La tente

Marc Lorenzi

9 mars 2023

Résumé

La *tente* est une fonction f extrêmement simple de l'intervalle $[0,1]$ sur lui-même. Le comportement des suites récurrentes $(u_n)_{n\geq 0}$ définies par $u_0 \in [0,1]$ et, pour tout $n \in \mathbb{N}$, $u_{n+1} = f(u_n)$ est cependant très compliqué. Nous allons dans cet article nous intéresser à de telles suites, et plus particulièrement aux suites de ce type qui sont périodiques.

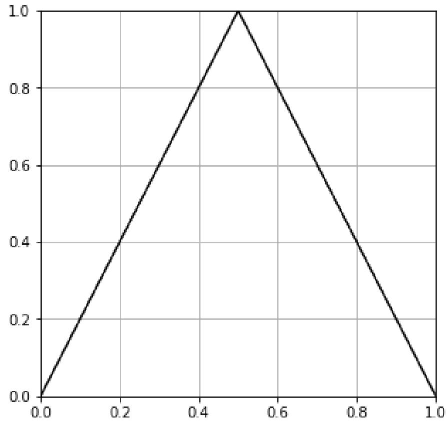
1 Introduction

1.1 La tente

Dans tout l'article, nous considérerons l'application $f : [0,1] \longrightarrow [0,1]$ définie pour $x \in [0,1]$ comme suit.

- Si $x \in [0, \frac{1}{2}]$ alors $f(x) = 2x$.
- Si $x \in [\frac{1}{2}, 1]$ alors $f(x) = 2(1-x)$.

Voici le graphe de f.



La fonction f est appelée la *tente* parce que son graphe ressemble à . . . une tente. Nous allons étudier les propriétés de f vue comme un *système dynamique*. Mais qu'est-ce qu'un système dynamique ?

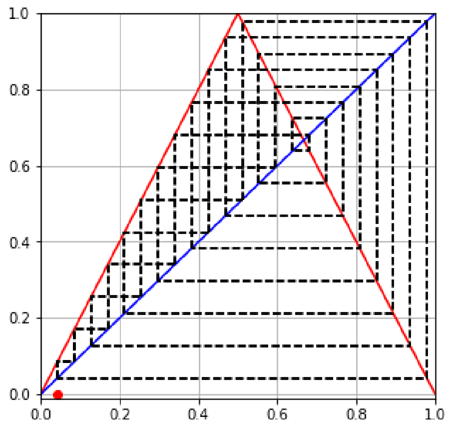
Définition 1. Le *système dynamique engendré par f* est l'ensemble

$$\mathcal{S} = \{f^n : n \in \mathbb{N}\}$$

où $f^0 = id_{[0,1]}$ et pour tout $n \in \mathbb{N}$, $f^{n+1} = f^n \circ f$. Pour tout $x \in [0,1]$, *l'orbite de x* suivant $\mathcal{S}$ est l'ensemble

$$\mathcal{O}(x) = \{f^n(x) : n \in \mathbb{N}\}$$

Pour simplifier, nous confondrons dans cet article la fonction f et le système dynamique qu'elle engendre. Nous parlerons donc du système dynamique f, de l'orbite de x suivant f, etc. Étudier le système dynamique f c'est, entre autres, étudier le comportement des orbites. Malgré la simplicité de la fonction f, cette étude peut être très compliquée. Nous nous intéresserons plus particulièrement aux *points périodiques* de f. Par exemple, $\frac{2}{47}$ est un point périodique de f, sa période est 23. Voici le tracé de son orbite.



1.2 Développements dyadiques

Avant d'entrer dans le vif du sujet, disons quelques mots sur le développement des réels en base 2, ce que l'on appelle leur *développement dyadique*. Nous admettons sans preuve les quelques résultats qui suivent.

Notons $\mathbf{2} = \{0, 1\}$.

Étant donnée une suite $(x_k)_{k\geq 1}$ d'éléments de $\mathbf{2}$, la série $\sum_{k\geq 1} \frac{x_k}{2^k}$ est convergente. Cela signifie que la suite $(S_n)_{n\geq 1}$ de terme général

$$S_n = \sum_{k=1}^{n} \frac{x_k}{2^k}$$

est convergente. La limite de cette suite est ce que l'on appelle la *somme de la série* (bien que ce ne soit pas une somme, mais une *limite* de sommes). On la note

$$\sum_{k=1}^{\infty} \frac{x_k}{2^k}$$

Cette somme appartient à $[0,1]$. Inversement, tout réel $x \in [0,1]$ peut s'écrire

$$x = \sum_{k=1}^{\infty} \frac{x_k}{2^k}$$

où les x_k appartiennent à **2**. Une telle suite $(x_k)_{k\geq 1}$ est appelée un *développement dyadique* de x. Pour tout $k \geq 1$, x_k est le k^{e} *bit* de x. Nous utiliserons les deux notations

$$x = [x_k]_{k\geq 1} = 0.x_1x_2x_3\ldots$$

La suite $(x_k)_{k\geq 1}$ est uniquement déterminée par la donnée de x, sauf dans certains cas où il existe *deux* suites qui conviennent. Précisons ce point. Appelons $\mathbb{D}$ l'ensemble des *nombres dyadiques* :

$$\mathbb{D} = \left\{ \frac{p}{2^n} : n \in \mathbb{N}, p \in [\![0, 2^n]\!] \right\} \subseteq [0,1]$$

Soit $x \in [0,1]$. Si $x \notin \mathbb{D}$ ou si $x = 0$ ou $x = 1$, alors x possède un unique développement dyadique. Si $x \in \mathbb{D}$ et $x \neq 0, 1$, x possède deux développements dyadiques. Il existe un unique entier $m \in \mathbb{N}^*$ et un unique $(m-1)$-uplet de bits $(x_1, \ldots, x_{m-1})$ tels que

$$\begin{aligned} x &= 0.x_1\ldots x_{m-1}1000\ldots \\ &= 0.x_1\ldots x_{m-1}0111\ldots \end{aligned}$$

Par exemple,

$$\frac{1}{2} = 0.1000\ldots = 0.0111\ldots$$

ou encore

$$\frac{5}{16} = 0.0101000\ldots = 0.0100111\ldots$$

Remarquons qu'avec nos définitions le réel 1 possède un unique développement dyadique :

$$1 = 0.111\ldots$$

Remarque. Dans la suite, nous parlerons fréquemment *du* développement dyadique de x, même si x possède deux développements dyadiques. Dans certaines preuves de théorèmes, il nous faudra montrer que cela ne présente pas d'ambiguïté. Les bits du réel x seront notés notés avec la même lettre x et un indice, c'est à dire x_1, x_2, etc. Lorsque x possède deux développements dyadiques, il y a ambiguïté lorsqu'on parle du k^{e} bit de x, parce que ce bit dépend du développement dyadique de x que l'on considère.

1.3 Opérations sur les bits

L'ensemble **2** peut être muni d'une opération que nous noterons $\oplus$, définie par la table

$\oplus$	0	1
0	0	1
1	1	0

Cette loi fait de **2** un groupe abélien.

Proposition 1.

- *Pour tout* $x \in [0, \frac{1}{2}[$, $2x = [x_{k+1}]_{k \geq 1}$.
- *Pour tout* $x \in [0, 1]$, $1 - x = [x_k \oplus 1]_{k \geq 1}$.

Démonstration.

- Soit $x \in [0, \frac{1}{2}[$. On a

$$\begin{aligned} 2x &= 2 \sum_{k=2}^{\infty} \frac{x_k}{2^k} \\ &= \sum_{k=2}^{\infty} \frac{x_k}{2^{k-1}} \\ &= \sum_{k=1}^{\infty} \frac{x_{k+1}}{2^k} \end{aligned}$$

- Soit $x \in [0, 1]$. Remarquons que pour tout $k \geq 1$, $x_k \oplus 1 = 1 - x_k$. De là,

$$\begin{aligned} [x_k \oplus 1]_{k \geq 1} &= \sum_{k=1}^{\infty} \frac{1 - x_k}{2^k} \\ &= \sum_{k=1}^{\infty} \frac{1}{2^k} - \sum_{k=1}^{\infty} \frac{x_k}{2^k} \\ &= 1 - x \end{aligned}$$

□

1.4 Tente et développements dyadiques

Pour tout $x \in [0, 1]$, $f(x)$ peut avantageusement être décrit en considérant le développement dyadique de x.

Proposition 2. *Soit* $x \in [0, 1]$. *On a*

$$f(x) = [x_{k+1} \oplus x_1]_{k \geq 1}$$

Démonstration. Considérons un certain nombre de cas.

- Supposons $x \in [0, \frac{1}{2}[$. Alors $x_1 = 0$. De là,

$$f(x) = 2x = [x_{k+1}]_{k \geq 1} = [x_{k+1} \oplus x_1]_{k \geq 1}$$

- Supposons $x \in]\frac{1}{2}, 1]$. Alors $x_1 = 1$ et $1 - x \in [0, \frac{1}{2}[$. De là,

$$f(x) = 2(1 - x) = 2[x_k \oplus 1]_{k \geq 1} = [x_{k+1} \oplus 1]_{k \geq 1} = [x_{k+1} \oplus x_1]_{k \geq 1}$$

- Supposons enfin $x = \frac{1}{2}$. On a $f(x) = 1$. Vérifions que les deux développements dyadiques de x donnent le bon résultat. Écrivons tout d'abord

$$x = 0.1000\ldots$$

On a alors

$$[x_{k+1} \oplus x_1]_{k\geq 1} = [x_{k+1} \oplus 1]_{k\geq 1} = 0.111\ldots = 1$$

Prenons maintenant l'autre développement dyadique

$$x = 0.0111\ldots$$

On a alors

$$[x_{k+1} \oplus x_1]_{k\geq 1} = [x_{k+1} \oplus 0]_{k\geq 1} = 0.111\ldots = 1$$

On obtient ainsi, dans les deux cas, le résultat correct.

□

Proposition 3. *Soit $x \in [0,1]$. On a pour tout $n \in \mathbb{N}^*$,*

$$f^n(x) = [x_{k+n} \oplus x_n]_{k\geq 1}$$

Démonstration. Faisons une récurrence sur n. Pour $n = 1$, il s'agit de la proposition précédente. Soit $n \geq 1$. Supposons le résultat vrai pour n. On a alors

$$\begin{aligned} f^{n+1}(x) &= f(f^n(x)) \\ &= f([x_{k+n} \oplus x_n]_{k\geq 1}) \\ &= [(x_{k+1+n} \oplus x_n) \oplus (x_{1+n} \oplus x_n)]_{k\geq 1} \end{aligned}$$

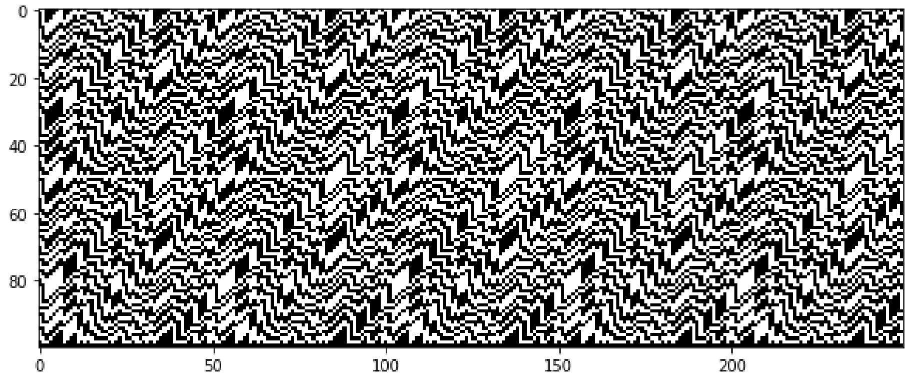
Il reste à remarquer que $\oplus$ est commutative et associative, et que $x_n \oplus x_n = 0$.
□

2 Les points périodiques de la tente

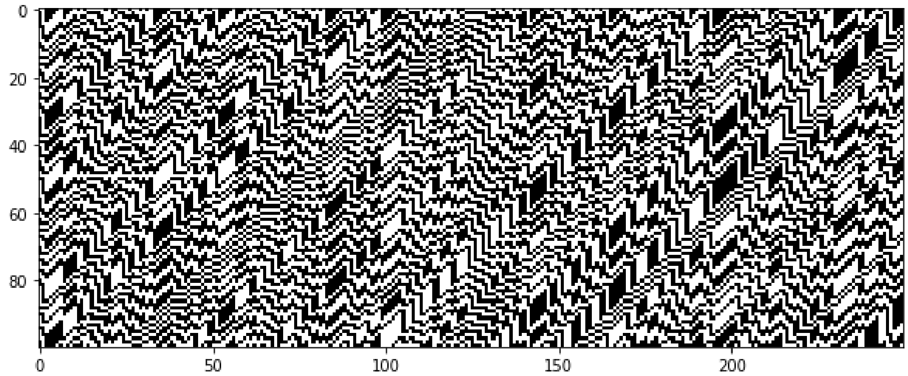
2.1 Introduction

La figure ci-dessous représente 300 itérations de f sur le réel $x = \frac{52}{101}$. Le développement dyadique de ce rationnel est périodique, de période 100. La k^{e} colonne de pixels représente les 100 premiers bits du développement dyadique de $f^k(x)$. En noir, un bit nul, et en blanc, un bit égal à 1. On remarque que le graphique présente une périodicité de la gauche vers la droite : un oeil exercé verra que les colonnes se répètent de 50 en 50.

On remarque aussi une ligne blanche horizontale, au milieu du schéma, et une ligne noire tout en bas (moins visible). Il s'avère que pour tout entier k, le 50^{e} bit de $f^k(x)$ vaut 1 et le 100^{e} bit de $f^k(x)$ vaut 0.



Voici maintenant ce qui se passe lorsqu'on prend un irrationnel comme point de départ. L'irrationnel en question a ses 100 premiers chiffres égaux à ceux de $\frac{52}{101}$. Les chiffres suivants sont choisis « aléatoirement ». La ligne blanche persiste pendant 50 itérations et la ligne noire a disparu. On ne voit plus de périodicité.



2.2 Le cas des nombres dyadiques

Rappelons que les nombres dyadiques sont les réels $x \in [0, 1]$ dont les bits sont nuls à partir d'un certain rang ou, de façon équivalente, égaux à 1 à partir d'un certain rang.

Proposition 4. *Soit $x \in \mathbb{D}$. Pour tout entier n assez grand, on a*

$$f^n(x) = 0$$

Démonstration. C'est clair si $x = 0$ ou $x = 1$. Supposons donc $x = [x_k]_{k\geq 1} \in]0, 1[$ en choisissant le développement dyadique de x qui finit par des zéros. Il existe un entier $m \geq 1$ (unique) tel que $x_m = 1$ et pour tout $k > m$, $x_k = 0$. On a alors

$$f^m(x) = [x_{k+m} \oplus 1]_{k\geq 1}$$

Comme $k+m > m$, $x_{k+m} = 0$ et donc $x_{k+m} \oplus 1 = 1$. Ainsi, $f^m(x) = 1$. De là, $f^{m+1}(x) = 0$ et donc, pour tout $n \geq m+1$, $f^n(x) = 0$. $\square$

Par exemple, prenons $x = \frac{5}{16}$. On a

$$\begin{array}{rclcl}
f^0(x) & = & 0.0101000\ldots & = & 0.0100111\ldots \\
f^1(x) & = & 0.1010000\ldots & = & 0.1001111\ldots \\
f^2(x) & = & 0.1011111\ldots & = & 0.1100000\ldots \\
f^3(x) & = & 0.1000000\ldots & = & 0.0111111\ldots \\
f^4(x) & = & 0.1111111\ldots & & \\
f^5(x) & = & 0.0000000\ldots & &
\end{array}$$

2.3 Points périodiques

Définition 2. Soit $x \in [0,1]$. On appelle *période* de x pour le système dynamique f tout entier $n \in \mathbb{N}$ tel que $f^n(x) = x$.

Nous noterons $\mathcal{T}(x)$ l'ensemble des périodes de x.

Définition 3. Soit $x \in [0,1]$. x est un *point périodique* du système dynamique f lorsque x possède une période non nulle. La plus petite période non nulle de x est sa *période primitive.*

Proposition 5. *Soit $x \in [0,1]$. Il existe un unique entier $\tau \in \mathbb{N}$ tel que*

$$\mathcal{T}(x) = \{k\tau, k \in \mathbb{N}\} = \tau\mathbb{N}$$

x est périodique si et seulement si $\tau > 0$. τ est alors la période primitive de x.

Démonstration. Si x n'est pas périodique, le résultat est évident puisque $\mathcal{T}(x) = \{0\} = 0\mathbb{N}$. Supposons donc x périodique. Soit τ la période primitive de x.

Montrons par récurrence sur k que pour tout $k \in \mathbb{N}$, $k\tau$ est encore une période de x. C'est évident si $k = 0$. Soit $k \in \mathbb{N}$. Supposons que $k\tau$ est une période de x. On a alors

$$\begin{array}{rcl}
f^{(k+1)\tau}(x) & = & f^\tau(f^{k\tau}(x)) \\
& = & f^\tau(x) \\
& = & x
\end{array}$$

Ainsi, $(k+1)\tau$ est une période de x.

Inversement, soit n une période de x. Effectuons la division euclidienne de n par τ. On a $n = k\tau + r$ où $k \in \mathbb{N}$ et $0 \leq r < \tau$. On a

$$\begin{array}{rcl}
x & = & f^n(x) \\
& = & f^r(f^{k\tau}(x)) \\
& = & f^r(x)
\end{array}$$

Ainsi, r est une période de x. Mais $r < \tau$ et τ est la plus petite période non nulle de x. On en déduit que $r = 0$ et donc $n = k\tau \in n_0\mathbb{N}$.

Montrons enfin l'unicité. Soient $\tau, \tau' \in \mathbb{N}$. Supposons $\tau\mathbb{N} = \tau'\mathbb{N}$. Comme $\tau \in \tau\mathbb{N}$, on a aussi $\tau \in \tau'\mathbb{N}$. Ainsi, τ' divise τ. De même, τ divise τ'. De là, $\tau = \tau'$. $\square$

2.4 Nombres dyadiques périodiques

Il y a un seul nombres dyadique périodique.

Proposition 6. *Soit $x \in \mathbb{D}$.*

- *Si $x = 0$, alors x est périodique, de période primitive 1.*
- *Si $x \neq 0$, alors x n'est pas périodique.*

Démonstration. On a $f(0) = 0$, d'où la première assertion. En revanche, si $x \neq 0$, pour tout $n \in \mathbb{N}$ assez grand $f^n(x) = 0 \neq x$, et donc n n'est pas une période de x. L'ensemble $\mathcal{T}(x)$ des périodes de x est donc majoré, ce qui entraîne que $\mathcal{T}(x) = \{0\}$. Ainsi, x n'est pas périodique. $\square$

2.5 Une caractérisation de la périodicité

Soient $x \in [0, 1]$ et $n \in \mathbb{N}^*$. Le point x admet-il n pour période ? Admet-il n pour période primitive ? Il est plus facile de répondre à la première question qu'à la seconde.

Proposition 7. *Soit $x \in [0, 1]$. Soit $n \in \mathbb{N}^*$. n est une période de x si et seulement si*

$$(\star)\ \forall k \geq 1, x_{k+n} = x_k \oplus x_n$$

Démonstration. Tout d'abord, $x = 0$ est périodique de période 1. De plus, pour tout $k \geq 1$,

$$x_{k+n} = 0 = x_k = 0 \oplus 0 = x_k \oplus x_n$$

et donc $(\star)$ est vérifiée.

Prenons maintenant $x = 1$. x n'est pas périodique. De plus, on a pour tout $k \geq 1$, $x_{k+n} = 1$ alors que $x_k \oplus x_n = 1 \oplus 1 = 0$. La propriété $(\star)$ n'est donc pas vérifiée.

Supposons maintenant que $x \in \mathbb{D} \setminus \{0, 1\}$. x n'est pas un point périodique de f puisque pour tout n assez grand, $f^n(x) = 0 \neq x$. Deux cas se présentent, selon le développement dyadique choisi pour x.

- Cas 1, pour tout k assez grand, $x_k = 0$. Comme $x \neq 0$, au moins un des x_k est non nul. Choisissons un k maximal tel que $x_k = 1$. On a alors $x_{k+n} = 0$. Par ailleurs
$$x_k \oplus x_n = 1 \oplus x_n$$

Si $x_n = 0$ on a montré que $(\star)$ n'est pas vérifiée. Si au contraire $x_n = 1$, alors $x_{(k+n)+n} = 0$ alors que

$$x_{k+n} \oplus x_n = 0 \oplus 1 = 1$$

et donc $(\star)$ n'est pas vérifiée.

- Cas 2, pour tout k assez grand, $x_k = 1$. Comme $x \neq 1$, au moins un des x_k est nul. On prend un tel k maximal. En procédant comme dans le cas 1, on montre que $(\star)$ n'est pas vérifiée.

Supposons enfin que $x \in [0,1] \setminus \mathbb{D}$.

Soit $n \in \mathbb{N}^*$. n est une période de x si et seulement si $f^n(x) = x$. Ceci est équivalent à

$$[x_{k+n} \oplus x_n]_{k \geq 1} = [x_k]_{k \geq 1}$$

Comme $x \notin \mathbb{D}$, x possède un unique développement dyadique. La condition ci-dessus équivaut donc à dire que pour tout $k \geq 1$,

$$x_{k+n} \oplus x_n = x_k$$

En ajoutant x_n des deux côtés de l'égalité, on obtient la condition équivalente $(\star)$. $\square$

2.6 Densité

La tente possède-t-elle beaucoup de points périodiques ? Oui, comme le montre le résultat suivant.

Proposition 8. *L'ensemble des points périodiques de f est dense dans $[0,1]$.*

Démonstration. Soit $a \in [0,1]$. Soit $n \geq 1$. Soient $a_1, \ldots, a_n$ les n premiers chiffres d'un développement dyadique de a. Soit

$$x = 0.\overline{a_1 \ldots a_n b_1 \ldots b_n}$$

où $b_i = a_i \oplus a_n$, et la barre horizontale signifie que la séquence $a_1 \ldots a_n b_1 \ldots b_n$ est répétée indéfiniment. Le point x est périodique, n est une période de x, et

$$|x - a| \leq \sum_{k=n+1}^{\infty} \frac{1}{2^k} = \frac{1}{2^n}$$

Il existe donc des points périodiques de f aussi proches de a que l'on désire. $\square$

3 Périodes 1, 2 et 3

Nous allons dans cette section déterminer tous les points périodiques de périodes primitives 1, 2 et 3.

3.1 Points fixes

Les points de période primitive 1, c'est à dire les points fixes de f, sont immédiats à déterminer. Soit $x \in [0,1]$.

- Si $x \in [0, \frac{1}{2}]$, $f(x) = x$ si et seulement si $2x = x$, c'est à dire $x = 0$.
- Si $x \in [\frac{1}{2}, 1]$, $f(x) = x$ si et seulement si $2(1-x) = x$, c'est à dire $x = \frac{2}{3}$.

Amusons-nous à retrouver ces deux points avec la condition que nous avons démontrée. Soit $x \in [0,1]$. x est de période primitive 1 si et seulement si pour tout $k \geq 1$,

$$x_{k+1} = x_k \oplus x_1$$

Deux cas se présentent.

- Si $x_1 = 0$, on a alors pour tout $k \geq 1$, $x_{k+1} = x_k$, et donc $x_k = 0$. Ainsi, $x = 0$.
- Si $x_1 = 1$, on a alors pour tout $k \geq 1$, $x_{k+1} = x_k \oplus 1$. De là, $x_k = 1$ si k est impair et $x_k = 0$ si k est pair. On a donc

  $$x = 0.\overline{10}$$

  où la barre horizontale signifie que la séquence 10 est répétée indéfiniment. Que vaut x ? Le développement dyadique de x étant de période 2, multiplions par 2^2. Il vient

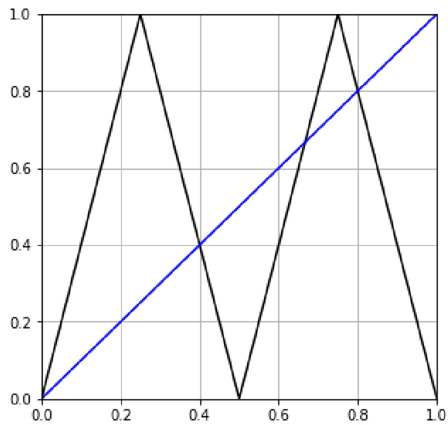
  $$4x = [10] + 0.\overline{10}$$

  où [10] est l'entier naturel dont l'écriture en base 2 est 10, c'est à dire le nombre 2. On a donc $4x = 2 + x$, d'où

  $$x = \frac{2}{3}$$

3.2 Points de période 2

Voici le graphe de la fonction f^2 ainsi que la droite d'équation $y = x$.



La fonction f^2, comme on le voit ci-dessus, possède 4 points fixes. Deux de ces 4 points sont 0 et $\frac{2}{3}$, les points fixes de f. Les deux autres sont les points de période primitive 2.

Soit $x \in [0,1]$. 2 est une période de x si et seulement si pour tout $k \geq 1$,

$$x_{k+2} = x_k \oplus x_2$$

Un tel réel x est caractérisé par la donnée de x_1 et x_2. Les valeurs possibles de x_1x_2 sont 00, 01, 10 et 11. Il y a donc 4 tels réels. Parmi ceux-ci, on retrouve les deux points fixes (en prenant 00 et 10). Calculons les deux autres, ce sont les points qui nous intéressent.

- Si $x_1x_2 = 01$, alors $x = 0.\overline{0110}$. On a donc

$$2^4x = [0110] + x = 6 + x$$

  et donc

$$x = \frac{6}{15}$$

  Inversement,

$$\begin{aligned} f\left(\frac{6}{15}\right) &= \frac{12}{15} \\ f^2\left(\frac{6}{15}\right) &= f\left(\frac{12}{15}\right) = \frac{6}{15} \end{aligned}$$

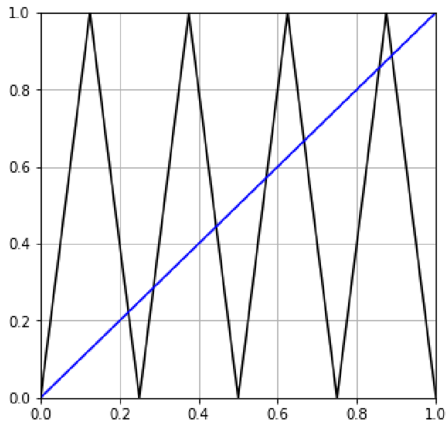
- Si $x_1x_2 = 11$, alors

$$x = 0.\overline{1100}$$

  Bien entendu, $x = \frac{12}{15}$, qui est l'image par f du point de période primitive 2 que nous avons déjà trouvé.

3.3 Points de période 3

Voici le graphe de la fonction f^3 avec la droite d'équation $y = x$.



f^3 possède 8 points fixes. Parmi ces 8 points, deux (0 et $\frac{2}{3}$) sont les points fixes de f. Les six autres sont les points de période primitive 3. Prenons

$$x = 0.\overline{100}\ldots$$

Ce point vérifie la condition de périodicité pour $n = 3$. Donc, sa période primitive divise 3, c'est donc 1 ou 3. Il est évident que x ne vérifie pas la condition de périodicité pour $n = 1$, donc x n'est pas de période 1. Il est donc de période primitive 3. Que vaut x ? On a

$$2^3 x = [100] + x = 4 + x$$

et donc

$$x = \frac{4}{7}$$

Vérifions. On a

$$\begin{aligned} f\left(\frac{4}{7}\right) &= \frac{6}{7} \\ f^2\left(\frac{4}{7}\right) &= f\left(\frac{6}{7}\right) = \frac{2}{7} \\ f^3\left(\frac{4}{7}\right) &= f\left(\frac{2}{7}\right) = \frac{4}{7} \end{aligned}$$

Remarquons que nous avons ainsi gratuitement deux autres points de période primitive 3, à savoir $\frac{2}{7}$ et $\frac{6}{7}$. Il nous reste trois points de période primitive 3 à trouver. Il suffit d'en avoir un. À partir de celui-ci nous aurons les deux autres. Prenons

$$x = 0.\overline{001110}$$

x vérifie la condition de 3-périodicité et pas la condition de 1-périodicité. C'est donc un point de période primitive 3. On a

$$2^6 x = [001110] + x = 14 + x$$

et donc

$$x = \frac{14}{63} = \frac{2}{9}$$

Vérifions.

$$\begin{aligned} f\left(\frac{2}{9}\right) &= \frac{4}{9} \\ f^2\left(\frac{2}{9}\right) &= f\left(\frac{4}{9}\right) = \frac{8}{9} \\ f^3\left(\frac{2}{9}\right) &= f\left(\frac{8}{9}\right) = \frac{2}{9} \end{aligned}$$

Finalement, les 6 points de période primitive 3 de f sont

$$\frac{2}{7}, \frac{4}{7}, \frac{6}{7}, \frac{2}{9}, \frac{4}{9}, \frac{8}{9}$$

Exercice. Déterminer les points de période primitive 4. Il y en a 12.

4 Périodicité et rationalité

La caractérisation des points périodiques que nous avons trouvée à la section précédente a ses avantages et ses inconvénients. L'un de ses avantages est qu'il est facile de lister tous les points de période n donnée. L'un de ses inconvénients est que ces points sont obtenus par leur développement dyadique, et que le résultat n'est pas très parlant. Est-il possible d'obtenir les points périodiques de f de façon plus explicite ? La réponse est oui, nous allons voir qu'il y a un lien entre périodicité et rationalité.

4.1 Rappels sur les rationnels

Avertissement. Dans cette section nous allons manipuler deux types différents de périodicité. D'une part, la périodicité d'un réel $x \in [0, 1]$ pour le système dynamique f. D'autre part, la périodicité d'une suite $(x_k)_{k \geq 1}$ d'éléments de $\mathbf{2}$. Nous allons en fait voir qu'il existe un lien entre les deux.

Nous admettrons sans démonstration les résultats suivants.

Soit $x \in [0, 1]$. x est rationnel si et seulement si son développement dyadique est périodique à partir d'un certain rang. On peut en fait dire mieux que cela. Écrivons $x = \frac{p}{q}$ où $q \geq 1$, $0 \leq p \leq q$ et $p \wedge q = 1$. Si q est impair (c'est le seul cas qui nous intéressera), alors le développement dyadique de x est périodique. Sa période primitive est l'ordre multiplicatif de 2 modulo q, c'est à dire le plus petit entier $n \geq 1$ tel que $2^n \equiv 1 \bmod q$. Nous noterons ω_q cet ordre. Voici les premières valeurs de ω_q.

q	1	3	5	7	9	11	13	15	17	19	21	23
ω_q	1	2	4	3	6	10	12	4	8	18	6	11

Par exemple, soit $x = \frac{3}{17}$. On a $\omega_{17} = 8$. De là, le développement dyadique de x est périodique, de période primitive 8. Ce développement est facile à obtenir. Il suffit de remarquer que

$$2^8 = 1 + 15 \times 17$$

En multipliant par x, on obtient

$$2^8 x = x + 45$$

L'écriture de 45 en base 2 avec 8 chiffres est [00101101]. De là,

$$x = 0.\overline{00101101}$$

4.2 Périodicité entraîne rationalité

Proposition 9. *Soit $x \in [0, 1]$. Si x est périodique, alors x est rationnel.*

Démonstration. Soit n une période de x. Supposons tout d'abord que $x_n = 0$. On a pour tout $k \geq 1$,

$$x_{k+n} = x_k \oplus x_n = x_k \oplus 0 = x_k$$

Ainsi, la suite $(x_k)_{k\geq 1}$ est périodique de période n.

Supposons maintenant que $x_n = 1$. On a alors pour tout $k \geq 1$,

$$x_{k+2n} = x_{k+n} \oplus x_n = x_k \oplus x_n \oplus x_n = x_k$$

Ainsi, la suite $(x_k)_{k\geq 1}$ est périodique de période $2n$.

Dans tous les cas, la suite la suite $(x_k)_{k\geq 1}$ est périodique. On en conclut que x est rationnel. $\square$

4.3 Une réciproque

Proposition 10. *Soit $x \in \mathbb{Q} \cap [0, 1]$. Écrivons $x = \frac{p}{q}$ où $q \geq 2$, $p \in [\![0, q]\!]$ et $p \wedge q = 1$. Alors, x est périodique si et seulement si p est pair et q est impair.*

Démonstration. Si $q = 2q'$ est pair, on a de façon évidente pour tout $n \geq 1$, $f^n(x) = \frac{p_n}{q'}$ où $0 \leq p_n \leq q'$. Il en résulte que pour tout $n \geq 1$, $f^n(x) \neq x$ et donc que x n'est pas périodique. Supposons donc à partir de maintenant que q est impair.

Supposons tout d'abord $x \in [0, \frac{1}{2}[$. On a

$$f(x) = \frac{2p}{q}$$

Comme q est impair et $p \wedge q = 1$, on a aussi $(2p) \wedge q = 1$.

Supposons maintenant $x \in [\frac{1}{2}, 1]$. On a

$$f(x) = \frac{2(q-p)}{q}$$

Comme dans le premier cas, $(2(q - p)) \wedge q = 1$.

On a donc par une récurrence facile que pour tout $n \geq 1$, $f^n(x) = \frac{p_n}{q}$ où p_n est pair. Ainsi, si p est impair, pour tout $n \geq 1$, $p_n \neq p$ et donc $f^n(x) \neq x$. Ainsi, x n'est pas périodique. Supposons dorénavant que p est pair.

Comme q est impair, le développement dyadique de x est périodique. Écrivons $x = 0.\overline{x_1 \dots x_m}$. où m est la période du développement dyadique de x. Rappelons que $m = \omega_q$ est l'ordre multiplicatif de 2 modulo q. On a

$$2^m x = a + x$$

où, en base 2,

$$a = [x_1 \dots x_m]$$

Ainsi,

$$x = \frac{p}{q} = \frac{a}{2^m - 1}$$

De là,

$$p(2^m - 1) = aq$$

et donc p divise aq. Comme p est premier avec q, le théorème de Gauss implique que p divise a. Or, p est pair, donc a est pair et donc $x_m = 0$. De là, pour tout $k \geq 1$,

$$x_k \oplus x_m = x_k \oplus 0 = x_k = x_{k+m}$$

Ainsi, x est un point périodique du système dynamique f, et de plus, la période primitive de x divise m. $\square$

4.4 La valeur de la période

Proposition 11. *Soit $x \in \mathbb{Q} \cap [0,1]$. Écrivons $x = \frac{p}{q}$ où $q \geq 2$, $p \in [\![0, q]\!]$, $p \wedge q = 1$, p est pair et q est impair. Soit τ la période primitive de x.*

- *Si $x_\tau = 0$, alors $\tau = \omega_q$.*
- *Si $x_\tau = 1$, alors $\tau = \frac{1}{2}\omega_q$.*

Démonstration. Notons $m = \omega_q$. En reprenant la démonstration précédente, τ divise m. Deux cas surviennent.

- Supposons $x_\tau = 0$. On a alors pour tout $k \geq 1$,

  $$x_{k+\tau} = x_k \oplus x_\tau = x_k$$

  Ainsi, le développement dyadique de x possède τ pour période. Comme m est la plus petite période de ce développement, on en déduit que m divise τ, d'où $\tau = m$.
- Supposons maintenant $x_\tau = 1$. 2τ est aussi une période de x. De plus,

  $$x_{2\tau} = x_\tau \oplus x_\tau = 0$$

  et donc, comme dans le premier cas, le développement dyadique de x possède 2τ pour période. Comme m est la plus petite période de ce développement, on en déduit que m divise 2τ. Or, τ divise m, donc $m = \tau$ ou $m = 2\tau$. Mais $x_{\tau+\tau} = 0$ alors que $x_\tau = 1$, donc $m \neq \tau$. Ainsi, $\tau = \frac{1}{2}m$.

$\square$

Proposition 12. *Soit q un entier impair. Les rationnels périodiques de dénominateur q ont tous la même période primitive.*

Démonstration. Si $q = 1$, c'est immédiat. Supposons donc $q \geq 3$. Soient $x = \frac{p}{q}$ et $y = \frac{p'}{q}$ deux rationnels de $[0,1]$ où p, p' sont pairs et premiers avec q. Les entiers p et p' sont inversibles dans l'anneau $\mathbb{Z}/q\mathbb{Z}$. Il existe donc $a \in [\![1, q-1]\!]$ premier avec q et tel que $p' \equiv ap \bmod q$. Considérons la fonction $\varphi : x \longmapsto ax \bmod q$. Cette fonction envoie bijectivement l'orbite de x sur l'orbite de y. Ainsi, ces deux orbites ont le même cardinal. $\square$

5 Dénombrements

Nous allons terminer cet article par un problème de dénombrement. Étant donné un entier $n \geq 1$, combien y a-t-il de points de période primitive n ? Commençons par une question plus simple.

5.1 Nombre de points de période donnée

Proposition 13. *Soit $n \geq 1$. La fonction f possède exactement 2^n points périodiques ayant n pour période.*

Démonstration. Un tel point x est caractérisé par la valeur de ses n premiers bits $x_1, \ldots, x_n$. $\square$

Passons à quelque chose de plus délicat.

5.2 Nombre de points de période primitive donnée

Pour tout $n \geq 1$, notons $\mathcal{T}_n$ l'ensemble des points dont la période primitive est égale à n. Notons $\pi(n)$ le cardinal de $\mathcal{T}_n$. Notons enfin $\mathcal{U}_n$ l'ensemble des points dont la période primitive divise n.

Nous avons déjà déterminé le cardinal de $\mathcal{U}_n$, qui est 2^n. Remarquons maintenant que

$$\mathcal{U}_n = \bigcup_{d|n} \mathcal{T}_d$$

où la réunion porte sur tous les diviseurs d de n. De plus, cette réunion est disjointe, donc

$$|\mathcal{U}_n| = \sum_{d|n} |\mathcal{T}_d|$$

ou encore

$$2^n = \sum_{d|n} \pi(d)$$

La fonction π et la fonction $n \longmapsto 2^n$ sont donc intimement reliées. Il existe de nombreux couples de fonctions vérifiant une égalité du type ci-dessus, et il s'avère qu'il existe une formule qui permet *d'inverser* cette relation, c'est à dire d'obtenir explicitement $\pi(n)$. Il s'agit de la *formule d'inversion de Möbius.* On obtient grâce à cette formule que

$$\pi(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) 2^d$$

où μ est la *fonction de Möbius*, définie sur $\mathbb{N}^*$ comme suit.

- $\mu(1) = 1$.
- Pour tout $n \geq 2$ produit de k nombres premiers distincts, $\mu(n) = (-1)^k$.
- Pour tout $n \geq 2$ divisible par le carré d'un nombre premier, $\mu(n) = 0$.

Voici les premières valeurs de la fonction de Möbius.

n	1	2	3	4	5	6	7	8	9	10	11	12
$\mu(n)$	1	-1	-1	0	-1	1	-1	0	0	1	-1	0

Voici maintenant les premières valeurs de $\pi(n)$. On donne aussi dans le tableau la valeur de 2^n.

n	1	2	3	4	5	6	7	8	9	10	11	12
$\pi(n)$	2	2	6	12	30	54	126	240	504	990	2046	4020
2^n	2	4	8	16	32	64	128	256	512	1024	2048	4096

Le tableau ci-dessus montre que $\pi(n)$ semble « proche »de 2^n. Nous allons effectivement montrer que lorsque n tend vers $+\infty$, $\pi(n) \sim 2^n$.

5.3 Quelques cas particuliers

Histoire de manipuler un peu la formule donnant $\pi(n)$, regardons quelques cas particuliers. Ils couvrent en fait tous les entiers $n \in [\![1, 59]\!]$.

Supposons que $n = p^\alpha$ où p est un nombres premier et $\alpha \geq 1$. Les diviseurs de n sont $1, p, p^2, \ldots, p^\alpha$. Si $k \geq 2$, on a $\mu(p^k) = 0$. Ainsi,

$$\pi(n) = 2^n - 2^{\frac{n}{p}}$$

En particulier, pour tout nombre premier p, $\pi(p) = 2^p - 2$.

Supposons maintenant que $n = p^\alpha q^\beta$ où p et q sont deux nombres premiers distincts et $\alpha, \beta \geq 1$. Les diviseurs de n qui n'annulent pas la fonction μ sont 1, p, q et pq. On a donc

$$\pi(n) = 2^n - 2^{\frac{n}{p}} - 2^{\frac{n}{q}} + 2^{\frac{n}{pq}}$$

En particulier,

$$\pi(pq) = 2^{pq} - 2^p - 2^q + 2$$

Le plus petit entier qui ne soit pas des deux formes étudiées est $n = 30 = 2\times3\times5$. Les diviseurs de 30 sont

- 1, en lequel μ vaut 1.
- 2, 3, 5, en lesquels μ vaut -1.
- 6, 10, 15, en lesquels μ vaut 1.
- 30, en lequel μ vaut -1.

On a donc

$$\pi(30) = 2^{30} - 2^{15} - 2^{10} - 2^6 + 2^5 + 2^3 + 2^2 - 2^1 = 107370810$$

Plus généralement, si p, q, r sont trois nombres premiers distincts,

$$\pi(pqr) = 2^{pqr} - 2^{pq} - 2^{qr} - 2^{pr} + 2^p + 2^q + 2^r - 2$$

Le plus petit entier qui n'est pas de l'une des formes que nous avons étudiées est $2^2 \times 3 \times 5 = 60$. Pour les amateurs,

$$\pi(60) = 1152921503532053580$$

5.4 Le comportement à l'infini de $\pi(n)$

Pour tout $n \geq 1$, posons $\varphi(n) = 2^n - \pi(n)$. Remarquons que comme $\pi(n) \leq 2^n$, on a $\varphi(n) \geq 0$. Commençons par un encadrement simple qui nous donnera immédiatement un équivalent de $\pi(n)$.

Proposition 14. *Pour tout $n \geq 2$,*

$$1 \leq \frac{\varphi(n)}{2^{\frac{n}{p}}} < 2$$

où p est le plus petit diviseur premier de n.

Démonstration. Les diviseurs de n différents de n sont tous inférieurs ou égaux à $\frac{n}{p}$. On a donc

$$\varphi(n) = -\sum_{d|n, d \leq \frac{n}{p}} \mu\left(\frac{n}{d}\right) 2^d$$

De là,

$$\begin{aligned} \varphi(n) &\leq \sum_{d=1}^{\frac{n}{p}} 2^d \\ &= 2 \times 2^{\frac{n}{p}} - 2 \\ &< 2 \times 2^{\frac{n}{p}} \end{aligned}$$

Minorons maintenant $\varphi(n)$. Parmi les points de période n, on trouve les points de période $\frac{n}{p}$. On a donc

$$2^n - \varphi(n) = \pi(n) \leq 2^n - 2^{\frac{n}{p}}$$

De là,

$$\varphi(n) \geq 2^{\frac{n}{p}}$$

□

Corollaire 15. *Si p est le plus petit diviseur premier de n, alors*

$$\varphi(n) = \Theta\left(2^{\frac{n}{p}}\right) = o\left(2^n\right)$$

Démonstration. Par la proposition précédente, la première égalité est claire. De plus, $p \geq 2$, et donc

$$0 \leq \varphi(n) \leq 2 \times 2^{\frac{n}{2}} = 2\sqrt{2^n} = o\left(2^n\right)$$

□

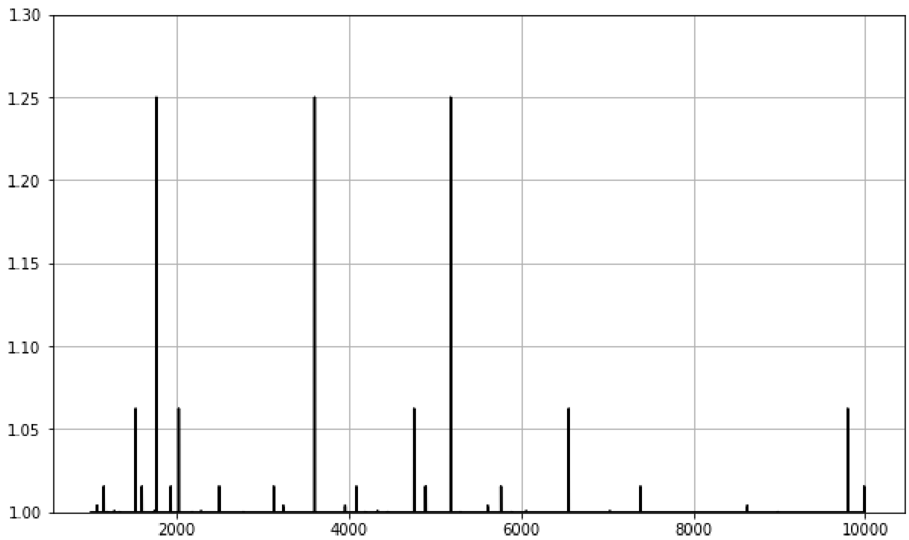
Corollaire 16. $\pi(n) \sim 2^n$.

Ce résultat montre que la « plupart » des points de période n sont en fait de période primitive n.

Dans la fin de cet article, nous allons estimer de façon plus fine la quantité $\varphi(n)$.

5.5 Des résultats plus fins

Voici le graphe, pour $n \in [\![1000, 10000]\!]$, de $\frac{\varphi(n)}{2^{\frac{n}{p}}}$ en fonction de n, où p est le plus petit diviseur premier de n.



À quoi correspondent les trois pics de hauteur $\frac{5}{4}$ (environ) ? Il sont obtenus pour $1763 = 41 \times 43$, $3599 = 59 \times 61$ et $5183 = 71 \times 73$. Ces trois entiers sont des produits de deux *nombres premiers jumeaux*, c'est à dire deux nombres premiers dont la différence est égale à 2.

Proposition 17. *Soient $p, q = p+2$ deux nombres premiers jumeaux. Soit $n = pq$. On a*

$$\varphi(n) = \frac{5}{4} 2^{\frac{n}{p}} - 2$$

Démonstration.

$$\begin{aligned}\varphi(n) &= 2^p + 2^q - 2 \\ &= 2^{q-2} + 2^q - 2 \\ &= \frac{5}{4}2^q - 2 \\ &= \frac{5}{4}2^{\frac{n}{p}} - 2\end{aligned}$$

□

À l'heure où cet article est écrit, on ne sait pas s'il existe une infinité de couples de nombres premiers jumeaux. Dans l'hypothèse où ce serait le cas, le quotient $\frac{\varphi(n)}{2^{\frac{n}{p}}}$ peut donc être rendu aussi proche que voulu de $\frac{5}{4}$.

Montrons maintenant que la constante $\frac{5}{4}$ convient pour tous les entiers $n \geq 2$.

Si $n = p^\alpha$ est une puissance d'un nombre premier, alors

$$\varphi(n) = 2^{\frac{n}{p}} \leq \frac{5}{4}2^{\frac{n}{p}}$$

Regardons maintenant ce qui se passe si n possède exactement deux diviseurs premiers.

Lemme 18. *Soit $n \geq 2$ possédant exactement deux diviseurs premiers $p < q$. On a*

$$\varphi(n) \leq \frac{5}{4}2^{\frac{n}{p}} - 2$$

Démonstration. On a

$$\varphi(n) = 2^{\frac{n}{p}} + 2^{\frac{n}{q}} - 2$$

Regardons tout d'abord le cas particulier $p = 2$, $q = 3$. Si $n = 6$, alors

$$\varphi(n) = 10 = \frac{5}{4}2^3$$

Si $n > 6$, alors $n \geq 12$ et donc

$$2^{\frac{n}{2} - \frac{n}{3}} = 2^{\frac{n}{6}} \geq 4$$

d'où

$$2^{\frac{n}{3}} \leq \frac{1}{4}2^{\frac{n}{2}}$$

De là,

$$\varphi(n) = 2^{\frac{n}{2}} + 2^{\frac{n}{3}} - 2 \leq \frac{5}{4}2^{\frac{n}{2}} - 2$$

Supposons maintenant que $(p, q) \neq (2, 3)$. On a alors $q - p \geq 2$. En remarquant que $n \geq pq$, il vient

$$2^{\frac{n}{p} - \frac{n}{q}} = 2^{\frac{n(q-p)}{pq}} \geq 2^{q-p} \geq 4$$

De là,

$$\varphi(n) = 2^{\frac{n}{p}} + 2^{\frac{n}{q}} - 2 \leq \frac{5}{4} 2^{\frac{n}{p}} - 2$$

□

Regardons enfin le cas où n possède au moins trois diviseurs premiers. Établissons deux lemmes.

Lemme 19. *Soient $n \geq 2$. Supposons que n possède r diviseurs premiers $p = p_1 < \ldots < p_r$, où $r \geq 3$. Alors,*

$$\sum_{k=1}^{r} 2^{\frac{n}{p_k}} \leq \frac{8}{7} 2^{\frac{n}{p}}$$

Démonstration. Le multiplicateur $\frac{8}{7}$ est en fait largement surestimé, mais il nous suffira. On a

$$\sum_{k=1}^{r} 2^{\frac{n}{p_k}} = 2^{\frac{n}{p_1}} \sum_{k=1}^{r} 2^{\frac{n(p_1 - p_k)}{p_1 p_k}}$$

Pour tout $k \in [\![1, r]\!]$,

$$\frac{p_k - p_1}{p_1 p_k} \geq \frac{k-1}{p_1 p_r}$$

De là,

$$\begin{aligned}
\sum_{k=1}^{r} 2^{\frac{n(p_1 - p_k)}{p_1 p_k}} &\leq \sum_{k=1}^{r} 2^{\frac{-n(k-1)}{p_1 p_r}} \\
&= \sum_{k=1}^{r} \left(2^{-\frac{n}{p_1 p_r}}\right)^{k-1} \\
&= \frac{1 - \left(2^{-\frac{n}{p_1 p_r}}\right)^{r}}{1 - 2^{-\frac{n}{p_1 p_r}}} \\
&< \frac{1}{1 - 2^{-\frac{n}{p_1 p_r}}}
\end{aligned}$$

Remarquons maintenant que

$$\frac{n}{p_1 p_r} \geq p_2 \geq 3$$

On a donc

$$\frac{1}{1 - 2^{-\frac{n}{p_1 p_r}}} \leq \frac{1}{1 - 2^{-3}} = \frac{8}{7}$$

Ainsi,

$$\sum_{k=1}^{r} 2^{\frac{n}{p_k}} \leq \frac{8}{7} 2^{\frac{n}{p_1}}$$

□

Lemme 20. *Soit $n \geq 2$. Soient $p_1, \ldots, p_r$ les diviseurs premiers de n. On a*

$$\varphi(n) \leq \sum_{k=1}^{r} 2^{\frac{n}{p_k}}$$

Démonstration. Rappelons les notations vues au tout début de cette section. Pour tout $n \geq 1$, $\mathcal{U}_n$ est l'ensemble des points de $[0,1]$ de période n et $\mathcal{T}_n$ est l'ensemble des points de $[0,1]$ de période *primitive* n.

Soit $x \in [0,1]$. x est de période primitive n si et seulement si il est de période n, mais n'est pas de période $\frac{n}{p_k}$, ceci pour tout $k \in [\![1, r]\!]$. Ainsi,

$$\mathcal{T}_n = \mathcal{U}_n \setminus \bigcup_{k=1}^{r} \mathcal{U}_{\frac{n}{p_k}}$$

De là, en passant aux cardinaux,

$$\pi(n) = 2^n - \left| \bigcup_{k=1}^{r} \mathcal{U}_{\frac{n}{p_k}} \right|$$

Il reste à remarquer que

$$\left| \bigcup_{k=1}^{r} \mathcal{U}_{\frac{n}{p_k}} \right| \leq \sum_{k=1}^{r} \left| \mathcal{U}_{\frac{n}{p_k}} \right| = \sum_{k=1}^{r} 2^{\frac{n}{p_k}}$$

Ainsi,

$$\pi(n) = 2^n - \varphi(n) \geq 2^n - \sum_{k=1}^{r} 2^{\frac{n}{p_k}}$$

d'où le résultat. □

En rassemblant les résultats précédents, nous obtenons donc la proposition ci-dessous.

Proposition 21. *Soit $n \geq 2$. Soit p le plus petit diviseur premier de n. On a*

$$2^{\frac{n}{p}} \leq \varphi(n) \leq \frac{5}{4} 2^{\frac{n}{p}}$$

Pour conclure, pour tout $n \geq 2$, en notant p le plus petit diviseur premier de n, on a les bornes optimales

$$\boxed{2^n - \frac{5}{4} 2^{\frac{n}{p}} \leq \pi(n) \leq 2^n - 2^{\frac{n}{p}}}$$