International Journal of Theoretical Physics, Vol. 27, No. 1, 1988

Example of Order and Disorder: $x_{n+1} = (Ax_n + B) \bmod C$

M. Wolf[1]

Received July 23, 1987

A simple model with discrete dynamics is studied. The behavior of this model is very sensitive to the particular choice of parameters determining the system.

1. In this paper I present a simple model exhibiting very complicated dynamics, which depends very strongly on the particular values of the driving parameters. For some parameters the motion can be ergodic and for others the system can reveal very ordered behavior.

In recent years there has been great interest in deterministic systems displaying irregular dynamics [see, e.g., Lichtenberg and Lieberman (1983), where many examples of such systems are given]. In contrast to the most popular systems, for the description of the proposed model only *natural* numbers are needed.

Section 2 contains a description of the model. Section 3 is devoted to a chaotic motion. Section 4 discussess the regular behavior of the model. Section 5 contains a brief discussion of the intermediate behavior of the model and some remarks.

2. The model is two-dimensional and the "phase space" is discrete: both time and coordinate take natural values. The set of possible positions of the material point (a particle or a "small ball") performing the motion consists of nodes regularly distributed along the circle; see Fig. 1. Let the total number of points on the circle be C; denote them by $0, 1, \ldots, C-1$. The position of the ball at the instant of time n will be denoted by x_n, so $x_n \in \{0, 1, \ldots, C-1\}$. The "dynamics" is given by the following rule: Let

[1] Institute of Theoretical Physics, University of Wroclaw, Wroclaw, Cybulskiego 36, Poland.

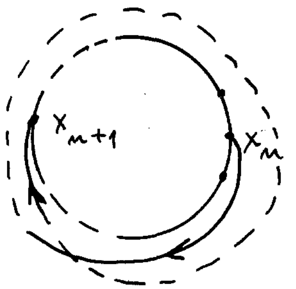

Fig. 1. Illustration of the model.

the moving ball be at the site x_n. During an elementary interval of time a ball shifts by $Ax_n + B$ nodes in, e.g., the clockwise direction. Here A and B are natural numbers smaller then C: $0 < A < C-1$, $0 < B < C-1$. This rule can be written as the following equation of motion:

$$x_{n+1} = (Ax_n + B) \bmod C \tag{1}$$

The particle constrained to the motion described by (1) is "jumping" from the node x_n at the time n to the node x_{n+1} at the time $n+1$. The number q_n of whole laps of the circle is given by

$$q_n = [(Ax_n + B)/C] \tag{2}$$

where the square brackets denote the *Entier* function: $[x]$ is the greatest integer $\leq x$. It turns out that there is a great variety of possible behaviors of the particle, according to the particular values of driving parameters A, B, and C. On one hand, the particle can perform a random walk around the circle. On the other hand, it is possible that the particle will fall after at most *two* jumps into such a node in which it will remain forever, *regardless of the initial value* x_0.

3. The behavior of the particle is fully determined by the properties of the sequence $\{x_n\}_{n=0}^{\infty}$ generated by the iterations (1). First, note that the elements of the sequence $\{x_n\}_{n=0}^{\infty}$ depend on the value x_0 and are natural numbers from the set $\{1, \ldots, C-1\}$. Due to this, the sequence $\{x_n\}_{n=0}^{\infty}$ starting at some index must be periodic, so there exist numbers $\mathcal{N}$ and $\mathbb{T}$ such that

$$x_{n+1} = x_{n+\mathbb{T}} \qquad \forall n > \mathcal{N} \tag{3}$$

It is well known that it is possible to choose parameters A, B, and C such that the period is maximal: $\mathbb{T} = C$. The following theorem asserts when this is possible (Knuth, 1981):

Theorem 1. The period $\mathbb{T}$ of the sequence generated by the iterations of equation (1) is equal to C if and only if:

(i) B and C are mutually prime.
(ii) $A-1$ is a multiple of each prime p, a divisor of C.
(iii) $A-1$ is a multiple of 4 if C is a multiple of 4.

Integers A, B, and C fulfilling the requirements of the above theorem exist such that the successive x_n are weakly correlated in the statistical sense (Knuth, 1981). In such a case equation (1) is used for the generation of random numbers in computers (of course for great C, e.g., $C = 2^{31} - 1 =$ 2,147,483,647). So, with appropriately chosen A, B, and C the particle will perform a random walk around the circle. This represents disorder in our system: each site of the phase space will be occupied after each C units of time—the motion is ergodic and Poincaré's recurrence theorem holds (with time of recurrence equal to C).

4. Now let us focus on the exactly opposite case, namely let us look for the fixed points of (1). Let us introduce the function

$$f(x) = (Ax + B) \bmod C \tag{4}$$

Now we can write

$$x_{n+1} = f(x_n) \tag{5}$$

The nth element x_n can be expressed by the first one x_0 as in the following superposition:

$$x_n = \underbrace{f \circ f \circ \cdots \circ f}_{n \text{ times}}(x_0) \equiv f^n(x_0) \tag{6}$$

Let x^* denote the fixed point of (4):

$$x^* = f(x^*) \tag{7}$$

The above equation can be written in the following form:

$$x^* = Ax^* + B - Cq^* \tag{8}$$

where

$$q^* = [(Ax^*/ + B)/C] \tag{9}$$

The existence of fixed points of the mapping (4) is equivalent to the existence of integer solutions x^* and q^* of equation (7). The equations of the form

$$ax + by = c \tag{10}$$

where a, b, and c are given integers for which one seeks solutions x, y in integers, are called *Diophantine equations* (e.g., Courant and Robbins, 1947). Such an equation can have a finite number of solutions, infinitely many, or none. As is well known, equation (10) has integer solutions if and only if c is the multiple of the greatest common divisor (GCD) of the numbers a and b. It is common to denote the GCD of a and b as (a, b). As q^* is an integer, equation (8) is an example of a Diophantine equation. Writing (8) in the form

$$Cq^* - (A-1)x^* = B$$

we see that the following lemma holds:

Lemma 1. The necessary condition for the existence of fixed points of the mapping (3) is that B should be a multiple of $(C, A-1)$.

If the condition for the existence of solutions of equation (10) is fulfilled, then the number of different solutions is equal to (a, b) and if one particular solution $(x^{(0)}, y^{(0)})$ is known, then all the remaining ones are given by the formula (Courant and Robbins, 1947)

$$x^{(r)} = x^{(0)} + rb/(a, b)$$
$$y^{(r)} = y^{(0)} - ra/(a, b), \qquad r \in \mathbb{N}$$

Let us assume that $(C, A-1) = d$, so there exist numbers a and c such that $A = ad+1$, $C = cd$. Then for the existence of fixed points we should have by Lemma 1 that $B = bd$. Then it follows that the sequence

$$x_{n+1} = ((ad+1)x_n + bd) \bmod cd$$

will possess d fixed points. Denoting the smallest one by $x^{*(0)}$, we have that all remaining fixed points are given by the formula

$$x^{*(r)} = x^{*(0)} + rc, \qquad r = 0, 1, \ldots, d-1$$

In particular it is possible to have, for the rather pathological choice $A = 1$ and $B = C$, C fixed points, since from

$$x_{n+1} = (x_n + C) \bmod C \qquad (\equiv x_n \bmod C)$$

it follows that $x_{n+1} = x_n$. It is also easy to write down the formula describing the "uniform" motion of the particle along the circle in which the ball shifts by the same number K of nodes in each interval of time:

$$x_{n+1} = (x_n + K) \bmod C$$

Now let us look more closely at the case when only one single fixed point exists. The computer experiments showed that, for a given C, values of A exist such that, *regardless of B, all* x_0 are mapped into a *unique* fixed point after only a *few* iterations of (4). It is natural to consider the fixed point of (4) as an attractor. Each attractor has its own domain of attraction called a *basin*. For the case of natural numbers we take the following definition.

Definition. The basin $\mathscr{B}(x^*)$ of the attractor x^* is the set of initial points $x_0^{(i)}$ $(i = 1, 2, \ldots, b)$ of the sequences (1) for which there exist numbers $\mathscr{N}^{(i)}$ such that

$$f^{\mathscr{N}^{(i)}}(x_0^{(i)}) = x^*$$

Let us remark that for real numbers (continuous case) the fixed point is usually reached after an infinite number of iterations.

We will confine ourselves to the case when $b = C$, so the basin consists of all natural numbers: $x_0 \in \{0, 1, \ldots, C-1\}$. (It should be noted that $\{0, 1, \ldots, C-1\} = \mathbb{N} \bmod C$, where $\mathbb{N}$ denotes the set of natural numbers.)

Theorem 2. $\mathscr{B}(x^*) = \{0, 1, \ldots, C-1\}$ if and only if there exists a natural number $\mathscr{N}$ such that $A^{\mathscr{N}}$ is divisible by C:

$$(A^{\mathscr{N}} \equiv 0) \bmod C. \tag{11}$$

Proof. First let us remark that the domain of the function (4) can be extended to all real numbers by means of the formula

$$f(x) = Ax + B - C[(Ax + B)/C] \tag{12}$$

The graph of this function consists of segments of a line; see Fig. 2a. The function (12) is periodic with period

$$T = C/A$$

Using the obvious relation

$$(a + kc) \bmod c = a \bmod c \tag{13}$$

one can prove by induction that

$$x_n = f^n(x_0) = \left(A^n x_0 + \frac{A^n - 1}{A - 1} B\right) \bmod C \tag{14}$$

so the superposition of linear functions is still a linear function. Since A is greater than 1, the slope of the successive superpositions of f becomes greater and greater; see Fig. 2b. The period of f^n is given by the formula

$$T^{(n)} = C/A^n$$

i.e.,

$$f^n(x + T^{(n)}) = f^n(x)$$

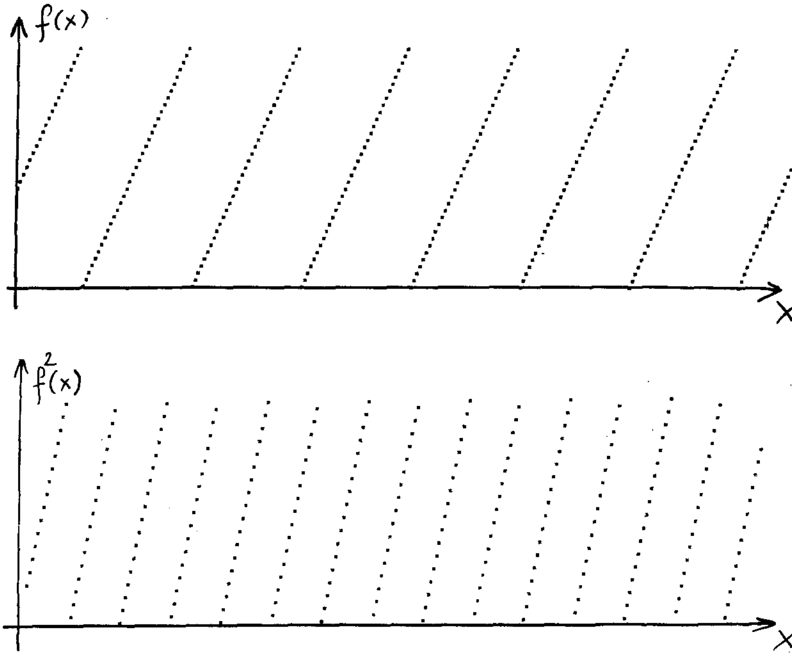

Fig. 2. (a) Graph of the function $f(x) = (2x+26) \bmod 70$. (b) Graph of the second superposition of function $f(x) = (2x+26) \bmod 70$.

For growing n the period decreases. If for some $\mathcal{N}$ it happens that the interval of length 1 contains a multiple of intervals of length $T^{(\mathcal{N})}$,

$$1 = KT^{(N)} = KC/A^N, \qquad K \in \mathbb{N} \tag{15}$$

then

$$f^N(x+1) = f^N(x)$$

In particular, the $\mathcal{N}$th superposition of f will take the same values on all natural numbers, which in turn means that all x_0 are mapped into the fixed point. But from (15) there follows (11), so the existence of a basin consisting of all natural numbers is equivalent to (11). ■

Self-consistency demands that from (11) fulfilled for some $\mathcal{N}$, it should follow that $(A^{\mathcal{N}'} \equiv 0) \bmod C$ for all $\mathcal{N}' > \mathcal{N}$: after reaching the fixed point, successive iterations would not move it. This is indeed so, since writing $\mathcal{N}' = \mathcal{N} + \mathcal{M}$, we have

$$A^{\mathcal{N}'} = A^{\mathcal{M}} A^{\mathcal{N}} = A^{\mathcal{M}} KC = K'C$$

The smallest $\mathcal{N}$ satisfying (11) is equal to the maximal number of iterations needed for turning all x_0 into the fixed point.

Because equation (11) does not involve B, the above consideration explains why the existence of a maximal basin as well as the number of iterations needed for obtaining the fixed point does not depend on the particular value of B. But the value of fixed point depends on B:

Corollary 1. If equation (11) is fulfilled, then the unique fixed point of (4) is given by the formula

$$x^* = \left(\frac{A^n - 1}{A - 1} B\right) \bmod C \tag{16}$$

Proof. Since the $\mathcal{N}$th superposition of f is constant, it is sufficient to put in (14) $x_0 = 0$. Using the property (13), one can easily see that x^* given by (16) satisfies $x^* = f(x^*)$. ■

Corollary 2. If C is prime, then equation (11) does not have integer solutions for A and $\mathcal{N}$.

Proof. The *modulo* operation possesses the following property (Courant and Robbins, 1947):

If c is prime, then from $(ab \equiv 0) \bmod c$ it follows that either $(a \equiv 0) \bmod c$ or $(b \equiv 0) \bmod c$.

Let $\mathcal{N}$ be the smallest integer fulfilling (11). Then, writing

$$(A^{\mathcal{N}} \equiv 0) \bmod C \Leftrightarrow (AA^{\mathcal{N}-1} \equiv 0) \bmod C$$

and applying the above property, we see that either $(A \equiv 0) \bmod C$ or $(A^{\mathcal{N}-1} \equiv 0) \bmod C$. But the first relation is impossible, since $A < C$, and the second relation is impossible by the definition of $\mathcal{N}$, as the smallest integer fulfilling (11). ■

Now let us dwell briefly on the problem when the equation (11) can have solutions. Let us decompose C into primes:

$$C = p_1^{\alpha(1)} p_2^{\alpha(2)} \cdots p_r^{\alpha(r)}$$

where all primes p_i are different. It is easy to see that if at least for one i one has $\alpha(i) > 1$, then taking

$$A = p_1^{\alpha(1)} \cdots p_i^{\alpha(i)-1} \cdots p_r^{\alpha(r)}$$

we can fulfill (11) with $\mathcal{N} = 2$. On the contrary, if $\alpha(i) = 1$ for every i, then (11) has no solutions (Corollary 2 is a special case of this observation). For large C it can be difficult to check whether all $\alpha^{(i)}$ are different from 1. But there is probabilistic information available. It is known (Kac, 1959) that the probability that for a randomly chosen natural number all $\alpha(i) = 1$ is equal to $6/\pi^2 \approx 0.608$. So we see that with probability 0.392 it is possible to find a number C such that there exist numbers A for which the basin of a unique fixed point consists of all natural numbers.

Finally let us remark that from the proof of Theorem 2 it follows that for A and C satisfying (11) the mapping (4) always has a fixed point regardless of the value of B. Lemma 1 tells us that this is possible only when B is divisible by $(A-1, C)$ for *every* B, even B prime, which can happen only if $(A-1, C)=1$. Indeed, we have the following result:

Corollary 3. If there is $\mathcal{N}$ such that $(A^{\mathcal{N}} \equiv 0) \bmod C$, then $(A-1, C)=1$.

Proof. Let us assume that $d=(A-1, C)$. Then there exist numbers a and c such that $A=ad+1$, $C=cd$. By assumption, $A^{\mathcal{N}}=KC$, so using the binomial theorem, we have

$$A^{\mathcal{N}}=1+\binom{\mathcal{N}}{1} ad+\binom{\mathcal{N}}{2} a^2d^2+\cdots+\binom{\mathcal{N}}{\mathcal{N}} a^N d^N = KC$$

and hence

$$d(Kc-\beta)=1 \tag{17}$$

where

$$\beta=\binom{\mathcal{N}}{1} a+\binom{\mathcal{N}}{2} a^2d+\cdots+\binom{\mathcal{N}}{\mathcal{N}} a^N d^{N-1}$$

But since d and $Kc-\beta$ are integers, (17) can only hold if $d=1$ (then also $Kc-\beta=1$, which is a tautology for $d=1$). ■

5. For parameters not fulfilling the assumptions of either Theorem 1 or Theorem 2, there is a variety of intermediate behaviors of the model. Some possible x_0 will fall into the fixed point and other x_0 will fall into limiting cycles. Some examples are given in Figs. 3–5. These figures show the evolution of the set of balls moving around the circle according to the

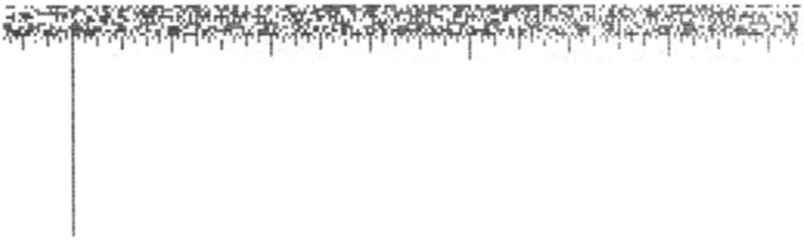

Fig. 3. Example of an attractor with a maximal basin. Sites occupied by the particles are black. Since the initial state was taken disordered, this figure shows how the order emerges from chaos. Here $C=65{,}536=2^{16}$, $A=1154=2\cdot 557$, so all particles fall into the attractor after at most 16 iterations.

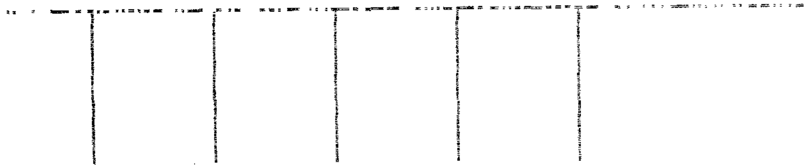

Fig. 4. Here $A = 78$, $B = 33$, $C = 195 = 3 \cdot 5 \cdot 13$. All particles fall after one unit of time either into the 4-cycle (33, 72, 189, 150) or into the fixed point $x^* = 111$.

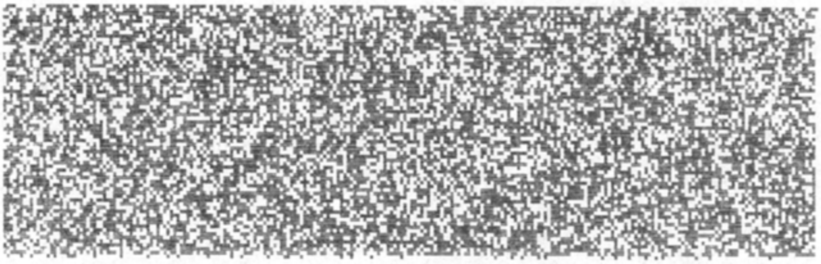

Fig. 5. An example of chaos for A, B, and C fulfilling the conditions of Theorem 1. Here $C = 243 = 3^5$, $A = 16$, $B = 17$. At all times each site is occupied by at most one particle.

rule (1). Let us remark that such a "gas" consists of *noninteracting* particles. On the top of each figure the initial positions of balls are plotted (the time is directed downward). Successive rows correspond to successive time steps in evolution. The starting positions as well as the number of particles were chosen randomly. In the example of Fig. 3 all particles fall into one node, so for A and B fulfilling requirements of Theorem 2 the particles resemble bosons and condense to one state. On the contrary, for A, B, and C fulfilling the requirements of Theorem 1 at all times each site will be occupied by at most one particle and they behave like fermions.

It is also tempting to consider the generalization of (1) corresponding to Brownian motion. Namely the values of A and B can be chosen randomly between 1 and $C-1$ at each instant of time. In this way the particle will perform jumps of random lengths. The inclusion of such noise is now under study, both numerically as well as analytically.

ACKNOWLEDGMENTS

I am very indebted to Prof. J. T. Łopuszański for a careful reading of the manuscript and some useful remarks. I am also grateful to my colleagues for discussions, especially to Drs. A. Górski, T. Nadzieja, and C. Oleksy.

REFERENCES

Courant, R., and Robbins, H. (1947, 1961). *What Is Mathematics?*, Oxford University Press.

Kac, M. (1959). *Probability and Related Topics in Physical Sciences*, Interscience, London.

Knuth, D. (1981). *The Art of Computer Programming*, Vol. 2, *Seminumerical Methods*, Addison-Wesley, New York.

Lichtenberg, A. J., and Lieberman, M. A. (1983). *Regular and Stochastic Motion*, Springer-Verlag, Berlin.