The Mathematics Enthusiast

Volume 7
Number 2 *Numbers 2 & 3*

Article 4

7-2010

Chaos in Physics and recurrence in Arithmetic Sets

Jean Dayantis

Recommended Citation
Dayantis, Jean (2010) "Chaos in Physics and recurrence in Arithmetic Sets," *The Mathematics Enthusiast*: Vol. 7 : No. 2 , Article 4.
DOI: https://doi.org/10.54870/1551-3440.1185
Available at: https://scholarworks.umt.edu/tme/vol7/iss2/4

Chaos in Physics and Recurrence in Arithmetic Sets

Jean Dayantis[1]
Pignan, France

Abstract: *After briefly recalling the concepts of recurrence and chaos in physics, the recurrence properties of arithmetic sets are examined following Gauss' method, as exposed in part three of his Disquisitiones Arithmeticae. This problem in number theory is related to the physical problem of recurrence in deterministic chaos. Most possible forms of moduli are examined in detail with respect to their recurrence properties, for application to the generalized Bernoulli mapping. The emphasis is put on period lengths, rather than on congruences. In an annex the recurrence properties of Arnold's cat map are briefly examined.*

Keywords: Arnold's cat map; *Disquisitiones Arithmeticae*; deterministic chaos; number theory; period lengths; recurrence

INTRODUCTION

A- The concept of recurrence

Recurrence is a very general concept and pervades almost every field of science : Astronomy, Physics, Chemistry, Geology, Biology and so on. In everyday language, recurrence means that something that has happened in the past will again happen in the future, and this many many times, if not an infinity number of times. Let us first give some examples: in astronomy, the revolution of the earth around the sun, responsible for the succession of seasons, is a recurring phenomenon; in the same way, the days in the week or the months in the year are recurrent; in physics, any oscillatory process, for example the frictionless pendulum is a recurrent process; in thermodynamics, the Carnot cycle is recurrent phenomenon, in so far as the engine is given the necessary feed to sustain its motion. In chemistry, the Belousov-Zhabotinski[1] reaction in far from equilibrium thermodynamics, is, among other chemical reactions, a recurrent one. In medicine and biology, the cardiac rhythm, the rhythm of breathing are recurrences. In dynamics, there is a theorem, the Poincaré recurrence theorem (1890), which states that "in a dynamical system having constant energy, any point of the trajectory in phase space[2] will again be approached as closely as wanted with time".[3] The fact that this Poincaré recurrence time may, in some instances and for all practical purposes, be infinite, shall not concern us here.

Of course, many if not most phenomena in nature are not recurrent. They are then said to be irreversible. For example, in chemistry, an explosion is not a recurrent phenomenon, since the initial products are consumed during the explosion to give final products which are stable in time; in the same way, the evolution of most chemical reactions is monotonous, heading to equilibrium; in astronomy, the life and death of a star is not recurrent, the stars follow roughly speaking the so-called Herzsprung-Russel diagram (1911-1913) [4], being blue

[1] * On leave from Institut Charles Sadron, Campus CNRS de Cronenbourg, 13, rue du Loess, 67034 Strasbourg Cedex France. E-mail : jeandayantis@aol.com. Any correspondence should be addressed to the following address 12, rue de l'Olivette, 34570 Pignan France

stars when born through accretion of matter and becoming white dwarfs, neutron stars or black holes with their death, according to the magnitude of their masses. The same may be said in biology with regard to the living organisms on earth, which are born, prosper and finally die.

Are there any recurrences in mathematics? Of course there are. In this article however the subject of recurrences in mathematics will be restricted to some properties of integer numbers, and this in relation to chaos theory.

B- Chaos theory.

It us outside the scope and the purpose of the present paper to give even a limited account of chaos theory. However, as the inception of this paper is related to chaos in physics, a few general notions will be here recalled.[5]

The intuitive, everyday language concept for "chaos" refers to a system where no order is apparent, one which appears to be very "disordered", one which does not seem to follow any law whatsoever. A more scientific definition is that, if a particular element in the system is chosen, the autocorrelation function[6] of this element as a function of time is of finite amplitude and tends more or less rapidly to zero. For example, choose a particular molecule in a gas enclosed in a container, large with respect to the dimensions of the molecule, and let x_0, y_0, z_0 be its coordinates at time t_0. It is assumed that the container plus the enclosed gas molecules form an isolated thermodynamic system, i.e. no exchange of matter or energy with the environment does occur. If at time τ_1 the coordinates are x_1, y_1, z_1, and if one is unable to determine these coordinates from the previous x_0, y_0, z_0, the autocorrelation function[5] is said to have reached the value zero at time τ_1. In other words, the "memory" of the system is lost, and the past does not define the future. This is a concept of particular importance.

Until near the end of the second third of the twentieth century scientists thought that chaos in physical systems resulted from the existence of a very large number of degrees of freedom. Thus, let the above container embody N molecules of a gas so that the system has 6N degrees of freedom. If N is equal to Avogadro's number, then $N=10^{23}$ molecules. If the position and velocity of each one of these molecules could be exactly known at a the time say τ_0, then, according to Newtonian mechanics and at least in principle, the position and velocity of each of these N molecules could be calculated at a later time τ_1.[7] In other words, the future evolution of the system would be entirely determined by its past history. However, as in practice it is not possible to solve at time τ_0 some 10^{23} scalar equations to find the positions and velocities of the N gas molecules at time τ_1, one is happy to be able to specify only values for some global parameters in the gas, as the mean temperature or the mean pressure. In other words, the "chaos" in the positions and velocities of the gas molecules at any time results here from a practical rather than a theoretical impossibility: the impossible knowledge of the trajectory of the physical system in phase space is here due to the large number of degrees of freedom involved. However, this is not always so, and there are many physical systems where the unpredictability of the evolution is of an intrinsic nature.

Such physical systems do not require a large number of degrees of freedom. Three are sufficient. These physical systems are mathematically described by systems of non-linear differential equations which are generally non-integrable, that is they have no analytical solution. The solutions can be found only numerically, using a step by step process in the variables, a procedure which generally necessitates the use of computers. This explains why such numerical solutions had to wait for the advent of computer science and computers.

The first physical system having only a few degrees of freedom and yet displaying chaos was discovered in 1963 by the American meteorologist Edward Lorenz.[8] The simplified model he used to follow the evolution of weather had only three degrees of freedom, yet the system was chaotic, it did not follow any regular law, which means that the weather is by essence unpredictable for long enough periods of time. Since Lorenz's discovery, many works have followed concerning physical systems having only a small number of degrees of freedom and being nevertheless chaotic. The chaos thus generated by systems displaying only a limited number of degrees of freedom is referred to as "deterministic chaos".[9] All such deterministic chaotic systems are "dissipative", which means that they "dissipate" energy: they are not thermodynamically isolated, they exchange matter or energy or both with the environment, contrary to the previous example of a gas enclosed inside a container.

A constant feature of chaotic systems is their instability, that is their sensitivity to initial conditions: if we very slightly vary the initial conditions, in other words the departure point in phase space, then the subsequent trajectories will wildly differ. As was aptly stated by Lorenz, "The flapping of a single butterfly's wing today produces a tiny change in the state of the atmosphere. Over a period of time, what the atmosphere actually does diverges from what it would have done. So, in a month's time, a tornado that would have devastated the Indonesian coast doesn't happen. Or maybe one that wasn't going to happen, does." [10]

C- Deterministic chaos and mapping.

Because of the difficulty of studying actual physical systems with respect to chaos and possible recurrence to the initial state (e.g. in Hamiltonian Mechanics the Poincaré theorem, see above), physicists and mathematicians have sometimes resorted to artificial models of chaos, in order to capture at least some features of the true, physical chaos. Such models are constructed using "mapping", that is an application of a given (phase) space to itself. The simplest possible example of such mapping is the Bernoulli mapping:[11] consider the linear segment [0,1], (here, the phase space) and take some point x_N inside this segment. The mapping consists in taking as next point $x_{N+1}=2x_{N+1}$ if $2x_{N+1}<1$, and $x_{N+1}=2x_N-1$ if $2x_N>1$. It is demonstrated that after a sufficient number of steps, the linear segment [0,1] will be uniformly covered by the step points. This Bernoulli mapping is not reversible, since if one takes x'=x/2, eventually, whatever the starting point x, the mapping will lead to the origin x=0. Nevertheless, it is recurrent (see part A.1 of the main text). Other "popular" mappings are the baker's map and Arnold'cat map[12] (See Annexe III). The present article however is particularly devoted to the case of the Bernoulli mapping.

RECURRENCE IN ARITHMETIC SETS

After this somewhat lengthy but necessary introduction in order to place the article in its context, it is time to proceed to the gist of the matter. This is the recurrence in arithmetic sets, and the topic is closely related to congruences in the theory of numbers.

The study of the recurrence in numerical sets involves considering the Z/Z(N) algebra[13]. Leonhard Euler (1707-1783) was the first to consider, to our knowledge, congruences modulo some integer and also recurrences, and he introduced the notion of primitive roots (see below). However the in depth study of recurrences and primitive roots is due to Carl Friedrich Gauss (1777-1855) in his *Disquisitiones Arithmeticae*[14] (denoted below D.A.). He was followed by many celebrated mathematicians as Poinsot, Jacobi and Tchebytcheff and numerous other distinguished mathematicians.[15] However, the focus of these authors was essentially the finding of primitive roots, not the length of sequences. The latter was not considered to be of particular interest.

As already started in the introduction, the problem here considered is to analyse the status of recurrence in deterministic mappings. To give a striking example, let us consider Arnold's cat map[12]: In this particular one to one transformation, after a relatively small number of successive transformations, the original picture of the cat completely disappears and chaos is being established. However, pursuing further the transformations, the picture of the cat finally reappears identically. This may take as many as several hundred of successive transformations, or even more. Though the reappearance of the cat's picture may at first seem something miraculous, the mathematical explanation of this remarkable phenomenon is quite simple. (See Appendix III).

Many of the results to follow are already present in the D.A., published more than two centuries ago. The derivations however are sometimes somewhat different, and it is hoped that this may provide some new insights. The elementary axiomatic status of this work will hopefully be easy and useful reading to physicists, non-career or amateur mathematicians, as also all propositions are clarified by numerical examples. However, some questions remain open and it is hoped that this might attract the interest of mathematicians for further clarification. (See e.g. the conjecture in C.1.2 or the last sentence in Part D). Because of the purpose of the paper, the emphasis is put on recurrences and length of periods, rather than on congruences to unity or other integers, as is the case in many classical works. Gauss' terminology will be followed throughout.

PART A. RECURRENCE MODULO A PRIME P.

Consider an odd prime number p, an integer $\alpha < p$ not divisible by p, and the successive powers $\alpha^1, \alpha^2 \ldots \alpha^{p-1}$ of α, designed as the base. Euler and Gauss have shown[16] that quite generally, for the power t of α, called the index, t residues taken among the p-1 possible appear modulo p (mod.p in what follows) before the series repeats itself. The number t is necessarily a divisor of p-1. If the repetition occurs at the power t = p-1, then all integers from 1 to p – 1 appear in the period as residues (mod.p), and α is then called a *primitive root* of p (in what follows PR). For example, one easily finds that 2 is a primitive root of five, but not of seven. It has been demonstrated by Euler and Gauss that any odd prime has primitive roots. In what follows, only the least residues (mod.p) are considered.

A.1. The base α is a primitive root of p, an odd prime.

According to convenience, enumeration of the elements in the set may start either from α^1 (enum.1), or from $\alpha^0=1$ (enum.2). Using here enum.1, one has for the last term in the series before repetition, from Fermat's theorem, $\alpha^{p-1} \equiv 1$ (mod. p). This involves that one necessarily has for the term $\alpha^{(p-1)/2} \equiv \pm 1$ (mod.p), for this is the only way by squaring each member of the above relationship to obtain $\alpha^{p-1} \equiv 1$ (mod. p). The value +1 (mod.p) = α^0 is excluded, since then the series would stop and recurrence will occur at the term $\alpha^{(p+1)/2}$, and therefore α will not be a primitive root, contrary to hypothesis. Consequently, one necessarily has $\alpha^{(p-1)/2} \equiv -1$ (mod.p)[17] and this says that the residue of the term $\alpha^{(p-1)/2}$ (mod.p) is equal to p – 1. This is easily checked. (Take for example $\alpha=2$ and p=13, or $\alpha=3$ and p=17 and write down the period). Let us then write the set of integers in the period (mod.p) as follows :

$$\alpha^1, \alpha^2, \ldots \alpha^{(p-3)/2}, \overset{\equiv p-1}{\alpha^{(p-1)/2}}, \alpha^{(p+1)/2}, \alpha^{(p+3)/2}, \ldots \alpha^{(p+(p-4))/2}, \overset{\text{last term} \equiv 1}{\alpha^{(p+(p-2))/2}} \quad \text{(mod.p)} \qquad (1)$$

This set can alternatively be written in the form

$\alpha^1, \alpha^2, \ldots \alpha^{(p-3)/2}, p-1, \alpha(p-1), \alpha^2(p-1), \ldots, \alpha^{(p+(p-4))/2}(p-1), 1 \quad (\text{mod.p}) \quad (1')$

Now it is evident that $\alpha+(-\alpha) \equiv p \equiv 0$ (mod.p), and more generally

$$\alpha^\nu+(-\alpha^\nu) \equiv 0 \text{ (mod.p).} \quad (2)$$

If in the above set we add two by two the terms α^ν ($\nu < (p-1)/2$) and $\alpha^{\nu+(p-1)/2} = \alpha^\nu(p-1)$, the result is

$$\sum_{\nu=1}^{\nu=(p-1)/2} [\alpha^\nu p+(\alpha^\nu+\alpha^{\nu+(p-1)/2})] \equiv 0 \quad (\text{mod.p}) \quad (3)$$

since the addition of the terms α^ν and $-\alpha^\nu$ is, according to (2), equal to p[18]. Relationship (3) provides another proof of Gauss' proof,[19] that the algebric sum of all the terms in the set (1) is zero (mod.p). Gauss' proof is of course the shortest. It is as follows : using enum.2 and writing the successive terms, one has :

$$1+\alpha^1+\alpha^2+ \ldots + \alpha^{p-1} = (\alpha^p-1)/(\alpha-1) = 0 \ (\text{mod.p}) \ \text{since } \alpha^p=1 \quad (4)$$

Now it is evident, since $\alpha^\nu \equiv \alpha^\nu - mp$ (mod.p), where the integer m = 0 if $\alpha^\nu < p$, that replacing the terms in (3) by their value mod.p leads to relationship (4).

Nevertheless, relationship (3) is useful in providing a somewhat better insight on the structure of the period, and the property that the term of index (p-1)/2 equals p-1 will be used later on.

. Example : take p=11, base 2. The residues in the period using enum.1 are, 2,4,8,5,10,9,7,3,6,1, then recurrence occurs. One has, according to (2), 2+9 =11, 4+ 7 = 11, etc, the sum of all the terms in the period is p(p-1)/2 =10x11/2 = 55 ≡ 0 (mod.11). Also, the multiplicity m is easily determined for the term $\alpha^{(p-1)/2}$ through

$$m = (\alpha^{(p-1)/2} + 1-p)/p \quad (5)$$

For p=11, α=2, one correctly finds m=2.

As a practical application, let us consider the simple one dimensional Bernoulli mapping $X_{N+1} = 2X_N$, (mod.1). Starting from the abscissa 1/11, recurrence will occur after 10 steps, the numerator taking all the above mentioned values for p=11, base α=2. Now one may of course choose as the denominator an integer for which 2 is not a primitive root, e.g. 17, and initiate the process at abscissa 1/17. In this case recurrence will not occur after p-1 steps, but only (p-1) /2. Also the denominator may be taken a composite integer, for example 3x11=33, 3x5x7=105 or 2^2x13=52, an even number. Therefore it is interesting to know the recurrence properties in these cases also, which will be examined in the following Parts and sections, excluding however irrational denominators.

A.2. The base α is not a primitive root of p, an odd prime. Open and closed groups.

If α is not a PR of p, then the period stops and recurrence is initiated, as shown by Gausss,[20] for an index ν which divides p-1. If p-1 is of the form p-1=2p', p'>3 prime, then the period has necessarily p'= (p-1)/2 terms. This is a sufficient but not a necessary condition in

order that the period be of (p-1)/2 terms. The alternative of having p' groups of two terms beginning with $\alpha^0 \equiv +1$ and $\alpha^1 \equiv p+1$ is impossible since necessarily a < p. Now since the period has only (p-1)/2 residues and there are p-1 integers from 1 to p-1, there are necessarily (p-1)/2 integers lacking in the period. The group of integers constituted by the (p-1)/2 residues corresponding to the actual powers taken by α before recurrence, will be called the *principal group*, noted Gr1.

This group includes necessarily unity. If further p-1=2p', p' prime, there can be only another group which shall be called the *secondary group* Gr2, containing the (p-1)/2) integers absent in Gr1. In other situations, however, there may be more than one secondary group (see below, paragraph A.3). How one will find the elements of Gr2 ? Choose the least prime ω not included in the period of Gr1, and multiply ω by α, α^2, … $\alpha^{(p-1)/2}$. One obtains in this way (p-1)/2 new integers (mod.p) all necessarily different from those of Gr1, which will be called "residues" to distinguish them from the residues of Gr1. For, suppose that Gr2 contains a term β already appearing in Gr1. Then necessarily one has $\beta=\omega\alpha^{\nu}=\alpha^{\mu}$ with $\mu > \nu$, since $\omega > 1$. By dividing both members of this relationship by α^{ν} one has $\omega= \alpha^{\mu-\nu}$, which means that ω is a residue of Gr1, contrary to hypothesis. Since there are in all p-1 integers in the range 1… p-1 (mod.p), the sum of the integers in Gr1 and Gr2 completes the set of all possible integers from 1 to p-1. Though it is convenient to choose ω as the least prime among those not included in Gr1 , this is not a necessary condition. On the contrary, ω should never be chosen to be a composite integer not in Gr1, since this will lead to redundancies. Another basic difference between the principal group Gr1 and the secondary group Gr2 (beyond the fact that the terms in this group are not residues (mod.p) of the powers of α), is that the elements of Gr2 in non modular algebra have always in factor ω, which is never the case for those in Gr1. Notice that the notation as groups for GrX complies to the usual definition of groups in mathematics.

Examples will make the above clear: Take p=23, base 2, so that p-1=2x11, and p'=11. One then finds in the period of Gr1 the residues [2,4,8,16,9,18,13,3,6,12,1]. To find the "residues" of Gr2, choose 5, the least prime not included in the period of Gr1, and multiply 5 by 2, 2^2 …$2^{(p-1)/2}$. This leads to the period [5,10,20,17,11,22,21,19,15,7,17]. Examination of these two periods shows that the residue p-1 appears in the group Gr2 and that all the elements of Gr2 are obtained by subtracting from 23 the elements of Gr1. More generally, within the constrain indicated, the terms in Gr2 are obtained by subtracting from p the residues of Gr1. If p - α^{ν} is such a term of Gr2, it cannot be also a residue α^{m} of Gr1, witch will lead to $\alpha^{\nu}+\alpha^{m}=p$. In the present case, no addition of terms appearing only in either Gr1 or Gr2 may add up to p.

PROOF : Suppose that two residues of Gr1, x_1 and x_2, were such that $x_1+x_2 = p$. The corresponding terms in Gr2 are then $y_1 = p - x_1$ and $y_2 = p - x_2$, which added lead to $2p = x_1+x_2$, a relationship not compatible with the previous one. Only one term of Gr2 when added to the corresponding residue of Gr1 makes up to p.

Such couples of groups Gr1 and Gr2 will be called *open*, since there is interconnection of the elements of each group with those of the other. As already stated, in *open* systems, no sum of two terms in the same group adds up to p.

Consider now p=17, p-1=16=2^4 and the base α=2. This base is not a PR of 17, as $2^8 = 256 = 2^{(p-1)/2} \equiv +1$ (mod.17). In principle p-1 might decompose to a principal group Gr1 of eight, or four elements, but the latter is impossible since $2^4 = 16 < 17$. Writing down the period leads to a series of eight residues [2,4,8,16,15,13,9,1] so there must be a group Gr2 having also eight terms. To find these terms take the least prime, here 3, not appearing in the period of the principal group, and multiply it by 2,2^2, … mod.17. One thus obtains the period [3,6,12,7,14,11,5,10].

In Gr1, because 4 divides 16 and $2^{(p-1)/2} \equiv +1$ one necessarily has $2^{(p-1)/4} \equiv \pm 1$ (mod.17), and since the period continues to eight terms as found above, one has $2^{(17-1)/4} \equiv -1$, that is, to follow Gauss' terminology, the residue (p-1)/2 "pertains" to the index 4. Here eq. (2) applies, and the sum of the corresponding terms two by two in Gr1 as well as in Gr2 equals 17=p. Also, one does not here obtain the elements of Gr2 by subtracting to the modulus p the residues in Gr1. If this is done, one obtains again the residues of Gr1, and vice-versa for the terms in Gr2 ; in other words, the groups are cyclic. Such groups will be called *closed*.

Generally, from the above, the rationality of *open* and *closed* groups is the following : if the period has an even number of terms, (p-1)/2, (p-1)/4, etc. then the term obtained by dividing by 2, of index (p-1)/4, (p-1)/8, etc. has value $\equiv -1$ (mod.p), or, to use Gauss' terminology, the residue p-1 pertains to the indices (p-1)/4, (p-1)/8, etc. In such occurrences, the group Gr1 is closed, since 1 and p-1 add to p, the property of *closed* groups. If now the period has an odd number of terms, then (p-1)/4, (p-1)/8, etc. do not correspond to any integer index, and the residue p-1 is shifted to Gr2. In mod.p arithmetic this means that no power of the base α, yields the residue p-1. Since unity is always to be found in Gr1, addition of the residue unity of Gr1 to the term p-1 of Gr2 adds to p, the property of *open* groups. If p-1 = 2p', p and p' primes, α not a PR of p, there are always two and only two groups, the principal Gr1 and the secondary Gr2, which are either both *open* or both *closed*.

There does not seem to exist any rule, which will permit to predict whether the groups mod.p, base α, α not a PR of p, are *open* or *closed*. One has to write down the periods. However, at least for small values of the modulus p, it seems that the groups are more often *open* than *closed*.

In secondary groups, beginning with the prime (that is using enum.1), there is also a rank or "index" in the integers of the period. This rank is here called "index", to distinguish it from the index of the integers of Gr1, since these integers are not actual residues of the powers of α.

A.3. p an odd prime, the base α not a primitive root of p, more than one secondary group.

What now about the general case where p is not such that p-1 = 2p', p' a prime? Then a priori, all the divisors δ of p-1 are possible, leading to periods (p-1)/δ, with the restriction that are forbidden those divisors of p-1 leading to periods of n terms for which $\alpha^n < p$. Of course, this means that one may have, besides the principal, 2,3 … secondary groups, in which groups, together with the principal, all the integers from 1 to p-1 will be present. To find all the secondary groups, it suffices to extend the procedure indicated in **A.2** : Take the least prime ω not part of the t residues in Gr1, and multiply it by α, α^2, … α^t, to find the "residues" in Gr2. Then choose the least prime ω' not present in Gr1 and Gr2, and multiply it by α, α^2, … α^t, to find the "residues" in Gr3. Continue in this way until all the secondary groups are found. Proof that not two of the groups may share a same residue, may follow along the lines developed in **A.2**. Here are a few examples of prime moduli where more than one secondary group exists :

Consider p=43, p-1 = 2x3x7, and the base 2, not a PR; writing down the principal group one finds the period :

[2,4,8,16,32,21,42,41,39,35,27,11,22,1], mod.43

This period has the even number of fourteen residues, and the residue p-1 pertains to the index (p-1)/2x3 = 7. The group is *closed*, the residue 42 appears at the index 14/2=7, and there are two secondary groups, which for convenience will be denoted here by the prime initiating the

period, that is Gr3 and Gr7. The elements of these two secondary groups are easily found as above indicated. They are:
[3,6,12,24,5,10,20,40,37,31,19,38,33,23] and [7,14,28,13,26,9,18,36,29,15,30,17,34,25].

Consider now p= 73, p-1 =72=$2^3 3^2$; neither 2 nor 3 are primitive roots of 73. Let us first write the period base 2. Principal group: [2,4,8,16,32,64,55,37,1]. There is an odd number of residues and the residue 72 does not appear in the principal group, but in the first secondary group Gr71, the period being [71,69,65,57,41,9,18,36,72]. Adding two by two the terms of given "indices" of two associated groups, will yield the value 73. There are six other secondary groups, namely Gr3, Gr5, Gr11, Gr13, Gr53 and Gr61 which are associated two by two, and summing one term of the first to the corresponding term of the second will yield 73= p. The association is as follows: Gr5 ⇔ Gr55, Gr11 ⇔ Gr13, and Gr3 ⇔ Gr61. In *open groups* the "residue" p-1 may appear in any group other than the principal and may pertain to any "index".

Let us now take p= 73, base 3. Here there are six groups of twelve terms each, all groups are *closed*, and the residue p-1=72 appears therefore in the principal group at the index 12/2=6. Here we give the period for only the principal group:

[3,9,27,8,24,72,70,64,46,65,49,1].

The five secondary groups are Gr5, Gr7, Gr13,Gr19 and Gr23.

A.4 The number of groups in base α modulo the powers of an odd prime p.

Let us first examine what happens modulo p^2, the base α being a PR of p, an odd prime. Firstly, the largest possible period has p(p-1) terms, since the multiples of p, which number p, cannot be residues. Let as now show that if α is a PR mod.p, it is also a PR mod.p^2 : one first remarks that if a residue is ≡ +1 mod.p^2, it is also necessarily ≡ +1 mod.p. The period mod.p is p-1, so that within the period mod.p^2 there are p periods mod.p. As the last term of the last period mod.p ≡ +1, this establishes the fact that if a residue is congruent to unity mod.p^2, it is also congruent to unity mod.p. Now if α is a PR mod.p, it is also necessarily a PR mod.p^2. For, let us assume that the period mod.p^2 were p(p-1)/q, q being some integer dividing p-1. This implies that the residue at the index p(p-1)/q would be ≡ +1 mod.p^2. However, this index will correspond to an index (p-1)/q inside some period mod.p, which cannot be ≡ +1, unless q = p-1. In the latter case, however, the period mod.p^2 would be p, which again is impossible, because this would imply that two adjacent terms mod.p, of indices p-1 and p would both be equal to ≡ +1. The conclusion is that if α is a PR of p, it is also a PR of p^2. This property has long being known.[21]
Example. The period of 5 base 3, a PR, is: [3,4,2,1] and that of 25 is [3,9,2,6,18,4,12,11,8, 24,22,16,23,19,7,21,13,14,17,1]. One immediately checks that the residue p-1 mod.p is at the index (p-1)/2=2, and that the residue p^2-1 mod.p^2 is at the index p(p-1)/2=10.

The above considerations generalize to any power of the odd prime p. The period mod.p^N is p^{N-1}(p-1), and if α is a PR of p, it will also be a PR of p^N. As a corollary the term of index p^{N-1}(p-1)/2 mod.p^N is equal to p^N-1.[22]

The next step is to see what happens when α is not a PR of p. In this case the period will be (p-1)/r mod.p, r dividing p-1. As shown above there will then exist mod.p r separate groups, covering as residues all the integers from 1 to p-1, that is the principal group Gr1 and r-1 secondary groups GrX. Now mod.p^2 there will also be r groups of equal periods p(p-1)/r. For, if the periods differed from the above value, the sum of all the residues of all the groups mod.p^2 would either exceed or be less than the permissible integers, and in both cases this would be irrelevant. The property holds for any integer power of p.

As already stated all the above considerations apply with no modification in mod.1 algebra, considering fractional abscissas α/p, α an integer less than p. This is used in particular by physicists in defining deterministic maps of chaos. As one further example, in base 2, and enum.2, let $p^2=49$. Since there are two groups mod.7, there are also two groups mod.49 of periods (7x6)/2 = 21 terms each. One indeed finds two open groups of 21 residues each where p^2-1 is found in the secondary group at the "index" 5. Conversion to mod.1 algebra is readily obtained by dividing each residue by 49.

For the physicist's sake, let us stress that the group he chooses is indifferent regarding the length of the period, as all groups have periods of equal length. If for instance he starts his mapping experiment with 1/p ($\Rightarrow$ enum.2), the residues will be those of the principal group, and the length of the period will be p-1, if the base is a PR of p. If he starts from p'/p, p' not to be found in the principal group, the period shall remain the same, only the "residues" are different.

PART B. RECURRENCE IN COMPOSITE MODULI C OF ODD PRIMES.

Let us first quote from Hardy and Wright the following excerpt, regarding the primitive roots of a congruence : *In what follows we suppose that the modulus m is a prime ; it is only in this case that there is a simple general theory*.[23] Regarding however the recurrence in composite moduli C which are the product of odd primes, the problem with which we shall now be concerned, it will be shown below that indeed some general rules do apply. The one major difference with the prime moduli of the previous part, as shown below, is that in this case there are not primitive roots, and therefore that the principal group cannot encompass all the permitted integers. There is therefore constantly at least one secondary group. However, there are also striking analogies. For example, in mod.p algebra, p prime, one cannot chose as modulus the base p. Analogously, if the modulus is composite, $C = p_1p_2 \ldots p_n$, the p_i being odd primes, the base α cannot be one of the primes p_i, and all the multiples of the p_i are excluded from the period. (See however Part D.) As a consequence, a parameter of major interest is the quantity $F = \Pi(p_i-1)$, which describes the number of permitted residues. In the simplest case of $C= p_1p_2$, the number of permitted residues is $C - (C/p_1+C/p_2) + 1$, the +1 coming from the fact that the last term p_1p_2 is deleted twice. This is equal to $(p_1-1)(p_2-1)$, and the relationship generalizes to the product of any number of the first powers of odd primes. (See Appendix I).

As for prime moduli, there are here also open and closed groups.

A point of interest is the following : while the period for prime moduli can only be determined though trial and error, that of composite moduli may be predicted, at least in principle, from the periods of the component primes.

The analysis to follow is based on the two following number properties : a) Fermat's theorem ; b) The property that if α^n , n integer, equals +1 mod.p_1, mod.p_2,… mod.p_r , then

$$\alpha^n \equiv +1 \mod p_1p_2\ldots p_r \qquad (6)$$

This congruence is a direct consequence of Eratosthenes' sieve, when applied to the powers of α. If powers q_i of the p_i enter into the definition of C, the congruences $\alpha^n \equiv +1 \mod p_i^{q_i}$ should also be respected. The converse property is true : if $\alpha^n \equiv +1 \mod p_1p_2\ldots p_r$, then $\alpha^n \equiv +1$ mod.p_1, mod.p_2, … mod.p_r. The relationship is not true if α^n is not $\equiv +1$, and then congruence to unity is not achieved for at least one of the primes entering in C at least one of the primes p_i.

The above will be detailed in what follows. For simplicity, it will often be assumed that C is the product of two or three odd primes. Generalization to r distinct primes is straightforward.

In what follows no distinction will be made between the residues and indices of the principal group and the "residues" of secondary groups. All indices and rests of division will be called indices and residues.

B.1. The modulus C is the product of r odd primes p_i, and the base α is a primitive root of all p_i.

Let as begin with C being the product of two primes p_1 and p_2. Here the number of permitted residues is $F=(p_1-1)(p_2-1)$. Since α is by hypothesis a primitive of both p_1 and p_2 one has by Fermat's theorem :

$$\alpha^{p_1-1} \equiv 1 \text{ (mod. } p_1) \qquad (7a)$$

$$\alpha^{p_2-1} \equiv 1 \text{ (mod. } p_2) \qquad (7b)$$

and

$$\alpha^{(p_1-1)/2} \equiv -1 \text{ (mod. } p_1) \qquad (8a)$$

$$\alpha^{(p2-1)/2} \equiv -1 \text{ (mod. } p_2) \qquad (8b)$$

One can elevate (8a) to the power (p_2-1) and (8b) to the power (p_1-1) to obtain

$$\alpha^{(p1-1)(p2-1)/2} \equiv +1. \qquad (9)$$

since both p_1-1 and p_2-1 are even. Because of (7a), (7b), the relationship holds mod.p_1 as well as mod.p_2, and considering (6) above, the relationship holds also mod.p_1p_2.

As a result, for $C=p_1p_2$, *the period stops and recurrence occurs at most for the index $(p_1-1)(p_2-1)/2$, never for the index $(p_1-1)(p_2-1)$.* Thus the modulus C, the product of two odd primes, *has no primitive roots*. The principal group Gr1 contains $(p_1-1)(p_2-1)/2$ elements among the permitted integers and there is therefore a secondary group Gr2, which will contain those integers which are not residues of Gr1. To find the residues in Gr2, one should proceed as in the case of prime moduli. Here again one will find *open* and *closed* groups.

Examples: take C = 3x5 = 15, base 2. One has, in enum.1, the period [2,4,8,1] forming the principal group Gr1, and the period [7,14,13,11] forming the secondary group Gr2. Multiples of 3 and 5 cannot of course be residues. The groups are *open*. In open groups the residue C-1 = p_1p_2-1 never pertains to the principal group, since this is the characteristic property of *closed* groups. It is to be found into the secondary group, at some undetermined index. Take now C = 3x11 = 33; the principal group Gr1 in base 2 is [2,4,8,16,32,31,29,25,17,1] and the secondary group Gr2 is [5,10,20,7,14,28,23,13,26,19]. The groups are *closed*, and the residue p_1p_2-1 pertains to the index $(p_1-1)(p_2-1)/4 = 5$ of Gr1.

Though the period cannot exceed F/2, it can be shorter. Example : take C=5x37=185, F=144, F/2=72, F/4=36. Writing down the period base 2, one finds that it has 36 terms, that is it is equal to F/4.

The above can be generalized for $C=p_1p_2 \ldots p_r$. For example, if one takes r=3, then $F=(p_1-1)(p_2-1(p_3-1)$ and a reasoning analogous to the one above will permit to find that

$\alpha^{(p1-1)\,(p2-1)(p3-1)/4} \equiv +1$, so that the period of a triple product cannot exceed F/4, though it can be shorter. Thus, here there are at least four groups, and generally, if $C=p_1p_2 \ldots p_n$, the maximum period is at most equal to $\Pi(p_n-1)/2^{n-1}=F/2^{n-1}$.

Whether the period is exactly $F/2^{n-1}$ or less, is a problem examined below. As an example, the period base 2 of C=3x5x11=165, with F=80, is of F/4=20 terms, while that of C=3x5x13=195, with F=96 terms, is of F/8=12 terms. The reason for this difference is that C=195 divides $2^{F/8}-1$, while C=165 divides $2^{F/4}-1$, but not $2^{F/8}-1$. (See the next section and Appendix II.)

As was the case for prime moduli, it does not seem that there exists any rule, that will permit to predict whether the groups of a composite modulus C are *open* or *closed*. One has to write down the periods to check. However, as above and at least for small values of C, it seems that the groups are more often open than closed. The above results can be summarized in the following theorem:

THEOREM: *When besides the principal there are also secondary groups, as is necessarily the case for composite moduli, these groups are either all closed or all open*.

B.2. The modulus C is the product of r odd primes at the first power, and the base α is a primitive root of none of the component primes.

Taking again the simplest case of $C= p_1p_2$, one can write

$$\alpha^{(p1-1)/D1} \equiv 1 \ (\text{mod}.p_1) \qquad (10a)$$

$$\alpha^{(p2-1)/D2} \equiv 1 \ (\text{mod}.p_2) \qquad (10b)$$

As in the previous case we can rise (10a) to the power $(p_2-1)/D_2$ and (10b) to the power $(p_1-1)/D_1$ to obtain $\alpha^{(p1-1)\,(p2-1)\,/D1D2}$, mod.$p_1$ and mod.p_2. Referring again to relationship (6), one also has $\alpha^{(p1-1)\,(p2-1)/D1D2} \equiv 1$ mod.p_1p_2. The period is $P=(p_1-1)(p_2-1)/D_1D_2$ and it is the longest possible, at least when D_1 and D_2 are relatively prime. For, in the latter case, if we divide P by say q an integer greater than 1, this q should either divide $(p_1-1)/D_1$ or $(p_2-1)/D_2$, which is impossible, if one wants relationships (10) to be preserved. The same considerations can be extended to $C=p_1p_2 \ldots p_r$, with r integer larger than 2.

Examples. Take C=7x17=119, base 2. Then F=6x16=96, F/2=48, F/4=24. Here $D_1=D_2=2$, so that the period should equal (at most) 96/4=24. One indeed finds for the principal group the period
[2,4,8,16,32,64,9,18,36,72,25,50,100,81,43,86,53,106,93,67,15,30,60,1]. If instead one considers C=7x43=301, then F=252 with $D_1=2$ and $D_2=3$, so that the periods could have *a priori* F/6=42 terms. One checks that this is indeed the case.

But consider now $C=2047=23x89=2^{11}-1$, with F=22x88=1936. Since it is found that $D_1=2$ and $D_2=8$, normally the period should have been of F/16=121 terms. But it is evident that the period is in fact of only 11 terms, since $2^{11}=2048$. One observes however that 22=11x2 and 88=11x8, so that D_1D_2 can be multiplied by 11, leading to a period of 11 terms and 121 associated groups.

<u>The unmistakable procedure to predict the length of the period for a given composite modulus</u>.

As shown above, some ambiguities may exist for the prediction of the length of the period for a given composite modulus C and an arbitrary base α, if the standard methods indicated above are used. Therefore it is convenient to dispose of a method devoid of any ambiguities and valid for all situations, whether all the components of C admit α as a PR, none of them, or part of them.

In this respect use shall be made of relationship (6). Let $C = p_1p_2 \ldots p_r$, and $F= (p_1-1)(p_2-1) \ldots (p_r-1)$. Compute all the divisors δ_i of F such that $F/2^{r-1} > F/\delta_i > C$.
Then compute the integers A corresponding to the powers F/δ_i and find, in for example a descending way for the δ_i's, the least divisor $\delta(min)$ for which the integer $A=\alpha^{F/\delta(min)}$ is congruent to unity mod.C. According to (6), as the integer A has a residue +1 mod.$(C=p_1p_2 \ldots p_r)$ it will also have a residue +1 for all the p_i's. The period shall stop and recurrence shall be initiated at the index $F/\delta(min)$. Notice that here one may have $p_i=p_{i+1}=p_{i+2} \ldots$ to take account of the powers involved in the primes defining C.

The method, certainly safe and of general validity, presents however an inescapable drawback: as soon as F is large enough (and especially when the base α is not chosen among the first few integers), the exponentiation may lead to numbers so large that they will elude the reach of even the most powerful computers in use. Therefore, in addition to this unmistakable and of general validity method, one may have, as a first approach, to examine the alternative method based on the value of F/D, as this does not imply integers larger than F.

B.3. The modulus C is the product of two or more odd primes p_i at the first power, and the base α is not a primitive root for some of the components of C.

This case is slightly more intricate than the two previous cases, and this is why it has been left last. As usual, we begin with the simplest case of C being the product of two odd primes, the base α not being a PR for one of these primes.
Quite generally, one has

$$\alpha^{p1-1} \equiv 1 \qquad \text{mod.p1} \tag{11a}$$

$$\alpha^{(p\,2-1)/D} \equiv 1 \qquad \text{mod.}p_2 \tag{11b}$$

where D is an integer such that $(p_2-1)/D$ is the period mod.p_2. As previously, one can raise (11a) to the power $(p_2-1)/D$, and (11b) to the power p_1-1 to obtain

$$\alpha^{(p1-1)(p\,2-1)/D} \equiv 1 \qquad \text{mod.}p_1$$

$$\alpha^{(p1-1)(p\,2-1)/D} \equiv 1 \qquad \text{mod.}p_2$$

and consequently, because of (6), also

$$\alpha^{(p1-1)(p\,2-1)/D} \equiv 1 \qquad \text{mod.}p_1p_2 \tag{12}$$

$(p_1-1)(p_2-1)/D$ gives the "standard" period when α is not a PR of one of the primes. But the period may be shorter (see below).

Examples. Take C = 5x7 = 35, F=24, α = 2, α is not PR of 7. One finds in enum.1 two groups of twelve residues each :

[2,4,8,16,32,29,23,11,22,9,18,1] mod.35 (principal group)

and

[6,12,24,13,26,17,34,33,31,27,19,3] mod.35 (secondary group)

The groups are *open*, since the residue C-1 = 34 is found in the secondary group at the index seven. The sum of each element of index ν of Gr1 when added to the element of the same index of Gr2 sums up to 35, if the index 7 of 34 in Gr2 is circularly pushed as to occupy the position of the index 12, previously being the index of 3.

Take now C = 3x43 = 129, F = 84, α = 2, α not PR of 43. Here one finds in enum.1 that there are in all six groups of fourteen elements each, while relationship (12) states that there should be three groups of 28 elements each, but as emphasized this is only the largest possible period. Therefore, whenever possible, one should predict the actual length of the period using the *unmistakable method* indicated in B.2. The principal group Gr1 has the following residues :

[2,4,8,16,32,64,128,127,125,121,113,97,65,1] mod.129 (principal group)

Obviously here the groups are *closed* and the element C-1 of index 7 of the principal group when added to unity of index 14 yields C = 129. More specifically, the sum of two residues of respective indices ν and ν+7 yields C = 129. The detailed residues of all six groups will not be given here, since this is not of great interest.

For C being the product of r primes p which admit the base α as a PR, and s primes q which do not, one can tentatively write as follows for the maximum possible period:

$$P_{max}= 1/2\prod_{i,j} [(p_i-1) /2^{r-1}] \ (q_j-1)/D_j] \qquad (13)$$

B.4. The modulus C is the product of the powers of two or more odd primes p_i.

What now happens when C is of the form $C=(p_1)^u.(p_2)^v$ with at least one of the integers u,v, being larger than one? Let us assume first that the base α is a PR of both the components of C. Obviously, one should compare this case with the simpler case where one has as above $C = p_1.p_2$. In the latter case as already shown the number of permissible residues is $(p_1-1)(p_2-1)$. Taking the simplest case of only two groups, there will be $(p_1-1)(p_2-1)/2$ terms in each group. Assume now that C is of the form $C=(p_1)^2.p_2$. The number of permitted residues is clearly $(p_1)^2.p_2 -[(p_1)^2\ p_2]/p_1- [(p_1)^2.p_2]/p_2 +1$, the +1 coming from the fact that the term $(p_1)^2.p_2$ has been deleted twice. This is $p_1(p_1-1)(p_2-1)$ and thus, each period will have at most $p_1(p_1-1)(p_2-1)/2$ terms.

Example. Let $C=3^2x5=45$, base 2. The permitted residues are F = 3x2x4=24, so that the period of each group should be 12. Writing down the periods one finds indeed :

[2,4,8,16,32,19,38,31,17,34,23,1] (principal group)

[7,14,28,11,22,44,43,41,37,29,13,26] (secondary group)

The groups are *open*, and the residue 44, is found at the index six of the secondary group.

The above are of general validity: if $C=(p_1)^u.(p_2)^v$, then the number of permitted residues is $(p_1)^{u-1}.(p_2)^{v-1}(p_1-1)(p_2-1)$. If there are N distinct groups, the period of each, and especially the principal, will have $(p_1)^{u-1}.(p_2)^{v-1}(p_1-1)(p_2-1)/N$ terms.

The above generalize to C being the product of any number of odd primes for which the base is a PR . If only first powers are involved, by a reasoning analogous to that given in **B.,** the maximum period P of the product of r primes will be

$$P_{max} = \prod_{i=1}^{r} (p_i-1)/2^{n-1} \qquad (14a)$$

If powers u_i of the p_i are also involved, the maximum period will be

$$P_{max} = \prod_{i=1}^{r} p_i^{(ui-1)}(pi-1)/2n-1 \qquad (14b)$$

In the latter case of a maximum period the total number of groups will be 2^{n-1}, that is as usual the principal and 2^{n-1}-1 secondary groups.

Examples: Take C=3x5x7=105. Then the maximum period will be F/4=2x4x6/4 =12 terms. One indeed finds for the principal group base 2 the period:

[2,4,8,16,32,64,23,46,92,79,53,1], mod.105.

The maximum period is here achieved. The groups are *open*, and the maximum residue 104 is to be found in the secondary group Gr13 at the index 4.

Take now $C=3^2x5x7=315$. The maximum possible period will here be F=3(3-1)(5-1)(7-1))/4= 144/4=36, while the least possible will display at least x integers, where $2^x > 315$. However, it is found that the period is in fact again twelve, that is 144/12, so that the maximum period is not here achieved. The principal group is:

[2,4,8,16,32,64,128,256,197,79,156,1], mod.315

The groups are open, and the residue 314 is found in the secondary group Gr59 at the index 5.

The rationality of these distinct behaviours between C=3x5x7 and $C=3^2x5x7$ is explained in section C.2 and Appendix II.

In the general case where $C=p_1p_2 \ldots p_nq_1q_2 \ldots q_s$, the p_i admitting the base α as PR and the q_j not, one can tentatively write for the maximum possible period :

$$P_{max} = (1/2)\prod_{i,j} [p_i^{(ui-1)}(p_i-1)/(2^{r-1})][q_j^{(uj-1)}(q_j-1)/D_j] \qquad (15)$$

Because of the ambiguity of the above relationship, one should apply whenever possible the *unmistakable method* of B.2. If the numbers involved are too large to be managed by your computer, well, … then write a computer software ordering the computer to write down the period, whatever its length !

Part C. Even composite moduli.

One in two integers is an even number. Therefore it is necessary to examine also the case of even composite moduli, so the more that a physicist interested in deterministic mapping, as suggested in the introduction, is free to choose in his mod.1 congruences as denominators even integers, for example $D=2^3x5=40$ or $D=2x7^2x13=1274$. In what follows we first examine the case of even composite moduli of the form 2^N, and subsequently the general case of composite moduli of the form $2^N\beta^\xi\gamma^\psi\ldots$, where β, γ etc. are odd primes. The

definition of the parameter F of the previous case remains valid. For example, for $C=2^4x11=176$ will correspond the $F = 2^3x10=80$.

C.1 The modulus C is of the form 2^N.

One should distinguish two cases : two is PR of the base α, and two is not a PR of the base α.

C.1.1 Two is a primitive root of the base α.

Here the base α is necessarily an odd prime. Trials taking small values of α, α=3, 5, 11, … and varying the exponent N, suggested the following relationship, when 2 is a PR of the base α :

$$\alpha exp2^{N-2} \equiv 1 \quad mod.2^N \tag{16}$$

A proof of this relationship can be given by induction : first it is known[24] that for any odd integer β, one has $\beta^2 \equiv 1$ mod.(2^3=8). Thus, (16) is true for N=3, whatever the value of α, with 2 being a PR of α. To prove (16), it suffices to establish that if (16) is true for N, it is also true for N+1. For this, let us square both sides of this relationship :

$$[\alpha exp2^{N-2}]^2 = \alpha exp2^{N-1} = 1$$

However, when squaring the exponent in α, one also automatically doubles the period. Therefore, the above relationship is true mod.$2x2^N$ = mod.2^{N+1} and thus one can write

$$\alpha exp2^{N-1} \equiv 1 \quad mod.2^{N+1} \tag{16'}$$

which provides the proof of (16) for any N, by substitution of N'=N+1 in (16'). This result was known to Gauss who first proved it.[25]

Relationship (16) implies that the period is $2^N/4$ mod.2^N; since even integers are automatically excluded from the period, the period could have been equal to N/2. However, it was not *a priori* evident that the period is only N/4. Since however the correct period mod.2^N is $2^N/4$, it follows that there are always two groups, the principal and the secondary group.

Example. Let the modulus be 2^5=32 and the base α=5. 2 being a PR of 5, there should be two groups of eight terms each. One finds indeed,

[5,25,29,17,21,9,13,1] principal group

and

[3,15,11,23,19,31,27,7] secondary group

One immediately checks that all odd integers from 1 to 31 are covered. One also remarks, in this particular case (an unexpected result), that the succession of these ordered odd integers is to be found alternatively in the principal and the secondary groups: one finds

in the principal group the odd integers 1,5, 9, 13, 17, 21, 25, 29, and in the secondary 3, 7, 11, 15, 19, 23, 27, 31. In other cases, the alternation goes two by two, as for the base 3, mod.2^5 :

[3, 9, 27, 17, 19, 25, 11, 1] principal group

and

[5, 15, 13,7, 21, 31, 29, 23] secondary group

Other bases alternating one by one are α=13, 29, 37 …, while others alternating two by two are α= 3, 11, 19, ... Base 31 is special, because $31=2^5-1$. Since unity is always to be found in the principal group, and the last residue 2^N-1 in the secondary, it follows that the groups are necessarily *open*. That 2^N-1 appears in the secondary group is almost evident ; for, mod.(2^3=8), whether the alternation is one by one or two by two, 7=8-1 appears manifestly in the secondary group. If now the modulus is 2^4=16, one has to put side by side in succession two quartets of odd integers. And so on. We don't know if there are alternations of more than two successive odd residues. If there are, they should be of the form 2^{N-c}, c integer < N, in order that they divide 2^N. Whatever the case, one can safely enunciate : *if two is a PR of the base α, the two groups mod.2^N are never closed.*

One final remark is as follows : if one adds index ν_1 of the principal group and ν_2 of the secondary group, one obtains the residue $\nu_1+\nu_2$ of the secondary group. (If $\nu_1+\nu_2$ exceeds the number of terms ν in the period, one has to subtract ν from the sum.) This also is evident, since equal values of $\nu_1+\nu_2$ correspond to the same integer in non modular algebra, and therefore to the same residue in mod.2^N algebra.

This curious phenomenon of alternation is challenging, however, not being an essential feature of recurrences, it shall not be any further examined in this paper.

C.1.2 Two is not a primitive root of the base α.

If now one looks for the principal period of base 7 mod.2^3, which corresponds to $7\exp 2^{N-2} = 7^2$ one finds the expected period of two terms [7,1] which as above equals 2^{N-2} ; now, mod.(2^5=32), one has $7\exp 2^{5-2} = 7^8 = 5\ 764\ 801 \equiv 1$ mod.32 as expected, and the period should have been of eight terms; however, one finds that $7^4=2401 \equiv 1$ mod.32 also, and that the period displays only the four terms [7,17,23,1], being now equal to 2^{N-3}. The same phenomenon occurs for α = 23, and 41, but for α=17, 47 and 71, the period is 2^{N-4}.

One should perhaps be able to demonstrate that from the couple of congruences

$$2^{(\alpha-1)/q} \equiv 1 \ \text{mod.}\alpha \qquad (17\alpha)$$

$$\alpha^{N-c} \equiv 1 \quad \text{mod.}2^N, \qquad (17b)$$

q and c integers, q dividing α-1, one can establish a relationship between q and c, so that for q=1, c=2, and for q>1, c>2.

CONJECTURE: In the absence however of the proof for such a correlation, the conjecture is here made that *the length of the period is 2^{N-2} when 2 is a PR of α and 2^{N-3} or less when 2 is* not.[26]

As previously in C.1.1., the ordered odd integers are distributed in regular patterns among the groups, but now these patterns are more complicated.

C.2 The modulus is of the form $2^N\beta^\xi\gamma^\psi$..., or $\beta^\xi\gamma^\psi$ …, where β, γ, ... are odd primes.

Let us first come back to the examples of section B.2, where it was found that for C=(3x5x7)=105 and C=(3^2x5x7)=315, the periods base 2 had the equal length of twelve terms, corresponding respectively to F/4 and F/12. However, when one tries C=(3^3x5x7)=945, the period is three times as large, i.e. of thirty six terms, corresponding again to F/12. For C=2^Nx17 on the other hand, the period base 7 remains equal to sixteen terms, from N=0 (that is mod.17) up to N=6, that is mod.1088. Then the period doubles to thirty two terms for N=7, i.e. mod.2176. As a final example, for C=2^Nx11, base 3, for N=1 the period is of five terms, then for N =2,3 and 4 of ten terms, increases to forty terms for N=5 and goes to eighty terms for N=6.

At first sight there is no rationality in these examples. One can make first the following observation : Let the penultimate term of index ν of the period base α and mod.m^kC be T, where m= 2, β, γ, … is the integer defining the increase of the modulus when going from one modulus to the next one. Suppose that m^kC is such that αT mod.m^kC $\equiv$ 1. For this modulus the period will stop and the index ν+1 and recurrence will be initiated at the index ν+2. Let now the next modulus be m^{k+1}C, and the term of index ν again be T. If now the term αT of index ν+1 is less than the modulus m^{k+1}C, the period will not stop at the index ν+1 but will continue : the period is increased.

The above observation is however of very limited predictive power. The rationality of the question is again found using the *unmistakable procedure* of section B.2. Let for the modulus m^kC the period be determined by the associated parameter F_k/δ_k(min), which involves that $\alpha^{Fk/\delta(min)} \equiv 1$ mod.m^kC. As long as $\alpha^{Fk/\delta(min)} \equiv 1$ with respect to the moduli that follow, that is mod.m^{k+1}C, … mod.m^{k+p-1}C, the period length remains unchanged. If however at mod.m^{k+p}C the congruence to unity is no longer achieved, then the period is increased by a factor of m. For, in this case, congruence to unity is achieved at the new index F_{k+p}/δ_{k+p}(min). The examples given above are being detailed in this respect in Appendix II.

PART D. The modulus is composite, and the base is one of the factors of the modulus.

Prime moduli cannot of course display periods and recurrences, when the base is the same as the modulus. If for instance one takes as base 5 and modulus 5^4 = 625, the series will stop after four terms, the last one being $\equiv$ 0 mod.5^4. However, when C is the product of two primes at their first power, C=p_1p_2, and only in this case, a normal process of recurrence occurs, when one of the primes is taken as basis. To show this, let $p_2 > p_1$, and let $x = p_2 - p_1 > 0$. If one chooses $p_1 = \alpha$ as the base (to maintain the Greek symbol used throughout for the base), and if further it is first assumed that α is a PR of p_2, one can write as follows the residues:

$$\alpha,\ \alpha(p_2 - x),\ \alpha(p_2-x)^2,\ \ldots\ \alpha(p_2-x)^{p2-1} \qquad \text{mod.}\alpha p_2$$

Developing the powers of $(p_2-x)^t$, $1 \le t \le p_2-1$, it is easily seen that all the terms are $\equiv 0$ mod.αp_2, except for the last one, which is αx^t, and that all these residues are different. Now, since α is assumed a PR of p_2, and p_2 does not divide x, one has from Fermat's theorem

$$x^{p2-1} \equiv 1 \text{ mod.} p_2 \qquad (18)$$

It is now permitted to multiply both terms of the congruence (18) by α and at the same time also the modulus by α, (because if two integers differ by one, their product by α will differ also by α) to obtain :

$$\alpha x^{p2-1} \equiv \alpha \mod.\alpha p_2 \qquad (19)$$

Consequently, at the index p_2 the residue α is recovered, and there is a period of $p_2 - 1$ terms.

Example : mod.(51=3x17), base 3, 3 being a PR of 17, one finds the period of sixteen terms [3,9,27,30,39,15,45,33,48,42,24,21,12,36,6,18] and then back to 3. Conversely, one may choose as the base 17, leading to the period of two terms [17,34]. Of course, never unity appears as a residue, as both $\alpha=p_1$ and $p_2 > 1$. This is the essential difference with the normal procedure where the base is not part of the primes entering C, and where there is always a principal group containing unity, absent from the secondary groups.

If now α is not a PR of p_2, the period length will be $(p_2-1)/D$, D dividing p_2-1, with a total of D groups, the principal and D-1 secondary, the principal group being here defined as the one containing the base α.

Example : mod.(34=2x17), base 2, 2 not being a PR of 17. Here there are two groups base 2 :

[2,4,8,16,32,30,26,18] principal [6,12,24,14,28,22,10,20] secondary

In base 17 there is a period constituted by the single term 17. One checks that these residues cover exactly those integers which are forbidden residues in normal periods, i.e. those constructed taking as base a prime not entering the definition of the composite modulus C. (Except for the residue C, since this would put an end to the recurrence.)

The situation is more complex when more than two primes enter into the definition of C, or when C is the product of powers of primes. Analysis of such cases, though not devoid of interest, lies outside the scope of the present work.

CONCLUSION.

As emphasized in the introduction, the incentive for writing this article originates in the recurrence properties of deterministic mapping, a subject lying in the frontier between physics and modern mathematics. The emphasis was put on periods and groups, rather than on congruences.

The above analysis is especially oriented towards the Bernoulli mapping. This mapping has been generalized to any basis and any modulus, instead of been restricted to basis two and modulus one. Put another way, any rational point inside the segment [0,1] may be taken as a starting point using any integer modulus. Such a detailed analysis is not known to the author to have been made elsewhere. Emphasis was put on secondary groups, as defined in the text. Such secondary groups are always present in composite moduli while in prime moduli they may or may not be present, depending on whether the base is a primitive root of the modulus or not. The secondary groups have been classified as *open* or *closed* secondary groups. Also, special attention has been given to composite moduli, including even composite moduli.

All propositions have been followed by numerical examples, so that the reader, whatever his mathematical status, may acquire a good and easy knowledge of the topic.

In retrospect, it appears that the only difference between the principal and the secondary groups lies in the fact that unity appears only in the principal group. (Except in the case where the base is one of the components of a composite modulus which is the product of

two primes, in which case unity is never present, neither in the principal nor in the secondary groups). If one is not interested in this difference, there is a perfect symmetry in the properties of the groups. The periods are the same, the groups are all *open* or all *closed* at the same time. In even moduli, the scheme representing the distribution of the permitted odd integers within the groups respects perfectly regular patterns. Though for the mathematician the presence of unity may be important, for the physicist interested in deterministic mapping, the presence or absence of unity in the period is not necessarily of outstanding interest. He can as well use, with the same success as far as recurrence is concerned, the principal or a secondary group. He can also use the recurrence of a composite modulus being the product of two primes, and take as the basis one of the primes.

In Annexes I and II below some points in the main text are further analysed. In Annexe III, an interesting recurrent mapping, Arnold's cat map, is briefly examined.

APPENDIX I: The F parameter.

It was stated in **Part B**. that for composite moduli $C=\Pi p_i$, where the p_i are the primes entering into the definition of C, (first assumed to be at the first power), the number of permitted residues was given by the parameter $F = \Pi(p_i-1)$. A proof of this in the general case may be given by induction.

Let us begin, as in Part B, with the simplest case where C is the product of two distinct primes, $C_2=p_1p_2$. To C_2 should be subtracted as non possible residues the multiples of p_1 and p_2, which are $C_2/p_1+C_2/p_2= p_1 + p_2$. To this however should be added unity, for the term p_1p_2 has been subtracted twice instead of once, so the number of permitted residues is $p_1p_2 - (p_1 + p_2) + 1$. This is clearly equal to $F_2=(p_1-1)(p_2-1)$.

Let us now multiply C_2 by a third distinct prime p_3, so that the new modulus is $p_3C_2=C_3=p_1p_2p_3$. Again we have to exclude as non possible residues all the multiples of p_1, p_2, p_3, which number $C_3/p_1+C_3/p_2+C_3/p_3= p_1p_2+ p_1p_3+ p_2p_3$. However, a number of these excluded residues has been counted twice. These are the multiples of the p_{ij}, whose number is $C_3/p_1p_2+C_3/p_1p_3+C_3/p_2p_3= p_1+p_2+p_3$, and this quantity should be added to the previous one. Finally, one should remark that the term $p_1p_2p_3$ was counted three times instead of two as being a twice slashed non residue, so that –1 should be added to the final result, which is therefore $p_1p_2p_3-(p_1p_2+ p_1p_3+ p_2p_3)+(p_1+p_2+p_3) – 1$. This is clearly equal to $F_3=(p_1-1)(p_2-1)(p_3-1)$.

To continue, let us multiply C_3 by a fourth distinct prime p_4, so that $C_4= p_4C_3=p_1p_2p_3p_4$. Following the same procedure as above, one must search for the non residues being the multiples of p_1, p_2, p_3, p_4. These are $C_4/p_1+C_4/p_2+C_4/p_3+ C_4/p_4= p_1p_2p_3+ p_1p_2p_4+p_1p_3p_4+ p_2p_3p_4$. However, among these terms, a number have been counted twice. These are all the terms C_4/p_{ij} $(i \neq j)$, which here are six, respectively p_{12}, p_{13}, p_{14}, p_{23}, p_{24}, and p_{34}, yielding the term $–(p_{12}+p_{13}+p_{14}+p_{23}+p_{24}+p_{34})$; when so doing, however, some terms have been counted thrice instead of twice, and should therefore be subtracted to the partial result. These are all the terms of the form C_4/p_{ijk}, $(i \neq j \neq k)$, yielding the term $-(p_1+p_2+p_3+p_4)$. Finally, the last permitted residue, i.e. $p_1p_2p_3p_4$, has been deleted four times instead of three, so that unity should be added, and the final result is $F_4= p_1p_2p_3 p_4 – (p_1p_2p_3 + p_1p_2p_4+p_1p_3p_4+ p_2p_3p_4)– (p_{12}+p_{13}+p_{14}+p_{23}+p_{24}+p_{34}) - (p_1+p_2+p_3+p_4)+ 1$. This is equal to $F_4= (p_1-1)(p_2-1)(p_3-1))(p_4-1)$.

And so on, having constantly terms with alternating + and – signs. The last term is $(-1)^n$, so that when n is even unity should be added, and when n is odd, unity should be subtracted.

If now to C_n, (n=2, 3 …), one or more component primes are in present in some power

u, v, …, F_n is simply multiplied by the corresponding primes at the powers u-1, v-1, … For, it is readily seen that in such cases all the terms in the above sums are also multiplied by u-1, v-1, …

APPENDIX II: Moduli of the form $2^N\beta^\xi\gamma^\psi$...,

In this Appendix we shall work out in more detail the examples given in section C.2.

1) As a first exercise let us consider the second example of section C.2, the modulus 2^Nx17, base 3. Since 3 is a PR of 17, the period of 3 mod.17 ($\Rightarrow$N=0) has sixteen terms. Of course the period cannot be shorter for powers of $N \neq 0$. Thus for N=1, one finds mod.(2x17=34) the following period of sixteen terms :

[3,9,27,13,5,15,11,33,31,25,7,21,29,19,23,1]

Now the question arises up to what modulus (=which value of N) the period keeps the length of sixteen terms ? The F parameter is here equal to 2^{N-1}x16. Here however we can dispense ourselves from actually determining the values of F/δ(min) for each value of N, corresponding to the least value F/δ(min) for which $\alpha^{F/\delta(min)}$ is congruent to unity. We can use the following shortcut : let us first compute $A=3^{16}$ = 43 046 721 and let us divide A-1 by the successive moduli when increasing N, i.e. 34, 68, 136, 272, 564, 1088 and 2176. All these divisions up to 1088, corresponding to N=6, yield integer numbers, meaning that the period keeps the value of sixteen terms. Division however by 2176 yields 19785,5, a non integer, meaning that 3^{16} is not congruent to unity, mod.2197. To achieve congruence, the period has to be doubled to thirty-two terms, and this is verified by actually writing down the period.

2) For a second exercise consider now the case of $C=3^N$x5x7, base 2. This example will be worked out in detail.

First consider C=3x5x7=105, with F=2x4x6=48. The divisors δ_i of F are, in decreasing values, i.e. increasing period lengths, 24, 16, 12, 8, 6, 4 and 2. The divisors 24, 16, 12, and 8 are at once excluded, since these would lead respectively, for the last residues, to $2^2 = 4$, $2^3 =8$, $2^4=16$ and $2^6=64$ which are less than the modulus 105. Let as then try the divisor 6, F/6=8, $2^8 = 256$. F/6 –1 should be, if correct, ≡ 0 mod.105, that is 105 should divide 255. This is not the case, so that a period of eight terms is too short. Let us then try F/4=12, corresponding to a period of 12 terms ; now $2^{12} = 4096$, F/4-1=4095, which is divisible by 105, yielding 39. Thus δ(min)=4, and the period should be of twelve terms. One indeed finds the period,

[2,4,8,16,32,64,23,46,92,79,53,1], mod.105.

Consider now the modulus $C=3^2$x5x7=315, leading to F=3x48=144. Since by increasing the modulus the period cannot become shorter, let us first examine the case of a period of twelve terms as above, corresponding to F/12 : F/12 –1= 4095 should be divisible by 315, and this is the case, 4095/315=13. One finds again a period of twelve terms :

[2,4,8,16,32,64,128,256,197,79,158,1], mod.315.

Let now $C=3^3$x5x7=945, F=432. One can again try a period of twelve terms, corresponding to F/36. F/36-1= 4095, but this is not divisible by 945. So the period should be larger, necessarily a multiple by three of the previous one. F/12=36, 2^{36}= 68 719 476 736, and one checks that $2^{36} – 1$ is divisible by 945, yielding 72 719 023. The corresponding period is,
[2,4,8,16,32,64,128,256,512,79,158,316,632,319,638,331,662,379,758,571,197,394,788,631, 317,634,323,646,347,694,443,886,827,709,473,1], mod.945.

Finally, consider $C=3^4$x5x7=2835, with F=1296. One may try again the period of thirty-six terms, in case the period length had remained unchanged. However, 2835 does not divide 68 719 476 735, so that the period should be trice as large, that is of 108 terms, corresponding again to F/12. If now one computes 2^{108} = A, and divides this by 2835, one finds the integer, 114 468 625 629 074 683 168 661 735 653. Therefore 2835 divides A, and the period should have 108 terms. If he so wishes, the reader can check this for himself.

Of course, as already pointed out, if the exponentiation of the base leads to intractable numbers, and if consideration of the divisors of F leaves some doubts, the only solution would be to write a software directly computing the periods. However, the *unmistakable procedure* has at least the merit to explain the apparently irregular increase of the period when the exponents in the primes defining C are increased.

ANNEXE III : Arnold's cat map and Arnold numbers and series.[12,27]

This deterministic chaotic map was devised as an example of a recurrent mapping by the Russian mathematician Vladimir I. Arnold (1935-…) in his book with A. Avez. *Ergodic Problems in Classical Mechanics*.[12] (See Wikipedia at the link *Arnold's cat map.*) Here follow succinct indications on this mapping.

Restricting ourselves in what follows to integer values for the variables x and y, Arnold's cat map is defined as follows:

$$x_{k+1} = 2x_k + y_k \qquad y_{k+1} = x_k + y_k \qquad \text{(1a), (1b)}$$

or, equivalently, in matrix notation :

$$\begin{vmatrix} 2 & 1 \\ 1 & 1 \end{vmatrix} \text{X} \begin{vmatrix} x_k \\ y_k \end{vmatrix} \rightarrow \begin{vmatrix} x_{k+1} \\ y_{k+1} \end{vmatrix}$$

(In fact with respect to ref.12, x has been substituted for y and vice versa. This however has no effect on what follows.)

Arnold's matrix $A = \begin{vmatrix} 2 & 1 \\ 1 & 1 \end{vmatrix}$

has a determinant one and is therefore unitary. It is inversible, the inverse matrix being

$$A^{-1} = \begin{vmatrix} 1 & -1 \\ -1 & 2 \end{vmatrix}$$

The two eigenvalues of the Arnold's matrix are $\lambda_1 = (3+\sqrt{5})/2$ and $\lambda_2 = (3-\sqrt{5})/2$, so that $\lambda_1 > 1$ and $0 < \lambda_2 < 1$. To λ_1 corresponds an eigenvector in an expanding direction and to λ_2 a perpendicular eigenvector in a contracting direction.

As remarked by Dyson and Falk[27] there is a simple relationship between the matrix generating Arnold integers and that generating the well known Fibonacci integers: [28]

$$F = \begin{vmatrix} 0 & 1 \\ 1 & 1 \end{vmatrix}$$

that is $F^2 = A$. Also, from (1a) and ((1b) one easily finds that

$$x_{k+1} = 3x_k - x_{k-1} \text{ and analogously } y_{k+1} = 3y_k - y_{k-1} \qquad \text{(2a), (2b)}$$

Here one of the variables has disappeared, but by compensation two of the previous x_{k+1} or y_{k+1} are now needed to define the next term. However, x_{k+1} still defines the corresponding y_{k+1}, through $y_{k+1} = x_{k+1} - x_k$

These numbers we shall call here to forth Arnold numbers a_i, so that $a_i \equiv x_i$ in eq. (1a), in honor of the above indicated contemporary mathematician, V. I. Arnold, and correspondingly the succession of Arnold numbers, Arnold series. The definition of these a_i numbers presents the analogy with the definition of the Fibonacci numbers f_i, in that each a_i as each f_i are defined through the two previous terms in the series, a_{i-1}, a_{i-2} and f_{i-1}, f_{i-2}.

In modular algebra it is clear that both the Arnold A and Fibonacci F matrices are periodic. For, in eqs (1a) and (1b) mod.M there are $2M(M-1)/2 = M(M-1)$ couples of different integers x_j , y_k to which should be added M-1 couples of equal integers x_j , y_i , the identical couple 0, 0 being forbidden. The total sums up to $M^2 - 1$ possible couples. It follows that at most after $M^2 - 1$ steps some couple of integers which has already appeared should appear again, and so a new period initiated. If it is assumed that there are no closed loops after a number of initial steps which do not repeat themselves, the new period shall begin with the first two terms initiating the process. In fact, the periods are much shorter than $M^2 - 1$. In ref. 27 it has been shown that the period cannot exceed 3M.

It may be demonstrated that if the Arnold matrix A has a periodicity P mod.M, then the periodicity of a couple of numbes x_k, y_k initiating Arnold's mapping, or equivalently the periodicity of the unitary vector originating in x_k, y_k on a bidimensional grid on which acts the matrix (1) is also P. If this were not so, the length of the trajectories on the grid would be dependent on x_k, y_k, and an asymmetry introduced in the problem which would completely change the periodicity, and consequently the reappearance of the cat. Analogous reasoning holds for the periodicity of the Fibonacci series in modulo M algebra. However, for a same modulus M, the Arnold and Fibonacci periods are not the same.

The proper Fibonacci series begins with 1, 1. In the same manner one can define a proper Arnold series by putting in (1a) and (1b) $x_1=1$ and $y_1=1$. However, one may also consider a generalized Arnold series, in analogy with the generalized Fibonacci series, where x_1, and y_1 may be any integers. Considering such generalized Arnold series and taking into account eq. (2a), the following proposition is evident: *Any integer number may be an element of an Arnold series, and this in an infinity of ways.*

Example: Taking $x_1 = a_1 = 1$ and $x_2 = a_2 = 1$, the twenty first Arnold numbers of the proper Arnold series are, according to relation (2a):

1, 1, 2, 5, 13, 34, 89, 233, 610, 1597, 4181, 10 946, 28 657, 75 025, 196 418, 514 229, 1 346 269, 3 524 578, 9 227 465, 24 157 817.

The period mod.5 is: 1,1,2,0,3,4,4,3,0,2, that is P=2M; it is easily checked that the period mod.7 has eight terms, that is P=M+1, and mod.11 five terms, that is (M-1)/2.

Using (2a) it is found that

$$a_k a_{k+2} - (a_{k+1})^2 = a_{k-1}a_{k+1} - a_k^2 = \text{constant} \qquad (3)$$

whatever k. Therefore, from the above three first terms of the proper Arnold series one has

$$a_{k-1}\, a_{k+1} - a_k^2 = 1 \qquad \text{(for the proper Arnold series)} \qquad (4)$$

whatever k. Of course, if a different Arnold series is considered, (3) will take other values. For example, if the two first terms are $a_1 = 3$, $a_2 = 7$, leading to the series 3, 7, 18, 47, 123, 322, 843…, one finds from the three first terms of the series that relationships (3) equal

now 5.

Notice that to obtain Arnold series differing from the proper one, one should choose initial integers which are different from two successive integers appearing in the proper series.

Using relationships (2) and (4), one also finds that

$$a_{k+1}a_{k-2} - a_k a_{k-1} = \text{constant} \qquad (5)$$

whatever k, the constant being equal to 3 for the proper Arnold series.

Quite certainly other such relationships can be found, however we shall be content here with the two examples (3) and (5) given above.

As a final remark, notice that three successive Arnold numbers are mutually coprime, because the *sum or difference of two coprime integers never have common decomposition factors with these two coprimes*.[29] From this and eqs (2a), (2b) it follows that no Arnold number is divisible by three and from $y_{k+1} = x_{k+1} - x_k$ it follows that the x and y series are always distinct.

REFERENCES

1) The Belousov-Zhabotinsky reaction is a far from thermodynamic equilibrium oscillating chemical reaction, discovered during the nineteen fifties by Belousov and then rediscovered by Zhabotinky; see for example G. Nicolis and I. Prigogine, *Exploring Complexity*, Freeman, New York 1989; see also ref. 5.

2) Phase space: If a physical system has X degrees of freedom (parameters defining it), the state of this physical system at time τ is described in an X dimensional reference frame by a point in that frame, and the successive states by a trajectory in the frame. For example, the frictionless pendulum is defined by the angle θ with the vertical at time τ_0 and the corresponding angular momentum by $d\theta/d\tau$. There are two degrees of freedom, the phase space is defined in a two dimensional reference frame, and the trajectory for small oscillations in Cartesian coordinates θ, $d\theta/d\tau$, is an ellipse.

3) Henri Poincaré, *Sur le problème des trois corps et les équations de la dynamique*, Acta Mathematica, 13 , 1-270 (1890). See any text on ergodic theory, for example ref. 12.

4) Herzsprung-Russel diagram: see the articles for white dwarfs, neutron stars and black holes in Wikipedia.

5) Excellent as an introduction to chaos theory is the following book : Pierre Bergé, Yves Pomeau and Christian Vidal, *L'ordre dans le chaos*, Hermann, Paris 1988. (In French.)

6) The autocorrelation function $C(\tau)$ is defined by

$$C(\tau) = \lim_{T\to\infty} (1/T) \int_0^T X(t)X(t+\tau)dt$$

where X(t) is a function of time t, T the limits of integration and τ the advance time. For periodic systems $C(\tau)$ is periodic, while for chaotic systems $C(\tau)$ tends to zero with increasing τ .

7) This reasoning may satisfy the mathematician. However, in physics, the reasoning does not apply, because of Heisenberg's indeterminacy principle which excludes the exact knowledge of both the position and the velocity of a gas molecule at a given time.

8) Edward Lorenz, J.Atmos.Sci., 20,130 (1963); see also ref. 10.

9) H.G. Schuster, *Deterministic Chaos*, VGH Publishers, Berlin 1989.
10) Ian Stewart, *Does God Play Dice ? The Mathematics of Chaos* p.141.
11) For the Bernoulli map, see for example D.J. Driebe, *Fully Chaotic Maps and Broken Time Symmetry*, Kluwer Academic Publishers, Dordrecht 1999.
12) V. I. Arnold; A. Avez, *Problèmes Ergodiques de la Mécanique Classique*. Paris: Gauthier-Villars, 1967.; English translation: V. I. Arnold; A. Avez, *Ergodic Problems in Classical Mechanics*. New York: Benjamin, 1968.
13) See for example H.E. Rose, *A Course in Number Theory*, second edition, Oxford University Press 1994.
14) C.F. Gauss, *Disquisitiones Arithmeticae*, translated in English by A.A. Clarke, Yale University Press 1965. Gauss' work was published in Latin in 1801 and dedicated to the prince of Brunswick and Lunebourg. The first French translation was done as early as 1807 by Poulet-Delisle, probably at the instigation of Laplace : Ch.-Fr. Gauss, *Recherches arithmétiques*, traduites par A.-C.-M. Poulet-Delisle, à Paris, chez Courcier, Imprimeur-Libraire pour les Mathématiques, quai des Augustins 1807. Reproduced by the Editions Jacques Gabay, 92330 Sceaux 1989.
15) L.E. Dickson, *History of the Theory of Numbers*, vol. I : *Divisibility and Primality*, Dover 2005 ; unabridged republication of Publication Number 256 in Washington, D.C. by the Carnegie Institute of Washington in 1919.
16) D.A., part III .
17) This was already noticed by Gauss, D.A., article 62. According to Dickson, ref. 14 p. 184, this was also stated by J. Ivory in the Encyclopaedia Britannica of 1824.
18) Be careful that the absolute values of α^v and $-\alpha^v$ (mod.p) are different so that they do not cancel when subtracted as in usual algebra.
19) D.A., part III, article 79.
20) This section A.2 essentially details and develops D.A.'s proposition 49.
21) For Gauss' approach in D.A., see article 84 and the other articles he indicates.
22) D.A., chap. III, articles 88-89.
23) G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, fifth edition, Clarendon Press Oxford 1979, Chap. VII, 7.4 ; (first edition 1938).
24) See ref. 13 p.91. This is a special case of Gauss' proposition 90.
25) D.A., articles 86 and 90.
26) Gauss, D.A. chap. III, article 90, says, in Clarke's translation : *If some power of the number 2 higher than the second, e.g.* 2^n*, is taken as modulus, the* 2^{n-2}*th power of any odd number is congruent to unity* . Though this is perfectly correct, it is not equivalent to saying that the period is 2^{N-2} mod.2^N . As here shown the period is shorter if 2 is not a PR of α, the base chosen, the congruence to unity occuring in this case before the index 2^{N-2}. This is once more the illustration that in number theory, theory should constantly be confronted to numerical tests, so the more today that computational means are presently available that were not at Gauss' epoch.
27) F.J. Dyson and H. Falk, *Period of a Discrete Cat Mapping*, American Mathematical Monthly, 99, 603-614 (1992).
28) Number theory including Fibonacci series and their applications to various fields in physics and computer theory are elegantly developed in a no axiomatic way in the following book: M.R. Schroeder, *Number Theory in Science and Communication*, second edition, Springer-Verlag 1990.
29) J. Dayantis and J.-F. Palierne, *A search of primes from lesser primes*, Journal of Discrete Mathematical Sciences and Cryptography, 10, 581-602 (2007).