: R0
    R:=egészrész((R0*A+B)/10)
    R0:=R-100*egészrész(R/100)
  Ciklus vége
Program vége.
```

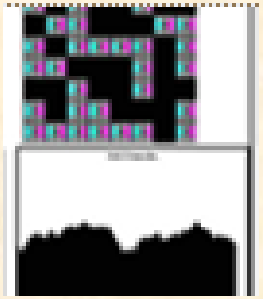
Ha pl. R0=73, akkor ezt kapjuk:

73, 85, 98, 13, 19, 26, 33, 41, 50, 60, 71, 83, 96, 10, 16, 22, 29, 37, 46, 55, 65, 76, 88, 2, 7, *13, 19...*

Véletlenszám előállítási módszerek





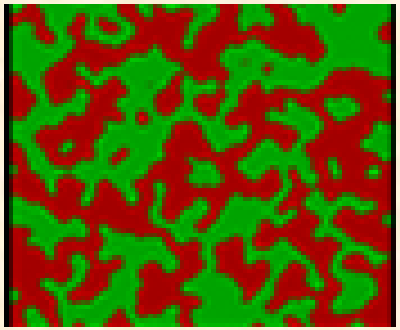


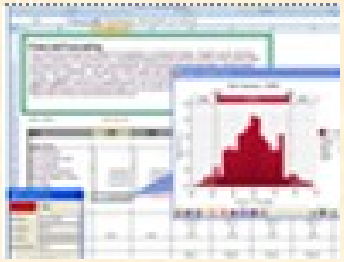
Lineáris kongruencia módszer

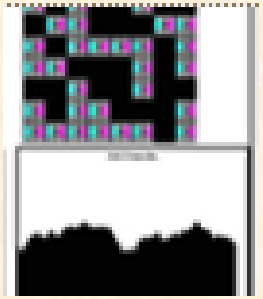
- v_0 :=tetszőleges egész szám
- v_{n+1}:=(a*v_n+c) mod m

Állítás: Ha $m=2^k$, a=4*x+1, (c,m)=1 (és m prímosztói a–1-nek is prímosztói) , akkor m lesz a periódushossz

Véletlenszám előállítási módszerek



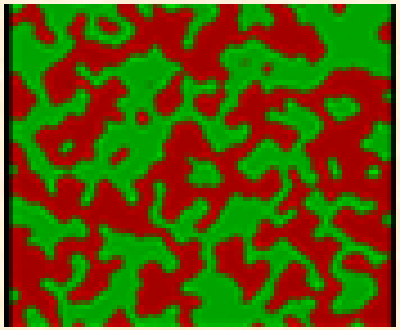


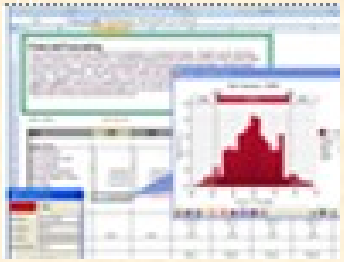


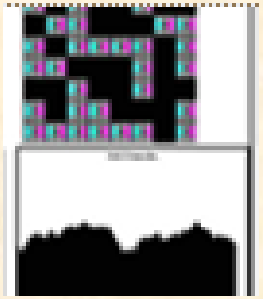
Nemlineáris kongruencia módszer

- $v_{n+1}:=f(v_n) \bmod m$ képletben f nemlineáris függvény,
- $v_{n+1}:=f(v_n...v_{n-k}) \bmod m$ képletben f több korábbi értéktől függ, …

Véletlenszám előállítási módszerek



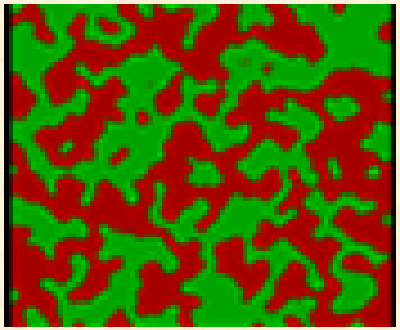


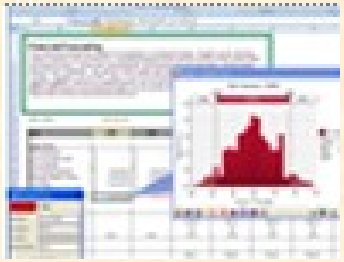


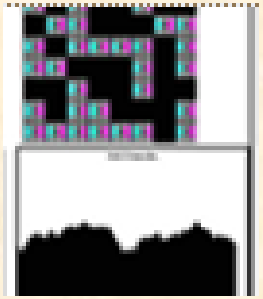
Megjósolhatóság kérdése

- v_0 :=nem ismert
- a,c nem ismert
- m nem ismert?
  - x_i:=v_i/m valós szám!
  - ha $0 \le v_i < m$, akkor $0 \le x_i < 1$!

Véletlenszám előállítási módszerek

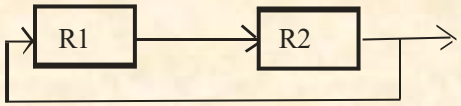




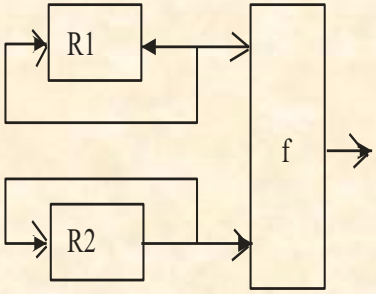


Kombinált módszerek

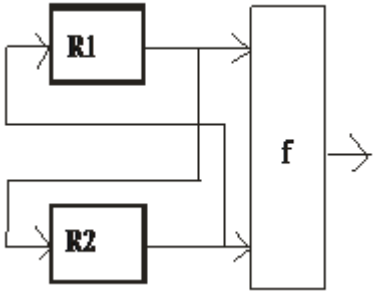
- soros kapcsolás



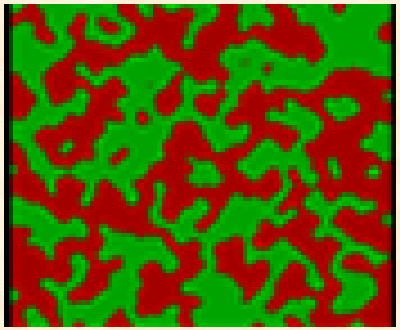
- párhuzamos kapcsolás

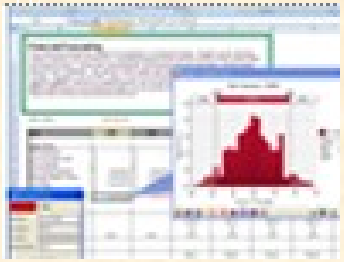


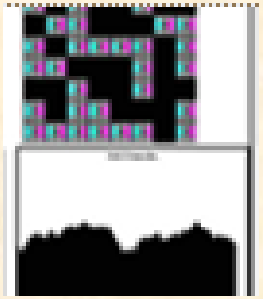
- visszacsatolásos kapcsolás



Véletlenszám előállítási módszerek



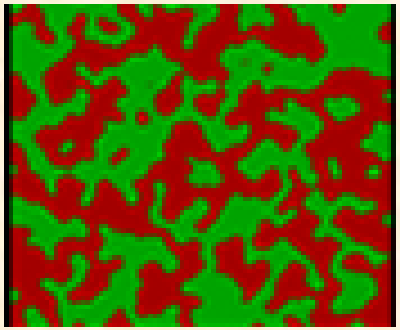


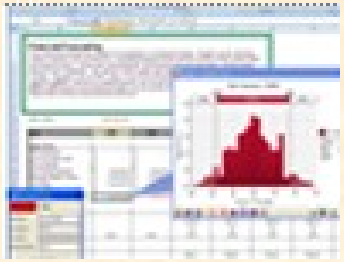


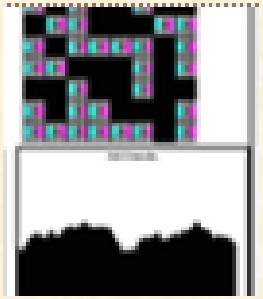
Kombinált módszerek

- Az f függvény megvalósítási lehetőségei
  - speciális művelet (pl. bitenkénti kizáró vagy) a 2 véletlenszám között
  - zavarás
  - keverés
  - egyik a másik számaiból választ
  - egyik a másik véletlen tagjait helyettesíti
  - …

Véletlenszámok ellenőrzése





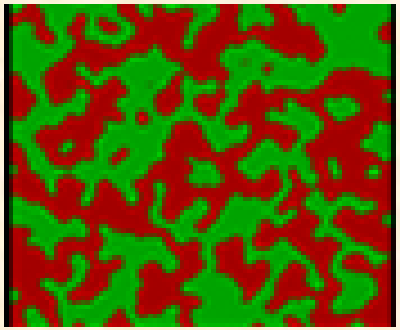


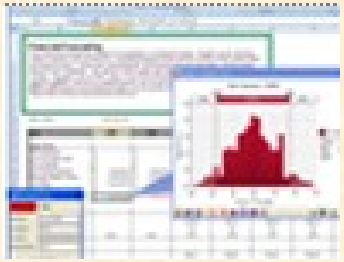
Mit nevezünk véletlennek

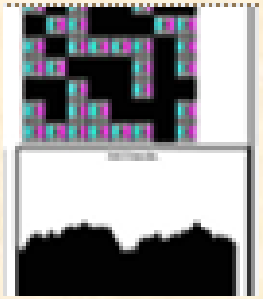
- 1-egyenletes – a v_i véletlenszámok a [0,M) intervallum bármely [a,b) részintervallumába esés valószínűsége csak az intervallum hosszától függ: $P(a \le v_i < b) = b-a$
- 2-egyenletes – a (v_i, v_{i+1}) véletlenszám párok a ([0,M), [0,M)) négyzet bármely ([a,b),[c,d)) résztéglalapjába esés valószínűsége csak a téglalap területétől függ:

$$P(a \le v_i < b,\ c \le v_{i+1} < d) = (b-a)*(d-c)$$

Véletlenszámok ellenőrzése







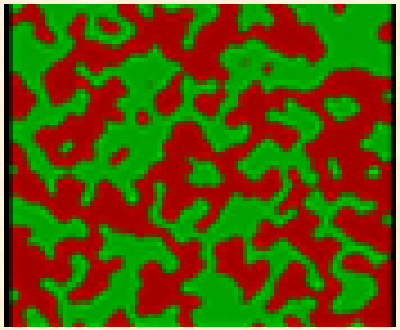
Mit nevezünk véletlennek

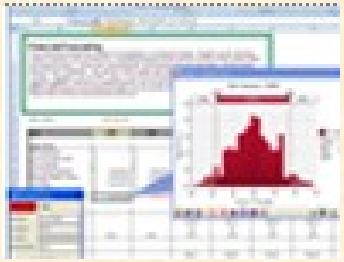
- K-egyenletes – a $(v_i,..v_{i+k-1})$ véletlenszám párok a ([0,M).. [0,M)) K-dimenziós test bármely $([a_1,b_1)\ldots[a_K,b_K))$ K dimenziós résztestébe esés valószínűsége csak a résztest méretétől függ:

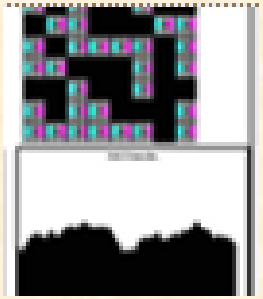
$$P(a_1 \le v_i < b_1, \ldots, a_K \le v_{i+K-1} < b_K) = \\ = (b_1-a_1)*\ldots(b_K-a_K)$$

- ∞-egyenletes – minden K-ra K-egyenletes

Véletlenszámok ellenőrzése







Módszerek véletlenszám sorozatra

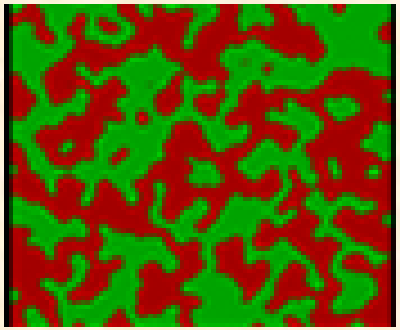
- Futampróba
  növekvő és csökkenő szakaszok átlagos hossza
- 1-, 2-egyenletesség vizsgálat

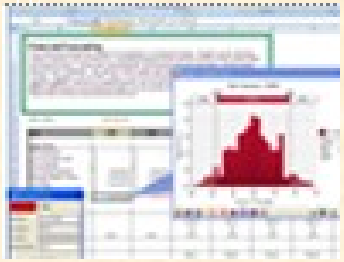
Módszerek véletlenszámjegy sorozatra

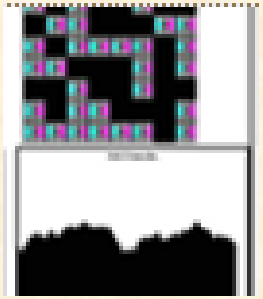
(n darab m-jegyű véletlenszámra $v_{1,1},\ldots,v_{1,m},v_{2,1},\ldots,v_{n,m}$)

- számjegy gyakoriság vizsgálat
  0,1,...9-es számjegy gyakorisága
- számjegysorozat gyakoriság vizsgálat
  pl. 00,01,...99 számjegypárok gyakorisága

Véletlenszámok ellenőrzése







Módszerek véletlenszámjegy sorozatra

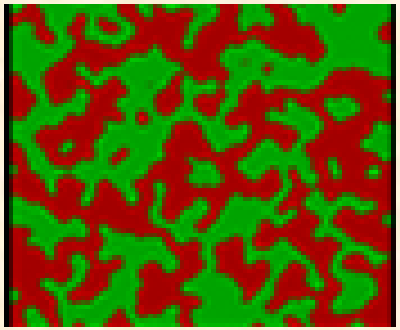
(n darab m-jegyű véletlenszámra $v_{1,1},\ldots,v_{1,m},v_{2,1},\ldots,v_{n,m}$)

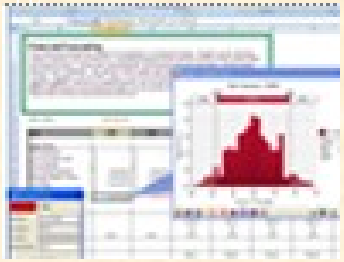
- kombinációk gyakorisága (póker teszt)
- szériavizsgálat

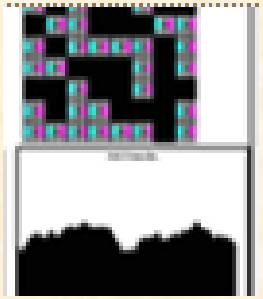
  x,xx,...,xxxxx soroztak gyakorisága minden számjegyre
- hézagpróba

  x...x távolságok gyakorisága minden számjegyre

Véletlenszámok







Megvalósítás programozási nyelvekben:

- V_0 kezdőszám választása – a program legelején egyszer hívandó eljárás vagy függvény (lehet paraméter nélküli – ekkor a belső órából veszi a kezdőértéket, lehet paraméteres belső órával vagy konstanssal – utóbbi esetben a sorozat megismételhető, mert ugyanazzal a kezdőszámmal kezd)
- $V_{n+1} := f(V_n)$ – paraméter nélküli függvény (valós [0,1)-beli vagy egész [0,X]-beli érték), lehetnek paraméteres változatok is (véletlen(N), véletlen(a..b), ...)