Fractions en folie !

Gaëtan Bayle des Courchamps

3 septembre 2002
(révision 20 Juillet 2011)

Table des matières

1 Période de fractions

1.1 Introduction

Le problème posé est en soi tout simple : Il est bien connu que les décimales de toute fraction $\frac{p}{q}$ se répètent périodiquement. Mais quelle est la période des décimales d'une fraction $\frac{p}{q}$ dans une base de numération b donnée ?
Par exemple pour $\frac{22}{7} = 3,1428571428...$, la séquence 142857 se répète, donc on peut dire que la période de $\frac{22}{7}$ est 6 en base 10 (c'est 3 en base 2 et 2 en base 6 ...)

1.2 Formalisation

Nous commencerons par montrer que les décimales d'une fraction quelconque sont bien périodiques, et que la période est exactement celle des restes obtenus quand on pose la division à la main.
Le dernier résultat, lui, donne une caractérisation simple de la période d'une fraction, que nous utiliserons amplement dans les sections suivantes.

Lemme 1.1 (Périodicité des décimales) *Soit une fraction p/q. On note $(a_i)_{i\in\mathbf{N}}$ la suite de ses décimales dans une base b fixée, et $(r_i)_{i\in\mathbf{N}}$ la suite des restes obtenus en procédant à la division de p par q.*
Alors les suites (a) et (r) sont périodiques à partir d'un certain rang, la période P de (r) est supérieure ou égale à celle de (a) et vérifie $P \leq q$.

Preuve : L'algorithme de la division euclidienne donne :

$$\begin{aligned} a_{n+1} &= \left\lfloor \frac{br_n}{q} \right\rfloor \\ r_{n+1} &= br_n \mod q \end{aligned}$$

avec pour conditions initiales :

$$\begin{cases} a_0 &= \left\lfloor \frac{p}{q} \right\rfloor \\ r_0 &= p \bmod q \end{cases}$$

Le développement décimal de p/q commence à partir du rang 1 de la suite (a). Une récurrence immédiate sur n montre, pour tout $n \geq 1$, l'encadrement $0 \leq r_n < q$, qui couvre q valeurs distinctes. Donc il existe deux indices n_0 et n_1, avec $0 < n_1 - n_0 \leq q$, tels que $r_{n_0} = r_{n_1}$. Posons alors $P_0 = n_1 - n_0$. Une simple récurrence sur n montre que, pour tout $n \geq n_0$, $r_{n+P_0} = r_n$.
La suite (r) est donc périodique à partir d'un certain rang. Notons P sa période la plus petite.
Alors $P \leq P_0$, et la relation de récurrence de (a) permet d'en déduire que, pour tout $n \geq n_0 + 1$, $a_{n+P} = a_n$.
Donc (a), comme (r), est périodique à partir d'un certain rang. CQFD. ∎

Lemme 1.2 (Égalité des périodes des décimales et des restes) *Soit une fraction p/q. On note $(a_i)_{i\in\mathbf{N}}$ la suite des decimales de cette fraction, dans une base b fixée. Notons de même $(r_i)_{i\in\mathbf{N}}$ la suite des restes obtenus en procédant à la division de p par q dans la base b.*
Alors les suites a et r sont périodiques à partir d'un certain rang, et leurs périodes sont indentiques.

Preuve : Soit n_0 le rang à partir duquel la suite des décimales (a) devient périodique, et notons P sa prériode.
Posons alors, pour tout $n \in \mathbf{N}$, $\Delta_n = r_{n+P} - r_n$. D'autre part, par définition de la suite des restes :

$$\begin{aligned} r_{n+1} &= r_n b - a_{n+1} q \\ r_{n+P+1} &= r_{n+P} b - a_{n+P+1} q \end{aligned}$$

Pour $n \geq n_0$, on a $a_{n+1} = a_{n+P+1}$, donc en soustrayant membre à membre les deux expressions, on obtient :

$$\Delta_{n+1} = b\Delta_n$$

Supposons à présent que les périodes de (a) et de (r) soient différentes. Alors, comme la période des restes est supérieure ou égale à celle des décimales, il existe $n_1 \geq n_0$, tel que $r_{n_1+P} \neq r_{n_1}$, c'est-à-dire : $\Delta_{n_1} \neq 0$.
La relation ci-dessus montre alors que, pour $n \in \mathbf{N}$, $\Delta_{n+n_1} = b^n \Delta_{n_1}$ tend vers l'infini (en valeur absolue).
Or Δ est une différence de restes, et ces restes, positifs, sont bornés par q, donc Δ devrait être bornée, en valeur absolue, par q.
C'est une contradiction flagrante, donc la période des restes et celle des décimales sont exactement les mêmes. CQFD. ∎

Théorème 1.3 (Caractérisation de la période et formule des restes) *Dans la division euclidienne de p par q en bas b, le reste r_n d'indice n est :*

$$r_n = pb^n \mod q$$

De plus, un entier $n \geq 1$ est une période de la fraction $\frac{p}{q}$ en base b si et seulement s'il existe un entier $N \geq 0$ tel que $pb^{N+n} \equiv pb^N \quad [q]$.

Preuve : L'algorithme de la division euclidienne donne $\begin{cases} r_0 &= p &\pmod q \\ r_{n+1} &= br_n &\pmod q \end{cases}$ ce qui donne par récurrence sur $n \geq 0$: $r_n = pb^n \bmod q$, donc le premier point du lemme est montré.
Le lemme précédent nous dit que la période des décimales de $\frac{p}{q}$ et celle des restes de la division de p par q sont identiques.
Or, à p, q et b fixés, le terme r_{n+1} ne dépend que de r_n. Donc il faut et il suffit que deux termes de la suite (r) soient égaux pour que la différence de leurs indices soit une période de (r).
En d'autres termes, un entier n est une période de (r) (et de $\frac{p}{q}$) si et seulement s'il existe un entier $N \geq 0$ tel que $r_{N+n} = r_N$, ce qui revient à $pb^{N+n} \bmod q = pb^N \bmod q$. En d'autres termes : $pb^{N+n} \equiv pb^N \pmod q$. CQFD. ∎

1.3 Un lemme utile

Le petit lemme de cette section jouera un rôle capital dans la solution du problème.

Lemme 1.4 (Lemme de division) *Soient deux entiers a et p. Si a et p sont premiers entre eux, alors :*

$$\forall (x,y) \in \mathbf{Z} \times \mathbf{Z}, \quad (x \equiv y \quad [a]) \Longleftrightarrow (px \equiv py \quad [a])$$

Preuve : Preuve : ($\Longrightarrow$) : Supposons $x \equiv y \quad [a]$. Multiplions par p. Alors $px \equiv py \quad [pa]$ et, en particulier, $px \equiv py \quad [a]$.
($\Longleftarrow$) : Réciproquement, si $px \equiv py \quad [a]$, alors $p(x-y)$ divise a. Or p est premier avec a, donc d'après le théorème de Gauss, $(x-y)$ divise a. Ceci équivaut à $x \equiv y \quad [a]$. CQFD. ∎

1.4 Simplification du problème

Le dernier résultat de la section des généralités permet de se ramener à l'étude des périodes de la suite des restes de la division de p par q.

Dans la suite de cette section, les décompositions en facteurs premiers vont nous être d'un grand secours. En effet, elles nous permettront d'abord d'éliminer le numérateur p de nos préoccupations, et de nous ramener ainsi au cas particulier $\frac{1}{q}$, où q et b sont premiers entre eux.
Nous serons alors en mesure de calculer simplement la période de $\frac{1}{q}$ en nous servant de la décomposition de q en facteurs premiers.

Lemme 1.5 (caractérisation de la période pour cas simple) *Soit un entier q_0 premier avec la base de numération b, et soit un entier $n \geq 1$. Alors :*

$$n \text{ est une période de } \tfrac{1}{q_0} \quad \Longleftrightarrow \quad b^n \equiv 1 \quad [q_0]$$

Preuve : On sait que n est une période de $\frac{1}{q_0}$ si et seulement s'il existe $N \geq 0$ tel que $b^{N+n} \equiv b^N \quad [q_0]$. Or $b \wedge q_0 = 1$, donc $b^N \wedge q_0 = 1$ et le lemme de division 1.4 nous dit que cette condition équivaut à $b^n \equiv 1 \quad [q_0]$. CQFD. ∎

Théorème 1.6 (pour se ramener au cas $\frac{1}{q_0}$ avec $q_0 \wedge b = 1$) *Soit une fraction $\frac{p}{q}$ où p et q sont deux entiers premiers entre eux. Ecrivons :*

$$\frac{p}{q} = \frac{p}{Mq_0}$$

En mettant dans M tous les facteurs premiers que q a en commun avec b. Ainsi q_0 est premier avec b. Alors la période de $\frac{p}{q}$ est de même longueur que celle de $\frac{1}{q_0}$.

Preuve : Ceci revient à montrer qu'un entier $n \geq 1$ est une période de $\frac{p}{q}$ si et seulement si $b^n \equiv 1 \quad [q_0]$.

Supposons que n soit une période de $\frac{p}{q}$. Alors il existe un entier $N \geq 0$ tel que $pb^{N+n} \equiv pb^N \quad [q]$.
Comme $p \wedge q = 1$, ceci revient (d'après le lemme de division) à $b^{N+n} \equiv b^N \quad [q]$.
Comme $q = Mq_0$, c'est encore équivalent à $b^N(b^n - 1) \equiv 0 \quad [Mq_0]$.
La relation de Bezout nous indique que b et $b^n - 1$ sont premiers entre eux. Comme par construction les facteurs premiers de M sont aussi des facteurs de b, on en déduit que $M \wedge (b^n - 1) = 1$. Le théorème de Gauss permet d'en déduire que M divise b^N. On peut donc poser $\alpha = \frac{b^N}{M}$.
Alors $M\alpha b^n \equiv M\alpha \quad [Mq_0]$, soit encore $\alpha b^n \equiv \alpha \quad [q_0]$. Or par construction les facteurs premiers de α sont des facteurs de b, donc $\alpha \wedge q_0 = 1$. On invoque alors de nouveau le lemme de division pour conclure victorieusement que $b^n \equiv 1 \quad [q_0]$ i.e. que n est une période de $\frac{1}{q_0}$.

Réciproquement, supposons $b^n \equiv 1 \quad [q_0]$. Soit N le plus grand exposant dans la décomposition de M en facteurs premiers. Alors $\alpha = \frac{b^N}{M}$ est un entier, et $\alpha b^n \equiv \alpha \quad [q_0]$.
En multipliant le tout par M et en se rappelant que $q = Mq_0$ et que $M\alpha = b^N$, on obtient $b^{N+n} = b^N \quad [q]$.
A fortiori $pb^{N+n} = pb^N \quad [q]$.
n est donc bien une période de $\frac{p}{q}$, ce qui termine la démonstration de l'équivalence. CQFD. ∎

Lemme 1.7 (Utilité de la décomposition en facteurs) *Soient q_0 et q_1 deux entiers premiers entre eux, et soit b une base de numération première avec q_0 et q_1.*
Alors un entier $n \geq 1$ est une période de $\frac{1}{q_0 q_1}$ si et seulement s'il est multiple commun des plus petites périodes de $\frac{1}{q_0}$ et de $\frac{1}{q_1}$ en base b.

Preuve : Tout d'abord, remarquons que $q_0 q_1$ est premier avec b et qu'en conséquence un entier n est période de $\frac{1}{q_0 q_1}$ si et seulement si $b^n \equiv 1 \quad [q_0 q_1]$.
Si c'est le cas, alors on a immédiatement $b^n \equiv 1 \quad [q_0]$ et $b^n \equiv 1 \quad [q_1]$. Donc n, période de $\frac{1}{q_0}$, est multiple de sa plus petite période. Il est de même multiple de la (plus petite) période de $\frac{1}{q_1}$.
Réciproquement, si n est un multiple commun des plus petites périodes de $\frac{1}{q_0}$ et $\frac{1}{q_1}$, c'est une période de ces deux fractions, donc $b^n \equiv 1 \quad [q_0]$ et $b^n \equiv 1 \quad [q_1]$. Alors il existe deux entiers α et β tels que $\begin{cases} b^n = 1 + \alpha q_0 \\ b^n = 1 + \beta q_1 \end{cases}$ En particulier, $\alpha q_0 = \beta q_1$. Or $q_0 \wedge q_1 = 1$, donc il existe un entier γ tel que $\alpha = \gamma q_1$.
Alors $b^n = 1 + \gamma q_1 q_0$, d'où $b^n \equiv 1 \quad [q_0 q_1]$.
Donc n est bien une période de $\frac{1}{q_0 q_1}$, et l'équivalence est démontrée. CQFD. ∎

Remarque : En particulier, la (plus petite) période de $\frac{1}{q_0 q_1}$ est le plus petit multiple commun de celles de $\frac{1}{q_0}$ et $\frac{1}{q_1}$.

1.5 Le cas $\frac{1}{q^n}$, avec q premier et premier avec b

La section précédente nous conduit tout naturellement à calculer la période des fractions de la forme $\frac{1}{q^n}$, où q est un nombre premier qui est aussi premier avec la base b.

Lemme 1.8 (La période de $\frac{1}{q}$ divise $\rho(q)$) *Si q est premier avec b (et p), alors la periode des decimales de p/q est l'ordre du groupe multiplicatif généré par b dans le groupe des éléments inversibles de $\mathbf{Z}/q\mathbf{Z}$.*
En particulier, cette période est un diviseur de $\rho(q)$, et elle est indépendante du numérateur p.

Preuve : Notons $U(\mathbf{Z}/q\mathbf{Z})$ l'ensemble des éléments inversibles de $\mathbf{Z}/q\mathbf{Z}$. Les relations de récurrence qui définissent (r) donnent $r_i = pb^i \mod q$. Soit i_0 l'indice à partir duquel la suite des restes est périodique, et soit P cette période (qui est aussi celle des décimales). Les relations suivantes sont alors équivalentes :

$$\begin{array}{rcll} r_{i_0+P} & = & r_{i_0} & \\ pb^{i_0+P} & \equiv & pb^{i_0} \quad [q] & \text{formule des restes} \\ b^{i_0+P} & \equiv & b^{i_0} \quad [q] & \text{car } p \wedge q = 1 \\ b^P & \equiv & 1 \quad [q] & \text{car } b^{i_0} \wedge q = 1 \end{array}$$

Or P est par définition le plus petit nombre entier non nul respectant la première relation. Comme les trois relations sont équivalentes, c'est aussi le plus petit entier naturel non nul vérifiant la dernière relation. On reconnaît la définition de l'ordre du groupe multiplicatif généré par b dans le groupe $U(\mathbf{Z}/q\mathbf{Z})$ (comme $q \wedge b = 1$, q fait bien partie de ce groupe).
On remarque au passage que la dernière relation ne fait pas intervenir p, et que la période P est par conséquent indépendante de p.

Or, le groupe généré par b étant un sous-groupe de $U(\mathbf{Z}/q\mathbf{Z})$, son ordre divise celui de $U(\mathbf{Z}/q\mathbf{Z})$ qui, par définition de l'indicateur d'Euler, est $\rho(q)$.

Enfin la dernière relation ne fait plus intervenir i_0. Donc n'importe quel $i_0 \in \mathbf{N}$ convient, et en particulier 0. La suite des décimales est donc périodique au moins à partir de la $(i_0 + 1)$-ième, c'est-à-dire la première. Comme il n'y a pas de décimale avant la première, c'est à partir de la première décimale exactement que la suite des décimales est périodique.CQFD. ∎

Lemme 1.9 *Soit une base de numération b fixée, et soit q un entier naturel positif premier avec b.*
Notons, p la période des décimales de $\frac{1}{q}$.
Supposons qu'il existe un entier positif α tel que $b^\alpha \equiv 1 [q]$. Alors p divise α.

Preuve : Comme b et q sont premier entre eux, p est le plus petit élément de $\left\{k \in \mathbf{N}^*, b^k \equiv 1[q]\right\}$. Procédons à la division euclidienne de α par p. Alors il existe un coupe d'entiers (β, r) tel que :

$$\left\{\begin{array}{lcl} \alpha & = & \beta p + r \\ r & \geq & 0 \\ r & < & p \end{array}\right.$$

Alors $b^\alpha \equiv b^{\beta p+r} \equiv b^r[q]$. Comme p est le plus petit entier strictement positif qui possède cette propriété et comme $r < p$, r ne peut pas être strictement positif. La seule possibilité qui reste est donc $r = 0$, ce qui donne $\alpha = \beta p$. CQFD. ∎

Lemme 1.10 *Soit une base de numération b et un entier naturel positif q premier avec b. Notons, pour tout entier positif n, p_n la période des décimales de $\frac{1}{q^n}$ en base b.*
Alors pour tout $n \in \mathbf{N}$, p_{n+1} est multiple de p_n.

Preuve : Comme q est premier avec b, on a $b^{p_{n+1}} \equiv 1[q^{n+1}]$. A fortiori, on a $b^{p_{n+1}} \equiv 1[q^n]$. On applique alors le lemme précédent qui nous donne $p_n | p_{n+1}$. CQFD. ∎

Lemme 1.11 *Soit q un nombre premier, qui soit aussi premier avec la base de numération b. Pour tout entier $n \in \mathbf{N}^*$, notons p_n la longueur de la période des décimales de $\frac{1}{q^n}$ en base b.*
Alors $p_{n+1} = p_n$ ou $p_{n+1} = qp_n$.
Plus précisément, si $p_{n+1} = qp_n$ et $((n \geq 1$ et $q \geq 3)$ ou $n \geq 2)$, alors $p_{n+2} = qp_{n+1}$.

Preuve : Comme q est premier avec b, on sait que p_n divise p_{n+1}. Donc il existe $k \in \mathbf{N}$ tel que $p_{n+1} = kp_n$. D'autre part, $b^{p_n} \equiv 1[q^n]$ donc il existe un entier a tel que $b^{p_n} = 1 + aq^n$. Alors :

$$\begin{array}{rcl} b^{p_{n+1}} & = & b^{kp_n} \\ & = & \left(b^{p_n}\right)^k \\ & = & \left(1 + aq_n\right)^k \\ & = & \sum_{i=0}^{k} \mathcal{C}_k^i \left(aq^n\right)^i \\ b^{p_{n+1}} & = & 1 + kaq^n + \sum_{i=2}^{k} \mathcal{C}_k^i a^i q^{ni} \end{array}$$

Or, pour $n \geq 1$ et $i \geq 2$, on a $n + 1 \leq ni$, donc la somme est multiple de q^{n+1}, ce qui nous donne :

$$\begin{array}{rcll} \left(b^{p_{n+1}} \equiv 1[q^{n+1}]\right) & \Longleftrightarrow & \left(kaq^n \equiv 0 \quad [q^{n+1}]\right) \\ & \Longleftrightarrow & \left(ka \equiv 0 \quad [q]\right) \end{array}$$

Comme $p_{n+1} = kp_n$, k doit être le plus petit possible. Deux cas se présentent alors : Si a n'est pas premier avec q, alors a est multiple de q puisque q est premier, ce qui fait que $k = 1$ suffit. Comme c'est le plus petit k possible, on a alors $p_{n+1} = p_n$
Si a est premier avec q, alors k doit être multiple de q. Le plus petit multiple de q supérieur à 1 étant q, on a donc $k = q$ et par conséquent $p_{n+1} = qp_n$.
On a donc démontré le premier résultat du lemme.
Montrons le second résultat. Le cas $p_{n+1} = qp_n$ correspond à $k = q$, donc notre dernière expression de $b^{p_{n+1}}$ donne :

$$\begin{array}{rcl} b^{p_{n+1}} & = & 1 + aq^{n+1} + \sum_{i=2}^{q} \mathcal{C}_q^i a^i q^{ni} \\ & = & 1 + \left(a + \sum_{i=2}^{q} \mathcal{C}_q^i a^i q^{ni-(n+1)}\right) q^{n+1} \end{array}$$

Si $n \geq 2$, alors pour $i \geq 2$, $ni - (n + 1) \geq 1$, donc la somme est multiple de q et, comme a est premier avec q, le total de ce qui est dans la parenthèse est premier avec q. Donc $b^{p_{n+1}}$ est de la forme $1 + \alpha q^{n+1}$, où α est premier avec q. Il n'y a plus qu'à recommencer la démonstration du premier point pour aboutir à $p_{n+2} = qp_{n+1}$.
Si $q \geq 3$ et $n \geq 1$, alors pour $i = 2$ on a $\mathcal{C}_q^i = \frac{q(q-1)}{2}$. Comme q est un nombre premier supérieur ou égal à trois, q est impair, donc $\frac{q-1}{2}$ est entier et par conséquent $\mathcal{C}_q^i$ est multiple de q. D'autre part, pour $i \geq 3$, $ni - (n + 1) \geq 1$. Alors, de même que ci-dessus, le contenu de la parenthèse est premier avec q, donc en recommençant la démonstration à partir du premier point, on obtient là encore $p_{n+2} = qp_{n+1}$.
Les deux points du lemme sont donc démontrés. CQFD. ∎

1.6 Formule générale de la période d'une fraction

A présent nous pouvons mettre à profit les résultats des sections précédentes pour aboutir à une formule générale de la période d'une fraction.

Définition 1.12 (Fonction ϕ) *Supposons fixée la base de numération b. Soit un entier $q \geq 1$.*
On note alors $\phi(q)$ la période de la fraction $\frac{1}{q}$ en base b.

Théorème 1.13 (Expression de $\phi(q^n)$ en fonction de $\phi(q)$ pour q premier et $q \wedge b = 1$) *La base de numération b étant fixée, soit q un nombre premier et premier avec b, et soit un entier $n \geq 1$.*
Posons $\begin{cases} n_q(b) = \max\left\{k \geq 1 \mid b^{\phi(q)} \equiv 1 \pmod{q^k}\right\} & \text{si } q \geq 3 \text{ ou } (q = 2 \text{ et } q \equiv 1 \pmod 4) \\ n_2(b) = \max\left\{k \geq 2 \mid b^2 \equiv 1 \pmod{q^k}\right\} & \text{si } b \equiv 3 \pmod 4 \end{cases}$ *Alors :*

- *Si $q \geq 3$ ou $q \equiv 1 \pmod 4$ alors* $\phi(q^n) = \begin{cases} \phi(q) & \text{si } n \leq n_q(b) \\ \phi(q)q^{n-n_q(b)} & \text{si } n > n_q(b) \end{cases}$
- *Si $q = 2$ et $b \equiv 3 \pmod 4$ alors* $\phi(2^n) = \begin{cases} 1 & \text{si } n = 1 \\ 2 & \text{si } 1 < n \leq n_2(b) \\ 2 \times 2^{n-n_2(b)} & \text{si } n > n_2(b) \end{cases}$

Remarque : Pour le cas $q = 2$, on ne considère pas les cas où b est pair, puisqu'il est censé être premier avec q.
Preuve : Ces résultats ne sont que des conséquences simples du dernier lemme (1.11) de la section qui précède. L'aspect fastidieux de la démonstration vient de ce qu'il faut distinguer plusieurs cas.
Commençons par le cas $q \geq 3$ ou ($q = 2$ et $b \equiv 1 \pmod 4$). Posons $A = \left\{k \geq 1 \mid b^{\phi(q)} \equiv 1 \pmod{q^k} \text{ ou } k = 1\right\}$.
Alors A est non-vide puisque par définition de $\phi(q)$, et comme $q \wedge b = 1$, on a $b^{\phi(q)} \equiv 1 \pmod q$. A est de plus majorée. En effet, il existe $k_0 \geq 1$ tel pour tout $k \geq k_0$, on a $q^k \geq b^{\phi(q)}$ et en particulier $b^{\phi(q)} \not\equiv 1 \pmod{q^k}$ donc $k \notin A$.
Alors $n_q(b)$ existe en tant que maximum d'un ensemble majoré non vide d'entiers.
Par définition de $n_q(b)$, $\phi(q^{n_q(b)}) \leq \phi(q)$. Or le lemme 1.10 impose que $\phi(q^n)$ croisse avec n, donc pour tout $n \leq n_q(b)$, $\phi(q^n) = \phi(q)$.
Qu'en est-il pour $n > n_q(b)$?. Par définition de n_q on a $\phi(q^{n_q+1}) > \phi(q^{n_q})$. Si $q \geq 3$, le lemme 1.11 impose alors $\phi(q^{n_q+1}) = q\phi(q^{n_q})$, il permet de conclure par récurrence sur n.
Si $q = 2$, comme $b \equiv 1 \pmod 4$, on a $n_2(b) \geq 2$ donc $n \geq 2$; on peut alors, comme précédemment, appliquer le lemme 1.11 et conclure de même par récurrence sur n.
Reste le cas $q = 2$ avec $b \equiv 3 \pmod 4$. Alors $b \equiv 1 \pmod 2$ donc $\phi(2) = 1$.
Comme $b \not\equiv 1 \pmod 4$ et $b^2 \equiv 1 \pmod{2^2}$, $\phi(2^2) = 2$.
De même qu'au cas $q \geq 3$ on montre que $n_2(b)$ existe (il suffit de remplacer $\phi(q)$ par 2).
Par définition de $n_2(b)$, on a $\phi(q^{n_2(b)}) \leq 2$ donc le lemme 1.10 dit que pour n compris entre 2 et $n_2(b)$, on a $\phi(q^n) = \phi(q^2)$.
De même qu'au cas $q = 2$ avec $b \equiv 1 \pmod 4$, le lemme 1.11 permet de conclure si $n > n_2(b)$. ∎
Remarque : Il reste le problème du calcul de $\phi(q)$ pour q premier. Tout ce qu'on sait, c'est que ce doit être un diviseur de l'indicateur d'Euler $\rho(q)$.
D'autre part, $\phi(q)$ dépend en général de b.

Théorème 1.14 (Formule générale de la période d'une fraction) *Soit une fraction $\frac{p}{q}$ où $p \wedge q = 1$, et soit une base de numération b.*
Si l'on écrit $q = Mq_0$, où M n'a que des facteurs premiers de b et où q_0 est premier avec b, alors la période de $\frac{p}{q}$ est la même que celle de $\frac{1}{q_0}$, et elle est donnée par :

$$ppcm\ \{\phi(\alpha_i^{m_i}) \mid i = 1..N\}$$

où $\prod_{i=1}^{N} \alpha_i^{m_i}$ est la décomposition de q_0 en produit de facteurs premiers.

Remarque : Pour le calcul des $\phi(\alpha_i^{m_i})$, se reporter au théorème précédent !
Preuve : L'égalité entre les périodes de $\frac{1}{q_0}$ et de $\frac{p}{q}$ a déjà été montrée au lemme 1.6.
Pour tout couple (i, j) d'entiers, distincts et compris entre 1 et N, les nombres $\alpha_i^{m_i}$ et $\alpha_j^{m_j}$ sont premiers entre eux.
Or le lemme 1.7 s'étend facilement à un nombre quelconques de facteurs de q_0, et son application donne directement la formule. ∎.

1.7 Application de la formule

Appliquons les résultats pout calculer la période de la fraction $\frac{263}{53165}$ en base 10.

- Tout d'abord, on a bien $263 \wedge 53165 = 1$. On sait alors que le problème se ramène à calculer la période de $\frac{1}{53165}$.
- Décomposons 53165 en facteurs premiers : $53165 = 5 \times 7^3 \times 31$.
- Eliminons les facteurs qui figurent aussi dans 10. Il reste $7^3 \times 31$. La période P cherchée est alors $P = \text{ppcm}(\phi(7^3), \phi(31))$.
- Or $\phi(31) = 15$ et $\phi(7^3) = 7^{3-1}\phi(7) = 7^2 \times 6 = 294$ (en effet, $10^{\phi(7)} \not\equiv 1 \pmod{7^2}$)).
- Finalement $P = \text{ppcm}(294, 15) = 1470$.

2 Approximations et suites diverses

2.1 Approximation par fractions, et suites de Farey

Théorème 2.1 (Théorème d'approximation) *Soient trois fractions (dénominateur dans $\mathbf{N}^*$) $\frac{a}{p} < \frac{m}{n} < \frac{b}{q}$ telles que $bp - aq = 1$. Alors :*

$$m \geq a + b \quad \text{et } n \geq p + q$$

Preuve : En effet, $bp - aq = 1$ entraîne $n = (bp - aq)n = (bn - mq)p + (mp - an)q$. Or $\frac{b}{q} > \frac{m}{n}$, donc $bn - mq > 0$, et, puisque c'est un entier, $bn - mq \geq 1$. De même, $mp - an \geq 1$ et par conséquent $n \geq p + q$. De même, $m = (bp - aq)m = (bn - mq)a + (mp - an)b \geq a + b$. CQFD. ∎

Lemme 2.2 *Soit $\frac{m}{n}$ une fraction irréductible ($n \in \mathbf{N}^*$) telle que $n \geq 2$. On condidère l'ensemble E des fractions irréductibles de dénominateur $< n$, et on note respectivement $\frac{a}{p}$ et $\frac{b}{q}$ le plus grand et le plus petit des éléments de E tels que $\frac{a}{p} < \frac{m}{n} < \frac{b}{q}$. Alors :*

$$n = p + q \quad m = a + b \quad bn - mq = 1 \quad mp - an = 1$$

Preuve : Comme $m \wedge n = 1$, il existe, d'après le théorèm de Bézout, un unique couple $(a, p) \in \mathbf{Z} \times \mathbf{N}^*$ tel que $mp - an = 1$ et $1 \leq p < n$.
Alors, d'apès le lemme 2.1 page 7, toute fraction $\frac{a'}{p'}$ telle que $\frac{a}{p} < \frac{a'}{p'} < \frac{m}{n}$ vérifie $p' \geq p + n > n$. En particulier, $a'/p' \notin E$, donc a/p est bien le plus petit élément de E supérieur strictement à p/q.
Posons $q = n - p$ et $b = m - a$. D'une part, on a $1 \leq q < n$ donc $\frac{b}{q} \in E$. D'autre part, $bn - mp = (m - a)n - (n - p)m = mp - an = 1$ donc $\frac{a}{p} < \frac{m}{n}$ et, de même que précédemment, le lemme 2.1 page 7 nous assure que $\frac{b}{q}$ est le maximum des éléments de E supérieurs à $\frac{m}{n}$. CQFD
∎

Lemme 2.3 (Suites de Farey) *On appelle suite de Farey F_n d'ordre $n \geq 1$ la suite des fractions irréductibles de dénominateur $\leq n$. Alors, pour tout $n \in \mathbf{N}^*$:*

- *Deux termes consécutifs $\frac{a}{p}$ et $\frac{b}{q}$ de F_n vérifient toujours $bp - aq = 1$*
- *Entre ces deux termes consécutifs de F_n il y a* au plus *un terme de F_{n+1}. Si c'est le cas, ce terme est $\frac{a+b}{p+q}$*

Preuve : Remarque préliminaire : si le premier point est vrai pour F_n, alors le second l'est aussi. En effet, soit $\frac{m}{n+1}$ un élément de F_{n+1} n'appartenant pas à F_n. Appelons $x = \frac{a}{p}$ et $y = \frac{b}{q}$ son prédécesseur et son successeur dans F_n.
Si le premier point est vrai, alors $bp - aq = 1$. et une application directe du lemme 2.2 page 7 donne $b(n + 1) - mq = 1$ et $mp - a(n + 1) = 1$.
Ce lemme donne aussi $n + 1 = p + q$ et $m = a + b$. Donc $\frac{m}{n+1}$ est le seul élément de F_{n+1} entre a/p et b/q.

Montrons maintenant le premier point par récurrence sur $n \geq 1$.

- Deux termes consécutifs de F_1 sont simplement deux entiers consécutifs, i.e. $p = q = 1$ et $b = a + 1$, d'où $bp - aq = 1$ et le premier point est vrai.
- Supposons que ce soit vrai pour F_n ($n \geq 1$). Donc pour deux termes consécutifs x et y de F_{n+1}, trois

cas sont possibles :
-$(x, y) \in F_n \times F_n$, et alors ils s'écrivent, par hypothèse de récurrence, sous la forme $x = a/p$ et $y = b/q$ avec $bp - aq = 1$. -$y \in F_{n+1}$ et $y \notin F_n$. Alors $x \in F_n$. Appelons z le successeur de x dans F_n. Comme $y \notin F_n$, z n'est pas y donc $x < y < z$. Le raisonnement de la remarque préliminairemontre que x,y et z s'écrivent sous la forme a/p, $m/(n+1)$ et b/q telle que $mp - a(n+1) = 1$ et $b(n+1) - mq = 1$.
-$x \in F_{n+1}$ et $x \notin F_n$. On appelle t le prédécesseur de x dans F_n, et comme ci-dessus on montre $t < x < y$, avec $t = a/p$, $x = m/n + 1$ et $y = b/q$ tels que $mp - a(n+1) = 1$ Dans ces trois cas, x et y vérifient donc le premier point du lemme. Par récurrence, il est donc vérifié pour tout n.

Notre remarque préliminaire assure alors la véracité du second point. CQFD. ∎

Lemme 2.4 (Cercles de Ford) *Soit un nombre rationnel x de dénominateur p. Posons $u = \frac{1}{2p^2}$ et tra cons le cercle de centre $x, u)$ et de rayon u.*
Alors aucun cercle n'en chevauche un autre, et deux cercles d'abscisses $x = a/p$ et $y = b/q$ sont tangents si et seulement si $(bp - aq)^2 = 1$.

Preuve : Soient deux fractions irréductibles $x = a/b$ et $y = c/d$. Les cercles correspondants se chevauchent si et seulement si la somme de leurs rayons $u + v$ est strictement supérieure à la distance entre leurs centres. En exprimant le carré de cette distance à l'aide de Pythagore, la condition s'écrit :

$$(u+v)^2 > (u-v)^2 + (x-y)^2 \quad (1)$$

Or $(u+v)^2 - (u-v)^2 = 4uv = \frac{1}{b^2d^2}$ et $(x-y)^2 = \frac{(ad-bc)^2}{b^2d^2}$, donc la condition devient $1 > (ad-bc)^2$. Or $x \neq y$ donc $|ad - bc| \geq 1$ donc la condition n'est jamais remplie et les cercles ne se chevauchent donc pas. De même, la condition de tangence est $(u+v)^2 = (u-v)^2 + (x-y)^2 \quad (1)$ et se résume à $(bp - aq)^2 = 1$.
∎

3 Fractions continues : l'essentiel

3.1 Introduction

Soit une suite $(a_i)_{i \in \mathbf{N}}$ d'éléments de $\mathbf{N}$ telle que pour tout $n \geq 1$, $a_n \geq 1$.
On s'intéresse aux fractions de la forme :

$$\frac{p_n}{q_n} = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{\cdots}{a_n}}}}$$

Nous montrerons en particulier que ces fractions tendent toujours vers une limite $x \in \mathbf{R}^{+*}$, que $\lfloor x \rfloor = a_0$, et que pour tout $n \in \mathbf{N}^*$, p_n/q_n est une fraction irréductible, qui est la plus proche de x parmi toutes celles dont le dénominateur est inférieur ou égal à q_n.
En outre, la suite des p_n/q_n est alternée et vérifie les relations $p_{n+2} = a_{n+2}p_{n+1} + p_n$, $q_{n+2} = a_{n+2}q_{n+1} + q_n$ et $p_{n+1}q_n - q_{n+1}p_n = (-1)^n$.

3.2 Formalisation

Définition 3.1 (Fraction continue) *Etant donnée une suite $(a_i)_{i \in \mathbf{N}}$ d'éléments de $\mathbf{N}$ telle que pour tout $n \geq 1$, $a_n \geq 1$, on définit une suite de fonctions de R^+ par :*

$$f_0(x) = a_0 + x \quad f_{n+1}(x) = f_n(\frac{1}{a_{n+1} + x})$$

On définit alors la n-ième réduite de la fraction continue $[a_0, a_1, \ldots]$ comme $\frac{p_n}{q_n} = f_n(0)$, avec p_n et q_n premiers entre eux, et on la note $[a_0, a_1, \ldots, a_n]$.

Lemme 3.2 (Relations de récurrence sur p_n et q_n) *Pour tout $n \geq 1$,*

$$f_n(x) = \frac{p_n + p_{n-1}x}{q_n + q_{n-1}(x)} \quad (1)$$

$$p_{n+1} = a_{n+1}p_n + p_{n-1} \text{ et } q_{n+1} = a_{n+1}q_n + q_{n-1} \quad (2)$$
$$p_n q_{n-1} - q_n p_{n-1} = (-1)^{n-1} \quad \text{avec } p_n \geq 0, q_n > 0 \quad (3)$$

avec les conditions initiales :

$$p_0 = a_0, \quad q_0 = 1, \quad p_1 = 1 + a_0 a_1, \quad q_1 = a_1$$

Preuve : Commencons par montrer les conditions initiales.
Comme $f_0(0) = \frac{a_0}{1}$ il est clair que $p_0 = a_0$ et $q_0 = 1$.
On a $f_1(x) = a_0 + \frac{1}{a_1+x} = \frac{a_0a_1+1+a_0x}{a_1}$. Donc $\frac{p_1}{q_1} = f_1(0) = \frac{a_0a_1+1}{a_1}$. Or $(a_0a_1+1) - a_0a_1 = 1$, donc a_0a_1+1 et a_1 sont premiers entre eux, d'où $p_1 = a_0a_1 + 1$ et $q_1 = a_1$.

Il est alors clair que $f_1(x) = \frac{p_1+p_0x}{q_1+q_0x}$. Procédons maintenant à une récurrence sur $n \geq 1$ pour montrer le reste du lemme.

S'il est vrai pour $n \geq 1$ fixé, alors :

$$f_{n+1}(x) = \frac{p_n + p_{n-1}\left(\frac{1}{a_{n+1}+x}\right)}{q_n + q_{n-1}\left(\frac{1}{a_{n+1}+x}\right)} = \frac{ux + p_n}{vx + q_n} \text{ avec } u = a_{n+1}p_n + p_{n-1}, v = a_{n+1}q_n + q_{n-1})$$

Alors $uq_n - vp_n = -(p_{n-1}q_n - q_{n-1}p_n)$ donc par hypothèse de récurrence $uq_n - vp_n = -(-1)^{n-1} = (-1)^n$.
En particulier, $u \wedge v = 1$. Or $f_{n+1}(x) = \frac{u}{v}$ donc $p_{n+1} = u$, $q_{n+1} = v$, et les relations (1), (2) et (3) sont vraies au rang $n+1$.
La récurrence est donc terminée. CQFD. ∎
Remarque : Il revient au même, et il est parfois pratique, d'appliquer la relation de récurrence en partant de $p_{-1} = 1$,$q_{-1} = 0$,$p_0 = a_0$ et $q_0 = 1$, mais c'est moins élégant puisque p_{-1}/q_{-1} n'est pas une fraction valable !

Lemme 3.3 (Convergence de la suite des réduites) *Notons x_n la n-ième réduite p_n/q_n. Alors les suites $u_k = x_{2k}$ $v_k = x_{2k+1}$ sont adjacentes.*
En particulier, u_k, v_k et x_n et convergent vers une limite commune L, telle que pour tout $k \geq 0$, $x_{2k} < L < x_{2k+1}$.
Par la suite on notera $L = [a_0, a_1, a_2, \ldots]$. En particulier, a_0 est la partie entière de L.

Preuve : Tout d'abord, les suites u et v sont strictement monotones. En effet, pour tout $n \geq 0$, la différence $x_{n+2} - x_n = \frac{p_{n+2}}{q_{n+2}} - \frac{p_n}{q_n}$ est du signe de $p_{n+2}q_n - q_{n+2}p_n = (a_{n+2}p_{n+1}+p_n)q_n - (a_{n+2}q_{n+1}+q_n)p_n = (p_{n+1}q_n - q_{n+1}p_n)a_{n+2} = (-1)^n a_{n+2}$.
La différence $x_{n+2} - x_n$ est donc du signe de $(-1)^n$. En particulier, $u_{k+1} - u_k$ et $v_{k+1} - v_k$ sont du signe de $(-1)^2 k = 1$ et de $(-1)^{2k+3} = (-1)$.
Donc u est strictement croissante et v strictement décroissante.

Etudions maintenant la différence $v_k - u_k = x_{2k+1} - x_{2k} = \frac{p_{2k+1}q_{2k} - q_{2k+1}p_{2k}}{q_{2k}q_{2k+1}} = \frac{(-1)^{2k}}{q_{2k}q_{2k+1}} = \frac{1}{q_{2k}q_{2k+1}}$.
La relation de récurrence $q_{n+2} = a_{n+2}q_{n+1} + q_n$ avec les conditions initiales $q_0 = 1, q_1 = a_1 \geq 1$ nous permet de montrer que q_n croît strictement vers l'infini.
En particulier, le quotient $\frac{1}{q_{2k+1}q_{2k}}$ tend vers 0, donc la différence $v_k - u_k$ aussi, ce qui nous permet de conclure que les suites sont bien adjacentes.
En particulier, elles convergent vers une limite L telle que $x_0 < L < x_1$. Or $x_0 = a_0$ et $x_1 = a_0 + \frac{1}{a_1}$ avec $0 < \frac{1}{a_1} \leq 1$, donc $a_0 = \lfloor L \rfloor$. CQFD. ∎

Lemme 3.4 (Associativité des fractions continues) *Soit L la fraction continue $L = [a_0, a_1, a_2, \ldots]$ et $u_n = p_n/q_n$ sa n-ième réduite. Soit $t \geq 1$. Posons $L' = [a_t, a_{t+1}, a_{t+2}, \ldots]$. Notons $v_n = r_n/s_n$ sa n-ième réduite. Alors pour tout $n \geq 0$:*

$$u_{t+n} = f_{t-1}(\frac{1}{v_n}) \text{ avec } f_{t-1}(x) = \frac{p_{n-2}x + p_{n-1}}{q_{n-2}x + q_{n-1}}$$

i.e. $L = [a_0, a_1, \ldots, a_{t-1}, L']$

Preuve : Comme $f_{t-1}(\frac{1}{v_n}) = \frac{p_{t-2}\frac{s_n}{r_n}+p_{t-1}}{q_{t-2}\frac{s_n}{r_n}+q_{t-1}} = \frac{p_{t-2}s_n+p_{t-1}r_n}{q_{t-2}s_n+q_{t-1}r_n}$, il nous suffit de montrer, par récurrence sur $n \geq 1$, les relations :

$$\begin{cases} p_{t+n} &= p_{t-2}s_n + p_{t-1}r_n \qquad (1) \\ q_{t+n} &= q_{t-2}s_n + q_{t-1}r_n \qquad (2) \end{cases}$$

Les relation de récurrence de p_n et q_n nous donnent celles de r_n et q_n :

$$\begin{cases} r_{n+1} &= a_{t+n+1}r_n + r_{n-1} \quad \text{avec } r_{-1} = 1, r_0 = a_t \\ s_{n+1} &= a_{t+n+1}s_n + s_{n-1} \quad \text{avec } s_{-1} = 0, s_0 = 1 \end{cases}$$

D'après les relations de récurrence sur p et r, on a $p_t = a_t p_{t-1} + p_{t-2} = r_0 p_{t-1} + s_0 p_{t-2}$ donc (1) est vraie pour $n = 0$. De même, $q_t = a_t q_{t-1} + q_{t-2} = r_0 p_{t-1} + s_0 p_{t-2}$ et (2) est vraie.
Soit $n \geq 0$ et supposons (1) et (2 vraies. Alors :

$$\begin{array}{lll} p_{t+n+1} & = a_{t+n+1}p_{t+n} + p_{t+n-1} & \text{(propriété de } p\text{)} \\ & = a_{t+n+1}(p_{t-2}s_n + p_{t-1}r_n) + (p_{t-2}s_{n-1} + p_{t-1}r_{n-1} & \text{(hypothèse de récurrence)} \\ & = p_{t-2}(a_{t+n+1}s_n + s_{n-1}) + p_{t-1}(a_{t+n+1}r_n + r_{n-1}) & \\ & = p_{t-2}s_{n+1} + p_{t-1}r_{n+1} & \text{(propriétés de } r \text{ et } s\text{)} \end{array}$$

Donc (1) est vraie au rang $n+1$. Rebelote pour la relation (2) :

$$\begin{array}{lll} q_{t+n+1} & = a_{t+n+1}q_{t+n} + q_{t+n-1} & \text{(proqriété de } q\text{)} \\ & = a_{t+n+1}(q_{t-2}s_n + q_{t-1}r_n) + (q_{t-2}s_{n-1} + q_{t-1}r_{n-1} & \text{(hypothèse de récurrence)} \\ & = q_{t-2}(a_{t+n+1}s_n + s_{n-1}) + q_{t-1}(a_{t+n+1}r_n + r_{n-1}) & \\ & = q_{t-2}s_{n+1} + q_{t-1}r_{n+1} & \text{(propriétés de } r \text{ et } s\text{)} \end{array}$$

Donc par récurrence (1) et 2 sont valables pour tout $n \geq 0$.

La fonction f_{t-1} est continue et la suite v_n converge vers L'.
Donc la limite L de $u_{n+t} = f_{t-1}(v_n)$ quand n tend vers l'infini est aussi $L = f_{t-1}(L')$, i.e.$L = [a_0, a_1, \ldots, a_{t-1}, L']$.
CQFD. ∎

Lemme 3.5 *Comparaison de fractions continues, unicité Soient deux fractions continues $L = [a_0, a_1, \ldots]$ et $L'[b_0, b_1, \ldots]$. Si les suites a et b sont distinctes, alors la différence $L - L'$ est du signe de $(-1)^n(a_n - b_n)$, où n est le plus petit nombre tel que $a_n \neq b_n$.*
D'autre part, si $n \leq m$, la différence entre $[a_0, \ldots, a_{n-1}] - [a_0, \ldots, a_m]$ est du signe de $(-1)^n$. Un développement en fraction continue est donc unique.

Preuve : Posons $A = [a_n, a_{n+1}, \ldots]$ et $B = [b_n, b_{n+1}, \ldots]$. Le lemme 3.4 page 9 nous donne alors $L = f(1/A)$ et $L' = f(1/B)$ où $f_{n-1}(x) = \frac{p_{n-2}x+p_{n-1}}{q_{n-2}x+q_{n-1}}$.
Or la dérivée $f'(x)$ vaut $\frac{p_{n-2}q_{n-1}-q_{n-2}p_{n-1}}{q_{n-1}q_{n-2}}$ et est donc du signe de $p_{n-2}q_{n-1} - q_{n-2}p_{n-1} = (-1)^{n-2} = (-1)^(n-1)$.
Donc $L - L'$ est du signe de $(-1)^n(A - B)$. Comme a_n et b_n sont distincts et sont les parties entières respectives de A et B, $A - B$ est du signe de $a_n - b_n$, ce qui montre le premier point du lemme.
Montrons le second point. Par définition des réduites, $[a_0, \ldots, a_{n-1}] = f(0)$ et le lemme 3.4 page 9 donne $[a_0, \ldots, a_m] = f(A)$ avec $A = [a_n, \ldots, a_m] > 0$ puique $\lfloor A \rfloor = a_n > 0$.
La différence $f(0) - f(A)$ est du signe de $(-1)^{n-1}(0 - A) = (-1)^n$. CQFD. ∎

Lemme 3.6 (Réduites et meilleure approximation rationnelle) *Pour tout $n \geq 1$, la n-ième réduite p_n/q_n de la fraction continue $[a_0, a_1, a_2, \ldots]$ est, parmi toutes les fractions de dénominateur $\leq q_n$, la plus proche de la limite L de ce côté-ci de L.*
D'autre part, si la suite (a) est infinie, la limite L est irrationnelles.

Preuve : Si n est impair, et le lemme 3.3 page 9 donne $x_{n-1} < L < x_n$. Toute fraction c telle que $L \leq c < x_n$ véerifie donc $x_{n-1} < c < x_n$. Or d'après le lemme 3.2 page 8 $x_{n-1} = p_{n-1}/q_{n-1}$ et $x_n = p_n/q_n$ avec $p_n q_{n-1} - q_n p_{n-1} = 1$.
Le lemme 2.1 page 7 nous dit alors que le dénominateur de c est au moins aussi grand que $q_{n-1} + q_n > q_n$.
Il en va de même si a est pair. d'où le premier point du lemme.
Même raisonnement si n est pair.
S'il existait une fraction c prenant la valeur de L, son dénominateur serait plus grand que celui de chacune de ses réduites, qui tend vers l'infini. L n'est donc pas rationnel. CQFD. ∎