Université de Haute Alsace
ENSISA – Mathématiques discrètes
Augustin Fruchard

Année 2024-2025

Cours de mathématiques discrètes I

Voici deux problèmes typiques des mathématiques discrètes.

a. Combien de tours au maximum peut-on placer sur un échiquier sans que deux soient en prise l'une de l'autre ? Même question avec des rois, puis avec des cavaliers, des fous, et des dames. (Pour les tours, on pourra aussi compter le nombre de solutions.)

b. Alice et Bob jouent au *jeu de Nim*, qui est le suivant. Ils constituent un certain nombre de tas de cailloux, chacun de taille arbitraire, par exemple un tas de 17 cailloux, un de 23, un de 14 et un de 7, puis chacun à tour de rôle peut en prendre autant qu'il veut, mais au moins un et dans un seul tas à la fois. Lorsqu'un joueur ne peut plus jouer (parce qu'il ne reste plus de caillou) il ou elle a perdu. Qui gagne ?

Dans ce cours, l'expression “Mathématiques discrètes” signifie mathématiques finies. Le mot *discret* peut avoir d'autres significations mathématiques.

Un outil important des mathématiques discrètes est le *principe des pigeons* (appelé aussi principe des tiroirs) : si au moins $Np+1$ pigeons habitent un pigeonnier comportant N trous d'envol, alors au moins un trou contient au moins $p+1$ pigeons. Ce principe nous sera souvent utile dans ce cours.

Exemple : montrons que, parmi cinq points du plan à coordonnées entières, au moins deux d'entre eux ont leur milieu à coordonnées entières.

Soit $M_1 = (x_1, y_1)$ et $M_2 = (x_2, y_2)$ deux points dont les coordonnées x_1, y_1, x_2, y_2 sont des entiers relatifs. Leur milieu a pour coordonnées $\frac{1}{2}(x_1 + x_2)$ et $\frac{1}{2}(y_1 + y_2)$. Ce sont des entiers si, et seulement si, x_1 et x_2 d'une part, et y_1 et y_2 d'autre part, ont la même parité, i.e.[1] si et seulement si :

$$\Big((x_1 \text{ et } x_2 \text{ sont pairs}) \text{ ou } (x_1 \text{ et } x_2 \text{ sont impairs}) \Big)$$
$$\text{et}$$
$$\Big((y_1 \text{ et } y_2 \text{ sont pairs}) \text{ ou } (y_1 \text{ et } y_2 \text{ sont impairs}) \Big)$$

Ceci nous conduit à considérer les quatre “trous d'envol” :
$T_1 = 2\mathbb{Z} \times 2\mathbb{Z}$, l'ensemble des points dont les deux coordonnées sont paires,
$T_2 = 2\mathbb{Z} \times (2\mathbb{Z}+1)$, les points d'abscisse est paire et d'ordonnée impaire,
et de même $T_3 = (2\mathbb{Z}+1) \times 2\mathbb{Z}$ et $T_4 = (2\mathbb{Z}+1) \times (2\mathbb{Z}+1)$.

1. i.e. signifie “c'est-à-dire” (*id est* en latin).

Deux points dans le même trou ont bien leur milieu à coordonnées entières, or on a cinq points et seulement quatre trous, donc forcément au moins deux poins dans l'un des trous.

1 Systèmes de numérations

Primitive : I, II, III, . . . , IIIIII, . . .

Mésopotamie : $\uparrow$ (clou = 1) et $<$ (chevron = 10), base 60. Vestiges : minutes et secondes des heures, minutes et secondes d'arc des degrés.

Romain : I, II, III, IV, V, . . . , X, L = 50, C = 100, D = 500, M = 1000.

Numération “de position” chinoise, puis indienne, puis arabe.

1.1 Écriture en base 10

On rappelle le théorème de la division euclidienne.

Pour tout entier $a \in \mathbb{Z}$ et tout entier $b \in \mathbb{N}^*$, il existe des entiers $q \in \mathbb{Z}$ et $r \in \{0, \ldots, b-1\}$ uniques tels que $a = bq + r$.

a est le *dividende*, b le *diviseur*, q le *quotient* et r le *reste*.

Proposition 1.1. — *Pour tout entier $N \in \mathbb{N}^*$, il existe $p \in \mathbb{N}$ et $a_0, \ldots, a_p \in \{0, \ldots, 9\}$ uniques tels que*

$$a_p \neq 0 \text{ et } N = a_0 + a_1 10 + \cdots + a_p 10^p = \sum_{k=0}^{p} a_k 10^k$$

On écrit $N = a_p a_{p-1} \ldots a_0$; c'est l'écriture décimale de N.

Preuve. — Récurrence *complète* sur N :
Initialisation. Si $N < 10$, on a $N = 1$ ou $2, \ldots,$ ou 9 et c'est fini.
Hérédité. Soit $N \geq 10$ et supposons que tous les entiers entre 1 et $N-1$ ont une écriture décimale. On effectue la division euclidienne de N par 10 : $N = 10\,q + r$ avec $1 \leq q \leq N/10$ et $0 \leq r < 10$. Comme $q \leq N-1$, on applique l'hypothèse de récurrence à q : $q = b_0 + b_1 10 + \cdots + b_p 10^p$. On a alors

$$N = a_0 + a_1 10 + \cdots + a_{p+1} 10^{p+1}$$

avec $a_0 = r$ et $a_k = b_{k-1}$ pour $k = 1, \ldots, p+1$. $\square$

Remarque. — La preuve fournit un algorithme, qui sera présenté pour la base b.

1.2 Écriture en base b

Soit b un entier ≥ 2.

Proposition 1.2. — *Pour tout entier* $N \in \mathbb{N}^*$, *il existe* $p \in \mathbb{N}$ *et* $a_0, \ldots, a_p \in \{0, \ldots, b-1\}$ *uniques tels que* $N = a_0 + a_1 b + \cdots + a_p b^p$ *et* $a_p \neq 0$.

L'écriture $N = a_p \ldots a_0$ s'appelle l'*écriture en base* b de N ; elle est aussi notée $N = (a_p \ldots a_0)_b$.

Principale bases utilisées : $b = 2, 10, 16, 20$ (Maya), 60 (Mésopotamie), 256 (octets). En base 16, utilisée par les informaticiens à 16 doigts, on ajoute les symboles A, B, C, D, E et F pour désigner les “chiffres” de 10 à 15.

Exemple 1.3. — $2^{10} = 1024$ en base 10, $2^{10} = 10\,000\,000\,000$ en base 2, $2^{10} = 400$ en base 16.
$2^{16} = 65\,536 = (2^4)^4 = (10\,000)_{16}$. $(11)_{10} = 1 + 1 \times 2 + 1 \times 2^3 = (1011)_2$.

Remarque 1.4. — La conversion d'une base $b \geq 2$ vers la base 10 est plus facile : on calcule b^n puis $a_n b^n$ et on additionne.

1.2.1 Conversion vers la base b

On dispose d'un nombre $N \in \mathbb{N}$ écrit dans un système de numération dans lequel on sait effectuer la division entière. On veut l'écrire en base b. On effectue succesivement la division euclidienne par b jusqu'à obtenir un quotient nul, puis on écrit les restes en commençant par la fin.

Exemple 1.5. — Écrire 3980 en base 8. On a (en base 10) :

$$3980 = 497 \times 8 + \mathbf{4} \qquad 497 = 62 \times 8 + \mathbf{1} \qquad 62 = 7 \times 8 + \mathbf{6} \qquad 7 = 7 \times 0 + \mathbf{7}$$

d'où

$$(3980)_{10} = ((7 \times 8 + 6) \times 8 + 1) \times 8 + 4 = \mathbf{7} \times 8^3 + \mathbf{6} \times 8^2 + \mathbf{1} \times 8^1 + \mathbf{4} \times 8^0 = (7614)_8.$$

Exemple 1.6. — Écrire 263 en base 2.

$$\begin{array}{rl}
263 = 2 \times 131 + 1 & a_0 = 1 \\
131 = 2 \times 65 + 1 & a_1 = 1 \\
65 = 2 \times 32 + 1 & a_2 = 1 \\
32 = 2 \times 16 + 0 & a_3 = 0 \\
16 = 2 \times 8 + 0 & a_4 = 0 \\
8 = 2 \times 4 + 0 & a_5 = 0 \\
4 = 2 \times 2 + 0 & a_6 = 0 \\
2 = 2 \times 1 + 0 & a_7 = 0 \\
1 = 2 \times 0 + 1 & a_8 = 1
\end{array}$$

Conclusion : $263 = (10000111)_2$.

Remarque 1.7. — Pour convertir un nombre de la base b à la base b', il est commode de passer par la base 10. On peut aussi faire directement les calculs dans la base b.

Exemples. — $(123)_5 = (53)_7$, $(123)_7 = (231)_5$.

Remarque 1.8. — [ALGORITHME] Donnée : $N \in \mathbb{N}^*$, sortie : liste $(a_0, \ldots, a_p)$

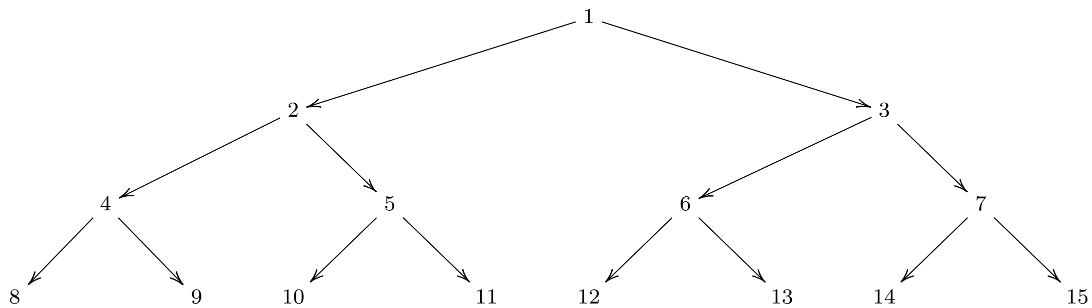
$p \leftarrow 0$;
Tant que $N > 0$ faire
$\{N = bq + r$;
$a_p \leftarrow r$;
$N \leftarrow q$;
$p \leftarrow p + 1$;
$\}$

1.2.2 Numérotation des nœuds d'un arbre binaire complet

Un *arbre binaire* est un arbre orienté avec une *racine* dans lequel chaque *nœud* (ou *sommet*) a au plus deux *fils*[2]. Un *arbre binaire entier* est un arbre dont tous les nœuds possèdent zéro ou deux fils. Un *arbre binaire complet* est un arbre binaire entier dans lequel toutes les *feuilles* (nœuds n'ayant aucun fils) ont la même *profondeur*, i.e. sont à la même distance de la racine. Tout ensemble de nœuds à égale distance de la racine s'appelle une *ligne*.

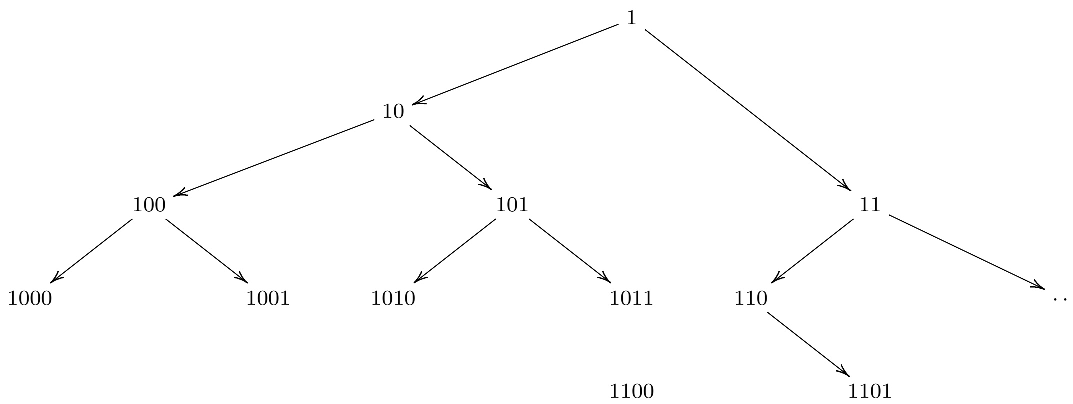
La *profondeur* d'un arbre binaire complet est la profondeur de ses feuilles. Si un arbre binaire complet est de profondeur n, il a $n+1$ lignes, 2^{n-1} feuilles et $2^n - 1$ nœuds (puisque $1 + 2 + \cdots + 2^{n-1} = 2^n - 1$).

Si l'on numérote les nœuds de haut en bas et, dans chaque ligne, de gauche à droite, pour un arbre binaire complet de profondeur 3, on obtient :

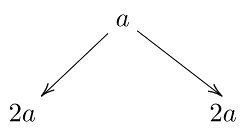


et avec une numérotation en base 2 :

2. j'utilise le mot *fils* au lieu de *descendant* uniquement parce qu'il est plus court.

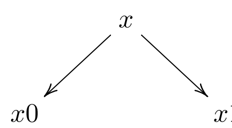


Soit un nœud numéroté a ; ses fils gauche et droit sont alors numérotés $2a$ et $2a+1$:



En effet, si les lignes sont numérotées $0, 1, 2, \dots$ et si a se trouve à la ligne n et à la place m dans cette ligne (avec $0 \leq m \leq 2^n - 1$), alors $a = 2^n + m$ et donc son fils gauche est numéroté $2^{n+1} + 2m$, puisque si a est précédé de m nœuds alors son fils gauche est précédé de $2m$ nœuds.

Si x est l'écriture de a en base 2, alors $2a = x0$ et $2a+1 = x1$:



Cela résulte de l'égalité

$$2\sum_{k=0}^{n} a_k 2^k = \sum_{k=0}^{n} a_k 2^{k+1} = \sum_{k=1}^{n+1} a_{k-1} 2^k.$$

On peut aussi numéroter l'arbre binaire infini à l'aide des rationnels, voir l'exercice 18 de la feuille de TD. Une comparaison des deux numérotations fournit alors une bijection explicite entre les deux ensembles $\mathbb{N}$ et $\mathbb{Q}$.

1.3 Nombre décimaux

Ce sont les nombres réels dont l'écriture décimale est finie. Par exemple $3,14 = \dfrac{314}{100} = \dfrac{157}{50}$ est un nombre décimal (alors que π ne l'est pas).

Définition 1.9. — On dit qu'un réel x est un *nombre décimal* s'il existe $p, q \in \mathbb{Z}$, avec $p \leq q$, et $a_p, \dots, a_q \in \{0, \dots, 9\}$ tels que

$$x = \pm \sum_{k=p}^{q} a_k 10^k.$$

Attention : p peut être positif ou négatif.

Proposition 1.10. — *Un nombre réel x est un nombre décimal si et seulement s'il existe $n \in \mathbb{N}$ tel que $10^n x$ soit un entier, si et seulement si x est un nombre rationnel dont l'écriture en fraction irréductible a un dénominateur n'ayant que des 2 et des 5 dans sa décomposition en facteurs premiers, i.e. $x = \frac{a}{b}$ avec $a \in \mathbb{Z}$, $b \in \mathbb{N}^*$, $\mathrm{pgcd}\,(a,b) = 1$ et $b = 2^\alpha 5^\beta$, $\alpha, \beta \in \mathbb{N}$. Le nombre de chiffres après la virgule est alors égal à $\min\{n \in \mathbb{N} \; ; \; 10^n x \in \mathbb{Z}\} = \max\{\alpha, \beta\}$.*

Remarque 1.11. — Les nombres qui s'écrivent

$$x = \pm \sum_{k=p}^{q} a_k 2^k \ ,$$

i.e. ayant un développement en base 2 fini s'appellent les nombres *dyadiques*.

1.4 Développement décimal d'un réel positif

Rappelons quelques définitions et notations.

La *partie entière* d'un entier y (en anglais : "floor") est

$$\lfloor y \rfloor = \max\{n \in \mathbb{Z} \; ; \; n \leq y\}.$$

C'est l'unique entier n tel que $n \leq y < n+1$. Ainsi $\lfloor -\pi \rfloor = -4$ (et non -3).

La *partie entière supérieure* de y (en anglais : "ceil") est

$$\lceil y \rceil = -\lfloor -y \rfloor = \min\{n \in \mathbb{Z} \; ; \; n \geq y\}.$$

L'*entier le plus proche* de y (en anglais "round") est

$$\lfloor y \rceil = \lceil y - \tfrac{1}{2} \rceil.$$

Ainsi $\lfloor 2,5 \rceil = 2$. Pour simplifier, nous n'utiliserons que la partie entière ("floor") d'un réel positif.

▷ Approximation décimale d'un réel positif. Soit x un nombre réel strictement positif. Pour tout $n \in \mathbb{N}$, posons

$$a_n = \frac{\lfloor 10^n x \rfloor}{10^n} \qquad \text{et} \qquad b_n = \frac{\lfloor 10^n x \rfloor + 1}{10^n}.$$

Montrons que les suites $(a_n)_{n\geq 0}$ et $(b_n)_{n\geq 0}$ sont adjacentes. Comme $b_n - a_n = 10^{-n}$ on a déjà que $b_n - a_n \to 0$ quand $n \to +\infty$. Ensuite, pour tout $y \in \mathbb{R}$, par définition de la partie entière, on a

$$\lfloor y \rfloor \leq y < \lfloor y \rfloor + 1 \quad \text{et donc} \quad y - 1 < \lfloor y \rfloor \leq y.$$

D'une part, en remplaçant y par $10y$ dans cette dernière double inégalité, on obtient $10y - 1 < \lfloor 10y \rfloor \leq 10y$ et, d'autre part, en multipliant cette double inégalité par -10, il vient $-10y \leq -10\lfloor y \rfloor < -10y + 10$. En additionnant, on obtient $-1 < \lfloor 10y \rfloor - 10\lfloor y \rfloor < 10$, et puisque $\lfloor 10y \rfloor - 10\lfloor y \rfloor$ est un entier, on a finalement

$$0 \leq \lfloor 10y \rfloor - 10\lfloor y \rfloor \leq 9. \tag{1}$$

Comme

$$a_{n+1} - a_n = \frac{\lfloor 10^{n+1}x \rfloor - 10\lfloor 10^n x \rfloor}{10^{n+1}}$$

et

$$b_{n+1} - b_n = \frac{\lfloor 10^{n+1}x \rfloor - 10\lfloor 10^n x \rfloor - 9}{10^{n+1}},$$

on déduit de (1) que les suites (a_n) et (b_n) sont, respectivement, croissante et décroissante, et donc sont adjacentes, donc convergentes vers une même limite. De plus, pour tout $n \geq 0$, on a $\lfloor 10^n x \rfloor \leq 10^n x < \lfloor 10^n x \rfloor + 1$, et donc $a_n \leq x < b_n$; par conséquent les deux suites (a_n) et (b_n) convergent vers x.

Pour tout $n \geq 0$, les nombres *décimaux* a_n et b_n sont appelés *approximation décimale par défaut* et *approximation décimale par excès* de x à 10^{-n} près.

▷ Développement décimal d'un réel positif. Pour $x \in \mathbb{R}$, $x > 0$, posons

$$x_0 = \lfloor x \rfloor \quad \text{et} \quad x_n = \lfloor 10^n x \rfloor - 10\lfloor 10^{n-1}x \rfloor \quad \text{pour} \quad n \geq 1.$$

Les x_n sont des entiers et, de plus, d'après (1), pour tout $n \geq 1$, on a $0 \leq x_n \leq 9$. Ensuite, pour $n \geq 1$, on a

$$\sum_{k=0}^{n} \frac{x_k}{10^k} = x_0 + \sum_{k=1}^{n} \left(\frac{\lfloor 10^k x \rfloor}{10^k} - \frac{\lfloor 10^{k-1}x \rfloor}{10^{k-1}} \right) = x_0 + \frac{\lfloor 10^n x \rfloor}{10^n} - \lfloor x \rfloor = \frac{\lfloor 10^n x \rfloor}{10^n}.$$

Par conséquent, compte tenu de ce qui a été vu plus haut, la série $\sum \frac{x_n}{10^n}$ est convergente et sa somme est égale à x. Ainsi

$$x = x_0 + \sum_{n=1}^{+\infty} \frac{x_n}{10^n}$$

Cette écriture s'appelle le *développement décimal* [3] de x ; on écrit parfois $x = x_0 + 0, x_1 x_2 \ldots x_n \ldots$. Pour chaque $n \geq 1$, le chiffre x_n est appelé la n-ième décimale de x.

Les nombres *décimaux* positifs sont ceux pour lesquels les décimales sont toutes nulles à partir d'un certain rang (*i.e.* la suite d'entiers $(x_n)_{n\geq 1}$ converge vers 0).

Une propriété du développement décimal d'un réel positif x est que la suite d'entiers $(x_n)_{n\geq 1}$ ne peut pas converger vers 9 ; autrement dit le développement décimal de x ne peut pas finir par une infinité de 9. En effet, si au contraire on suppose qu'il existe $n_0 \geq 1$ tel que $x_n = 9$ pour $n > n_0$, alors on aurait

$$\begin{aligned} x &= \sum_{n=0}^{n_0} \frac{x_n}{10^n} + \sum_{n=n_0+1}^{+\infty} \frac{9}{10^n} = \sum_{n=0}^{n_0} \frac{x_n}{10^n} + \frac{9}{10^{n_0}} \sum_{n=1}^{+\infty} \frac{1}{10^n} \\ &= \frac{\lfloor 10^{n_0} x \rfloor}{10^{n_0}} + \frac{1}{10^{n_0}} > \frac{10^{n_0} x}{10^{n_0}} = x, \end{aligned}$$

ce qui est absurde.

1.5 Le cas des rationnels

Proposition 1.12. — *Un nombre est rationnel si et seulement si son développement décimal est ultimement périodique.*

On dit aussi *périodique à partir d'un certain rang.*

Précisons cet énoncé : soit $x \in \mathbb{R}$ et $a_\ell \ldots a_0, x_1 x_2 \ldots x_n \ldots$ son développement décimal (avec $x_0 = a_\ell \ldots a_0 = \lfloor x \rfloor \in \mathbb{N}$, $a_i \in \{0, \ldots, 9\}$ pour $0 \leq i \leq \ell$ et $x_i \in \{0, \ldots, 9\}$ pour $i \geq 1$). Alors $x \in \mathbb{Q}$ si, et seulement si, il existe $m \in \mathbb{N}$ et $p \in \mathbb{N}^*$ tels que $x_{k+p} = x_k$ pour tout $k > m$. Si m et p sont choisis minimaux avec cette propriété, alors m est la longueur de la *prépériode* de x et p la longueur de la période de x. On écrit habituellement le développement de x sous la forme $a_\ell \ldots a_0, x_1 x_2 \ldots x_m \overline{x_{m+1} \ldots x_{m+p}}$. Ainsi $0,3171717\ldots$ s'écrit $0,3\overline{17}$.

Preuve. — Quitte à changer x en $x - \lfloor x \rfloor$, on peut supposer que $x \in [0,1[$. En effet on a $(x \in \mathbb{Q} \Leftrightarrow x - \lfloor x \rfloor \in \mathbb{Q})$ et le développement décimal de $x - \lfloor x \rfloor$ est le même que celui de x en remplaçant $x_0 = a_\ell \ldots a_0$ par 0.

Si $x = 0, x_1 x_2 \ldots x_m \overline{x_{m+1} \ldots x_{m+p}}$, soit $M = x_1 x_2 \ldots x_m \in \mathbb{N}$ et soit $y = 10^m x - M = 0, \overline{y_1 \ldots y_p}$ avec $y_i = x_{m+i}$ (on a décalé x de m crans vers la gauche et ôté la partie entière, donc les chiffres de y sont les mêmes que ceux de x décalés). Alors $10^p y = y_1 \ldots y_p + 0, \overline{y_1 \ldots y_p}$ (en décalant de p l'écriture de y, on obtient une partie entière égale à $y_1 \ldots y_p$ et la même

3. On dit aussi parfois *développement décimal illimité.*

partie décimale). En posant $N = y_1 \dots y_p \in \mathbb{N}$, on a donc $10^p y = N + y$, d'où $y = \frac{N}{10^p-1} \in \mathbb{Q}$, et donc $x = \frac{1}{10^m}(M + y)$ lui aussi est rationnel.

Réciproquement, soit $x = \frac{a}{b}$ avec $a, b \in \mathbb{N}$, $a < b$ (on a supposé $0 \leq x < 1$) et pgcd $(a, b) = 1$.

- Si x est un nombre décimal (i.e. $b = 2^\alpha 5^\beta$, $\alpha, \beta \in \mathbb{N}$) alors son développement est ultimement périodique : $x = 0, x_1 \dots x_m\overline{0}$.

- Sinon, pour calculer le développement décimal de x, on divise $10a$ par b : $10a = bq+r_1$. Le quotient q est le premier chiffre x_1 (qui est bien entre 0 et 9 puisque $a < b$) et le reste r_1 sert à calculer le chiffre suivant : $10r_1 = bx_2+r_2$ et ainsi de suite. Comme il n'y a que $b-1$ restes possibles parmi les nombres $1, \dots, b-1$ (le reste n'est jamais nul puisque x n'est pas décimal), d'après le *principe des pigeons*, on retombe nécessairement sur un reste déjà rencontré et ensuite les opérations se répètent en boucle, donnant un développement qui se répète. On est même sûr que $p \leq b - 1$. $\square$

Remarque. Dans le cas où b est premier, on peut dire encore un peu plus sur la longueur p de la période grâce au *théorème de Lagrange* (hors programme). En effet ce théorème nous dit que le cardinal de tout sous-groupe d'un groupe divise toujours le cardinal du groupe. En appliquant ce théorème au sous-groupe engendré par 10 dans le groupe multiplicatif $(\mathbb{Z}/b\mathbb{Z})^*$, on montre ainsi que, d'une part

- p est un diviseur de $b - 1$, et d'autre part

- les développements de k/b pour $k = 1, \dots, b-1$ se répartissent en ℓ classes avec $\ell = p/(b - 1)$.

Ainsi, par exemple :

- la longueur de période de $\frac{1}{13} = 0,\overline{076923}$ est 6, qui divise 12, et les $k/13$ se répartissent en 2 classes,
- la longueur de période de $\frac{1}{41} = 0,\overline{02439}$ est 5, qui divise 40, et les $k/41$ se répartissent en 8 classes,
- la longueur de période de $\frac{1}{37} = 0,\overline{027}$ est 3, qui divise 36, et les $k/37$ se répartissent en 12 classes.