Dependence of two simulated numbers generated by congruences

René Blacher

Dependence of two simulated numbers generated by congruences

René BLACHER

Laboratory LJK
Université Joseph Fourier
Grenoble
France

Summary : When we consider a congruence $T(x) \equiv ax$ modulo m as a pseudo random number generator, there are several means of ensuring the independence of two successive numbers. In this report, we show that this dependence depends on the continued fraction expansion of m/a. We deduce that the congruences such that m and a are two successive elements of Fibonacci sequences are those having the weakest dependence. We use this result in order to obtain sequences of random numbers proved IID.

Key Words : Fibonacci sequence, Random numbers, Congruence, Dependence, Correct models.

Résumé : Quand on considère une congruence $T(x) \equiv ax + b$ modulo m comme générateur de nombres pseudo-aléatoires, il y a plusieurs moyens de s'assurer de l'indépendance de deux nombres successifs. Nous avons deja vu que cette dépendance dépend du développement en fraction continue de m/a. Dans ce rapport nous continuons cette étude et nous majorons la distance entre la probabilité empirique d'un rectangle quelquonque et la probabilité uniforme. On a déduit de ces résultats que les congruences telles que m et a sont deux éléments successifs de la suite de Fibonacci sont celles ayant la dépendance la plus faible. Nous avons utilisé ce résultat pour obtenir des suites de nombres réellement aléatoires x_n.

Mots-clefs : Suite de Fibonacci, Nombres aléatoires, Modelès corrects, Congruence

Contents

Chapter 1

Presentation of results

1.1 Introduction

Congruences $T(x) \equiv ax + b \bmod(\mathrm{m})$, $0 < a < m$, $0 \leq b < m$ can be used as pseudo-random generators. But of course, all the parameters a, b and m are not suitable. They must check a certain number of conditions. In this report we are interested in conditions about the independence of 2 successive numbers simulated. More generally, we must impose that the dependence induced by $\big(T^n(x_0), ..., T^{n+p}(x_0)\ \big)$, n=1,2,....,m, is as small as possible when p is as large as possible. In fact, you can hardly go beyond $p = log(m)/log(2)$.

Recall first that the independence induced by $\big(T^n(x_0), T^{n+1}(x_0)\big)$, n=1,2,....,m, does not imply the independence of $\big(T^n(x_0), T^{n+1}(x_0), T^{n+2}(x_0)\ \big)$, n=1,2,....,m. And in fact, the conditions which ensure the best independence of two successive simulated numbers are not the ones which provide the best independences of 3 successive simulated numbers, and vice versa.

In this report we study the independence of two successive numbers simulated. However, we saw in [9] and [8] that the dependence of two successive simulated numbers depends on the development of $\frac{m}{a}$ as continued fraction.

Notations 1.1.1 *Let $r_0^a = m$, $r_1^a = a$. One denotes by r_n^a the sequence defined by $r_n^a = h_{n+1}^a r_{n+1}^a + r_{n+2}^a$ the Euclidean division of r_n^a by r_{n+1}^a when $r_{n+1}^a \neq 0$. One denotes by d^a the smallest integer such as $r_{d^a+1}^a = 0$.*

One sets $k_0^a = 0$, $k_1^a = 1$ and $k_{n+2}^a = h_{n+1}^a k_{n+1}^a + k_n^a$ if $n \leq d^a + 1$.

With theses notations, one can write

$$\frac{m}{a} = h_1^a + \frac{1}{h_2^a + \frac{1}{h_3^a + \frac{1}{h_4^a + \ldots}}}\ .$$

Then, in order that the independence of two successive simulated numbers is good, it is necessary that the h_i^a's are small.

Indeed, in [16] (cf also [10] [9] [15]), we have shown the following theorem.

Theorem 1.1.2 *Let $(x_0, y_0) \in E_2$. Let $n \in \{1, 2, ..., d^a + 1\}$.*

If n is even,

$$E_2 \cap R^0 = \big\{(x_0 + k_{n-1}^a \ell\ ,\ y_0 + r_{n-1}^a \ell)\big| \ell = 0, 1, 2, ..., h_{n-1}^a\big\}\ ,$$

where $R^0 = [x_0, x_0 + k_n^a] \otimes [y_0, y_0 + r_{n-2}^a[\subset [0, m[^2$.

If n is odd,

$$E_2 \cap R^0 = \big\{(x_0 + k_{n-1}^a \ell\ ,\ y_0 - r_{n-1}^a \ell)\big| \ell = 0, 1, 2, ..., h_{n-1}^a\big\}\ ,$$

where $R^0 = [x_0, x_0 + k_n^a] \otimes [y_0 - r_{n-2}^a, y_0[\subset [0, m[^2$ [1].

This allows to obtain a lower bound of the coefficient of discrepancy.

Definition 1.1.3 *For all* $z \in \mathbb{Z}$*, we denote by* $\overline{z}$ *the integer* $\overline{z}$ *such that* $\overline{z} \equiv z$ *modulo* m *and* $0 \leq \overline{z} < m$*. For all rectangle,* $R = [s_1, s_2] \times [t_1\, t_2] \subset [0, m]^2$*, we denote by* N_R^n *the number of points of the sample* $(\overline{T}^i(x_0), \overline{T}^{i+1}(x_0))$*, i=1,2,....,n, belonging to the rectangle* R *and by* S_R *the area* $S_R = (s_2 - s_1)(t_2 - t_1)$*. If* $n = m$*, one sets* $N_R = N_R^m$*.*

We call coefficient of discrepancy D_m^2 [2] *the number*

$$D_m^2 = Max_R\Big(\Big|N_R - \frac{S_R}{m}\Big|\Big) \ ,$$

where the maximum is taken over all the rectangles $R = [s_1, s_2] \times [t_1\, t_2] \subset [0, m]^2$ *such that* $(s_1, s_2, t_1, t_2) \in \{0, 1, ..., m\}^4$*.*

We shall deduce from theorem 3.1.1 the following proposition (proof is in lemma 3.1.3) .

Proposition 1.1.4 *The following inequality holds :*

$$\frac{Max_{i=1,...,d^a}(h_i^a)}{4} \leq D_m^2 \ .$$

It allows to understand that the independence of two successive simulated numbers depends on the h_i^a's. Naturally, the study of independence between two successive simulated numbers had already been studied by various authors, and for some ones, one recognizes a connection with the h_i^a's.

Thus the simplest test which springs immediately to mind is the serial test. This one is just the chi squared test with several dimensions (cf. [1] page 62). Unfortunately it does not use the best chi squared test. Indeed, in this case, it is better to use the chi squared independence test which is more powerful: in 2 dimensions it uses $\chi_{X,Y}^2 - \chi_X^2 - \chi_Y^2$ where $\chi_{X,Y}^2$, χ_X^2, χ_Y^2 are respectively, the classical chi square statistics with two dimensions, the classical chi square statistics for the first marginal distribution, and the classical chi square statistics for the secund marginal distribution (cf Blacher [7], [6]). In fact it means to use empirical higher order correlations coefficients (cf [5]) and Hilbertian test (cf [4], [6]).

Now the spectral test is also interested in the problem of n-tuples of successive numbers: in the case of two dimensions we therefore studied the sequence $(T^i(x_0), T^{i+1}(x_0))$, i=1,2,....,m. It is easy to see that the points of these sequences are distributed over the parallel lines of the plane. Then, by [1] page 94, in order to use the spectral test, one uses $1/\nu_2$ the maximum distance between lines taken over all families of parallel straight that cover the points $(T^i(x_0)/m, T^{i+1}(x_0)/m)$: the spectral test is based on the value of ν_2.

On the other hand, Marsaglia has studied lattices and showed how they are connected to the dependence of p successive numbers. Unfortunately, we know that, from this point of view, linear congruences are very bad random generators: they do not pass the test of lattices. This is due to the structure of hyperplane of the samples $(a^{j+1}x_0, a^{j+2}x_0, ...a^{j+j}x_0)$, j=1,2.....m. However, there are methods to mix a congruential generator in order to destroy its regularity of crystal : Knuth (cf [1], M. D Maclaren and G marsaglia (cf [21]). In the search of linear congruences candidates for this mixture, one chooses those ones of which the lattice (e.g. in size 2,3,4,5) is not too distant from the ideal lattice: it is assumed that this is the case when the quotient Beyer of its reduced base is close to 1 (cf [3]). There are examples in [2] page 73.

[1] There was an error of writing in [16] . Here, it is corrected

[2] This is a slightly different definition of the usual definition. Indeed, generally, one calls coefficient of discrepancy the number D_m^2/m : e.g. cf [1] page 110

Now, Dieter has studied in 1972 (cf [18]) the case of a two-dimensional dependence. In fact, he studied the discrepancy coefficients $D_m^2 = Max_R\big|N_R - \frac{S_R}{m}\big|$.

Indeed Dieter (1972) showed that the dependence between two successive numbers simulated depends generalized Dedekind sums $s(a,c|x,y) = \sum_{\mu=0}^{|c|-1} Q\Big(\frac{\mu+y}{c}\Big)Q\Big(a\frac{\mu+y}{c}+x\Big)$ where $Q(x) = 0$ if $x \equiv 0 \bmod 1$ and $Q(x) = x - \lfloor x \rfloor - 1/2$ if $x \not\equiv 0 \bmod 1$ when $\lfloor x \rfloor$ is the integer part of x.

For example suppose b=0, and $m = 2^e$. One supposes that m is the length of the generated pseudo random sequence. Then,

$$D_m^2 = \sum_{\lambda,\mu=1}^{2} (-1)^{\lambda+\mu} s(a,n|as_\lambda - t_\mu, 1/4 - ns_\lambda) + \rho$$

where ρ is bounded by 4.

It leads to the following rule for the choice of the factor a : The factor a has to be chosen in such a way that the Euclidean Algorithm for a and m ($b \neq 0$, or a and m/4 (b=0) should have small quotients q_i . As a matter of fact $q_i = h_i^a$ if $b \neq 0$.

We thus find the same conclusion as we got first in 1983 in [8] and [9]. However, our results were more detailed and more general. Some of those have been taken up by Niederreiter in 1985 (cf [19]), which has established (with Knuth) connections between the spectral test and serial test.

Let r be the function such that $1/r(u_1,u_2) = msin(\pi u_1/m)sin(\pi u_2/m)$ when $u_1 + au_2 \equiv 0$ modulo m . Then, Niederreiter proved

$$D_m^2 = O\Big(log(m)^2 Max_{u_1,u_2}|r(u_1,u_2)|\Big) \tag{1.1}$$

when the period is m. Moreover, Niederreiter has proved in 1985 that if m is prime and has a primitive root modulo m or if $m = 2^\beta$, $\beta \geq 3$, $a \equiv 5$ modulo m and b odd or b=0, then

$$D_m^2/m \leq \frac{C' log(m)^2}{\rho^2(a,m)} \tag{1.2}$$

where $\rho^2(a,m) = min(r'(2H_1,2H_2))$ when $r'(H) = \prod_{i=1}^2 max(1,|H_i|)$ for $H_i \in \mathbb{Z}$ for all i and where C' is a constant (cf also [2], page 79).

This result is similar to our result of 1983. Indeed, by [2], page 79, Zaremba has proved in 1966 that, under these assumptions, $\rho^2(a,m)$ depends on the development of m/a in continued fraction (cf [23]) : $\rho^2(a,m) \leq \frac{1}{4Max_i(h_i^a)}$, and then,

$$D_m^2 \leq C_4' Max(h_i^a) log(m)^2 \ .$$

Now our result of 1983 is more accurate. For example, it has been proved an increase more detailed than Niederreiter. We thus find a finite sequence of rectangles R_n such that $\Big|N_{R_n} - \frac{S_{R_n}}{m}\Big| \leq 1$. This helps to understand how rectangles R are filled by the points $(\overline{T}^i(x_0), \overline{T}^{i+1}(x_0))$.

Then, it is hoped that the following conjecture holds

$$\big|N_R - \frac{S_R}{m}\big| \leq Max_i(h_i^a) O\big(log\big(log(m)\big)\big) \ .$$

This is still a conjecture (cf conjecture 1.2.8). On the other hand, one can mathematically prove an increase more detailed than Niederreiter:

$$\Big|N_R - \frac{S_R}{m}\Big| \leq Max_i(h_i^a) \frac{2log(m) - log(2)}{log(2)} \ .$$

We will return to this below (cf corollary 1.2.5).

Therefore the h_i^a's must be small. Then, we were also interested in case they are minimum : $h_i^a = 1$ for $i = 1, 2, ..., d^a - 1$ and $h_{d^a}^a = 2$: This is the case of Fibonacci congruences. Thus, in this case, Zaremba gave an increase more accurate than $D_m^2 \leq \frac{C' 4Max(h_i^a) log(m)^2}{m}$. He proved that

$$\left| N_R - \frac{S_R}{m} \right| \leq 4A \frac{log[(A+1)m]}{log(A+1)} + 1 < (7/6) log(15m) \ ,$$

where $A = sup_{i=1,..,d^a-1}(h_i^a) = 1$ (cf [23]).

Unfortunately, congruences Fibonacci are very bad pseudo-random generators : indeed, in this case, $T^2 \equiv \pm Id$, where Id is the Identity function. On the other hand, they can be used effectively in order to calculate double integrals as it is shown by Zaremba (cf [23]).

Moreover, in [17], we have seen that the the congruential functions of Fibonacci T_q make uniform noises by a remarkable way.

Definition 1.1.5 *Let $q \in \mathbb{N}^*$. Let T be a congruence of Fibonacci. We define the congruential function of Fibonacci T_q by $T_q = Pr_q \circ \widehat{T} \in [0,1]$ where*
1) $\widehat{T}(x) = \overline{T}(xm)/m$, when $\overline{z} \equiv z$ modulo m and $0 \leq \overline{z} < m$ if $z \in \mathbb{Z}$,
2) $Pr_q(z) = \overline{0, b_1 b_2 .... b_q}$ when $z = \overline{0, b_1 b_2 ...}$ is the binary writing of z.

Indeed, for the great majority of noises y_n relatively unpredictable, the sequences $T_q(y_n)$ admit the IID model for correct model. It was the first time that such a result was obtained. For example, before this result, it was written in Handbook of Applied Cryptography ([20]) : "Designing a hardware device or software program to exploit this randomness and produce a bit sequence that is free of biases and correlation is a difficult task. Moreover, random bit generators based on natural sources of randomness are subject to influence by external factors, and also to malfunctions. It is imperative that such devices be tested periodically".

We will return later to the question of Fibonacci functions which make uniform the most part of noises (cf section 1.3).

In order to help to clarify these results we will now develop these different results. Unfortunately our report ([9]) and our thesis of 1983 ([8]) are written in French. Also in order to be more accessible, we will take up a large part of the proofs of 1983 in English. We detail them when it is necessary. Then we develop them in order to show how you can specify, by a fairly exact way, the number of points of the sample contained in each rectangle $R = [x, x + L[\times [y, y + L'[$ when x, y, L, $L' \in \{0, 1, ..., m\}$.

1.2 General case

We study the distribution of the points $\{\ell, T(\ell)\}$.

Notations 1.2.1 *Let $E_2 = \left\{ \ell, \overline{T(\ell)} \mid \ell \in \{0, 1, ..., m-1\} \right\}$ when $\overline{z} \equiv z$ modulo m and $0 \leq \overline{z} < m$ if $z \in \mathbb{Z}$.*

We have just to say that, in order that there have not strong dependences, it is necessary that the h_i^a's is small. Indeed, in [15] and [16], we proved that it is a necessary condition in order that there is empirical asymptotic independence (cf theorem 3.1.1). Thus, if n is even, if $x_0 = y_0 = 0$, theorem 3.1.1 means that the rectangle $[0, k_n^a/2] \otimes [r_{n-2}^a/2, r_{n-2}^a[$ does not contain points of E_2 if n is even : $E_2 \cap \left\{ [0, k_n^a/2] \otimes [r_{n-2}^a/2, r_{n-2}^a[\right\} = \emptyset$. If h_{n-1}^a is large, that will mean that an important rectangle of $\mathbb{R}^2$ is empty of points of E_2: that will mark a breakdown of independence.

For example suppose n=2 and b=0. First, $m = r_0^a$, $r_1^a = a$, $k_1^a = 1$ and $k_2^a = h_1^a = \lfloor m/a \rfloor$ where $\lfloor x \rfloor$ means the integer part of x. In this case, one regards the rectangles $[0, k_2^a[\otimes[0, m[$. One thus finds a traditional technique for n=2. Indeed when one makes chi-squared tests, one can use rectangles of same type as$[0, m/(2a)[\otimes[0, m/2[$.

Thus if "a" is not large enough compared to "m", there is rupture of independence. The rectangle $Rect_2 = [0, m/(2a)] \otimes [m/2, m[$ will not contain any point of E_2. However, this rectangle has its surface equal to $m^2/(4a)$: if the points of E_2 are distributed in a uniform way, one has about $m/(2a) = h_1^a/2 + r_2^a/(2a)$ points of E_2 (and not 0). Thus if "a" is not sufficiently large, i.e if h_1^a is too large, there is breakdown of independence.

For example, choose the congruence $T(x) = 10^3 x$ modulo $10^6 - 1$: $Rect_1 = [0, m/(2a)] \otimes [0, m/2[$ contains 500 points of E_2 roughly and $Rect_2$ contains 0 points. Then the chi-squared test that one could make with such rectangles are not satisfied.

Now choose m=99, a=5, $k_2^a = 19$: cf figure 1.1: $Rect_1$ roughly contains 10 points of E_2 for a total sample of 99.

Choose m=99, a=10, $k_2^a = 9$: cf figure 1.2: $Rect_1$ roughly contains 5 points of E_2 : the breakdown is less clear.

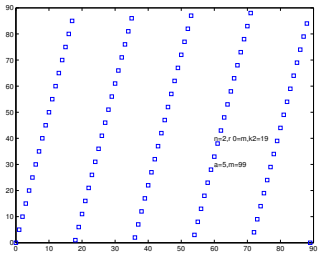

Figure 1.1: Points in rectangles a=5

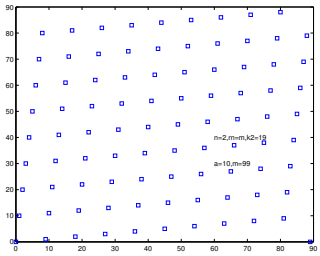

Figure 1.2: Points in rectangles a= 10

In these examples, we studied rectangles $[0, k_2^a/2] \otimes [0, m/2[\}$. In the general case, it is necessary that $[0, k_n^a/2] \otimes [r_{n-2}^a/2, r_{n-2}^a[\}$ has not a too big size. It is necessary thus that all the h_{n-1}^a's are small.

In fact, the results which we develop in this report will allow to prove that it is also a sufficient condition : if the h_i^a's are small enough one can suppose that there is independence (cf [10]).

Now we use a sequence h_i a little different from h_i^a in order to get the exact number of points contained in some rectangles $[x, x + L[\times[y, y + L'[$.

Notations 1.2.2 *One denotes by r_n the sequence defined by : $r_0 = m$, $r_1 = inf(a, m-a)$ and by $r_n = h_{n+1}r_{n+1} + r_{n+2}$ which denotes the Euclidean division of r_n by r_{n+1} when $r_{n+1} \neq 0$. One denotes by d the smallest integer such as $r_{d+1} = 0$ $(d \geq 1)$.*

One sets $k_0 = 0$, $k_1 = 1$ and $k_{n+2} = h_{n+1}k_{n+1} + k_n$ if $n \leq d+1$.

With these new notations, it will be also necessary that the h_i are small in order to have a good independence.

We can deduce an increase of D_m^2 (cf corollary 2.7.15).

Theorem 1.2.3 *Let x, y, L, $L' \in \{1, 2, ..., m\}$ and let R be the rectangle $R = [x, x+L[\times[y, y+L'[$. Let $h^s = sup(h_i)$ and S_R be the area of R $(S_R = LL')$, $N_R = card(E_2 \cap R)$. We suppose that T is invertible. Then*

$$\left| N_R - \frac{S_R}{m} \right| \leq \sum_{i=1}^{d} h_i + 2 \leq dh^s + 2 \ .$$

Moreover, the following proposition holds (cf proposition 2.7.8)

Proposition 1.2.4 *We have $d \leq 2\frac{log(m)-log(2)}{log(2)}$.*

Then, one deduce the following result.

Corollary 1.2.5 *Under the assumptions of theorem 1.2.5,*

$$\left| N_R - \frac{S_R}{m} \right| \leq \frac{2log(m) - log(2)}{log(2} h^s \ .$$

We see that this equality is more accurate than that obtained by Nederietter and Knuth (cf equations 1.1 and 1.2).

Remark 1.2.6 *In these theorems we require that T is invertible. But there could be results of the same type if T is not invertible. Indeed, we do not impose any conditions in our calculations for sections 2.2, 2.3, 2.4, 2.5. In particular, the fundamental proposition 2.5.3 is given under no hypothesis.*

But, to get answers in the general case would complicate the results of this report which are already long. Moreover, if T is not invertible, the period is smaller than m.

In fact, one can have more accurate results because we have a much more accurate increase for some rectangles R.

Indeed, the previous increases improve clearly the increase of Niederreiter and Knuth. But it is still too rough. It is enough to use again the proofs in order to understand that the points of E_2 are distributed by a much more uniform way. Thus, we will prove the following theorem (cf theorem 2.6.14).

Theorem 1.2.7 *Let T be a invertible linear congruence. Let $c \in \{1, 2, ..., d\}$. Let $\mathcal{T} \in \mathbb{N}$ such that $\mathcal{T} + c < d + 1$.*

Let $\lambda_i \in \mathbb{N}$, $i = 1, 2, ..., \mathcal{T}$ be a sequence checking $\lambda_1 < h_{c+1}$, and for all $i \in \{1, 2, ..., \mathcal{T}\}$, $\lambda_i \leq h_{c+i}$ and if $\lambda_i = h_{c+i}$, then, $\lambda_{i-1} = 0$. We suppose that $L = \sum_{i=1}^{\mathcal{T}} \lambda_i k_{c+i}$.

Let $f \in \mathbb{N}^*$ $f \leq h_c$. Let $R^o = [x, x + L[\times[y, y + fr_c[$. Then,

$$\left| N_{R^o} - \frac{S_{R^o}}{m} \right] \leq 1 \ .$$

This is not the only result that will allow us to refine the increase of D_m^2. Thus we can see in the proofs of Section 2.3 that we know how the rectangles R are filled by the points of E_2. We then realized that we can increase D_m^2 by a way more accurate than that given in the theorem 1.2.5.

It is shown by numerical studies which we have done for various different rectangles R and various congruences T (cf chapter 3). Of course, this study was simplified by the theoretical study that shows how the way points E_2 are distributed in the rectangles R (cf chapter 2).

Finally this numerical study and the different lemmas of chapter 2 suggests that the following conjecture is checked.

Conjecture 1.2.8 *The following inequalities hold*

$$\frac{h^s}{4} \leq Sup_R\Big(\Big|N_R - \frac{S_R}{m}\Big|\Big) \leq h^s O\big(log(log(m))\big) \ .$$

In fact it is even possible that there exists a constant C "such that $Sup_R\Big(\Big|N_R - \frac{S_R}{m}\Big|\Big) \leq C"h^s$ [3]. Then, a study should also be conducted in order to refine this result. We do not it here. This report is already big enough. But it will be the basis when we shall want to complete this study. So we will complete this proof later.

1.3 Fibonacci Congruence

By using the theorem 1.2.5, it was proved [10] that in some cases where the h_i's are small enough, one can consider that one has the independence between two successive elements. So we will take an interest in case where the h_i's are the smallest possible. As $h_i^a \geq 1$ and $h_{d^a}^a \geq 2$, the congruence which defines the best independence of E_2 will check $h_i^a = 1$ and $h_{d^a}^a = 2$. This case, is the case of congruences of Fibonacci already studied by Zaremba : cf [23].

Definition 1.3.1 *If T checks $h_i^a = 1$ and $h_{d^a}^a = 2$ and if T is invertible, we call T congruence of Fibonacci.*

Indeed, the following result holds

Proposition 1.3.2 *If there exists n_0 such that $a = fi_{n_0}$ and $m = fi_{n_0+1}$ where fi_n is defined by $fi_1 = fi_2 = 1$ and if $n \geq 1$, $fi_{n+2} = fi_{n+1} + fi_n$, $T(x) \equiv ax$ modulo m is a congruence of Fibonacci.*

Proof Because T is invertible, $r_d = 1$ (cf Lemma 2.6.3). Moreover, $r_{d^a}^a = 1$ (cf lemma 2.1.3). We deduce the result. ■

Of course, there exists an infinity of Fibonacci congruences.

In this case, $a = fi_{d^a+1}$ and $m = fi_{d^a+2}$, i.e. $n_0 = d^a + 1$. More generally, the sequences r_n and k_n are the sequence of Fibonacci except for the last terms. For example if $d^a = 6$:
$r_{d^a-d^a}^a = r_0^a = m = 21$, $r_{d^a-(d^a-1)}^a = r_1^a = a = 13$, $r_2^a = 8$, $r_3^a = 5$, $r_4^a = 3$, $r_{d^a-1}^a = r_5 = 2$, $r_{d^a}^a = r_6^a = 1$, $r_{d^a+1}^a = r_7^a = 0$.
$h_1^a = h_2^a = ... = h_{d^a-1}^a = 1$ and $h_{d^a}^a = 2$.
$k_0^a = 0$, $k_1^a = 1 = fi_1$, $k_2^a = 1 = fi_2$, $k_3^a = 2 = fi_3$, $k_4^a = 3 = fi_4$, $k_5^a = 5 = fi_5$, $k_6^a = k_{d^a}^a = 8 = fi_6$, $k_7^a = k_{d^a+1}^a = 21 = m = fi_8$.

[3] However, if this were the case, we would not understand why the coefficient $O\Big(log(log(m))\Big)$ would appear in the simulations which we have made about the proposition 1.3.7 (cf [17], cf also section 3.2).

More generally,
$r^a_{d^a-d^a} = r^a_0 = m = fi_{d^a+2}$, $r^a_{d^a-(d^a-1)} = r^a_1 = a = fi_{d^a+1}$, $r^a_2 = fi_{d^a}$, $r^a_3 = fi_{d^a-1}$,.....,
$r^a_{d^a-2} = 3$, $r^a_{d^a-1} = 2$, $r^a_{d^a} = 1$, $r^a_{d^a+1} = 0$.
$h^a_{d^a} = 2$, $h^a_{d^a-1} = h^a_{d^a-2} = ... = h^a_2 = h^a_1 = 1$.
$k^a_0 = 0$, $k^a_1 = 1 = fi_1$, $k^a_2 = 1 = fi_2$, $k^a_3 = 2 = fi_3$,.....,$k^a_{d^a} = fi_{d^a}$, $k^a_{d^a+1} = m = fi_{d^a+2}$.

These properties are reflected by the following proposition (cf also lemma 2.6.16).

Proposition 1.3.3 *We suppose that T is the congruence of Fibonnacci. Then,* $r_i = fi_{d^a-i+2}$.

We confirm by graphs that it is the Fibonaccci congruence which ensures the best independence between two simulated successive numbers. We suppose m=21. If a = 13, we have a Fibonacci congruence : cf figure 1.3. If one chooses a=10, $sup(h^a_i) = 20$: cf figure 1.4 . If one chooses a=5, $sup(h^a_i) = 5$: cf figure 1.5.

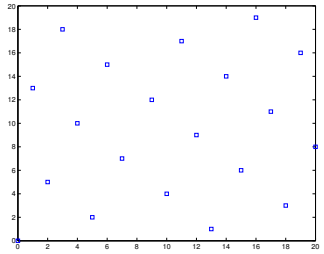

Figure 1.3: Fibonacci congruence

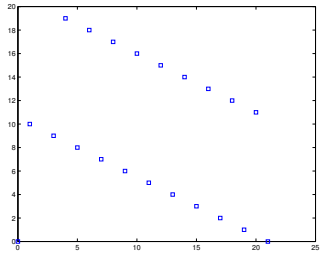

Figure 1.4: $sup(h^a_i) = 20$

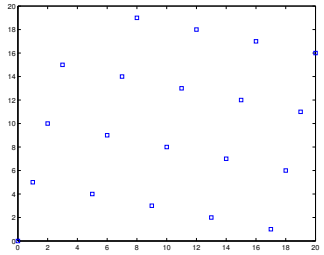

Figure 1.5: $sup(h^a_i) = 5$

Now, we can specify the theorem 1.2.5 for the Fibonacci congruence (cf proposition 2.7.8 and lemma 2.7.12, 2.7.7).

Proposition 1.3.4 *We suppose that T is the congruence of Fibonnacci where* $d \geq 13$. *Then, for all rectangle* $R = [x, x + L \times [y, y + L'[$,

$$\Big|N_R - \frac{S_R}{m}\Big| \leq 4\frac{log(m) - log(2)}{log(2)} \ .$$

Unfortunately if the Fibonacci congruence ensures the best independence between two simulated successive numbers, it is also a pseudo-random generator very bad. Indeed, by lemma 2.6.16, we have the following proposition.

Proposition 1.3.5 *If* $T(x) \equiv ax \ mod \ m$ *is the congruence of Fibonacci, then* $T^2 \equiv \pm Id$ *where* $Id(x) = x$.

Therefore, it can not be used as pseudo-random generator.

On the other hand, it can be used in order to make uniform noises. Indeed, we have seen that if we transform noise y_n, n=1,2,....,N, by using the congruential functions of Fibonacci, in most cases, we transform this noise in IID sequences $x_n = T_q(y_n)$, n= 1,2,....,N, when q and m are correctly chosen according to N : very precisely, x_n admits the IID model for correct model (cf [17]).

In order to prove this, we use the fact that Fibonacci congruences transform intervals into sets well distributed in $\{0, 1, ..., m - 1\}$.

Notations 1.3.6 *We suppose that T is the Fibonacci congruence. Let* $I = [c, c'[$, $c, c' \in \{0, 1, ..., m-1\}$ *and let N(I)=c'-c. Let* g^n *be the permutation of* $\{c, c+1, ..., c'-c\}$ *such that* $\overline{T}(g^1) < \overline{T}(g^2) < \overline{T}(g^3) < ..... < \overline{T}(g^{c'-c})$.

Because, $T^2 = \pm Id$, $T^{-1} = \pm T$ and $\overline{T}^{-1}(g^1) < \overline{T}^{-1}(g^2) < ..... < \overline{T}^{-1}(g^{c'-c})$ or $\overline{T}^{-1}(g^1) > \overline{T}^{-1}(g^2) > ..... > \overline{T}^{-1}(g^{c'-c})$.

Since $\overline{T}(I)$ behaves as independent of I, normally, we should find that $\overline{T}(I)$ and, therefore $\overline{T}^{-1}(I)$, is well distributed in $\{0, 1, ..., m - 1\}$. As a matter of fact it is indeed the case : for all numerical simulations which we made, one has always obtained, for r=1,2,....,c'-c-1,

$$\Big|\frac{\overline{T}(g^r)}{m} - \frac{r}{N(I)}\Big| \leq \frac{\varphi(m)}{N(I)} \ ,$$

where $\varphi(m) << Log(m)$: cf [10]. In fact, by numerical simulations which we have done, it seems $\varphi(m)$ is the order of Log(Log(m)). Moreover,

$$Max_{r=0,1,....,N(I)-1}\Big(\Big|\frac{N(I)T^{-1}(g^r)}{m} - r\Big|\Big)$$

seems maximum when I is large enough : $c' - c = O(m/2)$ (cf [10]).

In order to prove this result, we have used simulations. Now with the results of this report we can prove mathematically a result of the same type. Indeed, by proposition 2.7.16, we have the following theorem.

Proposition 1.3.7 *We suppose that T is the Fibonacci congruence with* $m \geq 377$. *Then, for all* $r \in \{1, 2, ..., N(I) - 1\}$,

$$|\frac{\overline{T}(g^r)}{m} - \frac{r}{N(I)}| \leq \frac{\phi'(m)}{N(I)},$$

ou $\phi'(m) = \frac{4Log(m)-2Log(2)}{log(2)}$.

By using these increases, it has been obtained in [17] a method in order to obtain a sequence proved IID, what gives a first solution to this search started since many years. For this, it is necessary that the noises y_n, n=1,2,....,N, admit for correct model a sequence of random variable Y_n, n=1,2,....,N, of which the conditional densities with respect to the uniform discrete measure have Lipschitz coefficients not too large, i.e. the noise y_n is not too deterministic.

At last Zaremba showed that we could use the Fibonacci congruences in order to calculate double integrals. He has given [23] an increase of the error in this case.

Chapter 2

Proofs

2.1 Introduction to the proofs

We study the set $E_2 = \{\ell, \overline{T(\ell)} \mid \ell \in \{0, 1, ..., m-1\}\}$.

2.1.1 Notations

Remark that we do not use the same notations as in [10] [9] [15] and [16]. Indeed, we suppose here that $r_1 = inf(a, m-a)$. As a matter of fact the sequences r_n, h_n, k_n of [10] [9] [15] and [16] are the sequences r_n^a, h_n^a, k_n^a of this report. We recall their definition.

Notations 2.1.1 *One denotes by r_n the sequence defined by : $r_0 = m$, $r_1 = inf(a, m-a)$ and $r_n = h_{n+1}r_{n+1} + r_{n+2}$ the Euclidean division of r_n by r_{n+1} when $r_{n+1} \neq 0$.*
Moreover, one denotes by d the smallest integer such that $r_{d+1} = 0$ ($d \geq 1$). One sets $r_{d+2} = 0$.

Now we define k_n for this new sequence r_n. The definition remains the same as before, except that we change r_1.

Notations 2.1.2 *One sets $k_0 = 0$, $k_1 = 1$ and $k_{n+2} = h_{n+1}k_{n+1} + k_n$ if $n \leq d+1$.*

Clearly k_n is strictly increasing and r_n strictly decreasing. Moreover, $h_n \geq 1$, $r_1 \leq m/2$.

Finally, there is no difference if $r_1 \leq m/2$. As a matter of fact the connections between the sequences r_n^a and r_n are clarified by the following lemma.

Lemma 2.1.3 *If $a < m/2$, $r_n^a = r_n$, $h_n^a = h_n$ and $k_n^a = k_n$.*
If $a > m/2$, $r_0^a = r_0 = m$, $r_1^a = a$, $r_2^a = r_1 = m-a$, $h_1^a = 1$, $h_2^a + 1 = h_1$ and for $n \geq 2$, $r_{n+1}^a = r_n$, $h_{n+1}^a = h_n$ and $d^a = d+1$.
Moreover, $k_0^a = k_0 = 0$, $k_1^a = k_1 = 1$, $k_2^a = 1$, $k_3^a = h_1 = k_2$ and for $n \geq 2$ $k_{n+1}^a = k_n^a$.

Proof If $a < m/2$, it is obvious.

If $a > m/2$, $r_0^a = r_0 = m$, $r_1^a = a$.
Now $r_0^a = m = a + (m-a)$ where $m - a < a = r_1^a$.
Therefore, $m = a + (m-a)$ is the Euclidean division of m by a, i.e. of $r_0^a = m$ by $r_1^a = a$.
Therefore $m = a + (m-a)$ is identical to $r_0^a = h_1^a r_1^a + r_2^a$.
Therefore, $h_1^a = 1$ and $r_2^a = m - a$.

On the other hand, $r_2^a = m - a$. Therefore, $r_2^a = r_1$.

Moreover, $m = r_0 = h_1 r_1 + r_2$ is written $r_0 = m = h_1(m-a) + r_2 = h_1 r_1 + r_2$ with $h_1 \geq 2$.
Therefore, $m - r_1 = (h_1 - 1)r_1 + r_2$ with $r_2 < r_1$. Thus it is an Euclidean division.
Because $r_1^a = h_2^a r_2^a + r_3^a$, $h_2^a = (h_1 - 1)$ and $r_3^a = r_2$.

Because $r_2^a = r_1$ and $r_3^a = r_2$ the following Euclidean divisions
$r_2^a = h_3^a r_3^a + r_4^a$ and $r_1 = h_2 r_2 + r_3$
are identical. QED

For the sequences k_n^a and k_n,
$k_0^a = 0$, $k_1^a = 1$,
$k_2^a = h_1^a k_1^a + k_0^a = 1 * 1 + 0 = 1$,
$k_3^a = h_2^a k_2^a + k_1^a = (h_1 - 1) * 1 + 1 = h_1$,
$k_4^a = h_3^a k_3^a + k_2^a = h_3^a h_1 + 1 = h_2 h_1 + 1$,
$k_5^a = h_4^a k_4^a + k_3^a$,

$k_0 = 0$, $k_1 = 1$,
$k_2 = h_1 k_1 + k_0 = h_1$,
$k_3 = h_2 k_2 + k_1 = h_2 h_1 + 1$,
$k_4 = h_3 k_3 + k_2$.
And so on. ■

Now we shall need the following notations.

Notations 2.1.4 *Let $J_t = \{0, 1, ..., t\}$ and $J_t^* = \{1, 2, ..., t\}$, $t \in \mathbb{N}^*$.*

Remark that J_{d+1}^* is the set of definition of h_n.

Notations 2.1.5 *We suppose that we have an integer $c \in J_d^*$ and an integer $f \in \mathbb{N}^*$ such that $f \leq h_c$. We denote by a_s the number belonging to $\{a, m-a\}$ such that $\overline{k_c a_s} = r_c$ (cf lemma 2.2.1). Moreover, in section 2.3, 2.4 and 2.5, we suppose $\overline{k_c a} = r_c$. We denote by M, M^+ and M^f the sets*

$$M = \{l \in \mathbb{N} | \overline{al} < r_c\},$$
$$M^+ = \{l \in \mathbb{N} | \overline{al} \leq r_c\},$$
$$M^f = \{l \in \mathbb{N} | \overline{al} \leq f r_c\}.$$

We are now going to clarify by graph what represent these notations. As a matter of fact, because $\{(\ell, \overline{a\ell + b}) | \ell = 0, 1, ..., m-1\} = \{\overline{(\ell, \overline{a\ell}) + (0, b)} | \ell = 0, 1, ..., m-1\}$, we are brought to the study of the sequence $\mathbb{R}^2 : U_\ell = (\ell, \overline{a\ell})$, $\ell \in \mathbb{N}$, or of the sequence $\{\overline{a\ell}\}$.

For example, suppose that a=24298 m= 199017. We see that $[0, m/a[\times [0, m[$ contains 9 points of E_2 of ordinates $a\ell$ and of abscissa ℓ. In this case, we have $r_1 = a$ and $r_2 = m - 8a$, i.e. $h_1 = 8$. Moreover, r_2 is the distance of y= 8a, the highest point of E_2 in $[0, m/a[\times [0, m[$, to y= m : cf figure 2.1.

Now, if we study the points U_ℓ of $\left[\frac{m}{a}, \frac{2m}{a}\right[\times [0, m[$, we understand that their ordinates are deduced of the ordinates of $[0, m/a[\times [0, m[$ by a translation of $-r_2$. It is the same for the points of $\left[\frac{2m}{a}, \frac{3m}{a}\right[\times [0, m[$ with respect to the points of $\left[\frac{m}{a}, \frac{2m}{a}\right[\times [0, m[$. And so on, untill the distance of the lowest point to 0 is equal to $r_3 = r_1 - h_2 r_2$: cf figure 2.2.

Then, we have obtained all the points of E_2 of the sequence U_ℓ of $\left[0, \frac{5m}{a}\right[\times [0, m[$.

If we continue, we see that the ordinates of the points of U_ℓ of $\left[\frac{5m}{a}, \frac{10m}{a}\right[\times [0, m[$ are deduced of the points of E_2 of $\left[\frac{m}{a}, \frac{5m}{a}\right[\times [0, m[$ by a vertical translation of r_3. And so on when r_n decreases (i.e. n increases).

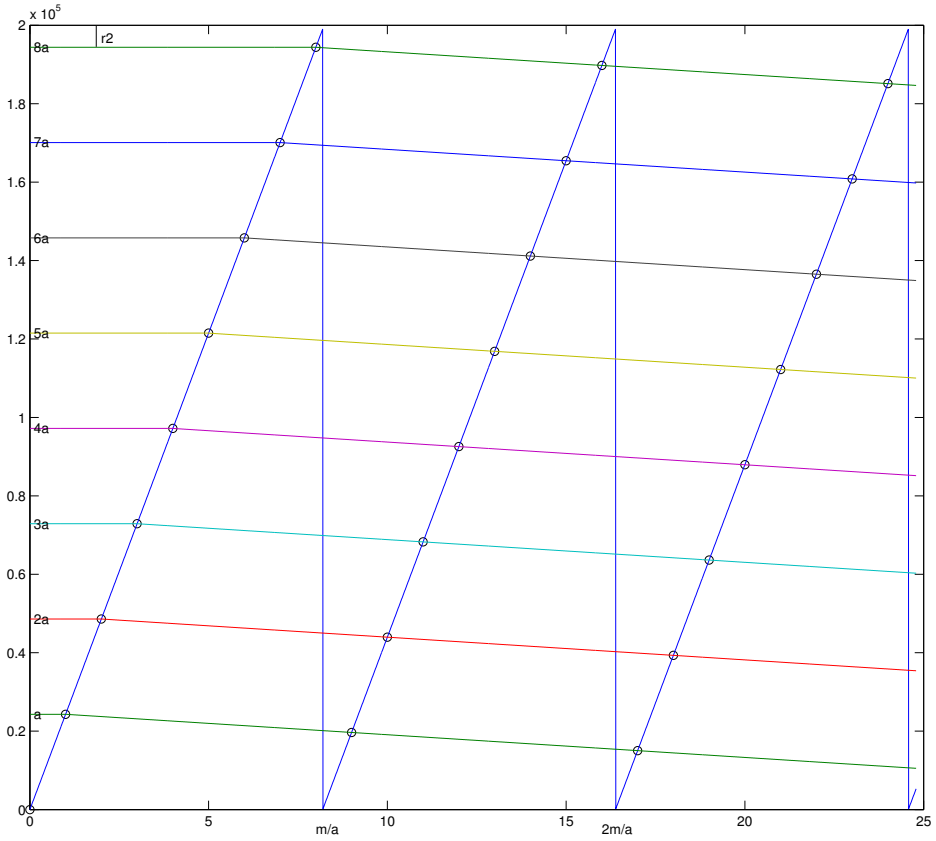

Figure 2.1: a=24298, m=199017, $r_2 = 4633$

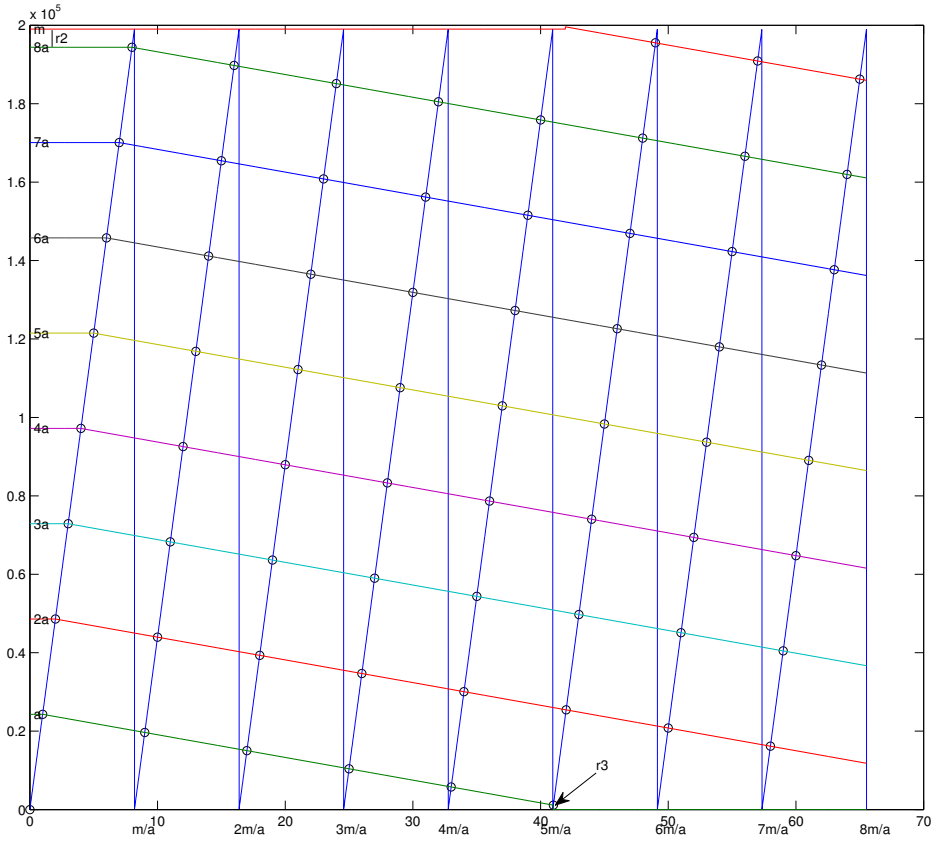

Figure 2.2: a=24298, m=199017, $r_2 = 4633$, $r_3 = 1133$

On the other hand, it is easy to understand that the points of ordinates $y = m - r_2$ or $y = r_2$ have abscissa equal to $x = k_2$ or $x = k_3$.

Then, the integers k_n are the smallest integers ℓ such that the distance of $y = \overline{\ell a}$ to y=0 or to y=m is smaller or equal to r_n. Then, the r_n's are the distances minimal between the $\overline{\ell a}$'s such that $\ell < k_{n+1}$.

The set M is the set of the $\ell \in \mathbb{N}$ such that $\overline{\ell a} < r_1 = a$ (when c=1).
At last, $\overline{k_1 a} = a = r_1$ ($k_1 = 1$), $\overline{k_2 a} = m - r_2$ and $\overline{k_3 a} = r_3$.

We shall prove these properties in the following section 2.2 after having given the plan of the proofs.

2.1.2 Plan of the proofs

In order to prove the announced results, the main part of our work will consist in proving the property fundamental 5-6. This one gives us in a almost exact way (to within about 1 point) the number of points of M^f include in intervals of about any length.

In order to obtain this property we prove at first in section 2.2 the general lemmas which we have just expressed.

Then in section 2.3.1, we shall show that the points of M deduct from each other by translations of length $k_{c+n'}$.

Thanks to this result, it will be easy to us to give in section 2.3.2 a unique decomposition of any point X of M with regard to the sequence $h_{c+n'}$, $n' \in J_{d+1-c}$.

Then we can give (in section 2.3.3) an also unique decomposition of the difference Y-X of two points X and Y of M with regard to the same sequence.

With these results we shall calculate in section 2.4 the number of points of M include in intervals of the form [X,Y [when X and Y belong to M

Finally, we shall deduct in section 2.5 the number of points of M^f contained in intervals [x, x+L [where $x \in \mathbb{N}$ and where L is about anything. This result is the fundamental property.

We shall generalize then this property in section 2.6 by studying the conditions for which T is invertible (untill now this condition was not imposed) and we shall obtain the fundamental theorem which will assert us that, for rectangles of height fr_c and of about any width, we have the inequality $|N_R - mS_R| < 1$ when we transform our results into $[0,1]^2$ by homotethy.

Then, we shall give in section 2.7 some mathematical consequences of these theorems.

2.2 General properties

We are now going to prove the observations which we have just written above. We shall prove in a meticulous way the first lemma and the beginning of the second one. But as the kind of arguments used here returns constantly and have not major difficulties (those are rather simple as soon as we assimilated the notations). So afterward we shall not rewrite the smallest steps of this kind of approach.

Lemma 2.2.1 *Let $n \in J^*_{d+1}$. Then, if $a = r_1$,*
$\overline{k_n a} = r_n$ if n odd and therefore $k_n a \equiv r_n$.
$\overline{k_n a} = m - r_n$ if n even and $r_n \neq 0$ and therefore $k_n a \equiv -r_n$.
$\overline{k_n a} = 0$ if $r_n = 0$ and therefore $k_n a \equiv 0$.

If $m - a = r_1$, then
$\overline{k_n a} = m - r_n$ if n odd and $r_n \neq 0$ and therefore $k_n a \equiv -r_n$.
$\overline{k_n a} = r_n$ if n even and $r_n \neq 0$ and therefore $k_n a \equiv r_n$.
$\overline{k_n a} = 0$ if $r_n = 0$ and therefore $k_n a \equiv 0$.

Proof Suppose $a = r_1$. We prove the lemma by induction.
If n=1, $r_1 = k_1 a$ by definition.
If n=2, because $m = h_1 r_1 + r_2$ and $k_2 = h_1$, then, $\overline{k_2 a} \equiv m - r_2$.
Now because $0 \leq m - r_2 < m$, (if $r_2 \neq 0$ [1]), then, $\overline{k_2 a} = m - r_2$.

Suppose that lemma holds for all integer $n' \leq n+1$ such that $r_{n+1} \neq 0$ and suppose n even. Then,

$$k_{n+2} a \equiv k_{n+1} h_{n+1} a + k_n a, \tag{2.1}$$

and therefore,

$$k_{n+2} a \equiv h_{n+1} r_{n+1} + m - r_n \ , (induction)$$

and therefore,

$$k_{n+2} a \equiv m - r_{n+2} \ . \tag{2.2}$$

Because $0 \leq m - r_{n+2} < m$ (if $r_{n+2} \neq 0$),

$$k_{n+2} a = m - r_{n+2}. \ QED$$

(if $r_{n+2} = 0$, then, obviously $\overline{k_{n+2} a} = 0$).

Suppose n odd and reason by the same way. Then,

$$k_{n+2} a \equiv h_{n+1}(m - r_{n+1}) + r_n \ ,$$

i.e. $k_{n+2} a \equiv r_{n+2}$, and therefore, $\overline{k_{n+2} a} = r_{n+2}$. QED

Suppose at last $r_1 = m - a$.
In this case, because the sequences r_n, k_n, and h_n are identical for congruences T and $T' \equiv r_1 x + b$, on proves easily the result. ■

Remark that we have used the following reasoning : in order to prove that, for example, $\overline{k_n a} = r_n$, we prove at first, $k_n a \equiv r_n$ and after $0 \leq r_n < m$.
This reasoning returns constanly afterward and has no difficulty. According to what we announced, we shall not specify it any more from now on.

Lemma 2.2.2 *Let $n \in J_{d+1}$, $n > 1$ and let $k \in \mathbb{N}$, such that $0 < k < k_n$. Then, $r_{n-1} \leq \overline{ka} \leq m - r_{n-1}$.*

Proof Suppose $a = r_1$ and let us prove this lemma by induction.

It holds if n=2. Indeed, remark that $h_1 \geq 2$ (because $a = r_1$), and then, $\{k \in \mathbb{N} | 1 \leq k < h_1 = k_2\} \neq \emptyset$.
Then, $r_1 = a \leq ka \leq (h_1 - 1)a = m - r_2 - a$. Then, $r_1 \leq \overline{ka} \leq m - r_2 - r_1 \leq m - r_1$. QED

Suppose that the lemma holds for all integer $n' \leq n$ such that $n > 1$ and $r_n \neq 0$ (that means that r_{n+1} exists. If $r_n = 0$, the proof is finished).
As a matter of fact, it is enough to prove the lemma for all integer k such that $k_n \leq k < k_{n+1}$. Indeed, if $k < k_n$, the induction and the fact that r_n is strictly decreasing prove the property.
Then, we can write the Euclidean division of k by k_n : $k = hk_n + \ell$. Then, the definition of k_n imposes that $h \leq h_n$, and that, if $h = h_n$, then $\ell < k_{n-1}$ (if not, one obtains $k \geq k_{n+1}$).

[1] If $r_2 = 0$, the lemma holds obviously

Suppose $\ell = 0$. Then, $h > 0$ and one obtains $hk_n a \equiv \pm hr_n$ (cf lemma 2.2.1).

On the other hand, $r_n \leq hr_n \leq h_n r_n = r_{n-1} - r_{n+1}$ (cf equation 2.2).

At last, because by our assumption, $n \geq 2$, we have $r_n < r_{n-1} \leq r_1 \leq m/2$ and $r_{n-1} \leq m/2 < m - r_n$. Therefore, $r_n \leq hr_n \leq m - r_n$.

We recall that $\overline{k_n a} = r_n$ or $m - r_n$ ($r_n \neq 0$) (cf lemma 2.2.1). Then, we understand that $r_n \leq \overline{hk_n a} \leq m - r_n$. QED

Suppose $\ell \neq 0$ *and* $h < h_n$.

Then, by the induction, because $\ell < k_n$, $r_{n-1} \leq \overline{\ell a} \leq m - r_{n-1}$, and because $k_n a \equiv \pm r_n$ (cf lemma 2.2.1), one obtains easily that $r_{n-1} - (h_n - 1)r_n \leq \overline{\ell a} \pm hr_n \leq m - r_{n-1} + (h_n - 1)r_n$, and therefore, that $r_n + r_{n+1} \leq \overline{\ell a} \pm hr_n \leq m - r_n - r_{n+1}$, and therefore, that $r_n \leq \overline{\ell a} \pm hr_n \leq m - r_n$, i.e. $r_n \leq \overline{(\ell + hk_n)a} \leq m - r_n$. QED

Suppose $h = h_n$ *and n=2.* Then, $\ell < k_{n-1}$, and therefore $\ell = 0$: it is a case which we have already seen.

That means that the lemma holds for n=2 and n=3.

Suppose $h = h_n$, $1 < \ell < k_{n-1}$ *and* $n > 2$. Then, the induction shows that $r_{n-2} \leq \overline{\ell a} \leq m - r_{n-2}$, and therefore, $r_{n-2} - h_n r_n \leq \overline{\ell a} \pm h_n r_n \leq m - r_{n-2} + h_n r_n$.

Now, because the definition of r_n involves that $r_{n-2} - h_n r_n \geq r_n$, then, one obtains $r_n \leq \overline{(\ell + hk_n)a} \leq m - r_n$. QED

Now if $a = m - r_1$, because T and $T'(x) \equiv r_1 x + b$ have the same sequences r_n, k_n and h_n, the result is almost immediate. ■

Corollary 2.2.3 *Let* $n \in J_{d+1}$, $n > 1$ *and* $k,\ k' \in \mathbb{N}$, *such that* $0 \leq k < k' < k_n$. *Then,* $m - r_{n-1} \geq |\overline{k'a} - \overline{ka}| = \overline{k'a} - \overline{ka} \geq r_{n-1}$.

Proof It is enough to remark that if $\overline{ka} = \overline{k'a}$, $\overline{(k-k')a} \equiv 0$, and therefore, $\overline{(k-k')a} = 0$. Now, by the previous lemma 2.2.2, $m - r_{n-1} \geq \overline{(k-k')a} \geq r_{n-1}$, where (because $n > 1$) $r_{n-1} > 0$. Then, it is impossible that $\overline{ka} = \overline{k'a}$.

Then, $\overline{ka} > \overline{k'a}$ or $\overline{ka} < \overline{k'a}$.

If $\overline{ka} > \overline{k'a}$, $\overline{(k-k')a} = \overline{ka} - \overline{k'a}$, and then, by the previous lemma 2.2.2, $m - r_{n-1} \geq \overline{(k-k')a} = \overline{ka} - \overline{k'a} = |\overline{ka} - \overline{k'a}| \geq r_{n-1}$.

If $\overline{ka} < \overline{k'a}$, $\overline{(k-k')a} = m + \overline{ka} - \overline{k'a}$, and then, by the previous lemma 2.2.2, $m - r_{n-1} \geq \overline{(k-k')a} = m + \overline{ka} - \overline{k'a} \geq r_{n-1}$.

Then, $\overline{k'a} - \overline{ka} \geq r_{n-1}$ and $\overline{k'a} - \overline{ka} \leq m - r_{n-1}$.

Then, $m - r_{n-1} \geq |\overline{k'a} - \overline{ka}| = \overline{k'a} - \overline{ka} \geq r_{n-1}$. ■

Corollary 2.2.4 *Let* $n \in J_{d+1}$, $n > 1$ *and* $k,\ k' \in \mathbb{N}$, *such that* $k' < k_n$ *and* $k < k_n$. *Then,* $\overline{ka} = \overline{k'a} \Longleftrightarrow k = k'$.

Proof The proof of this corollary is a direct consequence of corollary 2.2.3. ■

Corollary 2.2.5 *Let* $c \in J^*_{d+1}$ *such that* $\overline{k_c a} = r_c$. *Let* $n \in J_{d+1}$, $n > c$, *and let* $k \in M$, $k \neq 0$, $k \neq k_c$, $k < k_n$. *Then,* $r_{n-1} \leq \overline{ka} \leq r_c - r_{n-1}$.

Proof By Lemma 2.2.2, $r_{n-1} \leq \overline{ka}$. Because $k \in M$, $\overline{ak} < r_c$.

If $\overline{ka} > r_c - r_{n-1}$, $\overline{(k_c - k)a} = \overline{k_c a} - \overline{ka} = r_c - \overline{ka} = Di < r_{n-1}$. Let $k' = k_c - k$.

If $k_c - k > 0$, there exists $0 \leq k' = k_c - k < k_n$ such that $\overline{k'a} < r_{n-1}$. It is impossible because lemma 2.2.2.

If $k_c - k < 0$, $\overline{-k'a} \equiv -Di$, then $\overline{-k'a} = m - Di > m - r_{n-1}$. It is impossible because $0 \leq -k' < k_n$ and lemma 2.2.2. ■

Corollary 2.2.6 *We keep the notations of corollary 2.2.5. Let ℓ_1 and $\ell_2 \in M$ such that there does not exist $\ell \in M$, $\ell_1 < \ell < \ell_2$.*

Then, $\ell_2 - \ell_1 = k_{c+1}$ or $\ell_2 - \ell_1 = k_c + k_{c+1}$.

Proof Recall that $\overline{k_{c+1}a} = m - r_{c+1}$ and $\overline{k_c a} = r_c$ if $r_{c+1} \neq 0$.

If $\overline{\ell_1 a} \geq r_{c+1}$, then $r_c \geq \overline{(\ell_1 + k_{c+1})a} \geq 0$, and therefore, $\ell' = \ell_1 + k_{c+1} \in M$.

If not, $r_c > \overline{\ell_1 a} + r_c - r_{c+1} \geq 0$, and therefore, $\ell" = \ell_1 + k_c + k_{c+1} \in M$.

Therefore $\ell_2 \leq max(\ell', \ell")$.

If there exists $\ell \in M$, $\ell_1 < \ell \leq \ell_2$, $\ell \neq \ell'$, and $\ell \neq \ell"$,

or $\ell - \ell_1 < k_{c+1}$, or $\ell_2 - \ell < k_{c+1}$.

If $\ell - \ell_1 \leq k_{c+1}$, $m - r_c \geq \overline{(\ell - \ell_1)a} \geq r_c$ by lemma 2.2.2.

Then, if $\overline{(\ell - \ell_1)a} = \overline{\ell a} - \overline{\ell_1 a}$, $\overline{\ell a} - \overline{\ell_1 a} \geq r_c$ and $\ell \notin M$.

If $\overline{(\ell - \ell_1)a} = m + \overline{\ell a} - \overline{\ell_1 a}$, $\overline{\ell a} < \overline{\ell_1 a} < r_c$ and then, $\overline{(\ell - \ell_1)a} = m + \overline{\ell a} - \overline{\ell_1 a} > m - r_c$ what is a contradiction.

If $\ell_2 - \ell \leq k_{c+1}$, $m - r_c \geq \overline{(\ell_2 - \ell)a} \geq r_c$ by lemma 2.2.2.

Then, if $\overline{(\ell_2 - \ell)a} = \overline{\ell_2 a} - \overline{\ell a}$, $\overline{(\ell_2 - \ell)a} = \overline{\ell_2 a} - \overline{\ell a} < r_c$ what is a contradiction.

If $\overline{(\ell_2 - \ell)a} = m + \overline{\ell_2 a} - \overline{\ell a}$, $\overline{\ell a} > \overline{\ell_2 a}$ and, if $\ell \in M$, $\overline{\ell a} < r_c$. Then, $\overline{(\ell_2 - \ell)a} = m + \overline{\ell_2 a} - \overline{\ell a} > m - r_c$, what is a contradiction.

Then, $\ell \notin M$. It is a contradiction.

Therefore ℓ_2 is not different from ℓ' or $\ell"$.

If $r_{c+1} = 0$, the proof is identical. ■

Lemma 2.2.7 *Let $\{\lambda_i\}$, i=1,2,...,d, be a sequence of $\mathbb{N}$ such that $\lambda_i \leq h_i$ for i=1,2,...,d. Let $n \in \mathbb{N}^*$ and $k \in \mathbb{N}$ such that $3n + 2k \leq d$. Then,*

$$\sum_{i=n}^{n+k} \lambda_{n+2i} r_{n+2i} \leq r_{n-1} - r_{n+2k+1} \ .$$

Proof We have

$$\sum_{i=n}^{n+k} \lambda_{n+2i} r_{n+2i} \leq \sum_{i=n}^{n+k} h_{n+2i} r_{n+2i}$$

$$\leq \sum_{i=n}^{n+k} [r_{n+2i-1} - r_{n+2i+1}] = r_{n+2n-1} - r_{n+2(n+k)+1} = r_{3n-1} - r_{3n+2k+1} \ .$$

Then, if $n = 1$, $2 = 3n - 1 \geq n - 1 = 0$ and $(3n - 1) \geq [n - 1] + 2$.

Then if $n \geq 2$, $3n - 1 \geq n + 3$ and $[3n - 1] \geq [n - 1] + 4$.

Therefore, for all n such that $n + 2 \leq d + 1$,

$$r_n = h_{n+1} r_{n+1} + r_{n+2} \geq r_{n+1} + r_{n+2} \geq r_{n+1} \ .$$

Therefore,

$$r_n = h_{n+1} r_{n+1} + r_{n+2} \geq r_{n+1} + r_{n+2} \geq [r_{n+2} + r_{n+3}] + [r_{n+2}] \geq 2 r_{n+2} \ .$$

Therefore,

$r_{n-1} - r_{n+2k+1} \geq 2r_{[n-1]+2} - r_{n+2k+1} \geq 2r_{3n-1} - r_{n+2k+1} \geq r_{3n-1} \geq r_{3n-1} - r_{n+2k+1}$. ■

2.3 Study of M

Now, we study the points of M, i.e. the points of $\mathbb{N}$ such that $\overline{la} \leq r_c$. For this study, we assume the following assumptions hold.

Assumptions 2.3.1 *We assume that $0 < c < d$ and $\overline{k_c a} = r_c$ (in sections 2.3, 2.4 and 2.5). Under these assumptions, for all $n \in \mathbb{Z}$ such that $n + c \in J_{d+1}$, we set $K_n = k_{c+n}$, $R_n = r_{c+n}$ and $H_n = h_{n+c}$.*

Then, the following lemma is obvious.

Lemma 2.3.1 *We have $R_0 \leq m/2$, $\overline{K_n a} = R_n$, and $K_n a \equiv R_n$ if n is even,*
$\overline{K_n a} = m - R_n$, and $K_n a \equiv -R_n$ if n is odd, and $R_n \neq 0$,
$\overline{K_n a} = 0$, and $K_n a \equiv 0$ if $R_n = 0$.

Proof It is enough to apply lemma 2.2.1. ■

2.3.1 Properties of Translation

Now, look at figure 2.3 : it shows the points of M^+ in the case where a =24298 and m=199017 when c=1, i.e. $R_0 = a$.

We understand that the points of $M^+ \cap [0, K_2[$ are the points $\{0, K_0, K_0 + K_1, K_0 + 2K_1, K_0 + 3K_1, K_0 + 4K_1\}$, and that the points of $M \cap [2K_2, 3K_2[$, for example, are deduced from the points of $M \cap [0, K_2[$ by a translation of $2K_2$.

If we extend the graph towards the right, we would also see, for example, that the points of $M \cap [3K_3, 4K_3[$, are deduced from the points of $\{M^+ \backslash \{0\}\} \cap [0, K_3[$ by a translation of $3K_3$.

In this case indeed, this horizontal translation of abscissas is translated by one negative vertical translation of the ordinates and K_0 will play the role of 0 in the previous case.

They are these properties which we study now.

Proposition 2.3.2 *Let $n \in \mathbb{N}^*$ such that $n + c < d + 1$. Let $\ell \in [K_n, K_{n+1}[\cap \mathbb{N}$. Then, one can write $\ell = hK_n + \ell_0$ with $h \in \mathbb{N}^*$ and $\ell_0 \in \mathbb{N}$, $\ell_0 < K_n$ and $h \leq H_n$, and if $h = H_n$, then $\ell_0 < K_{n-1}$ and if n=1, then $h < H_1$.*

Then, $\ell \in M^+$ (resp M) if and only if $\ell_0 \in M^+ \backslash \{0\}$ if n is odd, and $\ell_0 \in M$ if n is even.

Proof The writing $\ell = hK_n + \ell_0$ is that of the Euclidean division. The associated inequalities are due to the definitions of K_n, H_n and ℓ.

In particular, if n=1, and $h = H_1$, $\ell = H_1 K_1 + \ell_0 = K_2 - K_0 + \ell_0 < K_2 : \ell_0 < K_0$. Then, by lemma 2.2.2, $\overline{\ell a} \geq r_{c-1} > r_c$ and $\ell_0 \notin M$.

Let ℓ_0 and h defined as in the statement ($\ell_0 \in M^+ \backslash \{0\}$ or $\ell_0 \in M$). We prove now that $\ell_0 + hK_n \in M^+$.

Suppose that n is even, i.e. $\overline{K_n a} = R_n$.

Then, $0 \leq \overline{\ell_0 a} \leq R_0 - R_{n-1}$ (by corollary 2.2.5). Then, $\ell_0 \in M$. We deduce $0 \leq \overline{\ell_0 a} + hR_n \leq R_0$, and then $0 \leq \overline{(\ell_0 + hK_n)a} \leq R_0$, i.e. $\ell = \ell_0 + hK_n \in M^+$. QED

If n+c is even, one uses the same reasoning.

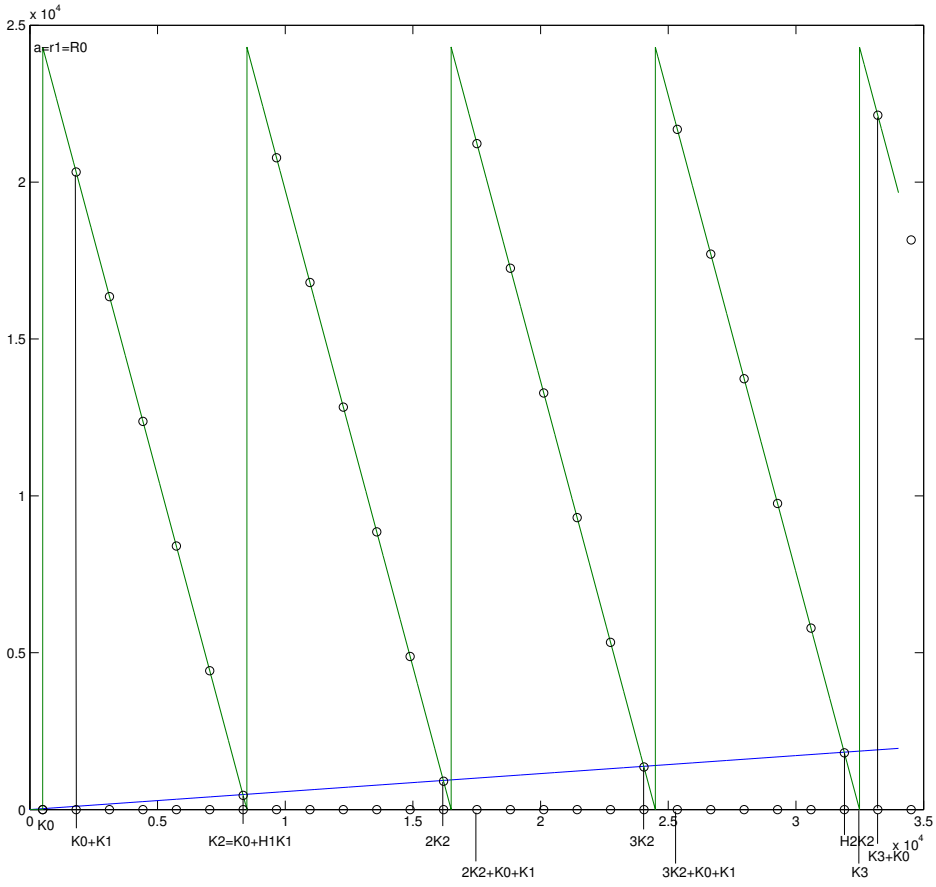

Figure 2.3: a=24298, m=199017, $r_2 = 4633$, $r_3 = 1133$

Reciprocally, let $\ell \in M^+ \cap [K_n, K_{n+1}[\,:\, \ell = \ell_0 + hK_n$.

Suppose n even, i.e. $\overline{K_n a} = R_n$. Because $R_n < R_0$, and $n + c \geq 2$ it is easy to understand that $R_0 < R_0 + hR_n < m$. Therefore that $\overline{(K_0 + hK_n)a} > R_0$, i.e. $K_0 + hK_n \notin M^+$, and therefore $\ell_0 \neq K_0$.

Because, on the other hand, $R_n \leq \overline{\ell a} \leq R_0$ (by lemma 2.2.2 and by assumption), then, $-(H_n - 1)R_n \leq \overline{\ell a} - hR_n < R_0$.

If $\overline{\ell a} - hR_n < 0$, then, $\overline{(\ell - hK_n)a} = m + \overline{\ell a} - hR_n$, and therefore, $m - R_{n-1} < \overline{(\ell - hK_n)a} < m$.

Now, $\ell - hK_n \leq K_n$, which is in contradiction with the lemma 2.2.2.

Therefore, $0 \leq \overline{\ell a} - hR_n < R_0$, i.e. $\ell_0 \in M$. QED

If n is odd the proof is identical.

Then, it remains to prove the equivalence between $\ell \in M^+$ and $\ell \in M$. It is due to the following lemma 2.3.3 which is a direct consquence of corollary 2.2.4. ■

Lemma 2.3.3 *The only point of* $M^+ \cap [0, k_{d+1}[$ *such that* $\overline{\ell a} = R_0$ *is the point* K_0.

Lemma 2.3.4 *We have*

$M \cap [0, K_2[= \{0, K_0 + K_1, K_0 + 2K_1, ..., K_0 + (H_1 - 1)K_1\}$,

$M \cap [0, K_1[= \{0\}$,

$M^+ \cap [0, K_1[= \{0, K_0\}$,

$M^+ \cap [0, K_2[= \{M \cap [0, K_2[\} \cup \{K_0\}$.

Proof It is enough to apply the previous results and corollary 2.2.6. ■

2.3.2 Writting of points of M

With the previous results, we understand that it is easy to give a writing of elements of M by induction.

Let $\ell \in M \cap [hK_T, (h+1)K_T[$ where $h + 1 \leq H_T$. Then, $\ell - hK_t \in M^+$ by proposition 2.3.2.

Finally, we shall come down easily to the elements of $M \cap [0, K_2[$ of which we know the form (cf lemma 2.3.4).

That means that ℓ can be written $\ell = \delta K_0 + \sum_{t=1}^{T} g_t K_t$ where $\delta = 0$ or $\delta = 1$ and $g_t \leq H_t$. At last, if $g_t = H_t$, proposition 2.3.2 shows that $\ell_0 < K_{t-1}$, i.e. $g_{t-1} = 0$.

Now, we shall prove these results and we shall understand that this writing of ℓ is unique.

Lemma 2.3.5 *Let* $\ell \in M^+$, $\ell < k_{d+1}$ *such that there exists* $T \in \mathbb{N}^*$ *checking* $c + T \leq d$ *and let* $g_T \in \mathbb{N}^*$, *such that* $\ell \in [g_T K_T, (g_T + 1)K_T[\cap [0, K_{T+1}[$.

Then, one can write ℓ *in the form*

$$\ell = \delta K_0 + \sum_{t=1}^{T} g_t K_t \ ,$$

with

1) $\delta = 0$ *or* $\delta = 1$,

2) $g_t \leq H_t$ *where* $t \in \mathbb{N}^*$, $t \leq T$,

3) If $g_t = H_t$, *then* $g_{t-1} = 0$,

4) $g_1 < H_1$.

Proof We prove this lemma by recurence. It holds for T=1 and T=2 (cf lemma 2.3.4).

Suppose that it holds for all integer $T' \leq T$ and suppose that $c + T + 2 \leq d + 1$.

Then, if $\ell = \ell_0 + g_{T+1}K_{T+1}$ means the Euclidean division of ℓ by K_{T+1}, $\ell_0 \in M^+$ (cf proposition 2.3.2) and it is enough to apply the induction in order to obtain the announced results. ■

Lemma 2.3.6 *Let g_t, t=1,2,...,T, be a sequence checking the conditions of lemma 2.3.5 where $T \in \mathbb{N}^*$, and $T \leq d-c$. Let $\delta = 0$ or $\delta = 1$.*

Then,

$$\delta K_0 + \sum_{t=1}^{T} g_t K_t \in [0, K_{T+1}[\ .$$

Proof The proof is easily done by induction by using definition of sequence K_n. ■

One deduce also easily the following lemma.

Lemma 2.3.7 *We keep the notations and assumptions of lemma 2.3.6. Then,*

$$\delta K_0 + \sum_{t=1}^{T} g_t K_t \in [g_T K_T, (g_T+1)K_T[\cap [0, K_{T+1}[\ .$$

Lemma 2.3.8 *The decomposition of $\ell \in M^+$ given in lemma 2.3.5 is unique.*

Proof In the decomposition of all $\ell \in M^+$ given in lemma 2.3.5, g_T is determined in a unique way by lemma 2.3.7. Then, we deduce the lemma . ■

We gave the only writing of any element $\ell \in M \cap [0, k_{d+1}[$. Now we have to generalize this result for all $\ell \in M$.

Proposition 2.3.9 *The lemma 2.3.5, 2.3.6, 2.3.7 and 2.3.8 hold again, if we replace the condition $c+T \leq d$ by $c+T \leq d+1$.*

Moreover, if $\ell \in [gk_{d+1}, (g+1)k_{d+1}[$, $g \in \mathbb{N}$, then $\ell \in M$ (resp $\ell \in M^+$) if and only if $\ell' = \ell - gk_{d+1} \in M$ (resp $\ell' \in M^+$).

Moreover, $\overline{\ell' a} = \overline{\ell a}$.

Proof It is enough to recall $r_{d+1} = 0$, i.e. $\overline{k_{d+1} a} = 0$. ■

2.3.3 Study of Y-X with $X,\ Y \in M$

Then, we have a decomposition of the points of M. But, later, when we want to compute the number of theses points belonging to an interval $[X, Y[$, where X and Y belongs to M, we had to know also a decomposition of Y-X. It is this problem that we study now.

This study is based on a simple idea. :
if $\overline{Ya} > \overline{Xa}$, then, $\overline{(Y-X)a} < R_0$ and therefore $Y - X \in M$.
If not, $m - R_0 \leq m + \overline{Ya} - \overline{Xa} < m$, that is to say $0 \leq R_0 + \overline{Ya} - \overline{Xa} < R_0$, and therefore, $K_0 + (Y - X) \in M$.

Lemma 2.3.10 *Let $\ell \in \mathbb{N}$ such that $\ell = \sum_{i=1}^{T} \lambda_i K_i$, where $T \in \mathbb{N}^*$ and checks $c+T \leq d+1$ and where $\lambda_i \in \mathbb{N}$, $\lambda_i \leq H_i$, $\lambda_1 < H_1$, and if $\lambda_i = H_i$, then $\lambda_{i-1} = 0$.*

And let $X \in M$. Then,
OR $\ell \in M$, and, in this case, or $X + \ell \in M$ or $X + \ell - K_0 \in M$,
OR $K_0 + \ell \in M$ and, in this case, or $X + \ell \in M$ or $X + \ell + K_0 \in M$.

Proof By lemma 2.2.1, we can write $\overline{\ell a} = \sum_{i=1}^{T} \lambda_i \overline{K_i a}$, in the form

$$\overline{\ell a} \equiv \sum_{i+c \in 2\mathbb{N}^*,\ i+c \leq T} \lambda_i R_i - \sum_{i+c \in 2\mathbb{N}+1,\ i+c \leq T} \lambda_i R_i \ .$$

Then, by lemma 2.2.7, $\sum_{i+c \in 2\mathbb{N}^*,\ i+c \leq T} \lambda_i R_i = \alpha_1 < R_0$ and $\sum_{i+c \in 2\mathbb{N}+1,\ i+c \leq T} \lambda_i R_i = \alpha_2 \leq R_0$ with $\alpha_s \in \mathbb{N}$ for s=1,2.

Therefore, if $\alpha_1 > \alpha_2$, then, $\overline{\ell a} = \alpha_1 - \alpha_2 < R_0$, and therefore $\ell \in M$. If not, $0 \leq \alpha_1 - \alpha_2 + R_0$ and $\ell + K_0 \in M$. QED

Then, let $X \in M$.
If $\ell \in M$, $0 \leq \overline{\ell a} + \overline{Xa} < 2R_0 \leq m$, and then
or $\overline{\ell a} + \overline{Xa} < R_0$, and then, $X + \ell \in M$,
or $\overline{\ell a} + \overline{Xa} \geq R_0$, and then, $X + \ell - K_0 \in M$.

If $\ell + K_0 \in M$, we use the same way. ■

Lemma 2.3.11 *Let X and Y belonging to* M^+ *such that* $X < Y$. *Let*

$$X = \delta' K_0 + \sum_{i=1}^{T} x_i K_i \quad and \quad Y = \delta" K_0 + \sum_{i=1}^{T} y_i K_i$$

be the decompositions of X and Y according to proposition 2.3.9 , i.e. lemma 2.3.5 if $c + T \leq d$ *(it is possible that* $x_T = 0$*).*
Then, Y-X is written, by a alone way

$$Y - X = \Delta K_0 + \sum_{i=1}^{T} z_i K_i \ ,$$

with $z_i \in \mathbb{N}$, $z_i \leq H_i$, $z_1 < H_1$, *and if* $z_i = H_i$, *then* $z_{i-1} = 0$,
and where $\Delta = 0$ *or 1 if* $\overline{Ya} \geq \overline{Xa}$, $\Delta = 0$ *or -1 if* $\overline{Ya} < \overline{Xa}$.

Proof If $\overline{Ya} \geq \overline{Xa}$, then, $Y - X \in M^+$, and then, $Y - X$ is decomposed by an alone way according criteria of proposition 2.3.9 (cf also lemma 2.3.8) : $Y - X = \delta K_0 + \sum_{t=1}^{T'} z_t K_t$.
If $\overline{Ya} < \overline{Xa}$, then, $K_0 + Y - X \in M^+$, and then, $K_0 + Y - X = \delta K_0 + \sum_{t=1}^{T'} z_t K_t$ and then, $Y - X = (\delta - 1)K_0 + \sum_{t=1}^{T'} z_t K_t$.

It remains to prove that $T' \leq T$.
If $Y - X \in M^+$, then $Y - X \leq Y < K_{T+1}$ (cf lemma 2.3.6), and therefore $T' \leq T$ (cf lemma 2.3.7).
If $K_0 + Y - X \in M^+$, $Y - X \notin M^+$ and if $X \neq 0$, then $X \geq K_0$ (cf lemma 2.2.2), and therefore $K_0 + Y - X \leq Y < K_{T+1}$ and therefore $T' \leq T$ (cf lemma 2.3.7).
At last, if X=0, then, $R_0 \geq \overline{Ya} - \overline{Xa} = \overline{Ya} \geq 0$. Then, $R_0 \geq \overline{(Y - X)a} = \overline{Ya} - \overline{Xa} \geq 0$. Then, $Y - X \in M^+$. ■

Lemma 2.3.12 *Let X and Y belonging to* M^+ *such that* $X < Y$. *Then the following logical equivalences holds*

$$1)\ \overline{Ya} \geq \overline{Xa} \Longleftrightarrow Y - X \in M^+ \ ,$$
$$2)\ \overline{Ya} < \overline{Xa} \Longleftrightarrow K_0 + Y - X \in M \ ,$$
$$3)\ \overline{Ya} \leq \overline{Xa} \Longleftrightarrow K_0 + Y - X \in M^+ \ ,$$

Proof In the previous proof, we have just proved the direct implications. It remains to prove the reciprocal implications.
They follow from the fact that the two conditions
$Y - X \in M^+$ and $K_0 + Y - X \in M$ are incompatible. ■

It is necessary to complete these properties by the following property.

Let us suppose that we have X belonging to M and ℓ defined as in the lemma 2.3.10 : $\ell = \sum_{i=1}^{T} \lambda_i K_i$.

Then, let $Y' \in M$ defined also by lemma 2.3.10 : $Y' = X + \ell \pm \delta K_0$ with $\delta = 0$ or 1.
Then, let us write Y'-X according to lemma 2.3.11 : $Y' - X = \Delta K_0 + \sum_{i=1}^{T} z_i K_i$.
It remains to be proved that $\lambda_i = z_i$ for i=1,2,...,T. It is what we do in the following lemma.

Lemma 2.3.13 *Let $X \in M$. Let $\ell \in \mathbb{N}$ defined as in lemma 2.3.10 : $\ell = \sum_{i=1}^{T} \lambda_i K_i$.*

If $\ell \in M$, we denote by Y' that of the two numbers $X + \ell$ and $X + \ell - K_0$ belonging to M (there is an only one by corollary 2.2.6).

If $K_0 + \ell \in M$, (what is incompatible with $\ell \in M$), then Y' is that of the two numbers $X + \ell$ and $X + \ell + K_0$ belonging to M (there is an only one by corollary 2.2.6).

With theses notations , the decomposition of Y'-X according to lemma 2.3.11 is

$$Y' - X = \Delta K_0 + \sum_{i=1}^{T} \lambda_i K_i \ .$$

Proof Assume $\ell \in M$. If $Y' = X + \ell$, then by our assumption $Y' \in M$ and $Y' - X \in M$. Therefore $\overline{Y'a} \geq \overline{Xa}$ (cf lemma 2.3.12), and therefore, $Y' - X = \delta K_0 + \sum_{i=1}^{T} \mu_i K_i$ by an only way by lemma 2.3.11 : because $\ell = Y' - X$, $\delta = 0$ and $\lambda_i = \mu_i$.

The other cases are proved by the same way. ■

Both lemmas which we prove now will be useful later when we shall need a recurrence about T about the writing of Y-X.

Lemma 2.3.14 *Let $T \in \mathbb{N}$ such that $c + T \leq d + 1$ and $2 \leq T$. Let X and $Y \in M^+ \cap [0, K_{T+1}[$, such that $X < Y$.*

Then, according proposition 2.3.2, there exists X' and $Y' \in M^+ \cap [0, K_T[$ such that $X = X' + x_T K_T$, $Y = Y' + y_T K_T$ (cf proposition 2.3.9) and $x_T \leq y_T$ [2] .

We assume $y_T \geq 1$ and $X' \neq Y'$. We denote by Y" $= Y' + K_T$ (by proposition 2.3.2 and lemma 2.3.3, Y" $\in M$).

Let $\Delta K_0 + \sum_{i=1}^{T-1} z_i K_i$ be the decomposition according lemma 2.3.11 of Y'-X' if $X' < Y'$ and of Y" $- X'$ if not.

Then, the decomposition of Y-X according to lemma 2.3.11 is

$$Y - X = \Delta K_0 + \sum_{i=1}^{T} z_i K_i \ ,$$

with $z_T = y_T - x_T$ if $X' < Y'$, and $z_T = y_T - x_T - 1$ if not.

Proof *Let us assume $X' < Y'$.*

Then, if $\overline{Xa} \leq \overline{Ya}$, $Y - X \in M^+$ by lemma 2.3.12.
Therefore $Y' - X' \in M^+$ by proposition 2.3.2.
Therefore, $Y' - X' = \delta K_0 + \sum_{i=1}^{T-1} z_i K_i$ by lemma 2.3.5, proposition 2.3.9.
Therefore, $Y - X = \delta K_0 + \sum_{i=1}^{T-1} z_i K_i + (y_T - x_T) K_T$. QED

If $\overline{Ya} < \overline{Xa}$, then $K_0 + Y - X \in M$ by lemma 2.3.12.
Therefore $K_0 + Y' - X' \in M^+$ by proposition 2.3.2.
Then, (because $Y' \neq X'$), if n is odd, it is easy to understand that $K_0 + Y' - X' \in M$ by lemma 2.3.3. If n is even, by proposition 2.3.2, $K_0 + Y' - X' \in M$. Then, in all the cases, $K_0 + Y' - X' \in M$.
Then, $K_0 + Y' - X' = \delta K_0 + \sum_{i=1}^{T-1} z_i K_i$ by lemma 2.3.5, proposition 2.3.9.

[2] By proposition 2.3.9, if $x_T > y_T$, $X - Y = X' - Y' + (x_T - y_T) K_T \geq -K_{T-1} + K_T > 0$, what is a contradiction

Therefore, $Y - X = (\delta - 1)K_0 + \sum_{i=1}^{T-1} z_i K_i + (y_T - x_T)K_T$. QED

Now, clearly $y_T - x_T \leq H_T$.

Moreover equality $y_T - x_T = H_T$ involves that $y_T = H_T$ and $x_T = 0$, and therefore, by lemma 2.3.5, proposition 2.3.9, that $Y' < K_{T-1}$. Then, $X' < Y' < K_{T-1}$ because by our assumption for this part of the proof, $X' < Y'$. Then, $z_{T-1} = 0$ by lemma 2.3.13.

At last $\overline{Xa} \leq \overline{Ya}$, involves indeed $\Delta = 0$ or 1 and $\overline{Ya} < \overline{Xa}$ involves $\Delta = 0$ or -1. QED

If $Y' < X' < Y"$, the result is proved by the same way. ■

Lemma 2.3.15 *Let X', Y' and Y" defined as in lemma 2.3.14 such that $Y' < X' < Y"$.*
Then the following inequalities are impossible : $\overline{Y'a} \leq \overline{X'a} \leq \overline{Y"a}$ or $\overline{Y"a} \leq \overline{X'a} \leq \overline{Y'a}$.

Proof By lemma 2.2.1, $\overline{(Y" - Y')a} \equiv \pm R_T$.

Therefore $\overline{Y"a} \equiv \overline{Y'a} \pm R_T$.

It is easy to deduce that $\overline{Y"a} = \overline{Y'a} \pm R_T$ if $Y' \neq 0$ because $R_T < R_{T-1} \leq \overline{Y'a} \leq m - R_{T-1} < m - R_T$ by lemma 2.2.2.

If $Y' = 0$, the assumptions $Y' \in M^+$ and $Y \in M^+$ will impose that T is even (proposition 2.3.2), and therefore, because by our assumption $T \geq 2$, $\overline{Y"a} = \overline{Y'a} + R_T$ (cf lemma 2.2.1).

Then, in all cases, we have $\overline{Y"a} = \overline{Y'a} \pm R_T$.

Then, let us assume $\overline{Y'a} \leq \overline{X'a} \leq \overline{Y"a}$ or $\overline{Y"a} \leq \overline{X'a} \leq \overline{Y'a}$.

Then, we have $|\overline{Y'a} - \overline{X'a}| \leq R_T$. That is a contradiction with corollary 2.2.3. ■

Corollary 2.3.16 *Let X', Y' and Y" defined as in lemma 2.3.15. Then the following logical equivalences holds :*

$$X' - Y' \in M \Longleftrightarrow K_0 + Y" - X' \in M.$$

$$K_0 + X' - Y' \in M \Longleftrightarrow Y" - X' \in M.$$

Proof Suppose $X' - Y' \in M$. Then, $\overline{X'a} \geq \overline{Y'a}$ by lemma 2.3.12. Then, by lemma 2.3.15 , $\overline{X'a} > \overline{Y"a}$. Then, by lemma 2.3.12, $K_0 + Y" - X' \in M$.

Suppose $K_0 + Y" - X' \in M$. Then, by lemma 2.3.12, $\overline{X'a} > \overline{Y"a}$. Then, by lemma 2.3.15 , $\overline{X'a} > \overline{Y'a}$. Then, by lemma 2.3.12, $X' - Y' \in M^+$.

Now it is impossible that $\overline{(X' - Y')a} = R_0$. Indeed, because $\overline{X'a} > \overline{Y'a}$, and by the definition of lemma 2.3.14, $\overline{X'a} \leq R_0$, $R_0 \geq \overline{X'a} - \overline{Y'a} > 0$. Then, $\overline{(X' - Y')a} = \overline{X'a} - \overline{Y'a}$. If $\overline{(X' - Y')a} = R_0$, it is necessary that $\overline{X'a} = R_0$ and $\overline{Y'a} = 0$. Now, because by the definition of lemma 2.3.14, $T \geq 2$, $m > R_{T-1} > 0$. Then, because $Y' < K_T$, by lemma 2.2.2, $\overline{Y'a} \geq R_{T-1} > 0$. Then, $\overline{Y'a} > 0$, what is a contradiction.

Then, $X' - Y' \in M$. QED

Now suppose $Y" - X' \in M$. Then, by lemma 2.3.12, $\overline{X'a} \leq \overline{Y"a}$. Then, by lemma 2.3.15 , $\overline{X'a} < \overline{Y'a}$. Then, by lemma 2.3.12, $K_0 + X' - Y' \in M$.

Now suppose $K_0 + X' - Y' \in M$. Then, by lemma 2.3.12, $\overline{X'a} < \overline{Y'a}$. Then, by lemma 2.3.15, $\overline{X'a} < \overline{Y"a}$. Then, by lemma 2.3.12, $Y" - X' \in M^+$.

Now it is impossible that $\overline{(Y" - X')a} = R_0$. Indeed, because $\overline{X'a} < \overline{Y"a}$, and by the definition of lemma 2.3.14, $\overline{Y"a} \leq R_0$, $R_0 \geq \overline{Y"a} - \overline{X'a} > 0$. Then, $\overline{(Y" - X')a} = \overline{Y"a} - \overline{X'a}$. If $\overline{(Y" - X')a} = R_0$, it is necessary that $\overline{Y"a} = R_0$ and $\overline{X'a} = 0$. Now because $c \geq 1$, $m > R_{T-1} > 0$. Now, because by the definition of lemma 2.3.14 $Y' < K_T$. Then, by lemma 2.2.2, $\overline{X'a} \geq R_{T-1} > 0$. Then, $\overline{X'a} > 0$, what is a contradiction.

Then, $Y" - X' \in M$. QED ■

2.4 Number of points of M in the intervals.

We keep the previous notations and we suppose again that assumptions 2.3.1 hold.

We shall calculate at first the number of points of M belonging to intervals in the form [0,X[, $X \in M$.

Look at again figure 2.3. We know alereadly the numbers of points of M belonging to intervals $[0, K_1[$ and $[0, K_2[$: cf lemma 2.3.4.

Then, we understand that it is easy from proposition 2.3.2 to calculate the numbers of points belonging to $[0, K_3[$: It will be the numbers of points belonging to $[0, K_2[$, $[K_2, 2K_2[$, ..., $[(H_2 - 1)K_2, H_2K_2[$ and $[H_2K_2, K_3[$.

Now the first intervals contain the same number of points because they are deduced from each other by translation (proposition 2.3.2) and the last one contains the same number as $[0, K_1[$ (proposition 2.3.2), and therefore

$$card\big([0, K_3[\cap M\big) = H_2 card\big([0, K_2[\cap M\big) + card\big([0, K_1[\cap M\big) \ .$$

They are these simple properties that we prove now.

Notations 2.4.1 *We denote by* $\overline{\overline{[x, y[}}$, $[x, y[\subset \mathbb{R}$, *the number* $\overline{\overline{[x, y[}} = card\big([x, y[\cap M\big)$.

We define the sequence $\{Q_n^c\}$, $n \in \mathbb{N}$, *by* $Q_0^c = 0$, $Q_1^c = 1$ *and* $Q_{n+1}^c = Q_n^c h_{n+c} + Q_{n-1}^c$ *when* $n \in \mathbb{N}^*$ *and* $n + c \leq d + 1$.

In order to simplify, in this section, we simplify Q_n^c *by* Q_n.

Lemma 2.4.2 *Let* $p \in \mathbb{N}^*$ *such that* $c + p \leq d + 1$. *Let* $h \in \mathbb{N}^*$, $h < H_p$. *Then the following equalities holds :*

$$\overline{\overline{[hK_p, (h+1)K_p[}} = \overline{\overline{[0, K_p[}} \ ,$$

$$\overline{\overline{[H_pK_p, K_{p+1}[}} = \overline{\overline{[0, K_{p-1}[}} \ , \quad if \quad p \geq 2 \ .$$

Proof It is enough to use proposition 2.3.2 by remarking that $card\big([0, K_p[\cap M\big) = card\big([0, K_p[\cap\{M^+ \setminus \{0\}\}\big)$. ■

Lemma 2.4.3 *Let* $p \in \mathbb{N}^*$ *such that* $p + c \leq d + 2$. *Then,* $\overline{\overline{[0, K_p[}} = Q_p$.

Proof It is enough to apply lemma 2.3.4 and, by inductive way, the equality quoted at the beginning of this section for p=3, as its proof. ■

Lemma 2.4.4 *Let* $X \in M$ *and* $Y = \delta K_0 + \sum_{i=1}^{T} g_i K_i$ *be the decomposition of* X *according proposition 2.3.9. Then,* $\overline{\overline{[0, X[}} = \sum_{i=1}^{T} g_i Q_i$.

Proof We prove this lemma by induction on T. It holds for T=0 and T=1 (cf lemma 2.3.4).

Then, it is enough to apply a simple induction. Suppose that this lemma holds for all $T' \leq T-1$. Then, $L' = \sum_{i=1}^{T-1} g_i K_i < K_T$ by lemma 2.3.6.

Now, by lemma 2.4.2 and 2.4.3, $\overline{\overline{[hK_T, hK_T + K_T[}} = Q_T$. Then, $\overline{\overline{[0, g_T K_T[}} = g_T Q_T$.

Now, by proposition 2.3.2 there exists a bijection beetwen $[g_T K_T, g_T K_T + x[\cap M$ and $[0, x[\cap M$ or $[0, x[\cap\{M^+ \setminus \{0\}\}$ when $g_T K_T + x < K_{T+1}$ and $x > K_0$.

Then, because $card\big([0, K_p[\cap M\big) = card\big([0, K_p[\cap\{M^+ \setminus \{0\}\}\big)$, $\overline{\overline{[g_T K_T, g_T K_T + L'[[}} = \overline{\overline{[0, L'[}} = \sum_{i=1}^{T-1} g_i Q_i$.

Then, $\overline{\overline{[0, \sum_{i=1}^{T} g_i K_i[}} = \sum_{i=1}^{T-1} g_i Q_i + g_T Q_T = \sum_{i=1}^{T} g_i Q_i$. ■

Lemma 2.4.5 *Let $T \in \mathbb{N}^*$, $c+T \leq d+1$, and let $Z \in [0, K_{T+1}[\cap M$ such that $Z+K_T \in [0, K_{T+1}[$. Then, $\overline{\overline{[Z, Z+K_T[}} = Q_T$.*

Proof It is easy to understand (thanks to proposition 2.3.2) that $Z + K_T \in M$, and therefore, $Z + K_T$ is written $Z + K_T = \delta K_0 + \sum_{i=1}^{T} \lambda_i K_i + K_T$, and Z : $Z = \delta K_0 + \sum_{i=1}^{T} \lambda_i K_i$.

The lemma 2.4.4 permits to conclude. ■

The lemma which we prove now will be useful in order to prove proposition 2.4.7.

Lemma 2.4.6 *Let $T \in \mathbb{N}^*$, $T \leq d+1$. Let ℓ' and $\ell"$ $\in M^+ \cap [0, K_T + K_0]$.*

Let $\ell' = \delta' K_0 + \sum_{i=1}^{T} \lambda_i K_i$ and $\ell" = \delta" K_0 + \sum_{i=1}^{T} \mu_i K_i$ the decompositions of ℓ' and $\ell"$ according 2.3.9. Assume that $\ell' + \ell" = K_T + K_0$.

Then, $\sum_{i=1}^{T} (\lambda_i + \mu_i) Q_i = Q_T$.

Proof At first, we prove this lemma when ℓ' (or $\ell"$) $\in [K_T, K_T + K_0]$.

It is easy to undersand that K_T or $K_T + K_0 \in M$ and that $[K_T, K_T + K_0]$ contains an only point of M (Cf corollary 2.2.6) : $\ell' = K_T + K_0$ for example. In this case, $\ell" = 0$. Then, $\lambda_T = 1$, $\lambda_i = 0$ if $i < T$ and $\mu_j = 0$

If $\ell' = K_T$, $\ell" = K_0$ and $\lambda_T = 1$, $\lambda_i = 0$ if $i < T$ and $\mu_j = 0$ for j=1,2,....,T. QED

Now, let us prove the rest of the lemma by induction.

Thanks to lemma 2.3.4, one understand easily that it holds for T=1 and T=2.

Let us suppose that it holds for all integer $T' \leq T$ when $T > 1$.

Let L' and $L" \in M^+$ such that $L' + L" = K_{T+1} + K_0$ and $L' < K_{T+1}$ and $L" < K_{T+1}$.

Let $L' = \delta' K_0 + \sum_{i=1}^{T} \lambda_i K_i$ and $L" = \delta" K_0 + \sum_{i=1}^{T} \mu_i K_i$ be the decompositions of L' and L" according proposition 2.3.9.

Let $\ell' = \delta' K_0 + \sum_{i=1}^{T-1} \lambda_i K_i$ and $\ell" = \delta" K_0 + \sum_{i=1}^{T-1} \mu_i K_i$.

Then, ℓ' and $\ell" \in [0, K_T[\cap M^+$ (cf proposition 2.3.2 and lemma 2.3.5), and therefore, $\ell' + \ell" - K_0 < 2K_T$.

We deduce easily that
or $\lambda_T + \mu_T = H_T - 1$, and therefore $\ell' + \ell" - K_0 = K_T + K_{T-1}$,
or $\lambda_T + \mu_T = H_T$, and therefore $\ell' + \ell" - K_0 = K_{T-1}$.

If $\lambda_T + \mu_T = H_T - 1$, and $\ell' + \ell" - K_0 = K_T + K_{T-1}$, then, OR $\lambda_{T-1} \neq 0$ OR $\mu_{T-1} \neq 0$. Indeed, if not, we have $\ell' + \ell" - K_0 < K_T + K_{T-1}$.

If $\lambda_{T-1} \neq 0$, for example, we set $\ell'_1 = \ell' - K_{T-1}$.

Then, if $\lambda_{T-1} = 1$, by proposition 2.3.2, $\ell'_1 \in M^+$.

Then, if $\lambda_{T-1} \neq 1$, by proposition 2.3.2, $\ell'_2 = \ell' - \lambda_{T-1} K_{T-1} \in M^+ \setminus \{0\}$ or $\ell'_2 \in M$. Then, by proposition 2.3.2, $\ell'_1 = \ell'_2 + (\lambda_{T-1} - 1) K_{T-1} \in M^+$.

Now, $\ell'_1 + \ell" - K_0 = K_T$. Then, the induction allows to write that $\sum_{i=1}^{T-1} (\lambda_i + \mu_i) Q_i - Q_{T-1} = Q_T$, and, therefore, $\sum_{i=1}^{T} (\lambda_i + \mu_i) Q_i = Q_{T+1}$. QED

If $\lambda_T + \mu_T = H_T$ and $\ell' + \ell" - K_0 = K_{T-1}$, OR $\ell' = K_{T-1}$ (or $\ell" = K_{T-1}$) OR $\ell' < K_{T-1}$ and $\ell" < K_{T-1}$.

If $\ell' = K_{T-1}$, $\ell" = K_0$. Then, $\lambda_{T-1} = 1$, $\lambda_i = 0$ if $i < T-1$ and $\mu_j = 0$ if $j \leq T-1$. Then, $\sum_{i=1}^{T} (\lambda_i + \mu_i) Q_i = Q_{T+1}$.

If $\ell' < K_{T-1}$ and $\ell" < K_{T-1}$, one can apply the induction. Then, $\sum_{i=1}^{T-1} (\lambda_i + \mu_i) Q_i = Q_{T-1}$. Then, $\sum_{i=1}^{T} (\lambda_i + \mu_i) Q_i = Q_{T+1}$.

■

We are then able to prove a very important theorem for the continuation of our study. We see that it will allow us a detailed knowledge of the distribution of points of M

Proposition 2.4.7 *Let $X \in M$ and $Y \in M$ such that $Y > X$. Let $Y - X = \Delta K_0 + \sum_{i=1}^{T'} z_i K_i$ the decomposition of Y-X according lemma 2.3.11. Then,*

$$\overline{\overline{[X, Y[}} = \sum_{i=1}^{T'} z_i Q_i \ .$$

Proof Let $X = \delta' K_0 + \sum_{i=1}^{T} x_i K_i$ and $Y = \delta" K_0 + \sum_{i=1}^{T} y_i K_i$ the decompositions of X and Y according proposition 2.3.9. Then, we prove the proposition by induction on T.

Remark that $T' \leq T$ (lemma 2.3.11) and $T \geq 1$ (cf corollary 2.2.6).

Then, the proposition holds for T=1 (cf lemma 2.3.4).

Then, let us assume $T \in \mathbb{N}^*$, $T \leq d - c$ and that the proposition holds for all integer $T' \leq T$.

Let $X = \delta' K_0 + \sum_{i=1}^{T+1} x_i K_i \in M$ and $Y = \delta" K_0 + \sum_{i=1}^{T+1} y_i K_i \in M$. Let $X', Y', Y"$ defined by $X' = X - x_{T+1} K_{T+1}$, $Y' = Y - y_{T+1} K_{T+1}$, $Y" = Y' + K_{T+1}$. Then, X', $Y' \in [0, K_{T+1}[\cap M^+$ (cf proposition 2.3.2) and $Y" \in M$ (cf proposition 2.3.2).

Let us assume Y'=X'. Then, by lemma 2.4.5, the proposition is almost obvious.

Let us assume $X' < Y'$. Let $Y' - X' = \Delta K_0 + \sum_{i=1}^{T} z_i K_i$ the decomposition of Y'-X' according lemma 2.3.11. Then, lemma 2.3.14 allows to write

$$Y - X = \Delta K_0 + \sum_{i=1}^{T} z_i K_i + (y_{T+1} - x_{T+1}) K_{T+1} \ .$$

Now,
$\overline{\overline{[X, Y[}} = \overline{\overline{[X', Y'[}} + \overline{\overline{[Y', Y[}} - \overline{\overline{[X', X[}}$,
$\overline{\overline{[X', Y'[}} = \sum_{i=1}^{T} z_i Q_i$ (by induction),
$\overline{\overline{[Y', Y[}} = y_{T+1} Q_{T+1}$ (by lemma 2.4.5) ,
$\overline{\overline{[X', X[}} = x_{T+1} Q_{T+1}$ (by lemma 2.4.5). QED

Let us assume $Y' < X'$. In this case, $Y' < X' < Y" \leq Y$.

If, $\overline{X'a} < \overline{Y"a}$, $Y" - X' \in M$. Then, by corollary 2.3.16, $K_0 + X' - Y' \in M$.

Therefore, $K_0 + X' - Y'$ and Y"-X' check the assumptions of lemma 2.4.6.

Therefore, if $Y" - X' = \delta K_0 + \sum_{i=1}^{T} z"_i K_i$, and $K_0 + X' - Y' = \delta' K_0 + \sum_{i=1}^{T} z'_i K_i$ according proposition 2.3.9, lemma 2.3.11, then, $\sum_{i=1}^{T} (z"_i + z'_i) Q_i = Q_{T+1}$ by lemma 2.4.6.

Now, $Y" - X' = \delta K_0 + \sum_{i=1}^{T} z"_i K_i$ is also the writing of $Y" - X'$ according lemma 2.3.11 because $\overline{X'a} < \overline{Y"a}$ and because this writing according lemma 2.3.11 is unique.

Then, by lemma 2.3.14,

$$Y - X = \Delta K_0 + \sum_{i=1}^{T} z_i K_i + (y_{T+1} - x_{T+1} - 1) K_{T+1} \ ,$$

where $z"_i = z_i$. Moreover, $\overline{\overline{[Y', X'[}} = \sum_{i=1}^{T} z'_i Q_i$ by induction and $\overline{\overline{[Y', Y[}} = y_{T+1} Q_{T+1}$ by lemma 2.4.5. Then, the equality $\overline{\overline{[X, Y[}} = \overline{\overline{[Y', Y[}} - \overline{\overline{[Y', X'[}} - \overline{\overline{[X', X[}}$ allows to conclude that $\overline{\overline{[X, Y[}} = \sum_{i=1}^{T} z_i Q_i$. QED

If $\overline{Y"a} < \overline{X'a}$, $K_0 + Y" - X' \in M$. Then, by corollary 2.3.16, $X' - Y' \in M$.

Therefore, by lemma 2.3.11, $Y" - X = \Delta K_0 + \sum_{i=1}^{T} z"_i K_i$ with $\Delta = 0$ or -1, i.e., $K_0 + Y" - X = \delta K_0 + \sum_{i=1}^{T} z"_i K_i$ with $\delta = 0$ or 1.

Moreover, $\overline{Y"a} < \overline{X'a}$. Then, by lemma 2.3.15, $\overline{Y'a} < \overline{X'a}$. Then, by lemma 2.3.11, $X' - Y' = \delta' K_0 + \sum_{i=1}^{T} z'_i K_i$ with $\delta' = 0$ or 1.

Now, $X' - Y'$ and $K_0 + Y" - X$' check the assumptions of lemma 2.4.6. Moreover, X',Y', $Y" \in M$. Then, $\sum_{i=1}^{T}(z"_i + z'_i)Q_i = Q_{T+1}$ by lemma 2.4.6.

Now, by lemma 2.3.14,

$$Y - X = \Delta K_0 + \sum_{i=1}^{T} z_i K_i + (y_{T+1} - x_{T+1} - 1)K_{T+1} \ ,$$

with $z"_i = z_i$.

Now, $\overline{\overline{[Y', X'[}} = \sum_{i=1}^{T} z'_i Q_i$ (by induction) and $\overline{\overline{[Y', Y[}} = y_{T+1}Q_{T+1}$ by lemma 2.4.5. Then, the equality $\overline{\overline{[X, Y[}} = \overline{\overline{[Y', Y[}} - \overline{\overline{[Y', X'[}} - \overline{\overline{[X', X[}}$ allows to conclude that $\overline{\overline{[X, Y[}} = \sum_{i=1}^{T} z_i Q_i$. QED

At last suppose $\overline{X'a} = \overline{Y"a}$. Now, $T + c \leq d$. Then, $T + c + 1 \leq d + 1$. Now, X', $Y" < K_{T+1} \leq K_{d+1}$. Then, by corollary 2.2.4, $Y" = X'$. But $X' < K_T$ and $K_T \leq Y"$. It is impossible. ■

2.5 Computation of the number of points of M^f contained in intervals

We keep the notations of section 2.3 and 2.4 (in particular, we suppose again that assumptions 2.3.1 hold).

One generalizes very easily the previous results at the case of M^f by remarking that $M^f = \{M\} \cup \{M + K_0\} \cup \{M + 2K_0\} \cup ..... \cup \{M + (f-1)K_0\}$. This is reflected in the two following lemma.

Lemma 2.5.1 *The points $\ell^f \in M^f$ such that $tR_0 \leq \overline{\ell^f a} < (t+1)R_0$, $t \in \mathbb{N}$, $t + 1 \leq f \leq H_0$, are the points of the form $\ell^f = \ell + tK_0$, $\ell \in M$.*

Proof It almost obvious.■

Lemma 2.5.2 *Let $X, Y \in M$, $X < Y$ and let $X - Y = \Delta K_0 + \sum_{i=1}^{T} z_i K_i$ be the decomposition of Y-X according lemma 2.3.11. Then $card\big([X, Y[\cap M^f\big) = f\big(\sum_{i=1}^{T} z_i Q_i\big)$.*

Proof Let $\ell^f \in M^f$. Let $X_1 \in M$, $X \leq X_1 < Y$. Then, $\ell^f = X_1 + tK_0 \in M^f$ according lemma 2.5.1.

Now, by corollary 2.2.6, $Y - X_1 \geq K_1$. Then, $X_1 + tK_0 \leq X_1 + (H_0 - 1)K_0 = X_1 + K_1 - K_{-1} - K_0 < X_1 + K_1 \leq Y$. Then, $\ell^f < Y$.

Then, $[X, Y[\cap M^f = \{\ell + tK_0 | \ell \in M, t \leq H_0 - 1\}$.

By using proposition 2.4.7, the proof is almost immediate.■

Now we can prove the fundamental proposition. We understand that, for an integer L, which is almost anything. We know almost exactly the number of points of M^f contained in any interval of length L. This result gives us a remarkable knowledge of the distribution of points of E_2.

Fundamental Proposition 2.5.3 *Let $L \in \mathbb{N}$ such that $L = \sum_{i=1}^{T} \lambda_i K_i$ with $\lambda_i \leq H_i$, $\lambda_1 < H_1$, and if $\lambda_i = H_i$, then, $\lambda_{i-1} = 0$.*

Let us denote by Q the number $Q = \sum_{i=1}^{T} \lambda_i Q_i$. Let $x \in \mathbb{N}$. Then,

$$card\big([x, x+L[\cap M^f\big) = fQ \quad or \quad fQ+1 \quad if \quad L \in M \ ,$$

$$card\big([x, x+L[\cap M^f\big) = fQ \quad or \quad fQ-1 \quad if \quad K_0+L \in M \ .$$

Proof In this proof, we set $\overline{\overline{[x,y[}} = card\big([x,y[\cap M^f\big)$ when [x,y[is an interval of $\mathbb{R}_+$.

Then, let $x \in \mathbb{N}$. Then there exists $X \in M$ and $X_1 \in M$ such that $X \leq x < X_1$. Let us set Y=X+L, y=x+L and s=x-X=y-Y.

We recall that $L \in M$ or $K_0 + L \in M$ by lemma 2.3.10.

Then, if $L \in M$, we denote by Y' the one of the two numbers Y or $Y - K_0$ which belongs to M according lemma 2.3.13 (cf also lemma 2.3.10).

If $K_0 + L \in M$, we denote by Y' the one of the two numbers Y or $Y + K_0$ which belongs to M according lemma 2.3.13 (cf also lemma 2.3.10).

At last, we denote by Y_1' the follow up of Y' in M, i.e. $Y' < Y_1'$ and $]Y', Y_1'] \cap M = \{Y_1'\}$.

Then, by lemma 2.3.13, proposition 2.4.7 and lemma 2.5.2, $\overline{\overline{[X,Y'[}} = \overline{\overline{[X_1,Y_1'[}} = fQ$.

Now, we need the following lemma.

Lemma 2.5.4 *Let $\alpha \in \mathbb{N}$ and let $Z_0,\ Z_1 \in M$ such that $Z_0 \leq \alpha < Z_1$ and such that there does not exist $Z' \in M$ checking $Z_0 < Z' < Z_1$.*

Let $t \in \mathbb{N} \cup \{-1\}$ such that $Z_0 + tK_0 < \alpha \leq Z_0 + (t+1)K_0$. Then, we denote $\alpha \in \mathcal{V}_t^{Z_0}$.

Then, $\overline{\overline{[Z_0,\alpha[}} = inf(f, t+1)$ and $\overline{\overline{[\alpha,Z_1[}} = f - inf(f, t+1)$.

Proof Lemma 2.5.1 shows that $[Z_0, Z_1[\cap M^f = \{Z_0, Z_0+K_0, Z_0+2K_0, ..., Z_0+(f-1)K_0\}$.

Moreover 2.5.2 shows that $\overline{\overline{[Z_0,Z_1[}} = f$. ■

Now we can prove the fundamental proposition. At first, we suppose Y'=Y.

Therefore $L \in M$ or $K_0 + L \in M$.

1-a) Let us assume $Y_1' - Y' \geq X_1 - X$. Then, if $x \in \mathcal{V}_t^X$, $y \in \mathcal{V}_t^{Y'}$. Then, $\overline{\overline{[x,y[}} = \overline{\overline{[X,Y[}} + \overline{\overline{[Y,y[}} - \overline{\overline{[X,x[}} = \overline{\overline{[X,Y[}} = fQ$.

On these figures, y-axis has no interest : it is just a matter of showing on two lines the location of Y,Y', Y_1', X_1, X.

1-b) Let us assume $Y_1' - Y' < X_1 - X$. Then, $X_1 - X = K_1 + K_0$ and $Y_1' - Y' = K_1$ by corollary 2.2.6. If $s \leq K_1$, it is the same proof as above in 1-a).

If $s > K_1$, then, $y \in]Y_1', Y_1' + K_0[$, and in this case, $K_0 + L \notin M$.

Indeed, because $X_1 - X = K_1 + K_0$, then $\overline{Xa} < R_1$. Indeed, $\overline{X_1 a} \equiv \overline{Xa} + \overline{K_1 a} + \overline{Ka} = \overline{Xa} - R_1 + R_0 < R_0$ because c is odd (cf lemma 2.2.1). Then, if $\overline{X_1 a} = \overline{Xa} + \overline{K_1 a} + \overline{Ka}$, $\overline{Xa} < R_1$. If $\overline{X_1 a} = m + \overline{Xa} + \overline{K_1 a} + \overline{Ka} \geq m + R_0 - R_1 + R_0 \geq m/2 + 2R_0$ because $c \geq 1$ and then, $R_1 < R_0 < m/2$. Then, $\overline{X_1 a} > R_0$ and $X_1 \notin M$: there is a contradiction.

Now if $K_0 + L \in M$, then, $m - R_0 \leq \overline{La} < m$.

Therefore, $m - R_0 - R_1 \leq \overline{Xa} + \overline{La} - R_1 < m$.

Now, Y=X+L, $Y_1' = Y + K_1$. Then, $\overline{Y_1' a} = \overline{(X+L+K_1)a} = \overline{Xa} + \overline{La} - R_1 \geq m - R_0 - R_1$. Then, $Y_1' \notin M$.

Now, $m - R_0 - R_1 \geq R_0$.

Indeed $R_0 + R_1 \leq R_{-1}$. Then, if $R_{-1} \leq r_1 \leq m/2$, it is obvious.

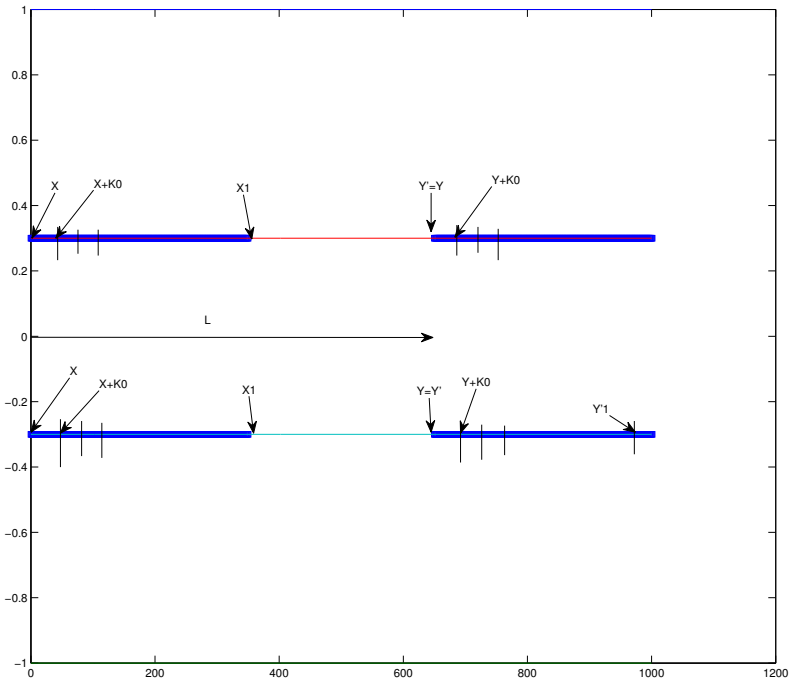

Figure 2.4: On this figure, y-axis to have no interest

If not, $R_0 = r_1$, $R_1 = r_2$ and then, because $r_1 \leq m/2$, $h_0 \geq 2$ and then, $r_1 + r_2 \leq m - r_1$. Therefore, $\overline{(X + L + K_1)a} \geq m - R_0 - R_1 \geq R_0$.
Now, Y=X+L, $Y'_1 = Y + K_1$. It means $Y'_1 \notin M$. Then, $L \in M$

Now, by lemma 2.3.13, Y'-X is written by an only way $Y - X = K_0 + \sum_{i=1}^{T} \lambda_i K_i$ according lemma 2.3.11. Then, $\overline{\overline{[X, Y[}} = fQ$ according proposition 2.4.7.

Moreover, because $y \in]Y'_1, Y'_1 + K_0[$, $\overline{\overline{[Y'_1, y[}} = 1$.

Moreover, with the notations of lemma 2.5.4 with $x = \alpha$, because $s \geq K_1 = H_0 K_0 + K_{-1}$, $t \geq f$, and then, $\overline{\overline{[X, x[}} = f$. Now, by lemma 2.5.2, $\overline{\overline{[Y, Y'_1[}} = f$.

Then, $\overline{\overline{[x, y[}} = \overline{\overline{[X, Y[}} + \overline{\overline{[Y, Y'_1[}} + \overline{\overline{[Y'_1, y[}} - \overline{\overline{[X, x[}} = \overline{\overline{[X, Y[}} = fQ + f + 1 - f = fQ + 1$. QED

Now we suppose $Y' = Y + K_0$. Therefore $K_0 + L \in M$.

Now, by lemma 2.3.13, Y'-X is written by an only way $Y' - X = K_0 + \sum_{i=1}^{T} \lambda_i K_i$ according lemma 2.3.11. Then, $\overline{\overline{[X, Y'[}} = fQ$ according proposition 2.4.7.

If x=X, then, $\overline{\overline{[y, Y'[}} = 0$ or 1 by lemma 2.5.1.
Therefore, $\overline{\overline{[x, y[}} = \overline{\overline{[X, Y'[}} - \overline{\overline{[y, Y'[}} = fQ$ or fQ-1 by using proposition 2.4.7.

If $X < x < X + K_0$, then, $\overline{\overline{[y, Y'[}} = 0$ by lemma 2.5.1. Moreover, $\overline{\overline{[X, x[}} = 1$ by lemma 2.5.1.
Therefore, $\overline{\overline{[x, y[}} = \overline{\overline{[X, Y'[}} - \overline{\overline{[X, x[}} - \overline{\overline{[y, Y'[}} = fQ - 1$.

If $X + K_0 \leq x$, then, $s < K_1 + K_0$ and $Y'_1 - Y' \geq K_1$ by corollary 2.2.6. Then, $Y' \leq y < Y'_1$.
Then, if $x \in \mathcal{V}_t^X$, $y \in \mathcal{V}_{t-1}^{Y'}$.
Therefore $\overline{\overline{[Y', y[}} = \overline{\overline{[X, x[}} - 1$.
Therefore, $\overline{\overline{[x, y[}} = \overline{\overline{[X, Y'[}} - \overline{\overline{[X, x[}} + \overline{\overline{[Y', y[}} = fQ - 1$.
Therefore, $\overline{\overline{[x, y[}} = fQ - 1$.

Now we suppose $Y' = Y - K_0$. Therefore $L \in M$.

Now, by lemma 2.3.13, Y'-X is written by an only way $Y' - X = -K_0 + \sum_{i=1}^{T} \lambda_i K_i$ according lemma 2.3.11. Then, $\overline{\overline{[X, Y'[}} = fQ$ according proposition 2.4.7.

If $y \in [Y, Y'_1]$, then if $x \in \mathcal{V}_t^X$, $y \in \mathcal{V}_{t+1}^{Y'}$. Then, $\overline{\overline{[x, X[}} + 1 = \overline{\overline{[Y', y[}}$.
Now, $\overline{\overline{[x, y[}} = \overline{\overline{[X, Y'[}} - \overline{\overline{[x, X[}} + \overline{\overline{[Y', y[}} = fQ + 1$.

Then, let us suppose $y \geq Y'_1$.

Now, it is impossible that $Y'_1 - Y' < X_1 - X$. Indeed, in this case, by corollary 2.2.6, $Y'_1 - Y' = K_1$ and $X_1 - X = K_1 + K_0$.

Now, as previously , $\overline{Xa} < R_1$. Indeed, $\overline{X_1 a} \equiv \overline{Xa} + \overline{K_1 a} + \overline{K_0 a} = \overline{Xa} - R_1 + R_0 < R_0$. Moreover, $\overline{Xa} - R_1 + R_0 < 2R_0 < m$ because $m/2 > r_1 \geq R_0 \geq R_1$. Then, $\overline{X_1 a} = \overline{Xa} - R_1 + R_0 < R_0$.

Then, $\overline{Xa} < R_1$ and $\overline{La} < R_0$. Then, $\overline{Xa} + \overline{La} - R_0 - R_1 < 0$. Then, $\overline{Y'_1 a} = \overline{(X + L - K_0 + K_1)a} = m + \overline{Xa} + \overline{La} - R_0 - R_1 < m$.

Moreover, $m + \overline{Xa} + \overline{La} - R_0 - R_1 > m - R_0 - R_1 \geq m - r_1 - r_2 \geq r_1$ because $h_1 \geq 2$. Then, $\overline{Y'_1 a} > r_1 \geq R_0$. Therefore $Y'_1 \notin M$.

Now, if $y \geq Y'_1$ and if $Y'_1 - Y' > X_1 - X$, then $Y'_1 - Y' = K_1 + K_0$ and $X_1 - X = K_1$. Then, $x - X < K_1$. Then, $y = Y + (x - X) = Y' + K_0 + (x - X) < Y' + K_0 + K_1 = Y'_1$. It is impossible.

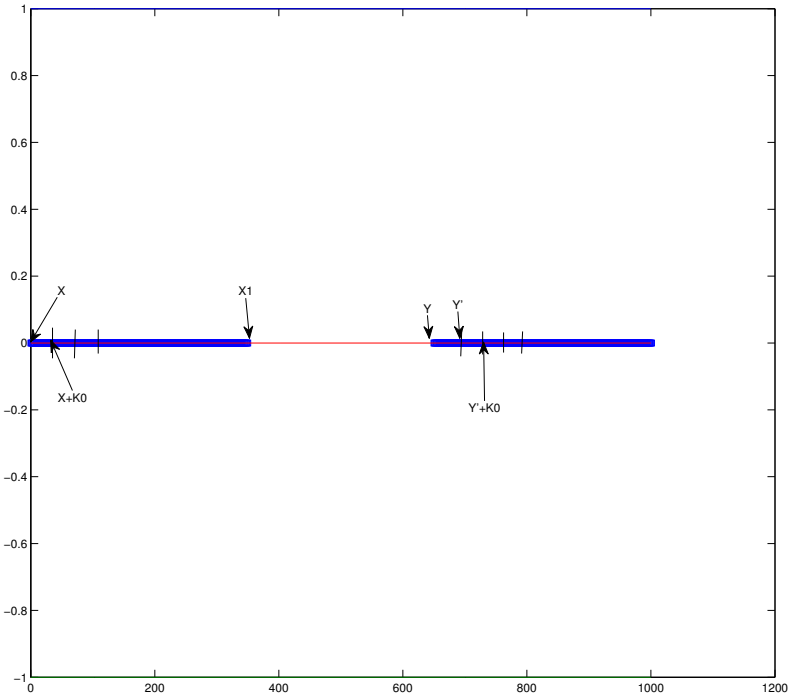

Figure 2.5: On this figure, y-axis to have no interest

Therefore, if $y \geq Y_1'$, $Y_1' - Y' = X_1 - X$. Then, if $y > Y_1'$, $y \in]Y_1', Y_1' + K_0[$ and $x \in]X_1 - K_0, X_1[$. Then, $\overline{\overline{[X, x[}} = f$ by lemma 2.5.1, $\overline{\overline{[Y', Y_1'[}} = f$ by lemma 2.5.2 and $\overline{\overline{[Y_1', y[}} = 1$ by lemma 2.5.1.

Therefore, $\overline{\overline{[x, y[}} = \overline{\overline{[X, Y'[}} - \overline{\overline{[X, x[}} + \overline{\overline{[Y', Y_1'[}} + \overline{\overline{[Y_1', y[}} = fQ + 1$. QED

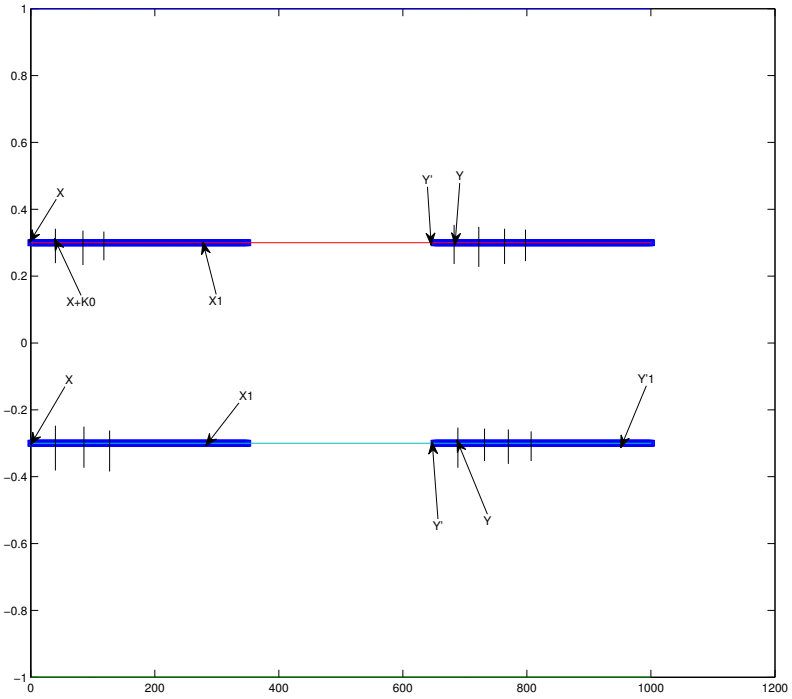

Figure 2.6: On this figure, y-axis to have no interest

Then, the theorem is proved. ■

2.6 Generalization

Now that proposition 2.5.3 is proved, one can easily obtain the announced results. Remark that up to now, we have not assumed that a is invertible. Then, we shall study at first criteria in order that T is invertible.

For this study, we assume the following assumptions hold.

Assumptions 2.6.1 *We assume that the assumptions 2.3.1 except that* $\overline{k_c a} = r_c$ *(except in proposition 2.6.10).*

2.6.1 Conditions in order that T is invertible

Lemma 2.6.1 *We have* $\overline{k_{d+1} a} = r_{d+1} = 0$.

Proof It is the lemma 2.2.1 and the definition of d. ■

Lemma 2.6.2 *The integer k_{d+1} is a divisor of m.*

Proof At first, $k_{d+1} \leq m$. If not $\overline{ma} = 0$ is a contradiction with lemma 2.2.2.

On the other hand, let D be the G.C.D. of m and k_{d+1}. Then, $D > 1$: if not k_{d+1} is invertible because $uk_{d+1} + vm = 1$, u, $v \in \mathbb{Z}$, admits solutions if and only if k_{d+1} and m are coprime : theoreme of Bezout. Then, $\overline{k_{d+1}a} \neq 0$, what is contrary to lemma 2.6.1.

Moreover, by Bezout identity , there exists u, $v \in \mathbb{Z}$ such that $uk_{d+1} + vm = D$. Therefore, by lemma 2.6.1, $\overline{Da} = 0$. Then, $D \geq k_{d+1}$ by lemma 2.2.2. Then, k_{d+1} is a divisor of m. ■

Lemma 2.6.3 *In order that a is invertible it is necessary and sufficient that $r_d = 1$.*

Proof If $r_d = 1$, then $\overline{k_d a} \equiv \pm 1$ (cf lemma 2.2.1).

Reciprocally, if a is invertible, we denote by k^i the integer $k^i = inf\big(k \in \mathbb{N} | ka \equiv \pm 1\big)$. Then, $k^i < k_{d+1}$: if not, $(k^i - k_{d+1})a \equiv \pm 1$ by lemma 2.6.1. Then, k^i it is not in accordance with its definition.

Therefore $0 < r_d \leq \overline{k^i a} \leq m - r_d < m$ (cf lemma 2.2.2).

Now, $\overline{k^i a} = 1$ or $\overline{k^i a} = m - 1$. Therefore, $r_d \leq 1$. Therefore $r_d = 1$. ■

Lemma 2.6.4 *Si a is invertible, then $\overline{k_d a} \equiv \pm 1$ and $k_d = inf\big(\overline{a^{-1}}, m - \overline{a^{-1}}\big)$.*

Proof The first congruence is deduced from lemma 2.2.1 and lemma 2.6.3.

Therefore, $k_d = \overline{a^{-1}}$ or $k_d = m - \overline{a^{-1}}$.

If $k_d > m/2$, then, $m - k_d < m/2 < k_d$ and $\overline{(m - k_d)a} \equiv \pm 1$, what is a contradiction with lemma 2.2.2. ■

Lemma 2.6.5 *The element a est invertible if and only if $k_{d+1} = m$.*

Proof By lemma 2.6.2, $k_{d+1} \leq m$.

If a is invertible, because $k_{d+1}a \equiv 0$ by lemma 2.6.1, we have $k_{d+1}aa^{-1} \equiv k_{d+1} \equiv 0$. Now, $1 = k_1 < k_{d+1} \leq m$. Therefore, $k_{d+1} = m$. QED

If $k_{d+1} = m$, then, $\overline{ka} \neq 0$ if $k \in \mathbb{N}$ and $k < k_{d+1}$ by lemma 2.2.2.

Then, the application $k \mapsto \overline{ka}$ is a bijective function $\{1, 2, ..., m-1\} \to \{1, 2, ..., m-1\}$. Therefore, there exists k such that $\overline{ka} = 1$. QED ■

Lemma 2.6.6 *Let us suppose a invertible. Let us denote by r^o_n, k^o_n, and h^o_n, the sequences r_n, k_n, and h_n, for the congruence T^{-1}. Then, $r^o_n = k_{d+1-n}$ for n=0,1,....,d+1, and $h^o_n = h_{d+1-n}$ for n=0,1,....,d, and $k^o_n = r_{d+1-n}$ for n=0,1,....,d+1.*

Proof We have $r^o_0 = m = k_{d+1}$ by lemma 2.6.5 and $r^0_1 = inf\big(\overline{a^{-1}}, m - \overline{a^{-1}}\big) = k_d$ by lemma 2.6.4.

Moreover, the sequence r^o_n is defined by the induction thanks to the Euclidean division $r^o_n = h^o_{n+1} r^o_{n+1} + r^o_{n+2}$ and k_{n-1} is defined by the Euclidean division of k_{n+1} by k_n when $n \geq 2$ (because $h_1 \geq 2$).

Then, $r^o_n = k_{d+1-n}$ when $d+1-n \geq 1$, i.e. $d \geq n$. Moreover, $h^o_n = h_{d+1-n}$ when $d+1-n \geq 2$, i.e. $d - 1 \geq n$.

Now, for n=d-1, $r^o_{d-1} = k_2$ and $h^o_{d-1} = h_2$. For n=d, $r^o_d = k_1 = 1$ (cf lemma 2.6.3). Now because $r^o_{n-1} > r^0_n$ for $n = 1, 2, ..., d^o + 1$, then $r^o_{d+1} = 0$ and then $d^0 = d$.

But $r^o_{d^o-1} = h^o_{d^o} r^o_{d^o}$ and $r^o_{d-1} = k_2 = h_1 k_1 + k_0 = h_1 k_1 = h_1 r^o_d$. Then, $h^o_d = h_1$. Moreover, $r^o_{d+1} = k_0 = 0$.

Now one can reverse the roles of T and T^{-1}. Therefore, by the previous results, $r_n = r^{oo}_n = k^o_{d^o+1-n} = k^o_{d+1-n}$ for n=0,1,....,d+1. Then, with n'=d+1-n, $r_{d+1-n'} = k^o_{n'}$ for n'=0,1,....,d+1. ■

2.6.2 Connection with the continued fractions

It is remarkable that the sequences r_n, k_n and h_n which are used in our study are those of the development of m/a in continued fractions : cf [22] when $a \leq m/2$. Then, we recall now lemma 2.1.3. The following proposition allows to complete this connection when $a > m/2$.

Proposition 2.6.7 *Let $r^a_0 = m$, $r^a_1 = \overline{a}$ and let $r^a_n = h^a_{n+1} r^a_{n+1} + r^a_{n+2}$ be the Euclidean division of r^a_n by r^a_{n+1}. Then, if $a > m/2$, we have*
$h^a_1 = 1$, $h^a_2 + h^a_1 = h_1$, $h^a_{n+1} = h_n$ if $n \geq 2$,
$r^a_1 = a$, $r^a_2 = m - a$ and $r^a_{n+1} = r_n$ if $n \geq 1$.

Corollary 2.6.8 *The integer a is invertible in $\mathbb{Z}/m\mathbb{Z}$ if and only if $Inf\{r^a_n | r^a_n > 0\} = 1$.*

Proof This proof is done without difficulty. ■

2.6.3 Generalization of the fundamental proposition

For this generalization, we proceed by steps : We first show that any rectangle $[0, m[^2$, height fr_c, and width L, contains Q or Q+1 points of E_2. Then, thanks to a simple bijection, we generalize easily to the case $\overline{k_c a} = m - r_c$.

Definition 2.6.9 *Let R^o be a rectangle of $\mathbb{R}^2_+$: $R^o = [x, x + L[\times[y, y + L'[$. We will call the quotient rectangle resulting from R^o the subset $\overline{\mathbb{R}^o} \subset [0, m[^2$:*

$$\overline{\mathbb{R}^o} = \left\{ (x', y') \in [0, m[^2 \middle| \exists (x, y) \in R^o : x' - x \equiv y' - y \equiv 0 \ mod \ m \right\} .$$

Proposition 2.6.10 *Let $\overline{\mathbb{R}^o}$ be a quotient rectangle resulting from R^o when $R^o = [x, x+L[\times[y, y+fr_c[$ with $(x, y) \in \mathbb{N}^2$, $L = \sum_{i=1}^T \lambda_i K_i$, $Q = \sum_{i=1}^T \lambda_i Q_i$ and $f \in \mathbb{N}^*$, $f \leq h_c$ according the criteria of proposition 2.5.3.*

We assume $\overline{k_c a} = r_c$ and that T is invertible : $T(x) \equiv ax + b$ modulo m. Then,

$$card(\overline{\mathbb{R}^o} \cap E_2) = fQ \quad or \quad fQ + 1 \quad if \ L \in M \ ,$$

$$card(\overline{\mathbb{R}^o} \cap E_2) = fQ \quad or \quad fQ - 1 \quad if \ k_c + L \in M \ .$$

Proof Because T is invertible, there exists an alone $x" \in [0, m[$ such that $\overline{ax"} = \overline{ax - y + b}$. Then, let ϕ be the function $\phi : R^o \cap E_2 \to \mathbb{N}^2$, defined by $\phi(x_1, y_1) = x" + x_1 - x$.

Because $ax_1 + b \equiv y_1$, $\overline{a(x" + x_1 - x)} \equiv ax" + ax_1 - ax \equiv ax - y + b + (y_1 - b) - ax = y_1 - y$. Then, $\overline{a(x" + x_1 - x)} = y_1 - y$ if $y \leq y_1 < y + fr_c$ and $0 \leq \overline{a(x" + x_1 - x)} < fr_c$.

Then, it is obvious that $\phi(R^o \cap E_2) \subset [x", x" + L[$: $\phi(R^o \cap E_2) \subset [x", x" + L[\cap M^f$.

Now, ϕ is an injection of $R^o \cap E_2$ in $[x", x" + L[\cap M^f$: $\phi(x_1, y_1) \neq \phi(x'_1, y'_1)$ if $(x_1, y_1) \neq (x'_1, y'_1)$. Indeed, if $x_1 \neq x'_1$, it is obvious. If $x_1 = x'_1$, then, $y_1 = \overline{T}(x_1) = \overline{T}(x'_1) = y'_1$. Therefore, $(x_1, y_1) = (x'_1, y'_1)$

Moreover, it is obvious that ϕ is a surjection. Therefore, it is a bijection. Then, it is enough to use fundamental proposition 2.5.3. ■

Proposition 2.6.11 *We keep the notations and assumptions of proposition 2.6.10 except* $\overline{k_c a} = r_c$ *which we replace by* $\overline{k_c a} = m - r_c$. *Let* $M' = \{\ell \in \mathbb{N} | \overline{\ell a'} \leq r_c\}$ *when a'=m-a. Then,*
$card(\overline{R^o} \cap E_2) = fQ$ *ou fQ+1 if* $L \in M'$,
$card(\overline{R^o} \cap E_2) = fQ$ *ou fQ-1 if* $k_c + L \in M'$.

Proof We know that $L < m$ and $fr_c < m$. Indeed, $L < K_{T+1} \leq k_{d+1} = m$ (cf proposition 2.3.9 and lemma 2.6.5). Moreover, $\overline{k_c a} = m - r_c > m/2$ if $c \geq 2$. Then, $fr_c \leq h_c r_c < m$.

Let $E_2' \subset \mathbb{Z}^2 : E_2' = \{(x,y) \in \mathbb{Z}^2 | y \equiv \overline{a'x - b}\}$ where a'=m-a. Then, $\overline{a'x - b} = \overline{mx - ax - b}$.

Suppose $\overline{\xi a + b} \neq 0$ for all ξ such that $x \leq \xi < x + L$ and $y \leq \overline{m - \xi a - b} \leq y + fr_c$. Then,

$$\left\{[x, x+L[\times[y, y+fr_c[\right\} \cap E_2'$$

$$= \left\{\xi | x \leq \xi < x + L \ : \ y \leq \overline{m - \xi a - b} < y + fr_c\right\}$$

$$= \left\{\xi | x \leq \xi < x + L \ : \ y \leq m - \overline{\xi a + b} < y + fr_c\right\}$$

$$= \left\{\xi | x \leq \xi < x + L \ : \ \overline{\xi a + b} \leq m - y \ , \ m - y - fr_c < \overline{\xi a + b}\right\}$$
$$= \left\{\xi | x \leq \xi < x + L \ : \ m - y - fr_c < \overline{\xi a + b} \leq m - y\right\}$$
$$= \left\{[x, x+L[\times[m - y - fr_c + 1, m - y + 1[\right\} \cap E_2 \ .$$

Then, $card(\overline{R^o} \cap E_2') = card(\overline{R^1} \cap E_2)$ where $R^1 = [x, x+L[\times[m - y - fr_c + 1, m - y + 1[$. Now sequences r_n and r_n' associated to a and a' are identical. So it's the same for sequences h_n, and therefore for the sequences k_n. So sequences Q_n^c are identical. Then,
$card(\overline{R^o} \cap E_2') = fQ$ or fQ+1 if $L \in M'$,
$card(\overline{R^o} \cap E_2') = fQ$ or fQ-1 if $k_c + L \in M'$. QED

Now we suppose that there exists ξ such that $\overline{\xi a + b} = 0$. For example it may be the case if $y < m \leq y + fr_c$.

Now it is clear that, for c even, $c \geq 2$, all rectangle $R^0 \cap E_2 = \left\{[x, x+L[\times[y, y+fr_c[\right\} \cap E_2$ is in bijection with the rectangle modulo m $\left\{[x', x'+L[\times[y', y'+fr_c[\right\} \cap E_2$ where $x' \geq 0$ and where $0 \leq y' < y' + fr_c < m$ or $m/2 < y' < m \leq y' + fr_c < 3m/2$. Then the proof is done in the case where $y < m \leq y + fr_c$ is sufficient.

Then, we suppose that $y < m \leq y + fr_c$. We are interested by ξ such that there exists ζ such that $x \leq \xi < x + L$ and $y \leq \zeta \leq y + fr_c$ where $\zeta \equiv \overline{m - \xi a - b}$. We can assume that $m/2 < y < m \leq y + fr_c < 3m/2$. Indeed, if $\overline{k_c a} = m - r_c$, then $c \geq 2$ and $c < d+1$ (if not, $r_c = 0$ and $0 = \overline{k_c a} \neq m = m - r_c$). Then, $fr_c \leq h_2 r_2 \leq r_1 \leq m/2$.

Let $\delta_\xi = 0, 1$ such that, for all $\xi \in \mathbb{N} \cap [x, x+L[$, $y \leq \delta_\xi m + \overline{m - \xi a - b} \leq y + fr_c$.

If $m/2 < \overline{m - \xi a - b} < m$, $\delta_\xi = 0$. Moreover, $m/2 > \overline{\xi a + b} > 0$ and $y \leq \delta_\xi m + \overline{m - \xi a - b} = \overline{m - \xi a - b} < m$.

If $m/2 > \overline{m - \xi a - b} > 0$, $\delta_\xi = 1$. Moreover, $m/2 < \overline{\xi a + b}$ and $m \leq \delta_\xi m + \overline{m - \xi a - b} = m + \overline{m - \xi a - b} < y + fr_c$.

If $\overline{m - \xi a - b} = 0$, $\delta_\xi = 1$. Moreover, $0 = \overline{\xi a + b} < m/2$ and $m \leq \delta_\xi m + \overline{m - \xi a - b} = m < y + fr_c$.

Let $\delta_\xi' = -1, 0$ such that $\delta_\xi m + \overline{m - \xi a - b} = \delta_\xi' m + m - \overline{\xi a + b}$.
Therefore, if $0 < \overline{\xi a + b} < m/2$, $m > \delta_\xi m + \overline{m - \xi a - b} = \overline{m - \xi a - b} = \delta_\xi' m + m - \overline{\xi a + b} \geq m/2$

: $\delta'_\xi = 0$.
Therefore, if $\overline{\xi a+b} > m/2$, then $m \le \delta_\xi m + \overline{m-\xi a-b} = m + \overline{m-\xi a-b} = \delta'_\xi m + m - \overline{\xi a+b}$: therefore $\delta'_\xi = 1$.
Therefore, if $\overline{\xi a+b} = 0$, $m > \delta_\xi m + \overline{m-\xi a-b} = m = \delta'_\xi m + m - \overline{\xi a+b} = m$: $\delta'_\xi = 0$.

Therefore, if $0 \le \overline{\xi a+b} < m/2$, $\delta'_\xi = 0$.
Therefore, if $\overline{\xi a+b} > m/2$, then $\delta'_\xi = 1$.

Let $\phi \in \{0, 1, ..., m-1\}$. We set $\overline{\phi}^\theta = \phi$ if $\phi \le m/2$ and $\overline{\phi}^\theta = \phi - m$ if $\phi > m/2$: $\overline{\phi}^\theta \equiv \phi$ and $-m/2 < \overline{\phi}^\theta < m/2$. Therefore, if y"=m-y and $m/2 < y < m \le y + fr_c < 3m/2$,

$$\big\{[x, x+L[\times[y, y+fr_c[\big\} \cap E'_2$$

$$= \big\{\xi | x \le \xi < x+L \ : \ y \le \delta_\xi m + \overline{m-\xi a-b} < y + fr_c\big\}$$
$$= \big\{\xi | x \le \xi < x+L \ : \ y \le \delta'_\xi m + m - \overline{\xi a+b} < y + fr_c\big\}$$
$$= \big\{\xi | x \le \xi < x+L \ : \ \overline{\xi a+b} \le \delta'_\xi m + m - y \ , \ \delta'_\xi m + m - y - fr_c < \overline{\xi a+b}\big\}$$
$$= \big\{\xi | x \le \xi < x+L \ : \ \delta'_\xi m + m - y - fr_c < \overline{\xi a+b} \le \delta'_\xi m + m - y\big\}$$
$$= \big\{\xi | x \le \xi < x+L \ : \ m - y - fr_c < \overline{\xi a+b} - \delta'_\xi m \le m - y\big\}$$
$$= \big\{\xi | x \le \xi < x+L \ : \ y" - fr_c < \overline{\xi a+b} - \delta'_\xi m \le y"\big\}$$

$$= \big\{\xi | x \le \xi < x+L \ : \ y" - fr_c < \overline{\xi a+b} \le y", \ \delta'_\xi = 0\big\}$$
$$\cup \big\{\xi | x \le \xi < x+L \ : \ y" - fr_c < \overline{\xi a+b} - m \le y", \ \delta'_\xi = 1\big\}$$

$$= \big\{\xi |\ y" - fr_c < \overline{\xi a+b} \le y", \ 0 \le \overline{\xi a+b} < m/2\big\} \cup \big\{\xi |\ y" - fr_c < \overline{\xi a+b} - m \le y", \ \overline{\xi a+b} > m/2\big\}$$
$$= \big\{\xi |\ 0 \le \overline{\xi a+b} \le y", \ 0 \le \overline{\xi a+b} < m/2\big\} \cup \big\{\xi |\ y" - fr_c < \overline{\xi a+b} - m < 0, \ \overline{\xi a+b} > m/2\big\}$$
$$= \big\{\xi | x \le \xi < x+L \ : \ y" - fr_c < \overline{\xi a+b}^\theta \le y"\big\}$$
$$= \big\{[x, x+L[\times[y" - fr_c + 1, y" + 1[\big\} \cap E_2$$
$$= \big\{[x, x+L[\times[m - y - fr_c + 1, m - y + 1[\big\} \cap E_2 \ .$$

Therefore,
$$card\big(\big\{[x, x+L[\times[y, y+fr_c[\big\} \cap E'_2\big) = card\big(\overline{R^o} \cap E'_2\big)$$
$$= card\big(\overline{R^1} \cap E_2\big) = card\big(\big\{[x, x+L[\times[m-y-fr_c+1, m-y+1[\big\} \cap E_2\big) \ .$$

Let $M' = \{\ell \in \mathbb{N} | \overline{\ell a'} \le r_c\}$ when a'=m-a. Then,
$card(\overline{R^o} \cap E'_2) = fQ$ or fQ+1 if $L \in M'$,
$card(\overline{R^o} \cap E'_2) = fQ$ or fQ-1 if $k_c + L \in M'$. QED ■

Proposition 2.6.12 *The propositions 2.6.10 and 2.6.11 remain true for the quotient rectangles resulting from rectangles in the form* $[x, x + f'k_c[\times[y, y + L'[$ *with* $L' = \sum_{i=1}^{T} \lambda'_i r_{c-i}$ *written according the criteria of proposition 2.5.3 when T is replaced by* T^{-1}.

Proof It is enough to use lemma 2.6.6 ■

Corollary 2.6.13 *Let* R^o *be a rectangle in the form* $R^o = [x, x + L[\times[y, y + r_c[$.
If $L = k_{c+1}$, *then,* $card(R^o \cap E_2) = 0$ *or* $card(R^o \cap E_2) = 1$.
If $L = k_{c+2}$, *then,* $card(R^o \cap E_2) = h_{c+1}$ *or* $card(R^o \cap E_2) = h_{c+1} + 1$.

Proof Suppose $L = k_{c+1} = K_1$. Then, f=1 and $Q_1 = 1$.
Suppose $\overline{k_c a} = r_c$ and $c + 1 < d + 1$. Then, $m - r_c \leq \overline{K_1 a} = m - r_{c+1} < m$. Then, $k_c + L \in M$. By proposition 2.6.10, $card(R^o \cap E_2) = 1$ or $card(R^o \cap E_2) = 1 - 1$.
Suppose $\overline{k_c a} = m - r_c$ and $c + 1 < d + 1$. Then, $\overline{k_c a'} = r_c$ with a'=m-a (cf proposition 2.6.11). Now, $m - r_c \leq \overline{La'} = \overline{k_{c+1} a'} = m - r_{c+1} < m$: i.e. $k_c + L \in M'$. Then, by proposition 2.6.11, $card(R^o \cap E_2) = 1$ or $card(R^o \cap E_2) = 1 - 1 = 0$.
Suppose $c+1 = d+1$. Then, $r_c = r_d = 1$ and $k_{c+1} = k_{d+1} = m$: cf lemma 2.6.3 and 2.6.5. Then, because T is invertible, it is obvious that $card(R^o \cap E_2) = 1$.

Suppose $L = k_{c+2} = K_2$. Then, f=1 and $Q_2 = h_{c+1}$.
Suppose $\overline{k_c a} = r_c$ and $c+2 < d+1$. Then, $L \in M$, and by proposition 2.6.10, $card(R^o \cap E_2) = h_{c+1}$ or $card(R^o \cap E_2) = h_{c+1} + 1$.
Suppose $\overline{k_c a} = m - r_c$ and $c + 2 < d + 1$. Then, $\overline{k_c a'} = r_c$ with a'=m-a (cf proposition 2.6.11). Now, $L = k_{c+2} = K_2$. Then, $\overline{La'} = \overline{k_{c+2} a'} = r_{c+2} < r_c$: $L \in M'$. Then, by proposition 2.6.11, $card(R^o \cap E_2) = h_{c+1}$ or $card(R^o \cap E_2) = h_{c+1} + 1$.
Suppose $c + 2 = d + 1$. Then, $r_c = r_{d-1} = h_d r_d = h_d = h_{c+1}$ and $k_{c+2} = k_{d+1} = m$: cf lemma 2.6.3 and 2.6.5. Then, because T is invertible, it is obvious that $card(R^o \cap E_2) = h_{c+1}$. ■

We can then enunciate the fundamental theorem. That gives us an idea of the quality of the distribution of points E_2 with respect to the rectangles of the type of propositions 2.6.10, 2.6.11 and 2.6.12 : we can compare this result with the test of Gauss. It will be sufficient then that these rectangles are not very large to ensure a good distribution of points of E_2.

Fundamental Theorem 2.6.14 *Let* $(x, y) \in [0, m[^2 \cap \mathbb{N}^2$. *Let T be a invertible linear congruence. Let* c', $c" \in \mathbb{N}$ *such that* $c' \leq d$ *and* $0 < c" < d + 1$. *Let* T', $T" \in \mathbb{N}$ *such that* $T' + c' < d + 1$ *and* $c" - T" > 0$.

Let $\lambda'_i \in \mathbb{N}$, *i=1,2,...,T' and* $\lambda"_j \in \mathbb{N}$, *j=1,2,...,T"* , *be two sequences checking*
$\lambda'_1 < h_{c'+1}$ *and* $\lambda"_1 < h_{c"-1}$,
and for all $i \in \{1, 2, ..., T'\}$ *and for all* $j \in \{1, 2, ..., T"\}$, $\lambda'_i \leq h_{c'+i}$ *and* $\lambda"_j \leq h_{c"-j}$
and if $\lambda'_i = h_{c'+i}$, *then,* $\lambda'_{i-1} = 0$,
and if $\lambda"_j = h_{c"-j}$ *then,* $\lambda"_{j-1} = 0$.

We set $L' = \sum_{i=1}^{T'} \lambda'_i k_{c'+i}$ *and* $L" = \sum_{j=1}^{T"} \lambda"_j r_{c"-j}$.

Let f', $f" \in \mathbb{N}^*$ *such that* $f' = 1$ *if c'=0, f"=1 if c"=d+1,* $f' \leq h_{c'}$ *if* $c' \neq 0$, $f" \leq h_{c"}$ *if* $c" \neq d + 1$.

Let $\overline{R^o}$ *be a quotient rectangle of* $[0, m[^2$ *resulting from a rectangle* R^o *in the form*

$$R^o = [x, x + L'[\times[y, y + f' r_{c'}[\quad or \quad R^o = [x, x + f" r_{c"}[\times[y, y + L"[.$$

Let N_{R^o} *be the integer* $N_{R^o} = card(\overline{R^o} \cap E_2)$ *and* S_{R^o} *be the area of* $\overline{R^o}$.

Then,

$$\left| N_{R^o} - \frac{S_{R^o}}{m} \right| \leq 1 \ .$$

Proof For example, assume that $R^o = [x, x + L'[\times[y, y + f'r_{c'}[$.

If $c' = 0$ or $c' = d$, it is obvious because $r_{c'} = m$ or $k_{c'+1} = m$ (L'=m), and because, T is invertible, we have $N_{R^o} = \frac{S_{R^o}}{m}$.

Then, let us suppose $c' \in \{1, 2, ..., d-1\}$ and $L' \in M$. Then, one can write $card(R^o \cap E_2) = f'Q'$ or $card(R^o \cap E_2) = f'Q' + 1$ with the same notations as in propositions 2.6.10 and 2.6.11.

For example, let us suppose $S_{R^o} < mf'Q'$. Then, all the rectangles $R_X = [x, x + L'[\times[0, f'r_{c'}[$ check $S_{R_X} < mf'Q'$.

Therefore, these rectangles have an empirical density strictly greater than $1/m^2$: the empirical probability is N_{R_X}/m and the empirical density is $\frac{N_{R_X}/m}{S_{R_X}} > \frac{(f'Q'+\delta)/m}{mf'Q'} \geq 1/m^2$ where $\delta = 0$ or 1. Therefore the rectangle R" $= [0, Km[\times[0, f'r_{c'}[$ - where Km is a multiple of L'- has an empirical density stricly larger than $1/m^2$. Therefore, its empirical probability [3] is strictly greater than Kfr_c/m.

Now, because T defines a bijection of $\{0, 1, 2, 3, ..., m-1\} \to \{0, 1, 2, 3, ..., m-1\}$, then $card(\{[0, m[\times[0, f'r_{c'}[\} \cap E_2) = f'r_{c'}$. Then the empirical probability of $[0, Km[\times[0, f'r_{c'}[$ is Kfr_c/m^2. Therefore, it is a contradiction.

Therefore $\frac{S_{R^o}}{m} \geq f'Q'$.

We prove by the same way that $\frac{S_{R^o}}{m} \leq f'Q' + 1$ and all the other cases. ■

Proposition 2.6.15 *Let $\overline{R^o}$ be any quotient rectangle in the form described in propositions 2.6.10 or 2.6.11 or 2.6.12 with $card(\overline{R^o} \cap E_2) = fQ$ or $card(\overline{R^o} \cap E_2) = fQ + \Delta$ where $\Delta = \pm 1$. Then,*

$$fQ \leq \frac{S_{R^o}}{m} \leq fQ + 1 \quad if \quad \Delta = 1 \ ,$$

$$fQ - 1 \leq \frac{S_{R^o}}{m} \leq fQ \quad if \quad \Delta = -1 \ .$$

Proof It is enough to use the proof of theorem 2.6.14. ■

2.6.4 Fibonacci congruences

We give some complementary results to the results of section 2.6.1.

Lemma 2.6.16 *If $T(x) \equiv ax \ mod \ m$ is the congruence of Fibonacci $a \equiv \pm a^{-1}$. Moreover $T^2 \equiv \pm Id$.*

Proof Assume $m < 5$. If m=3, a=2 and the lemma is obvious. If m=2, a=1 and the lemma is obvious.

Assume $m \geq 5$. By definition with the notations 2.1.1, $h_r^a = 1$ if $r < d^a$ and $h_{d^a}^a = 2$. Then, $m = r_0^a = h_1^a r_1^a + r_2^a = h_1^a a + r_2^a = a + r_2^a$ where $r_2^a < a$. Then, $a > m/2$. Then, by lemma 2.1.3, $r_1 = m - a$.

Moreover, by lemma 2.1.3, because $a > m/2$, $h_2^a + 1 = h_1$. Then, $h_1 = 2$.

[3] In fact, it is not a probability but a measure which is an extension of the probability over $[0, m[^2$.

By lemma 2.6.3, because T is invertible, $r_d = 1$.

Moreover, by lemma 2.1.3, $h^a_{n+1} = h_n$ if $n \geq 2$ and $d^a = d + 1$. Then, $h^a_{d^a} = h_d = 2$. Then, we know that $r_{d+1} = 0$, $r_d = 1$, $r_{d-1} = 2$ ($h_d = 2$), $r_{d-2} = 3$, $r_{d-3} = 5$, ...

Moreover, $k_0 = 0$, $k_1 = 1$, $k_2 = h_1 = 2$, $k_3 = 3$, $k_4 = 5$, $k_5 = 8$, ...

Then, $k_n = r_{d-(n-1)}$ if $n \leq d$. Moreover, by lemma 2.6.5, $k_{d+1} = m = r_0 = r_{d-d}$. Then, $k_n = r_{d-(n-1)}$ if $n \leq d + 1$.

Then, $k_d = r_{d-(d-1)} = r_1$.

Now, $k_d a \equiv \pm 1$ by lemma 2.6.4. Then, $k_d a = r_1 a = (m - a)a \equiv \pm 1$. Then, $a^2 \equiv \pm 1$. Because $T(x) \equiv ax$, $T^2(x) \equiv a^2 x \equiv \pm 1$. ■

For example, $r_0 = m = 89$, $a = 55$, $r_1 = 34$, $r_2 = 21$, $r_3 = 13$, $r_4 = 8$, $r_5 = 5$, $r_6 = 3$, $r_7 = 2$, $r_8 = r_d = 1$, $r_9 = r_{d+1} = 0$.

Now, $k_0 = 0$, $k_1 = 1$, $k_2 = h_1 = 2$, $k_3 = 3$, $k_4 = 5$, $k_5 = 8$, $k_6 = 13$, $k_7 = 21$, $k_8 = k_d = 34$, $k_9 = k_{d+1} = 89$.

2.7 Mathematical implications

In this section, we have some implications of the fundamental theorem.

From now on, we assume from now on the following hypothesis.

Assumptions 2.7.1 *We assume from now that T is invertible*

We imposed in rectangles R^o that L is defined in a precise way. We'll see from now on how we return to the general case : our first lemma give the writing of any integer based on the previous criteria.

Lemma 2.7.1 *Let $L \in \{0, 1, ..., m\}$ and $c \in J^*_{d-1} = \{1, 2, ..., d - 1\}$. Then there exists $T \in \mathbb{N}$, $T \leq d + 1 - c$ ($T \leq d + 1 - c \leq d$), and a sequence $\lambda_i \in \mathbb{N}$, i=1,2,....,T, and an integer $\epsilon \in \mathbb{Z}$ such that $\lambda_1 < h_{c+1}$, $\lambda_i \leq h_{c+i}$, and if $\lambda_i = h_{c+i}$, then, $\lambda_{i-1} = 0$ and $-k_c \leq \epsilon < k_{c+1}$ checking*

$$L = \sum_{i=1}^{T} \lambda_i k_{c+i} + \epsilon \ .$$

Proof We use here the notations of section 2.3. It is clear that there exists $T \in \mathbb{N}$ such that $L \in [K_T, K_{T+1}[$.

If $T < 1$ the proof is complete.

If not, there exists $g_T \in \mathbb{N}^*$ such that $L \in [g_T K_T, (g_T + 1)K_T[$ and $L - g_T K_T \in [0, K_T[$.

Then, by reasoning by induction, one can easily write

$$L = \sum_{i=1}^{T} g_i K_i + \epsilon'$$

with $\epsilon' < K_1$.

It is easy to understand that the g_i's checks the conditions of the λ_i's. Indeed, if $g_T = h_{c+T}$, $g_T K_T = K_{T+1} - K_{T-1}$. Then, $L - g_T K_T \in [0, K_{T-1}[$. It is the same for the other g_i. Then, the g_i's checks the conditions of the λ_i's, except maybe $g_1 < H_1$.

If $g_1 < H_1$, we set $\lambda_i = g_i$ and $\epsilon = \epsilon'$.

If $g_1 = H_1$, we set $\epsilon" = K_0 - \epsilon'$. Then, $0 < \epsilon" \leq K_0$, and $L = H_1 K_1 + \sum_{i=2}^{T} g_i K_i - \epsilon" + K_0 = K_2 + \sum_{i=2}^{T} g_i K_i - \epsilon"$. Because $g_1 = H_1$, then, $g_2 \neq H_2$.

Then, **if** $g_3 \neq H_3$, $L = (g_2+1)K_2 + g_3K_3 + \sum_{i=4}^{T} g_iK_i - \epsilon$". QED

If $g_3 = H_3$, then, $g_2 = 0$ and $g_2 + 1 = 1$ and the above decomposition does not check the imposed conditions.

Then, let s be the integer checking $g_{2i+1} = h_{2i+1}$, $g_{2i} = 0$ for i=1,2,....,s, and $g_{2s+3} \neq h_{2s+3}$.

Then, $L = K_2 + \sum_{i=2}^{2s+1} g_iK_i + \sum_{i=2s+2}^{T} g_iK_i - \epsilon$",

and therefore, $L = (g_{2s+2}+1)K_{2s+2} + \sum_{i=2s+3}^{T} g_iK_i - \epsilon$" because $K_2 + H_3K_3 = K_4$ for example.

Then, on check easily that this decomposition of L is in accordance with the hypotheses. ■

We will now proceed to the study of any rectangle, and for that we are reducing to the already studied case by dividing it horizontally.

Notations 2.7.2 *Let x, y, L, L′ ∈ ℕ ∩ [0, m] and let R be the rectangle* $R = [x, x+L[\times[y, y+L'[$.

We denote by r_c *the most big* r_n, $n \in J_{d+1}$ *such that* $r_c \leq L'$ *and by* $k_{c'}$, *the most big* k_n, $n \in J_{d+1}$ *such that* $k_{c'} \leq L$.

Then, we set c'=c+p and we assume that $p \in \mathbb{N}^*$.

Let $L = \sum_{i=1}^{p} \lambda_i k_{c+i} + \epsilon$ *and* $L' = \sum_{j=1}^{p} \mu_j r_{c+j-1} + \epsilon'$ *be the decomposition of L and L' according to lemma 2.7.1 .*

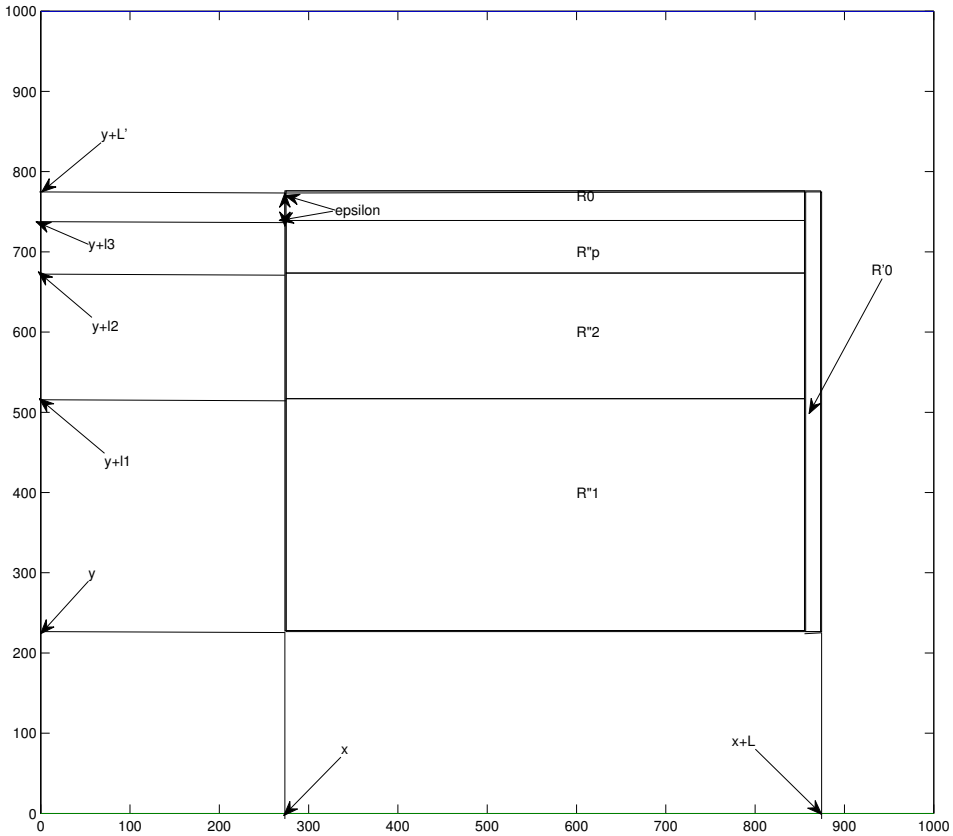

Figure 2.7: $l_1 = \mu_1 r_c$, $l_2 = \mu_1 r_c + \mu_2 r_{c+1}$, $l_3 = \mu_1 r_c + \mu_2 r_{c+1} + \mu_3 r_{c+2}$

In order to simplify the notations, we admit that $[x, x+\ell[$ *denote* $[x, x+\ell[$ *if* $\ell \geq 0$ *and* $[x+\ell, x[$ *if* $\ell < 0$.

Then, we denote by R_j, *(resp* R'_j, $R"_j$*) the rectangles*

$$I \times \Big[y + \sum_{t=1}^{j-1} \mu_t r_{c+t-1} \ , \ y + \sum_{t=1}^{j} \mu_t r_{c+t-1} \Big[\ ,$$

where I denotes the interval $[x, x+L[$, *(resp* $[x, x+L-\epsilon[$, $[x+L-\epsilon, x+L[$*).*

At last, R_0 *and* R'_0 *denote the rectangles* $I \times [y+L'-\epsilon', y+L'[$ *and* $[x+L+\epsilon, x+L[\times[y, y+L'[$ *if* $\epsilon < 0$.

We continue to denote by N_R *and* S_R *respectively, the number of points of* E_2 *included in R and the area of R.*

At last, we set $h^s = sup_i(h_i)$.

We shall study the different horizontal sections of R, i.e. to the study of the R_j's.

Reminder 2.7.3 *We remind that, any rectangle included in a rectangle height* r_c *and width* k_{c+1} *contains 1 or 0 points of* E_2 *: cf corollary 2.6.13.*

Lemma 2.7.4 *For all* $j \in \{1, 2, ..., p\}$, *we have*

$$\Big| N_{R_j} - \frac{S_{R_j}}{m} \Big| \leq \mu_j + 1 \ ,$$

$$\frac{S_{R_j}}{m} \geq \mu_j \Big[\sum_{t=j}^{p} \lambda_t Q_{t+1-j}^{c+j-1} \Big] - 2 \ .$$

Proof Each rectangle R_j, is written in the form

$$[x, x+L[\times \Big[y + \sum_{t=1}^{j-1} \mu_t r_{c+t-1} \ , \ y + \sum_{t=1}^{j} \mu_t r_{c+t-1} \Big[= [x, x+L[\times[y", y" + \mu_j r_{c+j-1}[$$

$$= [x, x+L[\times[y", y" + \mu_j r_{c^j}[\ ,$$

where $c^j = c+j-1$. Then, $L = L^j + \epsilon_j$ where $L^j = \sum_{i=1}^{T_j} \lambda_i k_{c^j+i}$ and $-k_{c^j} \leq \epsilon_j < k_{c^j+1}$ according the writing of L in lemma 2.7.1.

Then, for the rectangle $R_0^j = [x, x+L^j[\times[y", y" + \mu_j r_{c^j}[$ we have $\Big| N_{R_0^j} - \frac{S_{R_0^j}}{m} \Big| \leq 1$ by theorem 2.6.14.

For each rectangle $R_t^j = [x+L^j, x+L^j+\epsilon_j[\times[y" + (t-1)r_{c^j}, y" + tr_{c^j}[$, $t = 1, 2, ...\mu_j$, we have $R_t^j \subset Re_t^j = [x+L^j, x+L^j \pm k_{c^j+1}[\times[y" + (t-1)r_{c^j}, y" + tr_{c^j}[$. Now, for this rectangle Re_t^j, $Q^{c_j} = Q_1^{c_j} = 1$ with the notations of proposition 2.6.15. By reminder 2.7.3 (cf also corollary 2.6.13), $card(\overline{R^o} \cap E_2) = Q^{c_j} = 1$ or $Q^{c_j} - 1 = 0$ with the notations of proposition 2.6.15. Then, $0 \leq \frac{S_{Re_t^j}}{m} \leq 1$ by proposition 2.6.15. Then, $0 \leq \frac{S_{R_t^j}}{m} \leq 1$. Moreover, $N_{R_t^j} = 0$ or 1 by reminder 2.7.3. Then, $\Big| N_{R_t^j} - \frac{S_{R_t^j}}{m} \Big| \leq 1$.

Because $R_j = \cup_{t=0}^{\mu_j} R_t^j$, then,

$$\Big| N_{R_j} - \frac{S_{R_j}}{m} \Big| \leq \sum_{t=0}^{\mu_j} \Big| N_{R_t^j} - \frac{S_{R_t^j}}{m} \Big| \leq \mu_j + 1 \ . \ QED$$

By proposition 2.6.15, $\frac{S_{R_0^j}}{m} \geq fQ - 1 = fQ^{c+j-1} - 1 = \mu_j \Big[\sum_{t=j}^{p} \lambda_t Q_{t+1-j}^{c+j-1} \Big] - 1$ with the notations 2.4.1. Moreover, we should also take into account the surface of $Rs^j = [x + L^j, x + L^j + \epsilon_j[\times[y", y" + \mu_j r_{c^j}[$ which is positive if $\epsilon_j \geq 0$. In this case, the third inequality is proved

If $\epsilon_j < 0$, we must subtract the area of the rectangle Rs^j included in a rectangle $[x_0, x_0 + k_{c^j}[\times[y_0, y_0 + \mu_j r_{c+j-1}[\subset [x_0, x_0 + k_{c+j-1}[\times[y_0, y_0 + r_{c+j-2}[= R^i$ where $\frac{S_{R^i}}{m} \leq 1$ by proposition 2.6.15 and reminder 2.7.3 as we have seen above. ■

Lemma 2.7.5 *We have*

$$\Big| N_{R_0} - \frac{S_{R_0}}{m} \Big| \leq h_{c+p} + 1 \leq h^s + 1 \ .$$

Proof We know that $R_0 = [x, x + L[\times[y + L' - \epsilon', y + L'[$ where $|\epsilon'| < r_{c+p-1}$. Moreover, $L < k_{c+p+1} < (h_{c+p} + 1)k_{c+p}$. Then,

$$R_0 \subset [x, x+(h_{c+p}+1)k_{c+p}[\times[y_1, y_1+r_{c+p-1}[= \cup_{t=1}^{h_{c+p}+1}[x+(t-1)k_{c+p}, x+tk_{c+p}[\times[y_1, y_1+r_{c+p-1}[\ .$$

Then, $RS_t = [x + (t-1)k_{c+p}, x + tk_{c+p}[\times[y_1, y_1 + r_{c+p-1}[$ has a area less than m : $\frac{S_{RS_t}}{m} \leq 1$ by proposition 2.6.15 and reminder 2.7.3 as we have seen above in the proof of lemma 2.7.4.

Moreover, by reminder 2.7.3, $N_{RS_t} = 0$ or 1. Then, $\Big| N_{R_0} - \frac{S_{R_0}}{m} \Big| \leq h_{c+p} + 1$. ■

Lemma 2.7.6 *We set $p' = card\{i|\lambda_i \neq 0\}$, $p" = card\{j|\mu_j \neq 0\}$ and $p^o = inf(p', p")$. Then,*

$$\Big| N_R - \frac{S_R}{m} \Big| \leq \sum_{j=1}^{p} \mu_j + h_{c+p} + p + 1 \leq \sum_{i=1}^{d} h_i + 2 \leq dh^s + 2 \ ,$$

$$\Big| N_R - \frac{S_R}{m} \Big| \leq p^o(h^s + 1) + h^s + 1 \leq (d+1)(h^s + 1) \ .$$

Proof It is enough to remark that $\mu_j \leq h_{c+j-1}$ and that if $\mu_j = h_{c+j-1}$, $\mu_{j+1} = 0$. ■

Lemma 2.7.7 *We suppose that $m \geq 377$ and that T is a congruence of Fibonnacci : $h_i = 1$ if $1 < i < d$ and $h_d = h_1 = 2$ (cf proof of lemma 2.6.16). Then,*

$$\Big| N_R - \frac{S_R}{m} \Big| \leq 2(d-1).$$

Proof It is enough to use the proof of lemma 2.7.4. Then,

$$\Big| N_R - \frac{S_R}{m} \Big| \leq \sum_{j=0}^{p} \Big| N_{R_j} - \frac{S_{R_j}}{m} \Big| \ ,$$

where

$$\Big| N_{R_0} - \frac{S_{R_0}}{m} \Big| \leq h_{c+p} + 1 \ ,$$

and for all rectangle R_j, $j \geq 1$,

$$\Big| N_{R_j} - \frac{S_{R_j}}{m} \Big| \leq \mu_j + 1 \leq h_{c+j-1} + 1 \ .$$

Now, in lemma 2.7.1, $L = \sum_{i=1}^{p} \lambda_i k_{c+i} + \epsilon$ where $c \geq 1$. Then, $\lambda_1 < h_{c+1}$. Because $c \geq 1$, $h_{c+1} \leq 1$. Then, $\lambda_1 < 1$. Then, $\lambda_1 = 0$.

Moreover, $\lambda_{i-1} = 0$ if $\lambda_i = 1$ for $h_i \leq 1$, i.e. $i \leq d-1$.

At last, $\lambda_i \leq 2$ if c+i=d. In this case, if $\lambda_i = 2$, $\lambda_{i-1} = 0$.

At last, $c + p \leq d$ because lemma 2.6.5. Then, $p \leq d-1$.

Then, $\sum_{j=1}^{p}[\lambda_j + 1] + h_{c+p} + 1 \leq \sum_{j=1}^{p}[\lambda_j + 1] + 3 \leq \sum_{j=1}^{d-1}[\lambda_j + 1] + 3 = O(2d/3)$. Then, a fortiori, it is easy to understand that $\sum_{j=1}^{d}[\lambda_j + 1] + 3 \leq 2(d-1)$ if $m \geq 377 = fi_{14}$ (i.e. $d \geq 13$).

Of course, the same result holds for the μ_j : if $m \geq 377$, $\sum_{j=1}^{d}[\mu_j + 1] + 3 \leq 2(d-1)$. ■

We recall that by proposition 1.3.3, if T is the congruence of Fibonsacci, then, $r_0^a = m$ and $r_i^a = fi_{d-i+2}$. Moreover, T is invertible.

Proposition 2.7.8 *We have*

$$d < \frac{2log(m) - 2log(2)}{log(2)} \ .$$

Moreover, for all rectangle R checking the assumptions of notations 2.7.2,

$$\left| N_R - \frac{S_R}{m} \right| \leq (h^s + 1)\frac{4log(m) - log(2)}{log(2)} \ .$$

Proof Let $\lfloor b \rfloor$ is the integer part of b. We know that $r_1 \leq m/2$. By the same way $r_1 \geq r_2 + r_3$. Therefore, $r_3 < r_1/2 < m/4$.

By the same way $r_3 \geq r_4 + r_5$. Therefore, $r_5 < r_3/2 < m/8$. And so on.....

Then, $r_{2n+1} < m/2^{n+1}$.

Then, if 2n+1=d, $2 \leq r_d < m/2^{\lfloor \frac{d}{2} \rfloor + 1}$.

Then, $log(2) < log(m) - [\lfloor \frac{d}{2} \rfloor + 1]log(2)$.

Then, $n = \lfloor \frac{d}{2} \rfloor < \frac{log(m) - 2log(2)}{log(2)}$.

Then, $2n < \frac{2log(m) - 4log(2)}{log(2)}$.

Then, $d = 2n + 1 < \frac{2log(m) - 3log(2)}{log(2)}$.

Now, $r_{2n+2} < r_{2n+1} < m/2^{n+1}$.

Then, if 2n+2=d, $2 \leq r_d < m/2^{\lfloor \frac{d}{2} \rfloor}$.

Then, $log(2) < log(m) - \lfloor \frac{d}{2} \rfloor log(2)$.

Then, $\lfloor \frac{d}{2} \rfloor < \frac{log(m) - log(2)}{log(2)}$.

Then, $d < \frac{2log(m) - 2log(2)}{log(2)}$.

Then, $d + 1 < \frac{4log(m) - log(2)}{log(2)}$. Then, it is enough to use lemma 2.7.7. ■

Now, we give sufficient conditions in order that the hypothesis contained in the notation 2.7.2 is checked.

Lemma 2.7.9 *We suppose that T is the Fibonacci congruence. Suppose that* $card(R \cap E_2) \geq 3$. *Then, with the notations 2.7.2,* $p \in \mathbb{N}^*$.

Proof By the notations 2.7.2, c' is the geatest n such that $k_n \leq L$. Moreover c is the smallest n such that $r_n \leq L$. The assumption contained in notations 2.7.2 is c'=c+p where $p \in \mathbb{N}^*$, i.e. there exists $[x, x + k_{c+1}[\times[y, y + r_c[\subset R$.

If this is not the case, we can write any rectangle $[x_0, x_0 + k_{c'}[\times[y_0, y_0 + r_c[\subset R$ in the form $[x_0, x_0 + k_{c'}[\times[y_0, y_0 + r_c[= [x_0, x_0 + k_{c'}[\times[y_0, y_0 + r_{c'+q}[$ where $q \in \mathbb{N}$, i.e. c=c'+q. Then, $[x_0, x_0 + k_{c'}[\times[y_0, y_0 + r_{c'+q}[\subset [x_0, x_0 + k_{c'}[\times[y_0, y_0 + r_{c'}[$.

Now suppose $q \in \mathbb{N}$ and $R \subset [x_0, x_0 + k_{c'+1}[\times[y_0, y_0 + r_{c'+q-1}[\subset [x_0, x_0 + k_{c'+1}[\times[y_0, y_0 + r_{c'-1}[$. Then, the rectangle $[x_0, x_0 + k_{c'+1}[\times[y_0, y_0 + r_c[\subset [x_0, x_0 + k_{c'+1}[\times[y_0, y_0 + r_{c'}[$ contains at most

one point E_2 by corollary 2.6.13. By the same way, if $h_{c'} \leq 1$ (i.e. $r_{c-1} = r_c + r_{c+1}$), $[x_0, x_0 + k_{c'+1}[\times[y_0 + r_{c'}, y_0 + r_{c'-1}[\subset [x_0, x_0 + k_{c'+1}[\times[y_0 + r_{c'}, y_0 + 2r_{c'}[$ contains at most one point E_2 by corollary 2.6.13. Then, if si $h_{c'} \leq 1$, there exists two rectangles $Rec_1 = [x_1, x_1 + k_{c'+1}[\times[y_1, y_1 + r_{c'}[$ and $Rec_2 = [x_1, x_1 + k_{c'+1}[\times[y_1 + r_{c'}, y_1 + 2r_{c'}[$ such that $R \subset [x_1, x_1 + k_{c'+1}[\times[y_1, y_1 + r_{c'-1}[\subset Rec_1 \cup Rec_2 = [x_1, x_1 + k_{c'+1}[\times[y_1, y_1 + 2r_{c'}[$ which contains at most one point E_2.

Now, because T is the Fibonnacci congruence $h_{c'} = 2 \geq 1$ if $c' = d$ or if c'=1. If not, $h_{c'} = 1$.

If c'=d, $k_{c'+1} = m$ (cf Lemma 2.6.5) and $r_{c'} = 1$, $r_{c'-1} = 2$. Then, $[x_0, x_0 + k_{c'+1}[\times[y_0, y_0 + r_c[\subset [x_0, x_0 + k_{c'+1}[\times[y_0, y_0 + r_{c'-1}[= [x_0, x_0 + m[\times[y_0, y_0 + 2[$ which contains at most two points of E_2 because T is invertible ($r_d = 1$ and cf Lemma 2.6.3 or proposition 1.3.3).

If c'=1, $k_{c'+1} = k_2 = 2$ and $r_{c'} = inf(a, m-a)$, $r_{c'-1} = m$. Then, $[x_0, x_0 + k_{c'+1}[\times[y_0, y_0 + r_c[\subset [x_0, x_0 + k_{c'+1}[\times[y_0, y_0 + r_{c'-1}[= [x_0, x_0 + 2[\times[y_0, y_0 + m[$ which contains at most two points of E_2 because T is invertible ($r_d = 1$).

Therefore, the rectangle $[x_0, x_0 + k_{c'+1}[\times[y_0, y_0 + r_{c-1}[$ contains at most two points of E_2. Therefore, if the assumption contained in notations 2.7.2 does not hold, the rectangle $R = [x, x + L[\times[y, y + L'[$ contains at most two point E_2.
Then, any rectangle $R = [x, x + L[\times[y, y + L'[$ which contains three points of E_2 checks $p \in \mathbb{N}^*$. ■

We prove in the same way the following property.

Lemma 2.7.10 *We suppose that $card(R \cap E_2) > h^s + 1$. Then, with the notations 2.7.2, $p \in \mathbb{N}^*$.*

Proof We takes the same beginning of the proof as in lemma 2.7.9 : we suppose $p \notin \mathbb{N}^*$. Then, each rectangle $[x_0, x_0 + k_{c'+1}[\times[y_0 + (t-1)r_c, y_0 + tr_c[$ contains at most one point of E_2 . Then, the rectangle $[x_0, x_0 + k_{c'+1}[\times[y_0, y_0 + r_{c'-1}[\subset [x_0, x_0 + k_{c'+1}[\times[y_0, y_0 + (h_{c'} + 1)r_{c'}[$ contains at most $h_{c'} + 1$ points of E_2.

We deduce the result. ■

Lemma 2.7.11 *We suppose that T is the Fibonacci congruence. Let R such that $S_R/m \geq 3$. Then, with the notations 2.7.2, $p \in \mathbb{N}^*$.*

Proof One can write $R = [x, x + L[\times[y, y + L'[$. Then, one can assume $k_{c'} \leq L < k_{c'+1}$ and $r_c \leq L' < r_{c-1}$. Then, $c' \geq c + 1$.

If not by corollary 2.6.13, $R_0 = [x, x + k_{c+1}[\times[y, y + r_c[$ contains at most 1 point of E_2. As a matter of fact, with the notations of corollary 2.6.13 and proposition 2.6.15, Q=1 and $\delta = -1$ by the proof of corollary 2.6.13 . Then, by proposition 2.6.15, $S_{R_0}/m \leq 1$. Moreover $R \subset R_0$. Now, if $h_c = 1$, $R_1 = [x, x + k_{c+1}[\times[y + r_c, y + r_{c-1}[\subset R_2 = [x, x + k_{c+1}[\times[y + r_c, y + 2r_c[$: we deduce as previously $S_{R_2}/m \leq 1$ (Q=1, $\delta = -1$). Then $S_{R_0 \cup R_2}/m \leq 2$. Then $S_{R_0 \cup R_1}/m \leq 2$. If $h_c = 2$ and $c = d$, $[y + r_c, y + r_{c-1}[= [y + r_d, y + r_{d-1}[= [y + r_d, y + 2r_d[$ because $r_{d-1} = 2r_d$. Then, as previously by proposition 2.6.15 and the proof of corollary 2.6.13 , $S_{R_1}/m \leq 1$. Then $S_{R_0 \cup R_1}/m \leq 2$.

Moreover, $R = [x, x + L[\times[y, y + L'[\subset [x, x + k_{c+1}[\times[y, y + r_{c-1}[= R_0 \cup R_1$. Then, $S_R/m \leq 2$. It is impossible.

If $h_c = 2$, $c = 1$ and $c' \leq c = 1$. Then, $k_{c'} \leq L < k_{c'+1} \leq k_2 = 2$. Then, $L \leq 1$. Then, $S_R/m \leq 1$. It is impossible.

Then, $c' \geq c + 1$. Then, with the notations 2.7.2, $p \in \mathbb{N}^*$. ■

We deduce the following lemma .

Lemma 2.7.12 *We suppose that T is the Fibonacci Congruence. Let R such that, with the notations 2.7.2, $p \notin \mathbb{N}^*$. Then, if $m \geq 5$,*

$$\left|N_R - \frac{S_R}{m}\right| \leq 3 \leq 4\frac{log(m) - log(2)}{log(2)} \ .$$

Proof By lemma 2.7.9 and 2.7.11, $0 \leq N_R < 3$ and $0 \leq S_R/m < 3$. Then, $\left|N_R - \frac{S_R}{m}\right| \leq 3$.

Then, $3 < 5.2877 \approx 4\frac{log(5)-log(2)}{log(2)} \leq 4\frac{log(m)-log(2)}{log(2)}$. ■

Now we have another way to prove the lemma 2.7.10

Lemma 2.7.13 *Let R such that, with the notations 2.7.2, $p \notin \mathbb{N}^*$. Then, $\frac{S_R}{m} \leq h_c + 1$ and $N_R \leq h_c + 1$*

Proof With the notations 2.7.2, $L < k_{c'+1}$ and $L' < r_{c-1}$ where $c' \leq c$. Then, $L < k_{c+1}$.

By the proof of corollary 2.6.13, if $R' = [x, x + k_{c+1}[\times[y, y + r_{c-1}[$, $N_{R'} = h_{(c-1)+1}$ or $N_{R'} = h_{(c-1)+1} + 1$ with $\delta = 1$ with the notations of proposition 2.6.15.

Then, $h_c \leq \frac{S_{R'}}{m} \leq h_c + 1$ by proposition 2.6.15. Now $R \subset R'$. We deduce the result. ■

We deduce the following properties.

Corollary 2.7.14 *Let R such that, with the notations 2.7.2, $p \notin \mathbb{N}^*$. Then,*

$$\left|N_R - \frac{S_R}{m}\right| \leq h_c + 1 \ .$$

Corollary 2.7.15 *Let $R = [x, x + L[\times[y, y + L[$ such that x, y, L, $L' \notin \{0, 1, ..., m\}$. Then,*

$$\left|N_R - \frac{S_R}{m}\right| \leq \sum_{i=1}^{d} h_i + 2 \leq dh^s + 2 \ .$$

Proposition 2.7.16 *We suppose that T is the Fibonacci congruence with $m \geq 377$. Soit $I = [C, C'[$, C, $C' \in \mathbb{N}$, and N(I)=C'-C. Let k^n be the permutation of $\{C, C + 1, ..., C' - 1\}$ such that $\overline{T}(k^1) < \overline{T}(k^2) < ..... < \overline{T}(k^{C'-C})$. Then, for all $r \in \{1, 2, ..., N(I) - 1\}$,*

$$\left|\frac{\overline{T}(k^r)}{m} - \frac{r}{N(I)}\right| \leq \frac{\phi'(m)}{N(I)},$$

ou $\phi'(m) = \frac{4Log(m)-2Log(2)}{log(2)}$.

Proof Let $r \in \{1, 2, ..., N(I) - 1\}$. Let $D = 4\frac{log(m)-Log(2)}{log(2)}$.

Let $L_1 = \lfloor\frac{(r-D-1).m}{N(I)}\rfloor = \frac{(r-D-1).m}{N(I)} - e$ **where** $0 \leq e < 1$**.** Let $R_1 = I \times [L_1, m[$. Then, $\frac{S_{R_1}}{m} = \frac{(m-L_1)N(I)}{m} = N(I) - \frac{(r-D-1).m}{N(I)}\frac{N(I)}{m} + \frac{eN(I)}{m} = N(I) - r + D + 1 + e'$ where $e' = \frac{eN(I)}{m}$.

If $L_1 \geq 0$, then, $[L_1, m[$ contains $t_1 = N_{R_1}$ points $\overline{T}(k^s)$ of $\overline{T}(I)$: $\overline{T}(k^{C'-C-t_1+1})$,....., $\overline{T}(k^{C'-C-1}), \overline{T}(k^{C'-C})$ where $t_1 = N_{R_1} = card(R_1 \cap E_2)$.

Now, $D = 4\frac{log(m)-Log(2)}{log(2)} \geq 2.3399$ because $m \geq 3$. Then, $\frac{S_{R_1}}{m} \geq 3$ because $N(I) - r + D + 1 + e' \geq D + 1 \geq 3$. Then, by lemma 2.7.11, with the notations 2.7.2, $p \in \mathbb{N}^*$. Now, by proposition

2.7.8, we know that, for all rectangle R checking $p \in \mathbb{N}^*$, $\left|N_R - \frac{S_R}{m}\right| \leq D$.

Then, $\left|N_{R_1} - \frac{S_{R_1}}{m}\right| \leq D$, i.e. $-D \leq t_1 - [N(I) - r + D + 1 + e'] \leq D$,
i.e. $N(I) - r < -D + N(I) - r + D + 1 + e' \leq t_1 \leq N(I) - r + D + 1 + e' + D$,
i.e. $C' - C - t_1 + 1 = N(I) - t_1 + 1 < r + 1$, i.e. $C' - C - t_1 + 1 \leq r$. Then, $\overline{T}(k^{C'-C-t_1+1}) \leq \overline{T}(k^{t_r})$.
Then, $L_1 \leq \overline{T}(k^{C'-C-t_1+1}) \leq \overline{T}(k^{t_r})$.

Si $L_1 < 0$, then, obviously $L_1 \leq \overline{T}(k^{t_r})$.

Let $L_2 = \lfloor \frac{(r+D+1).m}{N(I)} \rfloor = \frac{(r+D+1).m}{N(I)} - f$ **where** $0 \leq f < 1$. Let $R_2 = I \times [0, L_2[$.

Suppose $L_2 \leq m$. Then, $\frac{S_{R_2}}{m} = \frac{L_2 N(I)}{m} = \frac{(r+D+1).m}{N(I)} \frac{N(I)}{m} - \frac{fN(I)}{m} = r + D + 1 - f'$ where $f' = \frac{fN(I)}{m}$. Now, $D = 4\frac{log(m) - Log(2)}{log(2)} \geq 2.3399$. Then, $\frac{S_{R_2}}{m} \geq 3$. Then, by lemma 2.7.11 we know that $p \in \mathbb{N}^*$. Then, by proposition 2.7.8, we know that, for all rectangle R checking $p \in \mathbb{N}^*$, $\left|N_R - \frac{S_R}{m}\right| \leq D$.

Now, $[0, L_2[$ contains $t_2 = N_{R_2}$ points $\overline{T}(k^s)$ of $\overline{T}(I) : \overline{T}(k^1), \overline{T}(k^2), \overline{T}(k^3), ..., \overline{T}(k^{t_2})$ where $\left|N_{R_2} - \frac{S_{R_2}}{m}\right| \leq D$ i.e. $\left|N_{R_2} - [r + D + 1 - f']\right| \leq D$.
Then, $r < r + 1 - f' \leq r + D + 1 - f' - D \leq N_{R_2} = t_2 \leq r + D + 1 - f' + D$.
Then, $\overline{T}(k^{t_r}) < \overline{T}(k^{t_2})$. Then, $\overline{T}(k^{t_r}) \leq L_2$.

If $L_2 > m$, obviously $\overline{T}(k^{t_r}) \leq L_2$.

Therefore, $L_1 \leq \overline{T}(k^{t_r}) \leq L_2$**. Then,**

$$\frac{(r - D - 1).m}{N(I)} - e \leq \overline{T}(k^{t_r}) \leq \frac{(r + D + 1).m}{N(I)} - f \ .$$

Therefore,

$$\frac{r}{N(I)} - \frac{D+1}{N(I)} - \frac{e}{m} \leq \frac{\overline{T}(k^{t_r})}{m} \leq \frac{r}{N(I)} + \frac{D+1}{N(I)} - \frac{f}{m} \ .$$

Therefore,

$$-\frac{D+2}{N(I)} \leq \frac{\overline{T}(k^{t_r})}{m} - \frac{r}{N(I)} < \frac{D+1}{N(I)} \ .$$

Therefore,

$$|\frac{\overline{T}(k^r)}{m} - \frac{r}{N(I)}| \leq \frac{D+2}{N(I)} \ .$$

Now, $D = 4\frac{Log(m) - Log(2)}{log(2)}$. Therefore,

$$|\frac{\overline{T}(k^r)}{m} - \frac{r}{N(I)}| \leq \frac{4\frac{Log(m) - Log(2)}{log(2)} + 2}{N(I)} = \frac{\frac{4Log(m) - 2Log(2)}{log(2)}}{N(I)} = \frac{4Log(m) - 2Log(2)}{log(2)N(I)} \ . \blacksquare$$

Remark 2.7.17 *There are ways in order to improve these inequalities in the previous proofs. For example, to use all the inequalities* $\left|N_{R_t'^j} - \frac{S_{R_t'^j}}{m}\right| \leq 1$ *seems too rough and can probably be improve. Moreover, if we use simulations, we find that* $|\frac{T(k^r)}{m} - \frac{r}{N(I)}| \leq \frac{\phi'(m)}{N(I)}$ *where* $\phi(m) = O\big(Log(Log(m))\big)$ *: cf [15] and [16].*

Chapter 3

Study of the Conjecture

3.1 First inequality of the conjecture

The first inequality of the conjecture give a lower bound to D_m^2 :

$$Max_{i=1,...,d^a}(h_i^a) \leq 4Sup_R\big(\big|N_R - \frac{S_R}{m}\big|\big) \ .$$

In fact this first inequality can be proved. In order to do it we recall the following theorem (cf [15]).

Theorem 3.1.1 *Let $(x_0, y_0) \in E_2$. Let $n \in \{1, 2, ..., d^a + 1\}$.*
If n is even, let $R^0 = [x_0, x_0 + k_n^a] \otimes [y_0, y_0 + r_{n-2}^a[\subset [0, m[^2$. Then,
$E_2 \cap R^0 = \big\{(x_0 + k_{n-1}^a \ell \ , \ y_0 + r_{n-1}^a \ell) \big| \ell = 0, 1, 2, ..., h_{n-1}^a\big\}$.
Moreover the points $(x_0 + k_{n-1}^a \ell \ , \ y_0 + r_{n-1}^a \ell)$ are lined up modulo m .
If n is odd, let $R^0 = [x_0, x_0 + k_n^a] \otimes [y_0 - r_{n-2}^a, y_0[\subset [0, m[^2$. Then,
$E_2 \cap R^0 = \big\{(x_0 + k_{n-1}^a \ell \ , \ y_0 - r_{n-1}^a \ell) \big| \ell = 0, 1, 2, ..., h_{n-1}^a\big\}$.
Moreover, the points $(x_0 + k_{n-1}^a \ell \ , \ y_0 - r_{n-1}^a \ell)$ are lined up modulo m.

Then, one can prove the following theorem.

Lemma 3.1.2 *We keep the notations of theorem 3.1.1 . Then, there exists a rectangle $Rv \subset R^0$ such that $S_{Rv} \geq \frac{k_n^a r_{n-2}^a}{4}$ and $Rv \cap E_2 = \emptyset$.*

Proof Suppose that n is even. We set $x_1 = x_0 + k_n^a$ and $y_1 = y_0 + r_{n-2}^a$.
Then, $x' = x_0 + k_{n-1}^a h_{n-1}^a = x_0 + k_n^a - k_{n-2}^a = x_1 - k_{n-2}^a$. In this point $y' = \overline{T}(x') = y_0 + r_{n-1}^a h_{n-1}^a = y_0 + r_{n-2}^a - r_n^a = y_1 - r_n^a$.
Therefore, one of the rectangles Rv_1 or Rv_2 does not contain points of E_2 where
$Rv_1 =]x_0 + k_n^a/2, x_0 + k_n^a[\times]\overline{T}(x_0), \overline{T}(x_0) + r_{n-2}^a/2[$,
$Rv_2 =]x_0, x_0 + k_n^a/2[\times]\overline{T}(x_0) + r_{n-2}^a/2, \overline{T}(x_0) + r_{n-2}^a[$.

If n is odd, one uses the same way. ■

Now one can prove the first part of the conjecture.

Lemma 3.1.3 *We have*

$$\frac{Max_{i=1,...,d^a}(h_i^a)}{4} \leq Sup_R\Big(\Big|N_R - \frac{S_R}{m}\Big|\Big) \ .$$

Proof By lemma 3.1.2 , $Rv \cap E_2 = \emptyset$. Then, $N_{Rv} = 0$.
Moreover, $N_{R^0} = h_{n-1}^a$ or $N_{R^0} = h_{n-1}^a + 1$ by corollary 2.6.13, i.e., by proposition 2.6.15, $h_{n-1}^a \leq \frac{S_{R^0}}{m} \leq h_{n-1}^a + 1$. Then, $h_{n-1}^a/4 \leq \frac{S_{Rv}}{m}$.

Then, $\left|N_{Rv} - \frac{S_{Rv}}{m}\right| = \frac{S_{Rv}}{m} \geq h^a_{n-1}/4$.

Now, this result holds for n-2=0 as far as $n = d^a + 1$. Then it holds for h^a_{n-1} such that $n - 1 = 1, 2, ..., d^a$. ■

3.2 Secund inequality of the conjecture : comparison with $T([c, c'[)$

In order to have a better increase of D^2_m we are going to compare to results which we had obtained on the distribution of the points of $T([c, c'[)$ in [16].

Notations 3.2.1 *We suppose that T is the Fibonacci congruence. Let $I = [c, c'[$, $c, c' \in \{0, 1, ..., m-1\}$ and let N(I)=c'-c. Let g^n be the permutation of $\{c, c+1, ..., c'-c\}$ such that $\overline{T}(g^1) < \overline{T}(g^2) < \overline{T}(g^3) < ..... < \overline{T}(g^{c'-c})$.*

This result is equivalent to know the distribution of the points of $T^{-1}([c, c'[)$ because, $T^2 = \pm Id$, $T^{-1} = \pm T$ (cf lemma 2.6.16).

Now, in [15] and [16], we have proved that

$$\left|\frac{\overline{T}(g^r)}{m} - \frac{r}{N(I)}\right| \leq \frac{\varphi(m)}{N(I)} ,$$

where $\varphi(m) << Log(m)$: as a matter of fact, it seems that $\varphi(m)$ is the order of Log(Log(m)). Moreover,

$$Max_{r=0,1,....,N(I)-1}\left(\left|N(I)T^{-1}(g^r)/m - r\right|\right)$$

seems maximum when I is large enough : $c' - c = O(m/2)$.

We thus had an increase of $\left|\frac{\overline{T}(g^r)}{m} - \frac{r}{N(I)}\right|$ sharper than the one that we had obtained in proposition 2.7.16. That was obtained thanks to the increase of $\left|N_R - \frac{S_R}{m}\right|$ of lemma 2.7.6. As a matter of fact, we shall see that we have the inverse implication: the increase of $\left|\frac{\overline{T}(g^r)}{m} - \frac{r}{N(I)}\right|$ can give us informations about the increase of $\left|N_R - \frac{S_R}{m}\right|$.

Lemma 3.2.2 *We have*

$$\left|\frac{\overline{T}(g^{r_1-1})}{m} - \frac{\overline{T}(g^{r_1})}{m}\right| \leq \frac{3m}{N(I)} .$$

Proof Suppose $r_c \leq N(I) < r_{c-1}$.

The points T(I) are the points with abscissa $x_1 \leq x \leq x_0 + L$. Therefore, they are the points $(x, \overline{T}(x))$, $x_1 \leq x \leq x_0 + L$, of the rectangle $I \times [0, m[$.

Now, in order to study the points of $I \times [0, m[$, one can also study the points of $[0, m[\times I$ because $T = \pm T^{-1}$.

The points $(x, \overline{ax + b})$ such that $y \leq \overline{ax + b} < y + L$ are the points $x = X + x_0$ such that $y \leq \overline{a(X + x_0) + b} < y + L$. Therefore, if $ax_0 + b = y$, they are the points $0 \leq x = X + x_0 < m$ such that $y \leq \overline{aX} + y < y + L$.

If $\overline{aX} + y < m$, they are the points $0 \leq x = X + x_0 < m$ such that $y \leq \overline{aX} + y < y + L$, i.e. the points such that $0 \leq \overline{ax} < L$.

Si $\overline{aX} + y > m$, they are the points $0 \leq x = X + x_0 < m$ such that $y \leq \overline{aX} + y - m < y + L$, i.e. the points such that $0 \leq \overline{ax} - m < L$. Now, it is impossible.

Therefore, the points $(x, \overline{ax+b})$ such that $y \leq \overline{ax+b} < y+L$ are the points $0 \leq x = X + x_0 < m$ such that $0 \leq \overline{aX} < L$.

Therefore, if $L = r_c$, the points $(x, \overline{ax+b})$ such that $y \leq \overline{ax+b} < y+L$ are the points of M for intervals $X \in [-x_0, 0[$ and $X \in [0, m - x_0[$.

By corolary 2.2.6, if $L = r_c$, these successive points which we shall denote ℓ_n check $\ell_{n+1} - \ell_n = k_{c+1} + k_c$ or $\ell_{n+1} - \ell_n = k_{c+1}$

By corollary 2.2.6, if $L = r_{c-1}$, these successive points ℓ_n check for n=d+1, $\ell_{n+1} - \ell_n = k_{c-1} + k_c$ or $\ell_{n+1} - \ell_n = k_{c-1}$.

Finally (because $k_{c-1} + k_c = k_{c+1}$ $(h_i = 1)$), if $r_c < L < r_{c-1}$, the successive points ℓ_n check $\ell_{n+1} - \ell_n = k_{c-1} + k_c$ or $\ell_{n+1} - \ell_n = k_{c-1}$ or $\ell_{n+1} - \ell_n = k_{c+1}$ or $\ell_{n+1} - \ell_n = k_{c+1} + k_c \leq k_{c+2}$. Therefore, $\left|\overline{T}(g^{r_1-1}) - \overline{T}(g^{r_1})\right| \leq k_{c+2}$.

Therefore, it is necessary that N(I) check $N(I)k_{c-1} \leq m \leq N(I)k_{c+2}$. Moreover, $k_{c+2} \leq 3k_{c-1}$. Then, $k_{c-1} \leq \frac{m}{N(I)} \leq k_{c+2}$. Therefore, $\frac{k_{c+2}}{3} \leq k_{c-1} \leq \frac{m}{N(I)} \leq k_{c+2}$.

Therefore, $\left|\overline{T}(g^{r_1-1}) - \overline{T}(g^{r_1})\right| \leq k_{c+2} \leq \frac{3m}{N(I)}$. ■

Let us remark that we saw in the proof of this lemma how the points of T(I) are distributed by using for example the proposition 2.3.9 in the case where $L = r_c$ or $L = r_{c-1}$. We can thus have a more precise idea of the distribution of these points and we shall can maybe improve the result of the proposition 2.7.16.

Now, one can prove the following proposition.

Lemma 3.2.3 *Let $R = I \times [y, y+L'[\subset [0, m[^2$. Then, under the previous assumptions, we have $\left|N_R - \frac{S_R}{m}\right| \leq 9 + 2\varphi(m)$.*

Proof Let r_1 and r_2 such that $\overline{T}(g^{r_1-1}) < y \leq \overline{T}(g^{r_1})$ and $\overline{T}(g^{r_2}) < y + L' \leq \overline{T}(g^{r_2+1})$.

Then, $N_R = r_2 - r_1 + 1$ and $S_R = (c' - c)L'$.

Now, there exists r'_1 and r'_2 such that $m\frac{r'_1-1}{N(I)} < y \leq m\frac{r'_1}{N(I)}$ and $m\frac{r'_2}{N(I)} < y + L' \leq m\frac{r'_2+1}{N(I)}$.

Then, $m\frac{r'_2-r'_1}{N(I)} \leq L' \leq m\frac{r'_2-r'_1+2}{N(I)}$.

Then, $L' = m\frac{r'_2-r'_1+2|Ob(1)|}{N(I)}$ where Ob(a) is the classical "O" with $|Ob(a)| \leq a$.

Then, $r'_2 - r'_1 = \frac{N(I)L'}{m} - 2|Ob(1)|$.

Now, $\overline{T}(g^{r_1-1})/m = \frac{r_1}{N(I)} + \frac{Ob(1)\varphi(m)}{N(I)}$.

Moreover, by lemma 3.2.2, $y/m - \overline{T}(g^{r_1-1})/m \leq \frac{3}{N(I)}$. And, $\frac{r'_1}{N(I)} - y/m \leq \frac{1}{N(I)}$. Then, $\left|\frac{r'_1}{N(I)} - \overline{T}(g^{r_1-1})/m\right| \leq \frac{4}{N(I)}$.

Then, $\left|\frac{r_1}{N(I)} - \frac{r'_1}{N(I)}\right| \leq \frac{4}{N(I)} + \frac{\varphi(m)}{N(I)}$.

By the same way, $\left|\frac{r_2}{N(I)} - \frac{r'_2}{N(I)}\right| \leq \frac{4}{N(I)} + \frac{\varphi(m)}{N(I)}$.

Then $\left|\frac{r_2-r_1}{N(I)} - \frac{r'_2-r'_1}{N(I)}\right| \leq \frac{8}{N(I)} + \frac{2\varphi(m)}{N(I)}$.

Then $\left|(r_2 - r_1) - (r'_2 - r'_1)\right| = \left|(N_R - 1) - \left[\frac{N(I)L'}{m} - 2|Ob(1)|\right]\right| \leq 8 + 2\varphi(m)$.

Then $\left|N_R - \frac{N(I)L'}{m}\right| \leq 9 + 2\varphi(m)$.

Then $\left|N_R - \frac{S_R}{m}\right| \leq 9 + 2\varphi(m)$. ■

The proof of this lemma shows that the increase of $\left|N_R - \frac{S_R}{m}\right|$ et $\varphi(m)$ are connected. That means that, if $\varphi(m) = O\big(log[log(m)]\big)$, it will be probably the same for $\left|N_R - \frac{S_R}{m}\right|$. It is thus logical to think that $D_m^2 = O\big(\varphi(m)\big)$. It allows to have thus a more precise idea of D_m^2.

3.3 Secund inequality of the conjecture : numerical study

In order to understand how the points in rectangles R are distributed, we made simulations, for example, for a=3243, m=12493, $h_i = 3, 1, 5, 1, 3, 2, 1, 4, 1, 1, 3$, we have figure 3.1.

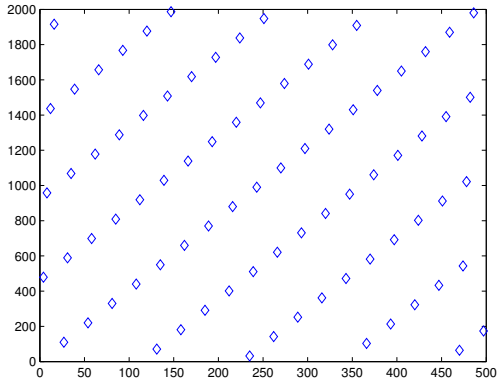

Figure 3.1: a=3243, m=12493, $h_i = 3, 1, 5, 1, 3, 2, 1, 4, 1, 1, 3$.

We understand well on this figure that the distribution of the points of E_2 is made well. It will be thus difficult to find rectangles R such as $\left|N_R - \frac{S_R}{m}\right|$ is big. We can try for example to draw them with a ruler or to study all the possible cases by computers. We see well that the distribution is good and that the breaks of the independence will be difficult to find on rectangles except the small ones : but it is normal.

In order to try to compute D_m^2, i.e. $Sup\left|N_R - \frac{S_R}{m}\right|$, simulations were also done.

Let us notice well that the results are obtained by simulations. We contented ourselves with estimations because as soon as m is a little big, the number of rectangles which we have to study is too much big because it is necessary to take the sup for any rectangle R : $sup_R\left|N_R - \frac{S_R}{m}\right|$. We thus chose the width of rectangles at random and we have done again the operation a large number of time: for example for m =1711 we have done again it 400.000 times.

At first we studied discrepances $\tilde{D}_m^2$ for Fibonacci congruences. These results are summarized in the following table.

m	144	1597	17711	121393	1346269	14930352
a	89	987	10946	75025	832040	9227465
log(log(m))	1.6034	1.9982	2.2805	2.4602	2.6471	2.8045
D_m^2	3.8958	4.1058	4.8353	5.1334	5.2338	5.2993

These results seem well to show that for the congruences of Fibonacci, $\tilde{D}_m^2 = \varphi(m) \leq O\big(Log[Log(m)]\big)$. In fact, it is possible that this increase can be again improved: maybe $\varphi(m)$

converges even more slowly to infinity, even $\varphi(m)$ can be bounded. But, it is rather difficult to see in the present state of power of computers.

We also studied the other congruences and we saw that we do not find an increase of the type $D_m^2 \leq h^s O\big(Log[Log(m)]\big)$ where $h^s = sup(h_i^a)$. In fact we notice that the increase depends rather on $\sum_i h_i^a$ than of h^s (it is not the case of the decrease of the lemma 3.1.3 which depends effectively directly on h^s).

More exactly, when there exists n_0 such that $m = fi_{n_0}$, we set $R_{Fib} = \frac{\tilde{D}_m^2}{\sum_i \tilde{h}_i^a}$. Let $\tilde{h}_i^a$, $i = 1, 2, ..., \tilde{d}_i^a$, be the sequence h_i^a in the case of Fibonacci congruence. Then, we find a relation of the type $D_m^2 \leq R_{Fib}\big(\sum_i h^a\big) = \frac{\sum_i h_i^a}{\sum_i \tilde{h}_i^a}\varphi(m)$ where $\varphi(m) = O\big(Log[Log(m)]\big)$.

Thus, for m=1597 , we have the following table.

a	987	983	985	986	988	900	901	902	903	42	41	11
$\sum_i h_i^a$	16	49	17	18	19	20	20	25	21	80	62	52
D_m^2	4.2	13.12	4.83	4.88	5.04	5.25	5.04	6.62	5.46	19.9	15.07	41.47
$D_m^2 \approx$	4.2	12.86	4.4	4.72	4.98	5.25	5.25	6.56	5.51	21	15.75	39.9

For m=17711 , we have the following table.

a	10946	10940	10941	9877	122	1421	9874	6874	20
$\sum_i h_i^a$	21	37	27	42	159	44	34	31	893
D_m^2	4.9	8.5	6.4	9	41	9.4	7.8	6.9	230
$R_{Fib}\big(\sum_i h_i^a\big) \approx$	4.9	8.63	6.3	9.8	37.1	10.27	7.93	7.23	208.36

In fact the situation is a little more complicated than that. We can see it if m is small: we indeed see that there is another parameter which we have to take in account if T is not invertible: $r_{d^a}^a$. Indeed, there is then differences between D_m^2 and $R_{Fib}\big(\sum_i h_i^a\big)$.

In that way for m=144, we have the following table.

a	89	88	87	86,	25	37	35	52
$r_{d^a}^a$	1	8	3	2	1	1	1	4
$\sum_i h_i^a$	11	7	13	18	15	16	16	9
D_m^2	3.6	9.6	6.7	6.5	6.5	5.5	4.9	6.4
$R_{Fib}\big(\sum_i h_i^a\big) \approx$	3.6	2.2909	4.2545	5.8909	4.9091	5.2364	5.2364	2.9455

Then, we find an inequality of the same type as that of the lemma 2.7.6. Indeed, let us recall that $\sum_{i=1}^d h_i^a \leq dh^s$ and $d \leq 2^{\frac{log(m)-log(2)}{log(2)}}$.

As a matter of fact, $\sum_{i=1}^d h_i^a$ is generally smaller than dh^s (cf example above) . It is translated by the fact that, in a concrete way, the invertible congruences such as $h^s \leq 10$ for example are generally good [1] congruences as soon as $m \geq 10^6$.

Then, the increase $D_m^2 \leq h^s log(m)$ can be improved and it seems that it is by $D_m^2 \leq \frac{\sum_{i=1}^d h_i^a}{\sum_{i=1}^d \tilde{h}_i^a} Log(log(m))$ when $m = fi_{n_0}$ (if $m \neq fi_{n_0}$, one compares with the case of the nearest number fi_{n_1}).

3.4 Conclusion

According to the simulations that we made we find that $D_m^2 \leq \frac{\sum_i h_i^a}{\sum_i \tilde{h}_i^a}\varphi(m)$ where $\varphi(m) = Log[Log(m)]$.

[1] from the point of view of the independence of two successive simulated numbers

It is an increase much more accurate than those of Zaremba, Knuth, Niederreiter and even as that of the theorem 1.2.5. It shows that there are many possibilities on the choices of a and m. We can thus impose with no problem the independences required in order to have the best possible simulation.

Then, it is necessary that $(T^{2i}(x_0), T^{2i+1}(x_0))$ behave as independent, but also, for example, $(T^{4i}(x_0), (T^{4i+2}(x_0))$: a sequence of IID random variables $\{X_n\}$ check also that the pairs (X_{2n}, X_{2n+2}) are independent. That means that $\frac{m}{a^2}$ can be written as a continued fraction with the h_i^2's not too big:

$$\frac{m}{a^2} = h_1^2 + \frac{1}{h_2^2 + \frac{1}{h_3^2 + \frac{1}{h_4^2 + \ldots}}} \ .$$

Let us remark that it is also necessary that $(X_{4n}, X_{4n+1}, X_{4n+2}, , X_{4n+3})$ behave as independent. But we know that this result must be checked on hypercubes of width wider in order to have enough points of the sample $(T^{4i}(x_0), T^{4i+1}(x_0), T^{4i+21}(x_0), T^{4i+3}(x_0))$, i=0,1,....,m, in the hypercubes. So, for the bidimensional dependence, we can consider the squares of width $1/2^q$ where $4^q = O\big(m\big)$. In dimension 4, it is necessary that q checks $16^q = O\big(m\big)$.

After, it is necessary that $\frac{m}{a^3}$ has an expansion in continued fraction with the h_i^3's not too large:

$$\frac{m}{a^3} = h_1^3 + \frac{1}{h_2^3 + \frac{1}{h_3^3 + \frac{1}{h_4^3 + \ldots}}} \ .$$

And so on.

Obviously, it will be necessary to check these conditions if we use the congruences in order to make simulations.

If we want to calculate double integrals by using the congruences, Zaremba studied the most favorable case, that of the congruences of Fibonacci. In the same way, if we want to do IID a noise, we saw that the best way was also to use the congruences of Fibonacci. On the contrary, these are very bad pseudo-random generator because $T^2 = \pm Id$.

Bibliography

[1] KNUTH D.E. (1998) The Art of Computer Programming; Vol 2. Third Edition, Addison-Wesley, Reading, Massachusetts.

[2] BAYA A. (1990) Contribution à la génération de vecteurs aléatoires et à la cryptographie. Thèse de l'université Joseph Fourier de Grenoble.

[3] BEYER W. A. (1972) Lattice structure and reduced bases of random vectors generated by linear recurrences. In applications of Number Theory to Numerical Analysis. Ed Zaremba S. K.

[4] BOSQ.D (1983) Lois limites et efficacité asymptotique des tests Hilbertiens de diverses lois sous des hypothèses adjacentes. Statistique et Analyse des Données, 8 n^o1, p 1-40.

[5] BLACHER R. (1993) Higher Order Correlation Coefficients. Statistics 25, 1-15.

[6] BLACHER R. (1990) Quelques applications des fonctions orthogonales en probabilité et statistique. Thèse de l'université Joseph Fourier. Grenoble.

[7] BLACHER R. (1988) A new form for the chi squared independence test. Statistics 19 519-536.

[8] BLACHER R. (1983) Indicateurs de dépendance fournis par le développement en série de la densité de probabilité. Thèse 3^o Cycle, Université Joseph Fourier de Grenoble. Hal archives ouvertes : http://tel.archives-ouvertes.fr

[9] BLACHER R. (1983) Quelques propriétés des congruences linéaires considérées comme générateur de nombres pseudo-aléatoires. Rapport de recherche n^o 345 IMAG, Université Joseph Fourier de Grenoble.

[10] BLACHER R. (2009) A Perfect Random Number Generator. Rapport de Recherche LJK. Université de Grenoble. http://hal.archives-ouvertes.fr/hal-00426555/fr/

[11] BLACHER R. (2010) A Perfect Random Number Generator II. Rapport de Recherche LJK. Université de Grenoble. http://hal.archives-ouvertes.fr/hal-00443576/fr/.

[12] BLACHER R. (2010) Correct models. Rapport de Recherche LJK. Université de Grenoble. http://hal.archives-ouvertes.fr/hal-00521529/fr/

[13] BLACHER R. (2004) Solution complète au problème des nombres aléatoires. Journées statistiques de Montpellier. http://www.agro-montpellier.fr/sfds/CD/textes/blacher1.pdf

[14] BLACHER R. (2009) File of random Number. http://www-ljk.imag.fr/membres/Rene.Blacher/GEAL/node3.html.

[15] BLACHER R. (2011) Fibonacci congruences and applications. Rapport de Recherche LJK. Université de Grenoble. http://hal.archives-ouvertes.fr/hal-0058t7108/fr/.

[16] BLACHER R. (2011) Fibonacci congruences and applications. Open Journal of Statistics, Vol 1, n^o 2, http://www.scirp.org/journal/PaperInformation.aspx?paperID=6551

[17] BLACHER R. (2011) A method for Building true random sequences. Far East Journal of Theoretical Statistics. Volume 36 n^o 2, 75-104.

[18] DIETER U. (1972) Statistical interdependence of pseudo-random numbers generated by the linear congruential method, Applications of Number Theory to Numerical Analysis (S. K. Zaremba, ed.), Academic Press, New York, 1972, pp. 287-317.

[19] NIEDERREITER H. (1985) The serial test for pseudo random numbers generated by the linear congruential method. Numer. Math 46 p 51-68.

[20] MENEZES A., VAN OORSCHOT P. , VANSTONE S. (1996) Handbook of Applied Cryptography, CRC Press, 1996.

[21] MACLAREN M.D. and MARSAGLIA G. (1965) Uniform random number generators. J.A.C.M. vol 12 n^o 1 83-89.

[22] VALIRON G. (1955) Théorie des fonctions. Hermann, Paris

[23] ZAREMBA S. K. (1966) Good lattice points, discrepancy and numerical integration. Annali di Mathematica Pura ed Applicata. IV 73, p 293-317.