

1. Public offices

2. Monte Carlo Method

3. Metropolis algorithm

4. Many particle systems # 10 <sup>30</sup>.

5. Kolmogorov Discrepancy  $D_N \sim c\sqrt{N'}$

6. Dynamical Systems  $T^t x_0 \rightarrow x_t$

7. Classification of Dynamical Systems:

K-systems, Entropy.

8.  $D_N(T)$ ;  $C_0 = 1/h(T)$

9. High Dimensional K-systems

10. Period of Generator on Galois field

$$C = p^\frac{d}{p-1}/p-1.$$

11. Examples

$$p = 2^{61} - 1 \quad d = 256$$

$$C \approx 2^{15000}$$

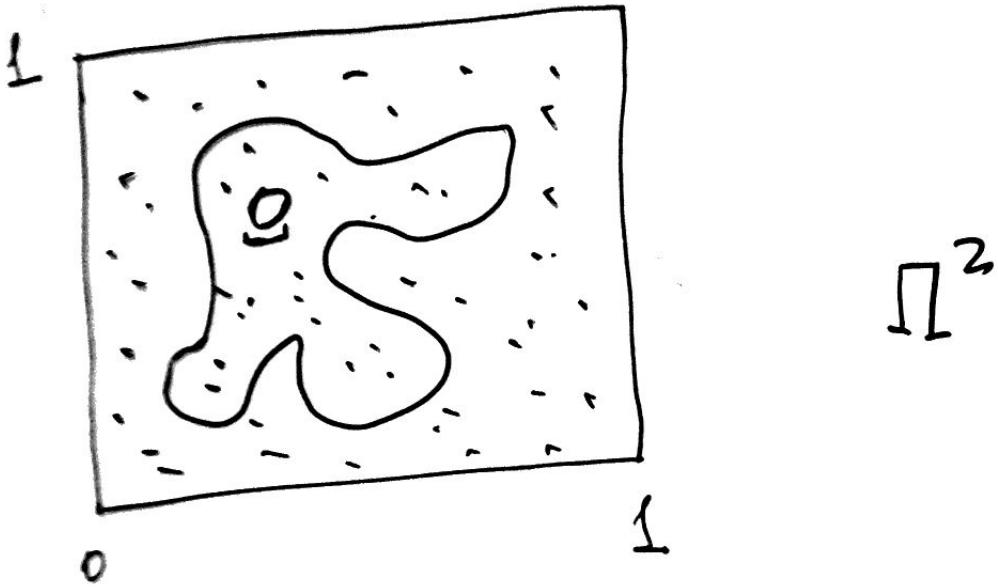
12.

## Publications.

1. J. Comp. Phys. 97 (1991) 566; Preprint EPI-1986
2. J. Comp. Phys. 97 (1991) 573; Preprint EPI-1986.
3. Preprint EPI-1986 „Sinai Billiards as Pseudorandom number generators”
4. Int. J. Mod. Phys. C 7 (1996) #3 „K-system generators on Galois field”.
5. F. James, Chaos, Solitons & Fractals 6 (1995) 221 „Chaos and Randomness”
6. M. Lüscher „A portable high-quality random number generator ...”  
Comp. Phys. Comm. 79 (1994) 100
7. F. James „RANLUX: A Fortran implementation of RNG” Comp. Phys. Comm 1994

In Yerevan: collaboration was with  
N. Akopyan - at DESY now.

# Monte Carlo method



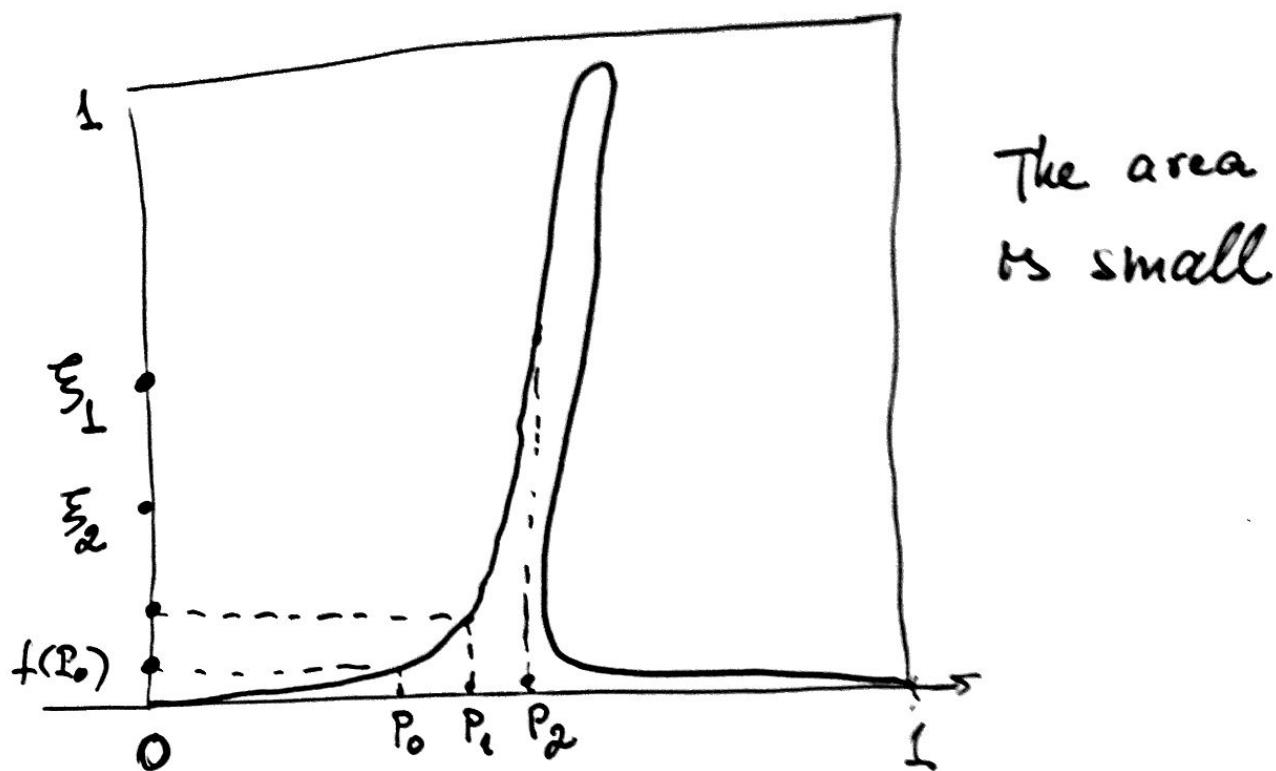
The area of  $\Omega$  ?

In probability theory :

$$\xi \in \Pi^2 \quad p(\xi) = 1$$

$$\text{Area } \Omega = \frac{\# \text{ inside } \Omega}{N}$$

# Metropolis algorithm.



$$P \in [0, 1] \quad \xi \in [0, 1]$$

take  $P_1$  and  $\xi_1$  and compare

$$f(P_1) \quad \xi_1$$

if  $f(P_1) < \xi_1$ , then stay at  $P_1$  and generate  $P_2$  and  $\xi_2$

if  $f(P_2) > \xi_2$ , then jump to  $P_2$ . and so on . . .



$$\rho(P) = f(P)$$

$$\int_{\Pi} f(P) dP = \frac{1}{N} \sum_{i=0}^{N-1} P_i$$

$$\int_{\Pi} f(P) \cdot g(P) dP = \frac{1}{N} \sum_{i=0}^{N-1} g(P_i)$$

$$Z(\beta) = \int e^{-\beta V(x_1, \dots, x_N)} dx_1 \dots dx_N$$

$$D=3 \quad N = 10^{30}$$

$$\rho = e^{-\beta V(x_1, \dots, x_N)}$$

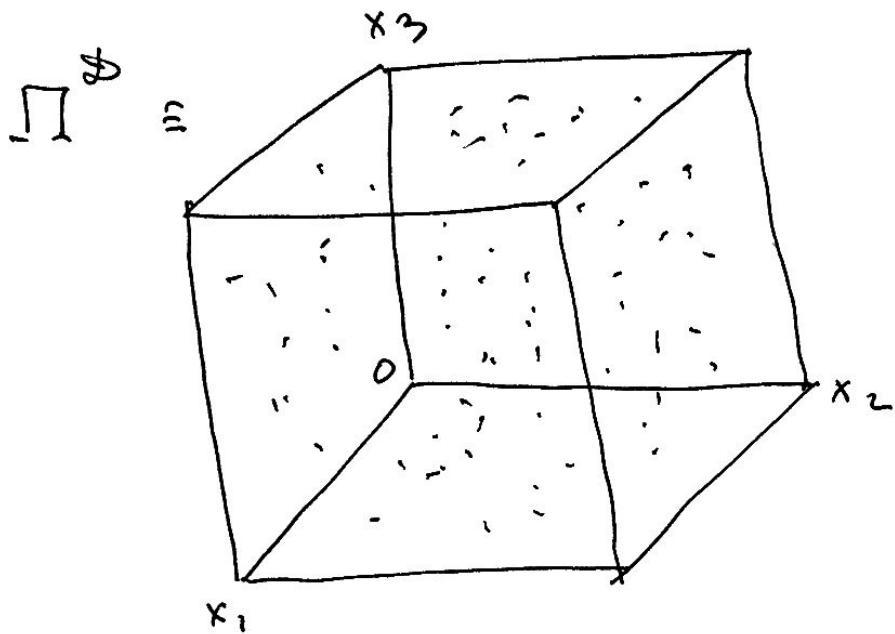
3D Ising	1979	Parisi
	1985	Mezard

# K-system generator of Pseudorandom Numbers.

$P_0, P_1, P_2, \dots, P_N$

$$P = (x_1, x_2, \dots, x_g)$$

$$0 \leq x_i \leq 1.$$



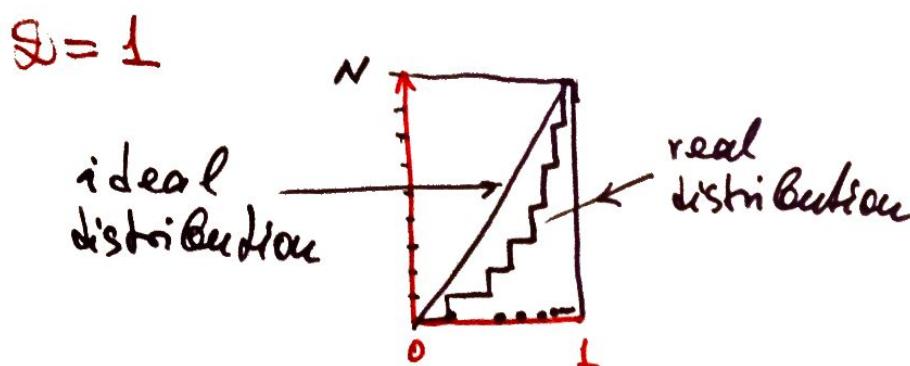
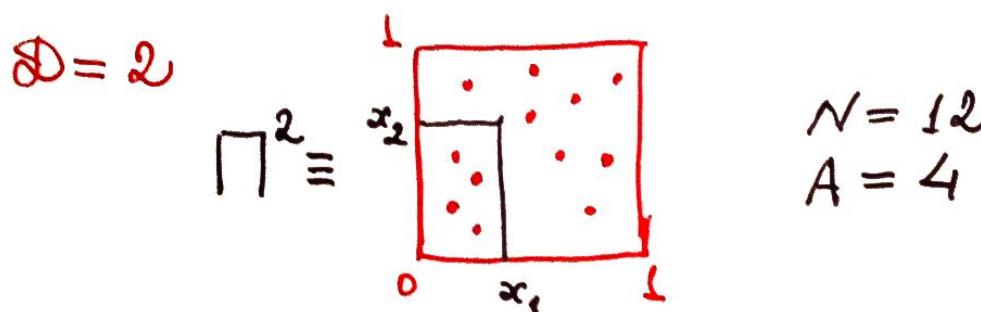
Quality of pseudorandom numbers?

# Kolmogorov discrepancy $D_N$

$$D_N(P_0, \dots, P_{N-1}) = \sup_{\{P\}} |N \cdot x_1 \dots x_N - A|$$

$A$  - is number of points  $P_i$  with coordinates  
 $0 \leq x_1^{(i)} \leq x_1; \dots \dots ; 0 \leq x_N^{(i)} \leq x_N$

$N \cdot x_1 \dots x_N$  - is the number of points for ideal uniform distribution.



Theorem.

$$\left| \frac{1}{N} \sum_{k=0}^{N-1} f(P_k) - \int f(P) dP \right| \leq \text{const. } \frac{D_N}{N}$$

$D_N$  - estimates a maximal deviation of real distribution of points from ideal one.  $D_N \leq N$ .

One should generate sequence  $P_k$ , so that  $D_N$  would grow as slowly as possible.

### Dynamical origin of $P_k$

- a) For random quantity  $\xi$ ,  $p(\xi) = 1$ , then by central limiting theorem

$$D_N(\xi) \approx \sqrt{N'}$$

so

$$\left| \frac{1}{N} \sum_{k=0}^{N-1} f(P_k) - \int f(P) dP \right| \leq \text{Const} \frac{1}{\sqrt{N'}}$$

- b) trajectory of dynamical system  $T$

$$P_1 = T P_0, \quad P_2 = T P_1 = T^2 P_0, \dots, \quad P_{N-1} = T^{N-1} P_0$$

and  $\Pi^D$  as the phase space of the dynamical system  $T$ , Liouville theorem should holds!

The rate of convergence is provided by the dynamical properties of a system  $T$

$$\left| \frac{1}{N} \sum_{k=0}^{N-1} f(T^k P_0) - \int f(P) dP \right| \leq \text{Const.} \frac{D_N(T)}{N}$$

How to get the best rate of convergence?  $D_N(T)$

1. Area preserving map of the phase space  $M$

$$M \xrightarrow{T^t} M \quad T^t A = A_t$$
$$T^t x_0 = x_t$$

in classical mechanics  $x = \begin{pmatrix} q \\ p \end{pmatrix}$ .

2. Classification of the map.

i) ergodic if

$$\lim_{t \rightarrow \infty} \frac{1}{t} \int dt \mu[T^t A \cap B] = \mu[A] \cdot \mu[B].$$

ii) mixing if

$$\lim_{t \rightarrow \infty} \mu[T^t A \cap B] = \mu[A] \cdot \mu[B]$$

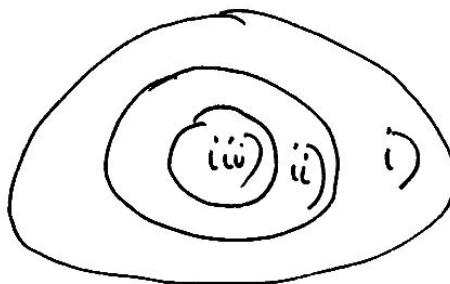
iii) n-fold mixing

$$\lim_{t_1 \dots t_n \rightarrow \infty} \mu[A_0 \cap T^{t_1} A_1 \cap T^{t_2+t_1} A_2 \cap \dots \cap T^{t_n+\dots+t_1} A_n]$$

$$= \mu[A_1] \dots \mu[A_n].$$

There is hierarchy of systems

$$\text{iii)} \supset \text{ii)} \supset \text{i)}$$



iv)  $n \rightarrow \infty$  mixing of any multiplicity

v) K-systems

Split-up  $\xi = \{C\}$ :  $\bigcup_{C \in \xi} C = M$ ,  $C \cap C' = \emptyset$

a)  $\bigvee_{-\infty}^{+\infty} T^t \xi = \xi$  split-up into separate points of  $M$

b)  $\bigwedge_{-\infty}^{+\infty} T^t \xi = \emptyset$  split-up coarsening of  $M$

$$\text{v)} \supset \text{iv)} \supset \text{iii)} \supset \text{ii)} \supset \text{i)}$$

K-systems have mixing of any multiplicity  $n -$

The best statistical property

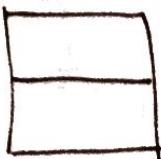
among all dynamical systems!

$h(\tau)$  - called the Kolmogorov entropy

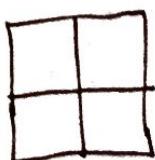
$$0 \leq h(\tau) \leq \infty$$

The entropy of  $\Xi = \{C\}$  is  $H(\Xi)$

$$H = - \sum_{C \in \Xi} \mu[C] \ln \mu[C]$$



$$H = -\frac{1}{2} \ln \frac{1}{2} - \frac{1}{2} \ln \frac{1}{2} = -\ln \frac{1}{2} = \ln 2$$



$$H = -\frac{1}{4} \ln \frac{1}{4} - \frac{1}{4} \ln \frac{1}{4} \dots = -\ln \frac{1}{4} = 2 \ln 2$$



$$\begin{aligned} H &= -\frac{1}{3} \ln \frac{1}{3} - \frac{2}{3} \ln \frac{2}{3} = -\ln \frac{1}{3} - \frac{2}{3} \ln 2 = \\ &= \ln 3 - \frac{2}{3} \ln 2 \end{aligned}$$

if many splits  $\Xi_1, \dots, \Xi_2, \dots$

$$H(\bigvee \Xi_\alpha) = - \sum \mu[\bigvee_\alpha C_\alpha] \ln \mu[\bigvee_\alpha C_\alpha]$$

$$T^{t=1} = T$$

$$\xi, T\xi, T^2\xi, \dots$$

$$H_n(T, \xi) = H(\xi \vee T\xi \vee T^2\xi \dots \vee T^n\xi)$$

$$h(T) = \sup_{\xi} \lim_{n \rightarrow \infty} \frac{1}{n} H(\xi \vee T\xi \vee \dots \vee T^n\xi)$$

$H_n(T, \xi)$  - quantity of information by the time  $t = n$ .

$h(T, \xi)$  - information per unit time.

Another definition  $f \in L_2(\mu)$

$$U^t \cdot f(x) = f(T^t x)$$

$U^t$  as one parameter unitary operator, all  $|\lambda_i| = 1$ .

i) ii) ... vi) - are spectral properties.  
countable-multiple Lebesgue

# Mixing, n-fold mixing and K-systems

(property  
of  
relaxation)  $\rightarrow$  (to uniform  
distribution)

Relaxation of K-systems is most rapid because of their exponential instability.

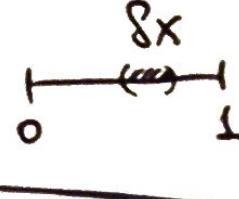
(Slow growth of  
free discrepancy)  $\equiv$  (quick relaxation)  
 $D_N(T)$  of dynamical system T

$$\text{Exp.} \quad P_K = r P_{K-1} \quad \text{mod } 1$$

$$R_N = \frac{\langle (P^{L+N} - \langle P^{L+N} \rangle)(P^L - \langle P^L \rangle) \rangle}{\langle (P^L - \langle P^L \rangle)^2 \rangle} \sim e^{-N \ln r}$$

Scale of correlation splitting

$$C_0 = \frac{l}{\ln r}$$

$$\left( \begin{array}{l} \text{time of uniform fill} \\ \text{(of } [0,1] \text{ from } 8x \end{array} \right) = C_0 \ln \left( \frac{1}{8x} \right)$$


Exp. Anosov K-systems.

$$P_k = T P_{k-1} \quad T = \| \alpha_{k+1} \|$$

$$\alpha) \det \| \alpha_{k+1} \| = 1$$

$$\beta) |\lambda_k| \neq 1$$

entropy  $h(T) = \sum_{|\lambda| > 1} \ln |\lambda_k|$

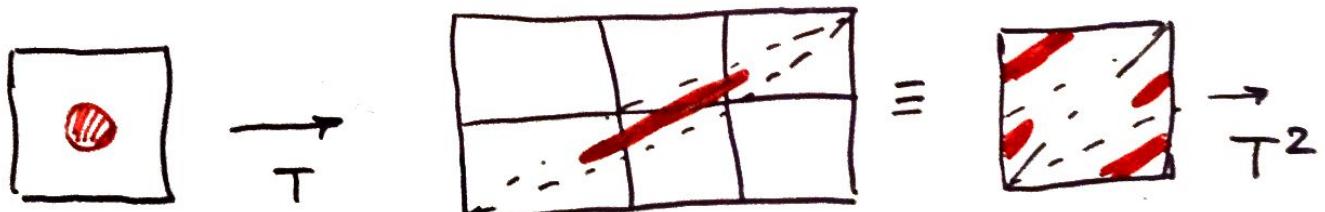


correlation splitting time

$$C_0 = \frac{1}{h(T)} = \frac{1}{\sum_{|\lambda| > 1} \ln |\lambda_k|}$$

$$d=2$$

$$\begin{pmatrix} x_1 \\ x_2 \end{pmatrix}_k = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}_{k-1}$$



$$\lambda_{1,2} = \frac{3 \pm \sqrt{5}}{2}$$

$$h(T) = \ln \frac{3 + \sqrt{5}}{2}$$

# High dimensional K-systems.

$$T_2 = \begin{vmatrix} 2 & 1 \\ 1 & 1 \end{vmatrix} \quad T_3 = \begin{vmatrix} 2 & 2 & 1 \\ 1 & 2 & 1 \\ 1 & 1 & 1 \end{vmatrix}$$

$$T_4 = \begin{vmatrix} 2 & 3 & 4 & 1 \\ 1 & 2 & 2 & 1 \\ 1 & 1 & 2 & 1 \\ 1 & 1 & 1 & 1 \end{vmatrix} \dots \quad T_d = \begin{vmatrix} 2 & 3 & 4 & \dots & d & 1 \\ 1 & 2 & 3 & \dots & d-1 & 1 \\ 1 & 1 & 2 & \dots & d-2 & 1 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 1 & 1 & 1 & \dots & 2 & 1 \\ 1 & 1 & 1 & \dots & 1 & 1 \end{vmatrix}$$

$$T_{120} \quad \lambda_{\max} = 1539.9 \quad h(T) = 108.9$$

$N$	1	2	$\dots$	$10 \times 10^5$
$D_N/\sqrt{N}$	1.714	-	-	3,302
$D_N/\sqrt{N}$	1.233	-	-	1,102

The entropy  $h(\tau)$  defines the number  $\pi(c)$  of periodic trajectories with period less or equal  $c$

$$\pi(c) \rightarrow \frac{e^{h \cdot c}}{h \cdot c}$$

in  $T_{170}$

$$\pi(c) \rightarrow \frac{e^{10^9 \cdot c}}{10^9 \cdot c} !$$

Only periodic trajectories  
can be simulated on a  
computer.

---



## APPENDIX I

# Memoir on the Conditions for Solvability of Equations by Radicals by Evariste Galois

Translated by Harold M. Edwards

## PRINCIPLES

I shall begin by establishing some definitions and a sequence of lemmas, all of which are known.

**Definitions.** An equation is said to be reducible if it admits rational divisors; otherwise it is irreducible.

It is necessary to explain what is meant by the word rational, because it will appear frequently.

When the equation has coefficients that are all numeric and rational, this means simply that the equation can be decomposed into factors which have coefficients that are numeric and rational.

But when the coefficients of an equation are not *all* numeric and rational, one must mean by a rational divisor a divisor whose coefficients can be expressed as rational functions of the coefficients of the proposed equation, and, more generally, by a rational quantity a quantity that can be expressed as a rational function of the coefficients of the proposed equation.

More than this: one can agree to regard as rational all rational functions of a certain number of determined quantities, supposed to be known *a priori*. For example, one can choose a particular root of a whole number and regard as rational every rational function of this radical.

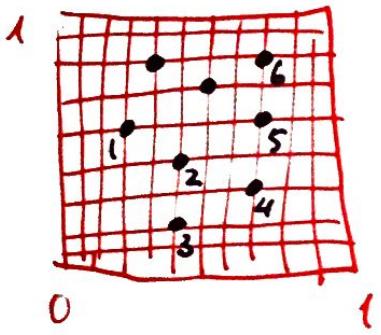
When we agree to regard certain quantities as known in this manner, we shall say that we *adjoin* them to the equation to be resolved. We shall say that these quantities are *adjoined* to the equation.

With these conventions, we shall call *rational* any quantity which can be expressed as a rational function of the coefficients of the equation and of a certain number of *adjoined* quantities arbitrarily agreed upon.

# The periodic trajectories of K-system.

If  $P_0 = \left( \frac{q_1}{p_1}, \frac{q_2}{p_2}, \dots, \frac{q_d}{p_d} \right)$   $T = \|a_{ik}\|$

$\|a_{ik}\|$  are integer and  $q_i, p_i$  also  
then  $P_0 = T^k P_0$  is periodic trajectory  
with period  $\infty$ .



$$0 \leq q_i \leq p$$

rational sublattice

If  $P_0 = \left( \frac{q_1}{p}, \frac{q_2}{p}, \dots, \frac{q_d}{p} \right)$

then trajectory will stay  
on the same sublattice.

The period  $\tau_p$ - on sublattice  $\leq p^d$

$$\frac{q_i^{(k+1)}}{p} = \sum_j a_{ij} \frac{q_j^{(k)}}{p} \pmod{1}$$

is equivalent to

$$q_i^{(k+1)} = \sum_j a_{ij} q_j^{(k)} \pmod{p}$$

If  $p$  is prime number then

$q_i$  - belongs to Galois field  $GF[p]$   
 $\{0, 1, \dots, p-1\}$

---

$$GF[3] \quad \{0, 1, 2\} \quad g = 2 \quad p = 3$$

$$g=2 \quad g^2=4=1$$

$$GF[5] \quad \{0, 1, 2, 3, 4\} \quad g = 3 \quad p = 5$$

$$g=3 \quad g^2=9=4 \quad g^3=2 \quad g^4=1$$

---

$g$  - is a primitive element of  $GF[p]$

$$g^{p-1} = 1 \quad \text{mod } p.$$

i) If eigenvalue  $\lambda$  of  $\|Q_{ik}\|$  coincides with primitive element  $g$  then maximal period  $\epsilon_p = p-1$ .

ii) If eigenvalue  $\lambda$  coincides with primitive element of quadratic expansion  $GF[\sqrt{p}]$ , then maximal period  $\epsilon_p = p^2 - 1$

$$GF[\sqrt{3}]$$

$$g = 2$$

$$h = \sqrt{2}$$

$$a + b \cdot h$$

$$a, b \in GF[3]$$

$$w = 1 + \sqrt{2}$$

$$w^2 = 2\sqrt{2}$$

$$w^3 = 1 + 8\sqrt{2}$$

$$w^4 = 2$$

$$w^5 = 2 + 2\sqrt{2}$$

$$w^6 = \sqrt{2}$$

$$w^7 = 2 + 2\sqrt{2}$$

$$w^8 = 1$$

$$\zeta_8 = 3^{\frac{2}{7}} - 1 = g$$

$$x^2 - 2 = 0$$

$$x = \sqrt{2}$$

iii) If  $\lambda$  coincide with  $\vartheta$ -dim.  
expansion of Galois field

$GF[\sqrt[d]{p}]$  then for  $\tau_p = p^{\frac{d}{\vartheta}} - 1$

the elements of  $GF[\sqrt[d]{p}]$  have the  
form

$$a + b h + \dots + e h^{\vartheta-1}$$

$$a, b, \dots, e \in GF[p]$$

$h$  - is primitive element of  
 $GF[\sqrt[d]{p}]$ .

The period is:

$$T = \frac{P^N - 1}{P - 1}$$

If we use the largest Mersenne number

$$p = 2^{61} - 1$$

and dimension of the generator  $N=256$

we can get:

$$T \approx 2^{61 \cdot 255} = 2^{15555}$$

In 2013 the largest known prime  
number is:

$$p = 2^{57,885,161} - 1$$

by „Great Internet Mersenne Prime Search“