Notes sur les développements décimaux périodiques

Robert Rolland(*)

1. Introduction

Dans cette note nous étudions quelques propriétés des développements décimaux des nombres de la forme m/n où m et n sont des entiers premiers entre eux tels que $1 \leq m < n$.

Nous supposons connus les aspects relevant de l'analyse, c'est-à-dire la définition des développements décimaux des nombres réels de l'intervalle [0,1] sous la forme :

$$x = \sum_{i=1}^{+\infty} \frac{q_i}{10^i}$$

où les q_i sont des entiers tels que $0 \leq q_i < 10$, ainsi que les conséquences simples qui en résultent. En particulier on rappelle l'existence dans le cas de nombres de la forme

---

(7) http://revue.sesamath.net/spip.php?article4

(*) Institut de Mathématiques de Luminy, Case 907, 13288 Marseille cedex 9.
E-mail: rolland@iml.univ-mrs.fr

$\frac{m}{10^k}$ ($m \neq 0$) et, uniquement dans ce cas, de deux développements décimaux distincts.

Ce qui nous intéresse ici ce sont les comportements particuliers de ces développements dans le cas des nombres rationnels et la présentation des outils d'algèbre très simples mis en œuvre pour expliquer ces comportements.

Nous rappelons dans un premier temps la classification habituelle :

• n est de la forme 2^a5^b auquel cas la fraction irréductible m/n admet un développement décimal fini :

$$\frac{m}{n} = 0,q_1q_2\ldots q_s$$

avec $q_s \neq 0$, ainsi qu'un développement décimal infini ne contenant que des 9 à partir d'un certain rang :

$$\frac{m}{n} = 0,q_1q_2\ldots q_s'999\ldots$$

où $q_s' = q_s - 1$.

• n n'est divisible ni par 2 ni par 5 auquel cas le développement décimal est illimité et périodique, c'est-à-dire que :

$$\frac{m}{n} = 0,q_1q_2\ldots q_sq_1q_2\ldots q_s\ldots,$$

ce qu'on note aussi :

$$\frac{m}{n} = 0,\overline{q_1q_2\ldots q_s}.$$

Nous adopterons la terminologie suivante : $q_1q_2\ldots q_s$ est la **partie périodique** et s la **période**.

• n est de la forme $2^a5^bn_1$ où $n_1 > 1$ n'est divisible ni par 2 ni par 5. Ce cas est un mélange des deux cas précédents. Il donne pour la fraction m/n un développement illimité périodique mixte, constitué d'une **partie irrégulière** et d'une **partie périodique** :

$$\frac{m}{n} = 0,u_1u_2\ldots u_k\overline{q_1q_2\ldots q_s}.$$

Puis nous détaillons un peu quelques comportements liés à la structure algébrique sous-jacente.

L'outil principal utilisé est la notion de classe résiduelle modulo n, autrement dit l'anneau $\mathbb{Z}/n\mathbb{Z}$. Nous noterons :

$$x \equiv y \quad (n)$$

la relation d'équivalence entre deux entiers x et y qui exprime que x et y sont dans la même classe résiduelle modulo n, c'est-à-dire que $x - y$ est divisible par n, ou encore que x et y ont le même reste dans leur division euclidienne par n.

Nous noterons :

$$y = x \mod n,$$

pour indiquer que y est le résultat de l'opération qui aux entiers x et n fait correspondre l'unique représentant y de la classe résiduelle de x modulo n qui vérifie $0 \leq y < n$.

Les comportements classiques que nous venons de citer sont connus depuis longtemps. On peut en trouver une preuve en des termes très proches de ceux qu'on pourrait utiliser de nos jours dans l'article d'Eugène Catalan [Cat42]. Eugène Catalan montre toute la force du petit théorème de Fermat :

« *La note suivante ne contient rien de neuf : si je me décide à la publier, c'est parce que la manière dont on présente ordinairement la théorie des fractions périodiques n'est, si je ne me trompe, ni très logique, ni très rigoureuse. En outre, cette théorie s'appuie assez naturellement sur le théorème de Fermat, et sur d'autres propriétés intéressantes, qu'il serait peut-être convenable de faire entrer dans les éléments.* »

Dans le cours de l'exposé, il utilise (sans lui donner ce nom) la fonction indicatrice d'Euler appelée aussi fonction *phi*, qui compte le nombre d'éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$ et qui permet de généraliser le petit théorème de Fermat.

L'exposé est repris en terme de groupes dans l'article [Ben09].

On trouvera enfin une approche pédagogique de cette question dans [And74].

Les outils mathématiques algébriques et arithmétiques utilisés dans la suite sont exposés dans [Dem97], [KR98], ainsi que dans l'annexe arithmétique de [BRV05].

2. Développement décimal d'un nombre de la forme $m/2^a5^b$

Théorème 2.1. — *Soient m et n deux entiers premiers entre eux tels que $1 \leq m < n$. La fraction irréductible m/n admet un développement décimal fini si et seulement si n est de la forme $n = 2^a5^b$ où a et b sont des entiers ≥ 0.*

Démonstration. — Supposons $n = 2^a5^b$ et notons $t = \max(a,b)$. On peut donc écrire :

$$\frac{m}{n} = \frac{2^{t-a}5^{t-b}m}{10^t}.$$

Si nous écrivons l'entier $2^{t-a}5^{t-b}m$ sous forme décimale :

$$2^{t-a}5^{t-b}m = v_{t-1}\ldots v_0,$$

alors :

$$\frac{m}{n} = 0, v_{t-1}\ldots v_0.$$

Remarquons que $v_0 \neq 0$.

Réciproquement, si la fraction irréductible m/n admet un développement décimal

fini, alors :

$$\frac{m}{n} = 0, v_{t-1} \dots v_0.$$

Donc on peut écrire :

$$\frac{m}{n} = \frac{v}{10^t},$$

où v est un entier, si bien que :

$$m10^t = nv.$$

Donc n divise $m10^t$ et comme n est premier avec m, il divise 10^t. L'entier n est donc de la forme 2^a5^b.

3. Développement décimal d'une fraction irréductible m/n où n n'est divisible ni par 2 ni par 5

Soit n un entier > 1 dont la décomposition en facteurs premiers ne contient ni 2 ni 5. Un tel n se repère facilement par son dernier chiffre en écriture décimale qui est 1, 3, 7 ou 9. Soit m un entier premier avec n tel que $1 \leq m < n$. Nous nous intéressons au développement décimal de la fraction irréductible m/n.

Le nombre m/n a, d'après le paragraphe précédent, un développement illimité sous la forme :

$$0, q_1 q_2 \dots q_s \dots$$

Les décimales se calculent par des divisions euclidiennes successives ayant des restes non nuls :

$$\begin{aligned} r_0 &= m, \\ 10r_0 &= q_1 n + r_1 \quad \text{avec } 0 < r_1 < n, \\ 10r_1 &= q_2 n + r_2 \quad \text{avec } 0 < r_2 < n, \end{aligned}$$

et par récurrence :

$$10r_{s-1} = q_s n + r_s \quad \text{avec } 0 < r_s < n.$$

Ce processus décrit parfaitement la division posée classique qu'on apprend à l'école primaire : ajout d'un zéro à la fin (multiplication par 10), recherche de q_i, calcul du reste.

Nous sommes donc amenés à étudier les deux suites qui interviennent dans les calculs précédents, c'est-à-dire d'une part la suite r des restes successifs :

$$r = (r_s)_{s \geq 0},$$

et d'autre part la suite des décimales :

$$q = (q_s)_{s \geq 1}.$$

Théorème 3.1. — *Pour tout entier $s \geq 0$ on a :*

$$r_s = 10^s r_0 \mod n.$$

Démonstration. — Le résultat est vrai pour $s = 0$. Supposons-le vrai pour s, alors :

$$10r_s = q_{s+1}n + r_{s+1},$$

ce qui prouve que :

$$r_{s+1} \equiv 10r_s \quad (n),$$

ou encore en utilisant l'hypothèse de récurrence :

$$r_{s+1} \equiv 10^{s+1} r_0 \quad (n),$$

et comme $0 < r_{s+1} < n$, on conclut que :

$$r_{s+1} = 10^{s+1} r_0 \mod n.$$

De cette proposition sur la suite r découle la proposition suivante sur les valeurs des termes de la suite q :

Théorème 3.2. — *Pour tout entier $s \geq 1$ on a :*

$$q_s = \left[\frac{10(10^{s-1} r_0 \mod n)}{n} \right].$$

Le comportement du développement de la fraction irréductible m/n est indiqué par le théorème suivant :

Théorème 3.3. — *Les suites r et q sont périodiques de période s. La période s est l'ordre de* 10 *dans le sous-groupe multiplicatif $(\mathbb{Z}/n\mathbb{Z})^*$ des éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$. En particulier, la période s ne dépend pas de m (pourvu bien sûr qu'il soit premier avec n).*

Démonstration. — Les restes successifs de la suite r sont tous $< n$. Donc on retombe forcément sur un reste déjà trouvé. Soit s le plus petit entier pour lequel cela se produit et supposons que le reste déjà trouvé soit r_u. On a donc :

$$10^s r_0 \equiv 10^u r_0 \quad (n),$$

où $0 < u < s$. Mais alors :

$$10^{s-u} r_0 \mod n = r_0,$$

et comme, par hypothèse, s est le plus petit entier pour lequel on retombe sur un reste déjà trouvé, c'est que $u = 0$ et donc que $r_s = r_0$.

Comme r_0 est premier avec n, il est inversible modulo n, et la relation :

$$10^s r_0 \equiv r_0 \quad (n)$$

implique :

$$10^s \equiv 1 \quad (n).$$

Il est facile de voir que, par construction de s, ceci ne se produit pas pour un entier u tel que $0 < u < s$.

La périodicité de la suite q découle de celle de r. Mais dans un premier temps il n'est pas clair que la période de q ne soit pas éventuellement strictement plus petite que celle de r. Supposons que la période de q soit $t \leq s$. Alors :

$$10^t \frac{r_0}{n} = q_1 q_2 \dots q_t + \frac{r_0}{n}.$$

Donc :

$$10^t \equiv 1 \quad (n).$$

On conclut qu'on a bien $t = s$.

Remarque : Les propositions précédentes nous permettent de calculer une décimale particulière dont on précise le rang sans calculer les autres. Ainsi on peut avoir une telle décimale même pour des très grands nombres alors même qu'il n'est pas envisageable de les calculer toutes.

Remarque : La formule donnant la somme d'une progression géométrique nous permet de reconstruire à partir d'un développement décimal périodique :

$$0,\overline{q_1 q_2 \dots q_s}$$

la fraction qui lui a donné naissance sous la forme :

$$0,\overline{q_1 q_2 \dots q_s} = \frac{q_1 q_2 \dots q_s}{99\dots9},$$

où le dénominateur comporte s chiffres 9. Bien entendu, à partir de là, on se ramène à une fraction irréductible.

4. Développement décimal d'une fraction irréductible m/n où n est de la forme $2^a5^b n_1$ avec $n_1 > 1$ non divisible ni par 2 ni par 5 et $a > 0$ ou $b > 0$

Théorème 4.1. — *Soit m/n une fraction irréductible telle que $0 < m < n$ et n de la forme $2^a5^b n_1$ avec $a > 0$ ou $b > 0$ et n_1 non divisible par 2 ou par 5. Alors le développement décimal de m/n est périodique mixte c'est-à-dire de la forme :*

$$0,u_1 u_2 \dots u_k \overline{q_1 q_2 \dots q_s},$$

où $u_k \neq q_s$. La partie $u_1u_2\dots u_k$ est appelée partie irrégulière, sa longueur est $k = \max(a,b)$. La partie $q_1q_2\dots q_s$ est la partie périodique, sa longueur est l'ordre de 10 dans le groupe multiplicatif $(\mathbb{Z}/n_1\mathbb{Z})^*$.

Démonstration. — Posons $w = 2^a5^b$. Par hypothèse $w > 1$. Grâce au théorème de Bézout on peut trouver deux entiers positifs k_1 et k_2 tels que :

$$m = k_1 n_1 - k_2 w.$$

Du fait que m et wn_1 sont premiers entre eux, les nombres k_1 et w sont premiers entre eux ainsi que les nombres k_2 et n_1. On peut écrire :

$$\frac{m}{n} = \frac{k_1}{w} - \frac{k_2}{n_1}.$$

Par division euclidienne on obtient :

$$k_1 = \alpha_1 w + \beta_1,$$
$$k_2 = \alpha_2 n_1 + \beta_2,$$

ce qui donne :

$$\frac{m}{n} = (\alpha_1 - \alpha_2) + \frac{\beta_1}{w} - \frac{\beta_2}{n_1}.$$

Remarquons que β_1 et w sont premiers entre eux, ainsi que β_2 et n_1. Comme $0 < m < n$, on a les deux cas suivants :

- $\alpha_1 - \alpha_2 = 0$ et $\dfrac{\beta_1}{w} - \dfrac{\beta_2}{n_1} > 0$,
- $\alpha_1 - \alpha_2 = 1$ et $\dfrac{\beta_1}{w} - \dfrac{\beta_2}{n_1} < 0$.

Le nombre $\dfrac{\beta_1}{w}$ est décimal de longueur de partie décimale $\max(a,b)$. Le nombre $\dfrac{\beta_2}{n_1}$ est décimal périodique de période s. Alors $\left|\dfrac{\beta_1}{w} - \dfrac{\beta_2}{n_1}\right|$ est périodique mixte : la partie irrégulière est la partie perturbée par le nombre $\dfrac{\beta_1}{w}$ et a pour longueur $\max(a,b)$. La partie périodique a pour longueur s, période de $\dfrac{\beta_2}{n_1}$. Si on est dans le premier cas, il n'y a rien à dire de plus ; si on est dans le second cas, il suffit de constater que le développement décimal cherché s'obtient à partir du développement décimal de $\left|\dfrac{\beta_1}{w} - \dfrac{\beta_2}{n_1}\right|$ par « complémentation à 9 », ce qui permet de conclure.

On peut tester l'exemple édifiant suivant :

$$\frac{1}{2^7 \times 5^2 \times 13}.$$

Dans cet exemple la partie irrégulière est de longueur 7.

5. Raisonnons sur les groupes

Nous supposerons dans toute la suite que n est un entier > 1 qui n'est divisible ni par 2 ni par 5.

5.1. Quotient de $(\mathbb{Z}/n\mathbb{Z})^*$ par le sous-groupe engendré par 10

Soit $G = (\mathbb{Z}/n\mathbb{Z})^*$ le groupe des éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$. Ce groupe a $\phi(n)$ éléments où ϕ est la fonction d'Euler (Euler's totient function).

L'ordre s de 10 dans ce groupe est un diviseur de $\phi(n)$. Soit H le sous- groupe de G engendré par 10. Ainsi H a s éléments :

$$\mathrm{H} = \left\{1, 10, 10^2, \ldots, 10^{s-1}\right\}.$$

On définit alors la relation ~ dans G par :

$$y \sim x \Leftrightarrow y \in x\mathrm{H}.$$

Cette relation est une relation d'équivalence dont toutes les classes ont s éléments. Il y a exactement $\phi(n)/s$ telles classes qui, bien entendu, forment une partition de G.

Les résultats déjà obtenus dans le paragraphe 3 permettent d'énoncer le théorème suivant :

Théorème 5.1. — (1) *La classe d'un élément x est exactement l'ensemble des restes successifs de x/n lors du développement décimal de cette fraction.*

(2) *Si x et y sont dans la même classe, il existe k tel que* $y = x10^k$ *et la partie périodique de y/n est, à une permutation circulaire près, la partie périodique de x/n. Plus précisément on obtient la partie périodique de y/n en faisant tourner la partie périodique de x/n de k positions sur la gauche.*

(3) *Si x et y sont dans des classes distinctes, les restes successifs de x/n sont tous distincts des restes successifs de y/n.*

Remarque : Si on se trouve dans le cas d'un développement m/n de longueur extrémale $\phi(n)$ ($p - 1$ dans le cas d'un nombre premier p), alors il n'y a qu'une classe et donc toutes les fractions irréductibles m/n ($0 < m < n$) ont des parties périodiques qui se déduisent les unes des autres par des permutations circulaires.

5.2. Calcul de la période.

Il faut donc calculer l'ordre de 10 dans le groupe des éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$. L'ordre maximal est $\phi(n)$ (nombre d'éléments du groupe). Dans le cas où p est premier, l'ordre maximal est $p - 1$. Le calcul de l'ordre d'un élément demande en général de connaître $\phi(n)$ ainsi que sa factorisation. Si $\phi(n)$ est inconnu ou est trop gros pour être factorisé et si n n'a pas été construit spécialement pour aider au calcul, alors en l'état actuel des choses, sauf cas très particulier où l'ordre de 10 serait un facteur suffisamment petit de $\phi(n)$ pour être trouvé, il ne sera pas possible de calculer la période de $1/n$.

Remarque : Le calcul de $\phi(n)$ lui-même peut être problématique. En effet supposons par exemple que n soit composé d'un produit de deux nombres premiers p et q. Alors la connaissance de $\phi(n)$ est équivalente à la connaissance de la décomposition de n. En effet, si on connaît p et q il est facile de calculer $\phi(n) = (p - 1)(q - 1)$ grâce à un algorithme polynomial. Si on connaît $\phi(n)$ il est tout aussi facile, par la résolution de l'équation du second degré :

$$\mathrm{X}^2 - (n + 1 - \phi(n))\mathrm{X} + n = 0,$$

de calculer p et q. Il est donc aussi difficile de calculer $\phi(n)$ que de calculer la

factorisation de n.

En revanche si on connaît $\phi(n)$ et qu'on peut le factoriser :

$$\phi(n) = \prod_{i=1}^{k} p_i^{\alpha_i},$$

alors il est facile de calculer l'ordre de 10 :

$s := \phi(n)$;
pour $i := 1$ jusqu'à k faire
début
tant que $\alpha_i \geq 1$ et $10^{s/p_i} \equiv 1 \quad (n)$ faire
début
$s := s/p_i$;
$\alpha_i := \alpha_i - 1$;
fin;
fin:
retourner s.

Le théorème suivant caractérise le cas où la période est maximale.

Théorème 5.2. — *Soit n un entier > 1 qui n'est divisible ni par 2 ni par 5. La période du développement décimal de $1/n$ (ou m/n) est exactement $\phi(n)$ si et seulement si pour tout facteur premier q de $\phi(n)$ on a :*

$$10^{\frac{\phi(n)}{q}} \not\equiv 1 \quad (n).$$

5.3. Quelques remarques.

Si e est l'ordre de 10 on a $10^e - 1 \equiv 0 \quad (n)$. Autrement dit : 99…9 (avec e chiffres 9) est divisible par n. Si de plus n n'est pas divisible par 3, alors n est premier avec 9, donc n divise 111…1 (avec e chiffres 1). C'est ce qui se passe si par exemple n est un nombre premier > 5.

Théorème 5.3. — *Les nombres qui divisent un nombre de la forme* 111…1 *sont les nombres qui ne sont ni divisibles par* 2 *ni divisibles par* 5.

Démonstration. — Si un nombre est divisible par 2 ou par 5 il ne divise sûrement pas un nombre de la forme 111…1 puisqu'il est visible sur le dernier chiffre qu'un tel nombre n'est divisible ni par 2 ni par 5. Réciproquement, soit n un nombre qui n'est divisible ni par 2 ni par 5. Alors, le développement décimal de $\frac{1}{9n}$ est de la forme :

$$\frac{1}{9n} = 0,\overline{q_1 q_2 \ldots q_s},$$

ce qui peut donc s'écrire :

$$\frac{1}{9n} = \frac{q_1 q_2 \ldots q_s}{999\ldots9}.$$

Donc :

$$999\ldots9 = (q_1 q_2 \ldots q_s)9n,$$

ou encore :

$$111\ldots1 = (q_1 q_2 \ldots q_s)n,$$

ce qui achève la preuve.

Remarque : Les nombres de la forme 111…1 s'écrivent aussi :

$$\frac{10^k - 1}{9}.$$

Ce sont des **nombres de Mersenne généralisés** (les nombres de Mersenne étant ceux de la forme $2^k - 1$). Il existe des nombres de la forme 111…1 qui sont premiers. Pour de tels nombres l'exposant k est nécessairement premier. En effet, sinon $k = uv$ avec $u > 1$ et $v > 1$. Le nombre considéré s'écrit alors :

$$\frac{10^{uv} - 1}{9} = \left(\frac{10^u - 1}{9}\right)\left(\left(10^u\right)^{v-1} + \ldots + 1\right),$$

$$\frac{10^{uv} - 1}{9} = (11\ldots1)\mathrm{K}.$$

On connaît des nombres premiers (ou vraisemblablement premiers) de ce type, par exemple ceux obtenus avec k = 2, 19, 23, 317, 1 031, 49 081, 86 453.

6. Nombres premiers de Sophie Germain

Un nombre premier q est dit de Sophie Germain si $p = 2q + 1$ est aussi premier. Supposons, en outre, $q > 5$ c'est-à-dire $p > 11$ pour éviter justement le couple ($q = 5$, $p = 11$).

Dans ce cas, 10 ne peut être que d'ordre q ou $p - 1$. Il suffit de tester $10^{(p-1)/2}$ pour savoir dans lequel des deux cas on est (cf. le package kruptor, sur le site de l'association *ACrypTA : www.acrypta.com*, développé par *Ainigmatias Cruptos*, qui permet en particulier de construire des nombres de Sophie Germain pour faire des essais. Ce package est conçu pour être utilisé avec le logiciel XCAS dont on trouvera une description dans [GPdG07]).

En fait il est facile de voir dans ce cas que :

(1) Si 10 est un résidu quadratique, alors il est d'ordre q.

(2) Si 10 n'est pas un résidu quadratique, alors il est d'ordre maximal $p - 1$.

Si on calcule le symbole de Legendre de 10, on obtient :

$$\left(\frac{10}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{5}{p}\right),$$

$$\left(\frac{10}{p}\right) = (-1)^{\frac{p^2-1}{n}}\left(\frac{p \mod 5}{5}\right).$$

Ceci nous donne le tableau suivant :

	$\frac{p^2-1}{8}$ pair	$\frac{p^2-1}{8}$ impair
$p \mod 5 = \pm 1$	ordre $= q$	ordre $= p-1$
$p \mod 5 = \pm 2$	ordre $= p-1$	ordre $= q$

7. Curiosité

Soit $p > 2$ un nombre premier. On suppose que la période du développement décimal de la fraction $1/p$ est paire. Nous noterons $2s$ cette période. Ainsi :

$$\frac{1}{p} = 0,\overline{q_1 q_2 \dots q_{2s}}.$$

On constate alors que :

$$q_1 q_2 \dots q_s + q_{s+1} q_{s+2} \dots q_{2s} = \overbrace{99\dots9}^{s \text{ fois}}.$$

Curieux, non ! Voyons pourquoi.

Notons $r_0 = 1$, r_1, r_2, … , r_{2s-1} le cycle des restes obtenus dans le processus de calcul des décimales de $1/p$. À partir de ce cycle des restes on voit que

$$\frac{r_s}{p} = 0,\overline{q_{s+1} q_{s+2} \dots q_{2s} q_1 q_2 \dots q_s}.$$

Mais souvenons-nous que

$$r_k = 10^k \mod p$$

et que

$$10^{2s} \equiv 1 \quad (p).$$

Donc r_s est une racine de 1 qui n'est pas 1 puisque l'ordre de 10 est $2s$. C'est donc $p - 1$ (il n'y a que deux racines carrées du fait que $\mathbb{Z}/p\mathbb{Z}$ est un corps). Par suite :

$$\frac{1}{p} + \frac{p-1}{p} = 1 = 0,\overline{q_1 q_2 \dots q_s q_{s+1} q_{s+2} \dots q_{2s}} + 0,\overline{q_{s+1} q_{s+2} \dots q_{2s} q_1 q_2 \dots q_s}.$$

Or on a nécessairement

$$q_1 q_2 \dots q_{2s} + q_{s+1} q_{s+2} \dots q_{2s} q_1 q_2 \dots q_s < 10^{2s},$$

sinon on aurait

$$0, q_1 q_2 \dots q_s q_{s+1} q_{s+2} \dots q_{2s} + 0, q_{s+1} q_{s+2} \dots q_{2s} q_1 q_2 \dots q_s \geq 1$$

et par suite

$$0,\overline{q_1 q_2 \dots q_s q_{s+1} q_{s+2} \dots q_{2s}} + 0,\overline{q_{s+1} q_{s+2} \dots q_{2s} q_1 q_2 \dots q_s} > 1,$$

ce qui n'est pas. Donc si on note

$$u_1 u_2 \dots u_{2s} = q_1 q_2 \dots q_s q_{s+1} q_{s+2} \dots q_{2s} + q_{s+1} q_{s+2} \dots q_{2s} q_1 q_2 \dots q_s,$$

alors

$$1 = 0,\overline{q_1 q_2 \dots q_s q_{s+1} q_{s+2} \dots q_{2s}} + 0,\overline{q_{s+1} q_{s+2} \dots q_{2s} q_1 q_2 \dots q_s} = 0,\overline{u_1 u_2 \dots u_{2s}}.$$

En conséquence puisque la somme vaut 1,

$$0,\overline{u_1 u_2 \dots u_{2s}} = 0,\overline{9},$$

ce qui prouve le résultat.

Dans la démonstration on utilise le fait que les racines carrées de 1 sont 1 et −1. Ceci n'est pas vrai dans $\mathbb{Z}/n\mathbb{Z}$ lorsque n n'est pas premier. On peut donc s'attendre à ce que ce comportement puisse ne pas avoir lieu dans ce cas. Par exemple si $n = 21$ alors

$$\frac{1}{21} = 0,\overline{047619}.$$

La taille de la période est paire et

$$047 + 619 \neq 999.$$

En fait, dans ce cas, 1 a quatre racines carrées qui sont 1, 20 (−1), 8, 13 (−8), et il se trouve que $10^3 \mod 21 = 13$ est justement une racine carrée qui n'est pas −1.

Il peut se faire que ça marche tout de même. Il faut et il suffit pour cela que $10^s \mod n = -1$. C'est le cas par exemple pour $n = 23 \times 47 = 1\,081$. La période du développement de $1/n$ est dans ce cas 506 et $10^{253} \mod n = -1$.

Références

[And74] J. Anderson – « Periodic decimals », *Mathematics Teacher* 67 (1974), p. 504-509.

[Ben09] E. Bennett – « Periodic decimal fraction », *The American Mathematical Monthly* XVI nº 5 (1909), p. 79-82.

[BRV05] P. Barthélémy, R. Rolland & P. Véron – *Cryptographie - principes et mises en œuvre*, Lavoisier, 2005.

[Cat42] E. Catalan – « Fractions décimales périodiques », *Nouvelles Annales de Mathématiques* 1 (1842), p. 457-471.

[Dem97] M. Demazure – *Cours d'algèbre : primalité divisibilité codes*, Cassini, 1997.

[GPdG07] M. Gandit, B. Parisse & R. De Graeve – « Mathématiques avec xcas », *Bulletin de l'APMEP* 468 (2007), p. 82-90.

[KR98] R. Kumanduri & C. Romero – *Number theory with computer applications*, Prentice Hall, 1998.