142857
nombres permutables

par Nathaly Lederman, Aline Gautier, Tatsuhei Iwasaki, Régis Lachaume et Stéphane Fischler, élèves de Tle C, lycée La Fontaine (Paris 16ème)

enseignants : Ghislaine Gaudemet et Jean Rouquette

chercheur : Alain Pajor

« Nous tenons à remercier :

— Monsieur LANCELIN, Proviseur du lycée Jean de La Fontaine, pour avoir contribué à la création de Math en Jeans au lycée ;

— Madame GAUDEMET et Monsieur ROUQUETTE, Professeurs de Mathématiques au lycée La Fontaine, pour avoir animé Math en Jeans dans notre établissement ;

— Monsieur PAJOR, Chercheur en Mathématiques à Paris VI, pour nous avoir aidés à mettre en forme nos résultats et nous avoir proposé des élargissements du sujet. »

Le nombre 142857 a une propriété exceptionnelle : quand on forme ses 6 permutations circulaires (à savoir 142857, 428571, 285714, 857142, 571428 et 714285), ces 6 nombres sont multiples de 142857. En effet :

$$142857 = 1 \times 142857$$
$$428571 = 3 \times 142857$$
$$285714 = 2 \times 142857$$
$$857142 = 6 \times 142857$$
$$571428 = 4 \times 142857$$
$$714285 = 5 \times 142857$$

Nous appellerons “6-permutable” ou “permutable à 6 chiffres” un tel nombre, puisqu’il est formé de 6 chiffres (un chiffre étant compris entre 1 et 9 et un nombre étant formé de chiffres).

Théoriquement, il faudrait spécifier dans quelle base on considère ce nombre ; mais comme on ne travaille qu’en base 10 (du moins dans les deux premières parties et le début de la troisième), cela sera implicite.

En revanche, il est capital de préciser à combien de chiffres un nombre donné est permutable. En effet, on peut par exemple considérer le nombre 123 à 5 chiffres ; on le complétera alors de deux zéros à gauche pour qu’il s’écrive avec 5 chiffres. Ses permutations circulaires seront donc 00123, 01230, 12300, 23001 et 30012. On peut vérifier que 123 est alors 5-permutable (on a : $23001 = 123 \times 187$ et $30012 = 123 \times 244$).

Un nombre donné est donc susceptible d’être q-permutable pour certains entiers q, mais pas pour d’autres (l’étude des entiers q pour lesquels un nombre donné est q-permutable fera l’objet de la troisième partie).

Le premier problème qui se pose est de trouver des nombres q-permutables, voire tous les nombres q-permutables, pour une valeur donnée de q. Pour aborder cette question, nous avons d’abord remarqué que 142857 (nombre 6-permutable) est un diviseur de $10^6 - 1$, et que 123 (nombre 5-permutable) est un diviseur de $10^5 - 1$.

Nous avons réussi à démontrer que tous les diviseurs de 10^q - 1 sont *q*-permutables : c'est l'objet de notre première partie.

Ensuite, nous avons cherché quels autres nombres sont q-permutables : c'est la deuxième partie.

Enfin, une troisième partie contient des élargissements possibles du sujet.

Première partie : démonstration directe

Soit A un diviseur de 10^q-1 (cette notation fait l'objet, comme toutes les autres notations et définitions utilisées, d'un récapitulatif à la fin de l'annexe).

Notons $A = a_1a_2\ldots a_q$: le nombre *A* s'écrit en base 10 avec les chiffres a_1, a_2, …, a_q. On peut avoir $a_1 = 0$, voire $a_1 = a_2 = 0$. Ainsi, pour $q = 6$, $A = 91$ est un diviseur de 10^6-1. On note alors $a_1 = a_2 = a_3 = a_4 = 0$, $a_5 = 9$ et $a_6 = 1$.

Considérons la fraction $A/(10^q\text{-}1)$. Comme *A* est un diviseur de 10^q-1, elle se simplifie en $1/k$ où *k* est un entier. Elle a pour écriture décimale (d'après le théorème 1 établi en annexe) :

$$1/k = 0,a_1a_2\ldots a_qa_1a_2\ldots a_qa_1a_2\ldots ;$$

cette écriture est périodique de période $a_1a_2\ldots a_q$, soit *A*. Désormais, on notera une telle écriture en gras et italique : $0,\boldsymbol{a_1a_2\ldots a_q}$.

Cherchons, pour une valeur fixée de *i* ($i \in [2, q]$, *i* entier), le réel *t* défini par :

$$t/k = 0,\boldsymbol{a_i\ldots a_qa_1\ldots a_{i-1}}.$$

Cette fraction a pour période le nombre $a_i\ldots a_qa_1\ldots a_{i-1}$, noté *F*. *F* est une permutation circulaire de *A*. Montrons qu'en fait, *t* est un entier.

On a :

$$10^{i-1}/k = a_1\ldots a_{i-1},\boldsymbol{a_i\ldots a_qa_1\ldots a_{i-1}},$$

par propriété de la multiplication par une puissance de 10.

Par soustraction, il vient :

$$(10^{i-1} - t) / k = a_1\ldots a_{i-1}.$$
$$10^{i-1} - t = k\ a_1\ldots a_{i-1}.$$

Le membre de droite est un entier, donc celui de gauche aussi : *t* est entier.

La démonstration est achevée : t/k vaut, par définition et d'après le théorème 1 de l'annexe, $F/(10^q\text{-}1)$. Or $1/k$ vaut $A/(10^q\text{-}1)$. Nous avons donc démontré que $F = t \times A$. Comme *t* est entier, la permutation circulaire *F* de *A* est multiple de *A*.

Cette démonstration est valable pour tout *i* compris entre 2 et *q*, c'est-à-dire pour toute permutation circulaire de *A* (sauf *A* lui-même, qui correspond à $i = 1$) : le nombre *A* est *q*-permutable.

THEOREME :

Tout diviseur *A* de 10^q-1 est *q*-permutable.

Le problème de la réciproque se pose alors : les diviseurs de 10^q-1 sont-ils les seuls nombres *q*-permutables ?

La réponse est non : le nombre 246 est 5-permutable et n'est pas un diviseur de 10^5-1. Déterminons donc tous les nombres *q*-permutables.

Deuxième partie : réciproque

Préambule et notations

Soit $D = d_1d_2\ldots d_q$ un entier *q*-permutable (on note en *italique* l'écriture d'un nombre en base 10).

De même que dans la démonstration directe, on peut avoir $d_1 = 0$, voire $d_1 = d_2 = 0$.

Toutefois, on exclut la possibilité que tous les d_i soient nuls, c'est-à-dire $D = 0$.

Pour tout entier i compris entre 1 et q, on note X_i l'entier $d_1d_2\ldots d_i$.

Ainsi, $X_1 = d_1$ et $X_2 = d_1d_2$ (il s'agit non du produit de d_1 et de d_2 mais du nombre qui s'écrit en base 10 avec les deux chiffres d_1 et d_2). X_i est donc l'entier que forment les i premiers chiffres de D.

On note X le nombre rationnel $0,\boldsymbol{d_1d_2\ldots d_q}$ (on note en **gras** et *italique* la période d'un nombre rationnel).

X s'écrit, d'après le théorème 1 de l'annexe, p/k où k est un diviseur de 10^q-1 et p et k sont premiers entre eux (c'est-à-dire qu'il n'existe aucun entier u différent de 1 tel que p et k soient simultanément multiples de u ; autrement dit, la fraction p/k est irréductible).

Ainsi, pour D = 246 considéré à 5 chiffres, X_4 vaut 0024 = 24 et $X = 0,\boldsymbol{00246}$ s'écrit 2/813, donc p = 2 et k = 813 (2 et 813 sont bien premiers entre eux).

Le but de cette démonstration est de montrer qu'on peut toujours se ramener à un cas où p vaut 1 (on retrouve alors pour D un diviseur de 10^q-1).

Le lemme 1 établit un résultat réutilisé par la suite ; le lemme 2 prouve que, avec les notations précédentes, on a $p \leq 9$ et montre dans quels cas on a : $p \in [2, 9]$.
Enfin, un théorème résume ces lemmes.

le lemme 1

Calculons la valeur de X_i/X pour montrer que cette valeur est entière.

On a :

$$X_i / X = d_1\ldots d_i / 0,\boldsymbol{d_1\ldots d_q}$$

(le dénominateur en gras-italique renvoie à la fraction de période $D = d_1d_2\ldots d_q$)

$$X_i/X = [d_1\ldots d_i,\boldsymbol{d_{i+1}\ldots d_qd_1\ldots d_i} / 0,\boldsymbol{d_1\ldots d_q}] - [0,\boldsymbol{d_{i+1}\ldots d_qd_1\ldots d_i} / 0,\boldsymbol{d_1\ldots d_q}]$$

Le premier terme de la différence vaut 10^i ; le second vaut un entier t car le nombre $D = d_1\ldots d_q$ est q-permutable : $d_{i+1}\ldots d_qd_1\ldots d_i$, qui est une permutation circulaire de D, est un multiple de D.

D'où $$X_i / X = 10^i - t.$$

Or $X = p/k$ (voir le préambule) : $(kX_i)/p$ vaut 10^i-t, donc est entier : p est diviseur de kX_i. Comme p est premier avec k, il est diviseur de X_i (lemme de Gauss).

LEMME 1 :

pour tout entier i, avec $i \in [1, q]$, X_i est multiple de p.

Dans cet énoncé, X_i est le nombre formé par les i premiers chiffres de D ; p est l'entier tel que $X = 0,\boldsymbol{d_1\ldots d_q}$ s'écrive p/k avec p et k premiers entre eux. Le nombre $D = d_1\ldots d_q$ est supposé q-permutable.

Donnons un exemple de ce lemme. Choisissons q = 5, D = 00369 (369 est bien 5-permutable) et i = 4.

On a donc :

$$X_4 = 0036 = 36.$$

Le réel $X = 0,00369$ s'écrivant p/k, p et k premiers entre eux, montrons que p est un diviseur de X_4 = 36. Pour cela, calculons X_4/X.

X_4/X = 36/0,0036900369…
X_4/X = 36,9003690036… / 0,0036900369…
- 0,9003690036… / 0,0036900369…

Or le premier terme de cette différence vaut 10^4, et le deuxième 90036/00369, c'est-à-dire 244, qui est entier car 369 est 5-permutable.

$X_4/X = 10^4$-244 = 9756.

D'où $(X_4 \times k) / p$ est un entier : d'après le lemme de Gauss, comme p et k sont premiers entre eux, p est un diviseur de X_4 = 36.

le Lemme 2

Démontrons que, en conservant toujours les notations du préambule, tous les chiffres qui forment le nombre D sont des multiples de p, c'est-à-dire que pour tout entier i, avec $i \in [1, q]$, d_i est multiple de p (p est défini comme l'entier tel que X s'écrive p/k avec p et k premiers entre eux, où X est le nombre $0,\boldsymbol{d_1 \ldots d_q}$ et $D = d_1 \ldots d_q$ est un entier q-permutable).

Ainsi, si D vaut 00369 (qui est 5-permutable), p doit être un diviseur de 3, de 6 et de 9 : p ne peut valoir que 1 ou 3. En réalité, $X = 0,00369$ s'écrit 3/813 : p vaut 3.

Le premier chiffre de D, noté a_1, est divisible par p d'après le lemme 1 appliqué au rang 1 (car $X_1 = d_1$).

Pour tout chiffre de D autre que le premier, notons i son rang ($i \in [2, q]$).

On a :

$$X_i = 10 \times X_{i-1} + d_i,$$

d'après la définition de X_i et de X_{i-1}.

D'où $$d_i = X_i - 10 \times X_{i-1} :$$

d_i est la différence de deux entiers divisibles par p (d'après le lemme 1), donc d_i est divisible par p.

LEMME 2 :

Si D est un nombre q-permutable, tous les chiffres d_i qui composent le nombre D sont divisibles par p.

Dans l'énoncé de ce lemme, p est l'entier tel que $X = 0,\boldsymbol{d_1 \ldots d_q}$ s'écrive p/k avec p et k premiers entre eux. L'entier $D = d_1 \ldots d_q$ est supposé q-permutable.

Une conséquence de ce lemme est que p, qui est un diviseur de d_i avec $d_i \leq 9$, est lui-même inférieur ou égal à 9.

Ainsi, si D vaut 00369 (qui est 5-permutable), p doit être un diviseur de 3, de 6 et de 9. Il ne peut valoir que 1 ou 3. En réalité, $X = 0,\boldsymbol{00369}$ s'écrit 3/813 : p vaut 3.

On peut former le quotient $A = D/p$.

Notons, pour tout entier $i \in [1, q]$, $a_i = d_i/p$. A est alors l'entier $a_1 a_2 \ldots a_q$.

On a : $$p/k = 0,\boldsymbol{d_1 \ldots d_q}$$
donc $$1/k = 0,\boldsymbol{a_1 \ldots a_q} = A/(10^q - 1)$$

d'après le théorème 1 démontré en annexe. A est donc un diviseur de $10^q - 1$ (puisque la fraction $A/(10^q - 1)$ se simplifie en $1/k$: on a $10^q - 1 = A \times k$).

Mais A a une particularité supplémentaire : pour tout entier i, avec $i \in [1, q]$, on a : $d_i \leq 9$ donc $a_i \leq 9/p$.

LEMME 2 bis :

Tout nombre D q-permutable s'écrit $p \times A$ où A est un diviseur de $10^q - 1$ et p est un entier tel que tous les chiffres qui composent A soient inférieurs ou égaux à $9/p$.

Tous les chiffres du nombre D sont alors divisibles par p.

le théorème final

La propriété $a_i \leq 9/p$ pour tout entier i s'écrit aussi : $max\ a_i \leq 9/p$, où $max\ a_i$ désigne le plus grand des a_i, pour i entier compris entre 1 et q. On peut en déduire que

$$(max\ a_i)/9 \leq 1/p, \text{ soit } p \leq 9/(max\ a_i).$$

Tout nombre D q-permutable s'écrit donc $p \times A$ où A est un diviseur de $10^q - 1$ et où p est un entier tel que :

$$1 \leq p \leq 9/(max\ a_i).$$

Réciproquement, les nombres qui s'écrivent $p \times A$, où A est un diviseur de $10^q - 1$ et p un

entier non nul inférieur à $9/(max\ a_i)$, sont q-permutables. C'est vrai pour $p = 1$ d'après la première partie. Si p est strictement supérieur à 1, le nombre $p \times A$ est q-permutable à condition que la multiplication de A par p s'effectue sans utiliser de retenues, ce qui est le cas si p est inférieur à $9/(max\ a_i)$.

Ainsi, $A = 123$ est un diviseur de 10^5-1. Dans cet exemple, $max\ a_i$ vaut 3, donc p doit être inférieur ou égal à $9/(max\ a_i) = 3$. On obtient donc les nombres 123, 246 et 369 qui sont tous 5-permutables.

Vérifions-le :

00123/123 = 00246/246 = 00369/369 = 1
01230/123 = 02460/246 = 03690/369 = 10
12300/123 = 24600/246 = 36900/369 = 100
23001/123 = 46001/246 = 69003/369 = 187
30012/123 = 60024/246 = 90036/369 = 244

THÉOREME :

Un nombre est q-permutable si, et seulement si, il s'écrit sous la forme $p \times A$ où A est un diviseur de 10^q-1 et p un entier compris entre 1 et $9/(max\ a_i)$ où $max\ a_i$ est le plus grand chiffre du nombre A.

Le nombre obtenu est alors tel que tous ses chiffres sont des multiples de p.

On peut en déduire une méthode pour déterminer si un nombre D est q-permutable.

Il faut d'abord chercher s'il existe un entier p compris entre 2 et 9 qui soit diviseur de chaque chiffre qui compose le nombre D.

Si un tel nombre existe, on considère le nombre D/p. On est donc ramené au cas où aucun entier p compris entre 2 et 9 n'est simultanément diviseur de tous les chiffres qui composent D (les chiffres de D sont alors dits "premiers dans leur ensemble").

Dans ce cas, D est q-permutable si, et seulement si, il est diviseur de 10^q-1.

Ainsi, pour tester si 84 est 6-permutable, on cherche un entier p diviseur de 8 et de 4. On a le choix entre 2 et 4. Si on opte pour 2, on est ramené à 42 dont les chiffres sont encore divisibles par 2 : on arrive donc à 21, comme si on avait directement divisé par 4. Or 21 est un diviseur de 10^6-1 (car 10^6-1 = 21 × 47619) donc 21, 42 et 84 sont 6-permutables.

Un autre intérêt de ce théorème est qu'il permet de trouver tous les nombres q-permutables, pour un entier q donné.

Il suffit en effet d'énumérer tous les diviseurs de 10^q-1, ce qui peut être réalisé de manière exhaustive à l'aide de la décomposition de 10^q-1 en facteurs premiers.

Ensuite, si A est l'un de ces diviseurs et si $max\ a_i$ est le plus grand des chiffres qui composent l'écriture de A en base 10, on forme les nombres $p \times A$ où p un entier compris entre 1 et $9/(max\ a_i)$. On est alors assuré d'après le théorème que tous les nombres obtenus par cette méthode sont q-permutables, et réciproquement que tous les nombres q-permutables sont obtenus par cette méthode.

On peut alors trouver des nombres qui ne sont jamais q-permutables, quel que soit l'entier q.

Il s'agit, tout d'abord, des nombres pairs dont au moins un chiffre est impair. Raisonnons par l'absurde : si un tel nombre D était q-permutable, il s'écrirait $p \times A$, avec les notations précédentes.

Or p ne peut être pair, sinon tous les chiffres qui composent D seraient pairs (d'après le lemme 2 bis). Donc p est impair ; mais A, diviseur du nombre impair 10^q-1, est aussi impair : $D = p \times A$ est donc impair, et il y a contradiction. Un tel nombre ne peut donc pas être q-permutable, quel que soit q. De même, un nombre divisible par 5 mais dont au moins un chiffre est différent de 0 et de 5 ne peut pas être q-permutable, quel que soit q.

La démonstration est la même, en remplaçant “pair” par “divisible par 5” et “impair” par “non divisible par 5”.

Ce résultat était d’ailleurs visible directement : soit, par exemple, le nombre 416. Considéré à q chiffres (q étant un entier supérieur ou égal à 3), l’une de ses permutations circulaires est 6000…0041, avec (q-3) zéros. Cette permutation circulaire, qui est impaire, ne peut être multiple du nombre de départ, qui est pair. Donc 416 n’est pas q-permutable quel que soit l’entier q.

Pour un entier D donné, notons E l’ensemble des entiers non nuls q tel que D soit q-permutable. Appelons “ensemble des occurrences de D” cet ensemble.

Il existe donc deux catégories de nombres dont l’ensemble des occurrences est l’ensemble vide ; quel est cet ensemble pour les autres entiers ?

Troisième partie : Elargissement du problème

Ensemble des occurrences d’un entier D

S’il existe un entier p compris entre 2 et 9 qui soit un diviseur de chaque chiffre qui compose le nombre D alors les entiers D et D/p ont le même ensemble des occurrences. On peut donc se ramener au cas où il n’existe pas de tel entier p supérieur ou égal à 2.

DÉFINITION : un entier D est dit irréductible s’il n’existe aucun entier p compris entre 2 et 9 qui divise chacun des chiffres qui composent l’écriture en base 10 du nombre D.

Remarque : la phrase “a divise b” signifie que a est un diviseur de b, c’est-à-dire que b est multiple de a.

Autre formulation de la définition :

B est irréductible si, et seulement si, ses chiffres sont premiers dans leur ensemble (c’est-à-dire si leur PGCD vaut 1).

Un entier irréductible D est alors q-permutable si, et seulement si, c’est un diviseur de 10^q-1 (d’après le théorème démontré dans la deuxième partie). Donc, pour tout entier q, $q \in E$ si, et seulement si, 10^q-1 est multiple de D.

Si D est pair ou divisible par 5 (c’est-à-dire si D n’est pas premier avec 10), alors D n’est pas q-permutable quel que soit l’entier q (on suppose en effet D irréductible ; ce résultat a déjà été démontré).

Sinon (c’est-à-dire si D est premier avec 10), pour démontrer que E n’est pas vide, utilisons l’anneau $\mathbb{Z}/D\mathbb{Z}$ présenté juste avant l’annexe. D’après le théorème 3 démontré en annexe, il existe au moins un entier T tel que :

$$10^T \equiv 1 \pmod{D},$$

c’est-à-dire tel que D soit permutable à T chiffres. L’ensemble E des occurrences de D est donc non vide pour tout entier D irréductible et premier avec 10. *On supposera doré - navant que ces deux conditions sont remplies.*

L’ensemble E, qui est une partie non vide de $\mathbb{N}^*$, a un plus petit élément u. L’entier u s’appelle l’ordre de 10 dans $\mathbb{Z}/D\mathbb{Z}$.

Montrons que E est l’ensemble $u\cdot\mathbb{N}^*$ des multiples strictement positifs de u.

Montrons d’abord que $u\cdot\mathbb{N}^*$ est inclus dans E. En effet, pour tout entier strictement positif a, on a :

$$10^{a\times u} \equiv (10^u)^a \equiv 1^a \equiv 1 \pmod{D},$$

donc $(a \times u) \in E$.

Montrons maintenant que E est inclus dans $u\cdot\mathbb{N}^*$.

Soit n un élément de E.

Alors, par division euclidienne de n par u, n s’écrit de manière unique sous la forme $s\times u+r$ avec r compris entre 0 et u-1 et s

entier. On a : $10^n \equiv 10^{(s\times u)+r} \pmod{D}$.
$\equiv (10^u)^s \times 10^r \pmod{D}$.
$\equiv 1^s \times 10^r \pmod{D}$.
$\equiv 10^r \pmod{D}$.
Or, comme n est un élément de E,
$10^n \equiv 1 \pmod{D}$.
Par transitivité, on a aussi :
$10^r \equiv 1 \pmod{D}$.
Si r est non nul, il est donc (par définition de E) un élément de E. Mais $r \leq u$-1, ce qui contredit la définition de u comme plus petit élément de E. Donc r est nul et n, qui s'écrit $s \times u$, est bien un élément de $u\cdot$N*.

L'ensemble E s'écrit donc bien $u\cdot$N*, où u est l'ordre de 10 dans Z/DZ.

Appliquons le théorème 3 démontré en annexe : u est un diviseur de $\varphi(D)$, où $\varphi(D)$ est l'indicatrice d'Euler, qui représente le nombre d'entiers inférieurs à D et premiers avec D.

D'autre part, u est supérieur ou égal au nombre de chiffres qui forment D quand D ne commence pas par un zéro ; ainsi, pour D = 6451, 10^2 et 10^3 ne peuvent pas, de façon évidente, être congrus à 1 modulo D, puisqu'ils sont inférieurs à D. Cela est en accord avec la définition même de nombre q-permutable : un nombre de 4 chiffres ne peut pas être 3-permutable.

THÉOREME :

L'ensemble *E* des occurrences d'un entier *D* est donné par :
• S'il existe un entier *p* compris entre 2 et 9 qui divise simultanément tous les chiffres qui composent le nombre *D*, l'ensemble des occurrences de *D* est le même que celui de *D*/*p* ;
•Si *D* est irréductible :
— *E* est l'ensemble vide si *D* et 10 ont un diviseur commun autre que 1, c'est-à-dire si *D* est pair ou divisible par 5 ;
— *E* est du type *u*·N* si *D* et 10 sont premiers entre eux ; *u* est compris entre le nombre de chiffres de *D* et φ(*D*). De plus, *u* est un diviseur de φ(*D*).

Une conséquence immédiate de ce théorème est que si D est irréductible et premier avec 10 alors $\varphi(D)$, qui est un multiple de u, est élément de E : D est $\varphi(D)$-permutable.

Exemple d'application de ce théorème : choisissons D = 123, qui est irréductible car les chiffres 1, 2 et 3 sont premiers dans leur ensemble. Comme, de plus, 123 est premier avec 10, $E = u\cdot$N*. On sait que u est compris entre 3 (le nombre de chiffres de 123) et $\varphi(123)$, et que u est un diviseur de $\varphi(123)$. Pour calculer $\varphi(123)$, on peut appliquer la formule suivante (dont une démonstration est donnée en annexe, au théorème 2) :

Ecrivons n sous la forme $\prod_{i=1}^{i=r} (p_i^{si})$ où le symbole $\prod$ désigne le produit [des p_i^{si} pour i entier compris entre 1 et r] (r est un entier qui dépend de n). On suppose $s_i \geq 1$ et p_i premier (les p_i sont tous distincts). Dans ce cas, on a :

$$\varphi(n) = n \times \prod_{i=1}^{i=r} (1\text{-}1/p_i),$$

ce produit étant effectué pour i entier compris entre 1 et r. Or 123 = 3 × 41. On a : p_1 = 3, p_2 = 41 et r = 2. Donc $\varphi(123) = 123 \times (2/3) \times (40/41) = 80$: u est un entier compris entre 3 (car dire, par exemple, que 123 est permutable à 2 chiffres n'a pas de sens) et 80. De plus, u est un diviseur de 80.

En cherchant la classe de 10^q modulo 123, pour q variant de 3 à 80, on s'aperçoit que cette classe est celle de 1 dès que q vaut 5 : u = 5 et $E = 5\cdot$N*, l'ensemble des multiples strictement positifs de 5.

L'entier u est donc, quel que soit l'entier D irréductible et premier avec 10, inférieur ou égal à $\varphi(D)$. On peut chercher à caractériser les entiers irréductibles D tels que u vaut exactement $\varphi(D)$. On appelle "réfractaire" un tel entier D. Par extension, cette définition s'appliquera aussi aux entiers non irréductibles ; elle signifie simplement que l'ensemble E des occurrences de D est l'ensemble $\varphi(D)\cdot$N* des multiples strictement positifs de $\varphi(D)$.

Entiers réfractaires

Notion de base

Tout ce qui a été démontré précédemment l'a été en base 10 ; mais la même démonstration est possible dans n'importe quelle autre base, à condition de remplacer, partout où il est employé, le nombre 10 par la base choisie.

Il peut être particulièrement intéressant de choisir pour base un nombre premier ; l'ensemble des occurrences de tout entier D non multiple de la base (c'est-à-dire dont l'écriture ne se termine pas par un zéro) est alors de la forme $E = u \cdot \mathrm{N}^*$.

Dorénavant, tous les calculs s'effectueront dans une base b quelconque ; les définitions de nombres irréductible, q-permutable, réfractaire et d'ensemble des occurrences sont à prendre dans cette base.

Appliquons le théorème 4 de l'annexe :

— Si $D = 2 \times A$, où A est un entier irréductible impair, alors D est réfractaire si, et seulement si, A l'est (dans la même base).

— Si $D = 2 \times A$, où A est un entier irréductible pair, ou si $D = p \times A$, où p est un entier supérieur ou égal à 3, alors D ne peut pas être réfractaire, quelle que soit la base considérée. On est donc ramené au cas où D est irréductible.

Si D, qui est irréductible, n'est pas premier avec la base b, D ne sera pas q-permutable, quel que soit q : D ne sera pas réfractaire. On supposera donc dorénavant que D est un entier irréductible (en base b) et que D est premier avec b.

Condition nécessaire pour qu'un entier soit réfractaire

Considérons d'abord le cas (très particulier) de 1. On a $\varphi(1) = 1$, donc 1 est réfractaire dans toute base b. On supposera désormais D supérieur ou égal à 2.

Considérons l'ensemble G des puissances successives de b dans $\mathrm{Z}/D\mathrm{Z}$, D étant premier avec b. $(G, \times)$ est un groupe cyclique commutatif (la démonstration de ce résultat fait l'objet du théorème 3, placé en annexe) dont l'ordre est u et admettant b pour élément générateur, en conservant les notations précédemment définies.

Si u vaut $\varphi(D)$, G est inclus dans $(\mathrm{Z}/D\mathrm{Z})^*$ (d'après le théorème 3) et comporte autant d'éléments que $(\mathrm{Z}/D\mathrm{Z})^*$: $G = (\mathrm{Z}/D\mathrm{Z})^*$, donc $((\mathrm{Z}/D\mathrm{Z})^*, \times)$ est un groupe cyclique qui admet b pour générateur (car il en est ainsi de G).

Réciproquement, si le groupe $((\mathrm{Z}/D\mathrm{Z})^*, \times)$ est cyclique de générateur b alors $u = \varphi(D)$.

THÉOREME :
En base *b*, un entier irréductible *D* premier avec *b* est réfractaire si, et seulement si, le groupe $(\mathrm{Z}/D\mathrm{Z})^*, \times)$ **est cyclique de générateur *b*.**

Exemple : Si D vaut 19 et si b vaut 10, 19 est bien irréductible (en base 10) et premier avec 10. Les restes modulo 19 des puissances successives de 10 sont :

$10^0 \equiv 1 \pmod{19}$	$10^1 \equiv 10 \pmod{19}$
$10^2 \equiv 5 \pmod{19}$	$10^3 \equiv 12 \pmod{19}$
$10^4 \equiv 6 \pmod{19}$	$10^5 \equiv 3 \pmod{19}$
$10^6 \equiv 11 \pmod{19}$	$10^7 \equiv 15 \pmod{19}$
$10^8 \equiv 17 \pmod{19}$	$10^9 \equiv 18 \pmod{19}$
$10^{10} \equiv 9 \pmod{19}$	$10^{11} \equiv 14 \pmod{19}$
$10^{12} \equiv 7 \pmod{19}$	$10^{13} \equiv 13 \pmod{19}$
$10^{14} \equiv 16 \pmod{19}$	$10^{15} \equiv 8 \pmod{19}$
$10^{16} \equiv 4 \pmod{19}$	$10^{17} \equiv 2 \pmod{19}$
$10^{18} \equiv 1 \pmod{19}$	

Le plus petit entier q tel qu'on ait : $10^q \equiv 1 \pmod{19}$ est donc $18 = \varphi(19)$; tous les entiers inférieurs à 19 et premiers avec 19 (ici, ils sont tous premiers avec 19 car 19 est lui-même un nombre premier) s'écrivent comme une puissance de 10 : 10 est générateur de $((\mathrm{Z}/19\mathrm{Z})^*, \times)$ et 19 est réfractaire en base 10.

Nous admettrons le théorème suivant : le groupe $((\mathbb{Z}/D\mathbb{Z})^*, \times)$ est cyclique (c'est-à-dire admet un ou plusieurs éléments générateurs) si, et seulement si, D vaut 2, 4, p^s ou $2p^s$ où p est un nombre premier impair et s un entier supérieur ou égal à 1.

Or pour que D soit réfractaire dans une certaine base b, il est nécessaire que le groupe $((\mathbb{Z}/D\mathbb{Z})^*, \times)$ admette des générateurs, c'est-à-dire que D fasse partie de la liste précédente. Mais cela n'est pas suffisant car dans un groupe cyclique, tout élément n'est pas générateur.

Le cas $D = 2$ est peu intéressant : 2 est réfractaire en base b si, et seulement si, 2 est permutable à 1 chiffre en base b. Il est nécessaire et suffisant que b soit au moins égal à 3.

THÉOREME :
Quelle que soit la base b, une condition nécessaire pour qu'un entier irréductible D soit réfractaire est qu'il soit premier avec b et qu'il vaille 2, 4 ou s'écrive p^s ou $2p^s$ où p est un nombre premier impair et s un entier non nul.

Nous travaillerons donc désormais sur un entier D irréductible (en base b), premier avec b et s'écrivant p^s, $2p^s$ ou valant 4.

Pour que D soit irréductible, il est nécessaire qu'il s'écrive avec au moins deux chiffres en base b, donc on doit avoir : $b \leq D$.

Etudions le cas particulier où D vaut 4.

On a : $b \leq 4$.

Comme 4 doit être premier avec b, b ne peut valoir que 1 ou 3, mais la base 1 n'existe pas donc $b = 3$ est la seule base dans laquelle 4 est éventuellement réfractaire. Or l'ensemble $(\mathbb{Z}/4\mathbb{Z})^*$ ne comporte que deux éléments, les classes de 1 et de 3 ; 3 est bien générateur de cet ensemble [$3^2 \equiv 1 \pmod 4$].

Donc 4 est réfractaire en base 3.

Dorénavant, D sera, de plus, différent de 4 : on suppose qu'il s'écrit p^s ou $2p^s$ où p est un nombre premier impair et s un entier non nul. Pour un tel entier D, on peut chercher dans combien de bases il sera réfractaire. Cela revient à chercher combien il existe de générateurs du groupe $((\mathbb{Z}/D\mathbb{Z})^*, \times)$.

Nombre de générateurs de $((\mathbb{Z}/D\mathbb{Z})^*, \times)$

Le groupe $((\mathbb{Z}/D\mathbb{Z})^*, \times)$ étant cyclique, il est isomorphe au groupe $(\mathbb{Z}/\varphi(D)\mathbb{Z}, +)$. L'isomorphisme est réalisé par la fonction g de $\mathbb{Z}/\varphi(D)\mathbb{Z}$ dans $(\mathbb{Z}/D\mathbb{Z})^*$ définie par

$$g(n) \equiv h^n \pmod D$$

où h est un élément générateur du groupe $((\mathbb{Z}/D\mathbb{Z})^*, \times)$ (h existe car ce groupe est cyclique).

En effet, cette fonction est bijective puisque h est générateur ; de plus, d'après les propriétés des opérations sur les puissances, elle réalise un morphisme de groupes :

$$g(l + m) \equiv g(l) \times g(m) \pmod D$$

pour tous l et m de $\mathbb{Z}/\varphi(D)\mathbb{Z}$.

Le nombre d'éléments générateurs étant conservé par isomorphisme, il suffit de chercher la valeur de ce nombre dans le groupe $(\mathbb{Z}/\varphi(D)\mathbb{Z}, +)$.

Or les éléments générateurs du groupe $(\mathbb{Z}/\varphi(D)\mathbb{Z}, +)$ sont les classes d'équivalence correspondant à des entiers n premiers avec $\varphi(D)$. En effet, dans ce cas, l'égalité

$$n \times k \equiv 0 \pmod{\varphi(D)}$$

implique, d'après le lemme de Gauss, que k soit multiple de $\varphi(D)$.

L'ordre de n dans $(\mathbb{Z}/\varphi(D)\mathbb{Z}, +)$ est $\varphi(D)$: n est générateur. Il y a donc autant d'éléments générateurs que d'entiers compris entre 1 et $\varphi(D)$ et premiers avec $\varphi(D)$, soit $\varphi(\varphi(D))$.

Donc le nombre de générateurs de $((\mathbb{Z}/D\mathbb{Z})^*, \times)$ est $\varphi(\varphi(D))$, d'où le théorème :

THÉOREME :

Pour tout entier *D* de la forme p^s ou $2p^s$, où *p* est un entier premier impair, il existe au moins $\varphi(\varphi(D))$ bases dans lesquelles *D*, s'il est irréductible, est réfractaire.

L'expression "s'il est irréductible" provient du fait qu'un entier est ou non irréductible suivant la base *b* considérée. Parmi les $\varphi(\varphi(D))$ bases qui correspondent à des éléments générateurs, il peut y en avoir certaines où *D* n'est pas irréductible et telles que *b* soit générateur de $((\mathbb{Z}/D\mathbb{Z})^*, \times)$. *D* n'est alors pas réfractaire s'il s'écrit $p \times A$ avec *p* supérieur ou égal à 3, *A* irréductible, ou $2 \times A$ avec *A* pair et irréductible (d'après le théorème 4 de l'annexe).

Si on omet l'hypothèse "*D* est irréductible", il peut y avoir des bases *b*, avec *b* générateur de $((\mathbb{Z}/D\mathbb{Z})^*, \times)$, dans lesquelles *D* n'est pas réfractaire. L'entier *D* peut donc être réfractaire dans moins de $\varphi(\varphi(D))$ bases.

L'expression "au moins" provient du fait qu'il peut exister une base *b* dans laquelle *D* n'est pas irréductible.

Or l'implication logique

"si *D* est irréductible alors *D* est réfractaire"

équivaut à

"*D* est réfractaire ou *D* n'est pas irréductible"

le "ou" étant inclusif.

Dans toute base *b* où *D* n'est pas irréductible, cette proposition est donc vraie, que *b* soit ou non générateur de $((\mathbb{Z}/D\mathbb{Z})^*, \times)$. C'est pourquoi cette proposition peut être vraie dans plus de $\varphi(\varphi(D))$ bases :

la formule "au moins" est nécessaire.

Un entier *D* de la forme p^s ou $2p^s$, où *p* est un entier premier impair et *s* un entier strictement positif, peut donc être réfractaire ou non selon la base considérée : il faut établir une méthode pour le tester.

Méthode de test

Comme nous l'avons démontré précédemment, on peut toujours se ramener au cas où *D* est irréductible et premier avec *b*. On cherche alors à savoir si *b* est générateur de $((\mathbb{Z}/D\mathbb{Z})^*, \times)$. De plus, il est nécessaire que *D* s'écrive p^s ou $2p^s$ (où *p* est un nombre premier impair), pour que le groupe $((\mathbb{Z}/D\mathbb{Z})^*, \times)$ soit cyclique.

Comme *b* est premier avec *D*, il existe des entiers *q* strictement positifs tels que

$$b^q \equiv 1 \pmod{D}.$$

Le plus petit de ces entiers *q* est appelé l'ordre de *b* dans $((\mathbb{Z}/D\mathbb{Z})^*, \times)$. Il est noté *h*. L'élément *b* est générateur si, et seulement si, son ordre *h* est égal au nombre d'éléments du groupe, soit $\varphi(D)$.

La méthode est la suivante :

soit $\prod_{i=1}^{i=r}(p_i^{si})$ la décomposition de $\varphi(D)$ en facteurs premiers, avec *i* entier compris entre 1 et *r*, $s_i \geq 1$ et p_i premier (les p_i sont tous distincts).

On suppose *D* irréductible, premier avec *b* et s'écrivant p^s ou $2p^s$ (où *p* est un nombre premier impair). Soit les entiers N_i définis par : $N_i = \varphi(D)/p_i$, pour *i* compris entre 1 et *r*. Alors *b* est générateur de $((\mathbb{Z}/D\mathbb{Z})^*, \times)$ si, et seulement si, b^{Ni} n'est jamais congru à 1 modulo *D*, quel que soit l'entier *i* compris entre 1 et *r*.

Justification :
la condition est nécessaire, car si l'un des N_i est tel que b^{Ni} soit congru à 1 modulo *D* alors l'ordre de *b* est inférieur ou égal à N_i , et il ne peut être égal à $\varphi(D)$.

Montrons que la condition est suffisante : supposons que l'ordre de b (noté h) est strictement inférieur à $\varphi(D)$ et montrons qu'il existe au moins un entier i tel que b^{N_i} soit congru à 1 modulo D.

D'après le théorème de Lagrange, l'ordre de chaque élément du groupe (et en particulier h, l'ordre de b) est un diviseur de $\varphi(D)$, le nombre d'éléments du groupe cyclique $((\mathbb{Z}/D\mathbb{Z})^*, \times)$ tout entier (ce groupe est cyclique car on suppose que D s'écrit p^s ou $2p^s$ où p est un nombre premier impair).

Le nombre $\varphi(D)/h$ est alors un entier, et un diviseur de $\varphi(D)$; il ne vaut pas 1 car par hypothèse h est strictement inférieur à $\varphi(D)$.

Comme $\varphi(D)$ s'écrit $\prod_{i=1}^{i=r} p_i^{si}$,

le nombre $\varphi(D)/h$ s'écrit $\prod_{i=1}^{i=r} p_i^{ti}$

où les p_i (qui sont les mêmes pour ces deux décompositions) sont des nombres premiers distincts et où t_i est un entier positif (éventuellement nul), avec $t_i \leq s_i$ pour tout entier i. On ne peut avoir $t_i = 0$ pour tout i car sinon $\varphi(D)/h$ vaudrait 1, ce qui est contraire à l'hypothèse.

Il existe donc un ou plusieurs entiers i tels que t_i est non nul. Si i_0 désigne l'un d'entre eux, on a :

$$\varphi(D) / h = p_{i_0} \times e,$$

où e est un entier quelconque. On a dans ce cas :

$$N_{i_0} = \varphi(D)/p_{i_0} = h \times e,$$

ce qui implique :

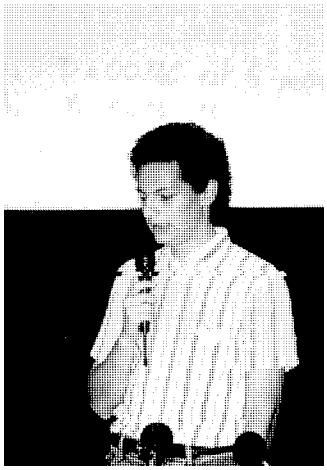
$$b^{N_{i_0}} \equiv b^{h \times e} \equiv (b^h)^e \equiv 1^e \equiv 1 \pmod{D}$$

car h vérifie : $b^h \equiv 1 \pmod{D}$. Il existe donc au moins un entier i tel que b^{N_i} soit congru à 1 modulo D. La méthode donne bien une condition nécessaire et suffisante pour que b soit générateur de $((\mathbb{Z}/D\mathbb{Z})^*, \times)$.

Exemple d'application de cette méthode : montrons que 19 est réfractaire en base 10. 19 est bien irréductible en base 10, premier avec 10 et s'écrit $p^s = 19^1$ avec p = 19, nombre premier impair.

$\varphi(19) = 18$ se décompose en facteurs premiers sous la forme : $18 = 2^1 \times 3^2$. Les nombres à tester sont donc $N_1 = 18/2 = 9$ et $N_2 = 18/3 = 6$.

On évalue donc les restes modulo 19 de 10^6 et de 10^9 ; on trouve respectivement 11 et 18. Aucun de ces deux nombres ne valant 1, 19 est réfractaire en base 10.



Présentation de l'anneau Z/*D*Z

On suppose fixé un entier $D \geq 2$.

Définition :
On dit que deux entiers *a* et *b* sont congrus modulo *D* si *b* est le reste dans la division euclidienne de *a* par *D*, c'est-à-dire si (*a*-*b*) est multiple de *D*.

On note :

$$a \equiv b \pmod{D}.$$

Ainsi, on a :

$$17 \equiv 2 \pmod 5 \text{ car } 17 - 2 = 15 = 3 \times 5.$$

On convient alors d'identifier (c'est-à-dire de considérer comme égaux) deux nombres *a* et *b* si, et seulement si, $a \equiv b \pmod D$.

Dans ce cas, on peut interpréter l'ensemble Z/*D*Z comme l'intervalle [0, *D*-1] de N, muni d'une addition et d'une multiplication.

Pour éviter la confusion avec les opérations dans N ou dans Z, on note l'égalité non = mais avec trois traits : ≡.

Ainsi, l'ensemble Z/5Z (c'est-à-dire Z/*D*Z pour *D* = 5) peut être considéré comme l'ensemble {0 ; 1 ; 2 ; 3 ; 4}, en identifiant deux nombres *a* et *b* si $a \equiv b \pmod 5$.

Par exemple, dans Z/5Z, on a : $2 + 1 \equiv 3$ et $2 \times 3 \equiv 6 \equiv 1$, car comme 6 - 1 = 5, écrire 1 ou écrire 6 revient au même (on a identifié ces deux nombres).

De même, dans Z/7Z, on a : $6 \times 5 \equiv 30 \equiv 2$ car on identifie les nombres 30 et 2 dont la différence vaut 28, qui est un multiple de 7.

Dans Z/8Z, on peut écrire : $4 \times 2 \equiv 8 \equiv 0$.

L'ensemble Z/*D*Z, muni de l'addition et de la multiplication, a alors une structure d'anneau commutatif, c'est-à-dire :

• L'addition possède les propriétés suivantes :

— Elle est interne :

pour tous *a* et *b* de Z/*D*Z,
(*a*+*b*) est un élément de Z/*D*Z.

Par exemple, dans Z/8Z, si on effectue la somme 7 + 6, il existe un entier *c* compris entre 0 et 7 tel qu'on puisse identifier 7 + 6 = 13 à *c*. Dans ce cas, *c* vaut 5 car 13 - 5 = 8.

— Elle est associative :

pour tous *a*, *b* et *c* de Z/*D*Z, on a :
$(a + b) + c \equiv a + (b + c)$.

Par exemple, dans Z/8Z, on a :
$(5 + 6) + 7 \equiv 11 + 7 \equiv 3 + 7 \equiv 10 \equiv 2$ et
$5 + (6 + 7) \equiv 5 + 13 \equiv 5 + 5 \equiv 10 \equiv 2$: la place des parenthèses n'a pas d'influence sur le résultat.

— Elle est commutative :

pour tous *a* et *b* de Z/*D*Z, $a + b \equiv b + a$.

— Elle admet 0 pour élément neutre :

pour tout *a* de Z/*D*Z, $a + 0 \equiv 0 + a \equiv a$.

— Tout élément *a* de Z/*D*Z admet un opposé, c'est-à-dire un élément *a*' de Z/*D*Z tel que $a + a' \equiv 0$.

Par exemple, dans Z/10Z, on a : $3 + 7 \equiv 0$, donc 7 est l'opposé de 3 et 3 celui de 7.

• La multiplication possède les propriétés suivantes :

— Elle est interne :

pour tous *a* et *b* de Z/*D*Z,
$(a \times b)$ est un élément de Z/*D*Z.

— Elle est associative :

pour tous *a*, *b* et *c* de Z/*D*Z,
$(a \times b) \times c \equiv a \times (b \times c)$.

— Elle est commutative :

pour tous a et b de Z/DZ, $a \times b \equiv b \times a$.

— Elle admet 1 pour élément neutre :

pour tout a de Z/DZ, $a \times 1 \equiv 1 \times a \equiv a$.

• La multiplication est distributive sur l'addition :

pour tous a, b et c de Z/DZ,
$a \times (b + c) \equiv (a \times b) + (a \times c)$.

Certains éléments de Z/DZ ont une propriété supplémentaire : pour ces éléments a, il existe un inverse b, c'est-à-dire un élément de Z/DZ tel que $a \times b \equiv 1$. Ainsi, dans Z/5Z, on a : $2 \times 3 \equiv 1$, donc 2 est l'inverse de 3 et 3 celui de 2.

En revanche, dans Z/10Z, 2 n'admet pas d'inverse car il n'existe aucun élément b de Z/10Z tel qu'on ait : $2 \times b \equiv 1$ (pour le vérifier, il suffit de tester la valeur de $2 \times b$ quand b varie entre 0 et 9).

Un élément qui admet un inverse sera dit inversible ; l'ensemble des éléments inversibles de Z/DZ sera noté (Z/DZ)*.

Le théorème 5 démontré ci-dessous exprime que dans l'anneau Z/DZ, un élément n est inversible si, et seulement si, il est premier avec D (c'est-à-dire si, et seulement si, il n'existe aucun entier supérieur ou égal à 2 qui soit diviseur de n et de D) ; quel que soit D, 0 n'est pas premier avec D mais 1 l'est.

Par exemple, 10 n'est pas premier avec 35 car 5 est à la fois diviseur de 10 et de 35 : on a (dans l'ensemble classique des entiers naturels) $10 = 5 \times 2$ et $35 = 5 \times 7$.

De même, 2 n'est pas premier avec 10 car $10 = 2 \times 5$ et $2 = 2 \times 1$. Pour démontrer que 8 n'est pas premier avec 12, on peut utiliser deux exemples : 2 ou 4. En effet, chacun de ces entiers est diviseur de 8 et de 12. En revanche, 5 est premier avec 7 et 25 l'est avec 81. Ces exemples permettent d'affirmer que 10 n'est pas inversible dans Z/35Z, ni 2 dans Z/10Z, ni 8 dans Z/12Z.

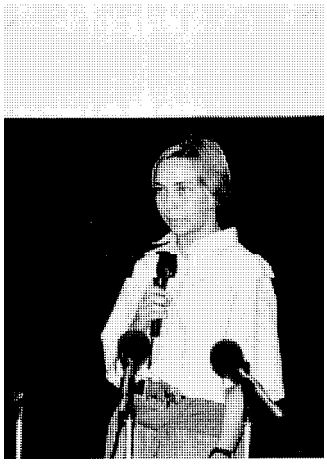
En revanche, 5 est inversible dans Z/7Z. Cela est bien vérifié car $5 \times 3 \equiv 15 \equiv 1$ dans Z/7Z.

De même, 25 est inversible dans Z/81Z car $25 \times 13 \equiv 325 \equiv 324 + 1 \equiv 81 \times 4 + 1 \equiv 1$ dans Z/81Z.

On peut, à l'aide de ce théorème, dresser la liste des éléments inversibles d'un anneau Z/DZ, par exemple de Z/12Z : il s'agit des éléments 1, 5, 7 et 11. En effet, ce sont les seuls entiers compris entre 0 et 11 et premiers avec 12. On remarque donc qu'il y a 4 éléments inversibles dans Z/12Z.

On définit une fonction φ (appelée indicatrice d'Euler) telle que pour tout entier D supérieur ou égal à 2, $\varphi(D)$ est le nombre d'éléments inversibles de Z/DZ. On pose en outre, par convention, $\varphi(1) = 1$.

La formule générale permettant de calculer $\varphi(D)$ pour un entier D quelconque est démontrée au théorème 2 de l'annexe.



Annexes

THEOREME 1 :

$A/(10^q-1) = 0,a_1a_2\ldots a_q$, où $A = a_1a_2\ldots a_q$.

[NDLR : rappelons que …
$0,a_1a_2\ldots a_q = 0,a_1a_2\ldots a_qa_1a_2\ldots a_qa_1a_2\ldots$]

Démonstration :

On a :

$$0,a_1a_2\ldots a_q = \sum_{w=1}^{\infty} (A \times 10^{-qw})$$

$0,a_1a_2\ldots a_q = (10^{-q} \times A) / (1 - 10^{-q})$ d'après les formules de sommes infinies.

$0,a_1a_2\ldots a_q = A / (10^q - 1)$ en multipliant le numérateur et le dénominateur par 10^q.

La fraction $A / (10^q - 1)$ est susceptible d'être simplifiée en p/k, où p et k sont premiers entre eux ; k est alors un diviseur de $10^q - 1$. Cela est utilisé au début de la deuxième partie.

THEOREME 2 :

$$\varphi(n) = n \times \prod_{i=1}^{i=r}(1-1/p_i)$$

où la décomposition de n en facteurs premiers est

$$\prod_{i=1}^{i=r} p_i^{si}$$

avec $s_i > 0$ pour tout entier i compris entre 1 et r.

Rappelons d'abord que $\varphi(n)$ est le nombre d'entiers compris entre 1 et n et premiers avec n (on pose par convention $\varphi(1) = 1$).

nota bene :
Ce théorème peut être démontré de manière très abstraite, en utilisant des anneaux isomorphes. Nous avons préféré essayer de trouver une autre démonstration, un peu plus intuitive. Cependant, le raisonnement perd une partie de sa rigueur.

Démonstration :

Pour chaque facteur premier p_i, il y a n/p_i entiers compris entre 1 et n qui sont multiples de p_i, donc $n - n/p_i = n\ (1-1/p_i)$ qui sont premiers avec p_i.

Pour tout i, la proportion d'entiers premiers avec p_i parmi les entiers compris entre 1 et n est donc $1-1/p_i$.

Or les évènements

"être premier avec p_i"
et "être premier avec p_j"

sont indépendants pour $i \neq j$, car p_i et p_j sont alors premiers entre eux.

L'évènement

"être premier avec n",

qui s'écrit aussi

"pour tout i, être premier avec p_i",

s'obtient comme l'intersection des évènements

"être premier avec p_i"
pour i variant de 1 à r.

La proportion, parmi les entiers compris entre 1 et n, de nombres premiers avec n est donc le produit des proportions d'entiers premiers avec p_i, c'est-à-dire

$$\prod_{i=1}^{i=r}(1-1/p_i).$$

Le nombre d'entiers compris entre 1 et n et premiers avec n est donc :

$$\varphi(n) = n \times \prod_{i=1}^{i=r}(1-1/p_i).$$

Remarque : cette formule permet d'établir que pour des entiers a et b premiers entre eux, $\varphi(a \times b) = \varphi(a) \times \varphi(b)$. Cette propriété sera utilisée dans la démonstration du théorème 4.

THÉOREME 3 :

Si *G* est l'ensemble des puissances successives de 10 dans Z/*DZ*, **où *D* est premier avec 10, *G* est un groupe multiplicatif cyclique et commutatif.**

De plus, *G* est inclus dans $(\mathbb{Z}/D\mathbb{Z})^*$, **ensemble des éléments inversibles de l'anneau** Z/*DZ* **et l'ordre *u* de 10 dans** Z/*DZ* **est un diviseur de** $\varphi(D)$.

Remarque : il est possible dans ce théorème de remplacer 10 par n'importe quel entier *b*, à condition que *b* soit premier avec *D*.

Définissons tout d'abord un groupe. C'est un ensemble (ici *G*) muni d'une opération (ici la multiplication), tel que :

• **Le produit de deux éléments de *G* est un élément de *G*** : c'est vrai d'après la définition de *G*.

• **La loi multiplication est associative**, ce qui est le cas car il en est ainsi de la multiplication entre nombres réels.

• **Il existe dans *G* un élément neutre pour la multiplication** : montrons que 1 est dans *G*, c'est-à-dire qu'il existe un entier strictement positif *T* tel que $10^T \equiv 1 \pmod{D}$.

Utilisons la fonction *f* de N* dans Z/*DZ* définie par $f(n) \equiv 10^n \pmod{D}$. Comme N* comporte une infinité d'éléments et Z/*DZ* seulement un nombre fini (*D* éléments), l'application *f* ne peut être injective : [NDLR : c'est le *principe des pigeons* dont il est question page 202.] il existe deux entiers naturels *q* et *T*, *T* non nul, tels que

$$f(q) \equiv f(q+T) \pmod{D},$$

c'est-à-dire $10^q \equiv 10^{q+T} \pmod{D}$.

Or, 10 étant inversible dans Z/*DZ* car 10 est premier avec *D*, 10^q l'est aussi (d'inverse $[inv(10)]^q$, où *inv*(10) est l'inverse de 10 dans Z/*DZ*).

En multipliant les deux membres de l'égalité précédente par $[inv(10)]^q$, il vient : $1 \equiv 10^T \pmod{D}$ d'après l'égalité $10^{q+T} = 10^q \times 10^T$. La multiplication a donc bien un élément neutre.

• **Chaque élément de *G* a un inverse dans *G***. Si 10^q désigne un élément quelconque de *G*, soit *q'* un entier naturel tel que *q*+*q'* s'écrive $a \times T$ où *T* désigne toujours un entier tel que $10^T \equiv 1 \pmod{D}$ et *a* un entier strictement positif quelconque. On a alors :
$10^q \times 10^{q'} \equiv 10^{q+q'} \equiv 10^{a \times T} \equiv (10^T)^a \equiv 1^a \equiv 1 \pmod{D}$ donc 10^q est bien inversible d'inverse 10^q.

L'ensemble ***G* muni de la multiplication est donc un groupe**. Ce groupe est dit commutatif (car la multiplication est commutative) et cyclique (car il est formé des puissances successives d'un même nombre).

De plus, toute puissance de 10 est inversible dans Z/*DZ*, donc *G* est inclus dans l'ensemble des éléments inversibles de Z/*DZ*, ensemble noté $(\mathbb{Z}/D\mathbb{Z})^*$. Cet ensemble forme un groupe multiplicatif.

L'ensemble $(\mathbb{Z}/D\mathbb{Z})^*$ est formé des classes d'équivalences correspondant aux entiers compris entre 1 et *D* et premiers avec *D* (d'après le théorème 5). Le cardinal de cet ensemble, noté $\varphi(D)$ (φ est l'indicatrice d'Euler), représente donc le nombre d'entiers naturels inférieurs à *D* et premiers avec *D* (pour le calcul de $\varphi(D)$, voir le théorème 2).

G est donc un sous-groupe cyclique du groupe multiplicatif $((\mathbb{Z}/D\mathbb{Z})^*, \times)$. Le théorème de Lagrange permet alors d'énoncer que l'ordre *u* de *G* [qui est à la fois son nombre d'éléments et le plus petit entier *T* tel que $10^T \equiv 1 \pmod{D}$] est un diviseur de l'ordre de $((\mathbb{Z}/D\mathbb{Z})^*, \times)$, qui vaut $\varphi(D)$. [NDLR : le *théorème de Lagrange* dit que le nombre d'éléments (l'ordre) d'un sous-groupe divise forcément le nombre d'éléments du groupe tout entier.]
Remarque : *u* s'appelle indifféremment l'ordre de *G* ou l'ordre de 10 dans Z/*DZ*.

THÉOREME 4 :

Soit *D* un entier non irréductible dans une base *b* donnée. Deux cas se présentent :

• Si $D = 2 \times A$ où *A* est un entier irréductible impair dont tous les chiffres (en base *b*) sont inférieurs ou égaux à (*b*-1)/2, alors *D* est réfractaire si, et seulement si, *A* l'est dans la même base.

• Sinon, c'est-à-dire si $D = 2 \times A$ avec *A* irréductible mais pair, ou si $D = p \times A$ avec $3 \leq p \leq (b\text{-}1)/(max\ a_i)$, alors *D* ne peut pas être réfractaire.

Remarque :
Dans cet énoncé, comme dans toute la deuxième partie, $max\ a_i$ est le plus grand des chiffres qui composent l'écriture de *A* dans la base considérée. Le nombre *b*-1 remplace 9 quand la base n'est plus 10 mais *b*.

Démonstration :
Posons $D = p \times A$ où *A* est irréductible et où *p* est un entier compris au sens large entre 2 et $(b\text{-}1)/(max\ a_i)$. D'après le théorème final de la deuxième partie, pour tout entier *q* :
• soit *D* et *A* sont tous deux *q*-permutables,
• soit ni *D* ni *A* ne le sont : *A* et *D* ont le même ensemble des occurrences.

Calculons $\varphi(D)$. Si $\varphi(D) = \varphi(A)$ alors *D* est réfractaire si, et seulement si, *A* l'est dans la même base.

Si $\varphi(D) > \varphi(A)$, *D* sera $\varphi(A)$-permutable car *A* l'est de toutes façons (car *A* est irréductible, donc $\varphi(A)$ fait partie de l'ensemble des occurrences de *A* : cela peut être démontré grâce au théorème de Fermat-Euler qui affirme que, si *A* est premier avec *b*, on a :

$$b^{\varphi(A)} \equiv 1 \pmod{A}).$$

D ne pourra donc pas être réfractaire, que *A* le soit ou non.

Cherchons donc les conditions nécessaires et suffisantes pour qu'on ait $\varphi(D) = \varphi(A)$.

Posons $p = \prod_{i=1}^{i=r} p_i^{si}$, la notation $\prod_{i=1}^{i=r}$ désignant le produit des p_i^{si}, où *i* est un entier qui varie entre 1 et *r*. On suppose $s_i \geq 1$ pour tout entier *i* compris entre 1 et *r*.

Posons $A = w \times A'$, où *A'* est premier avec *p* (on peut éventuellement avoir : $A' = 1$). Ecrivons la décomposition de *w* en facteurs premiers sous la forme

$$\prod_{i=1}^{i=r} p_i^{ti},$$

où les p_i sont les mêmes que dans la décomposition de *p* ; t_i est un entier, éventuellement nul, et *i* est toujours un entier compris entre 1 et *r*. On a alors : $D = (p \times w) \times A'$. *A'* étant premier avec *p* et avec *w*, il l'est avec leur produit d'où :

$$\varphi(D) = \varphi(p \times w) \times \varphi(A'). \quad (1)$$

D'autre part, $A = w \times A'$; comme *A'* est premier avec *w*, on a :

$$\varphi(A) = \varphi(w) \times \varphi(A'). \quad (2)$$

Les égalités (1) et (2) permettent d'écrire que $\varphi(D) = \varphi(A)$ équivaut à :

$$\varphi(p \times w) = \varphi(w).$$

En remplaçant *p* et *w* par leurs décompositions en facteurs premiers respectives, on obtient :

$$\varphi(\prod_{i=1}^{i=r} p_i^{si+ti}) = \varphi(\prod_{i=1}^{i=r} p_i^{ti})$$

En appliquant la formule de calcul de $\varphi(n)$ démontrée au théorème 2, il vient :

$$(\prod_{i=1}^{i=r} p_i^{si+ti-1}) \times \prod_{i=1}^{i=r} (p_i\text{-}1) = (\prod_{ti \geq 1} p_i^{ti-1}) \times \prod_{ti \geq 1} (p_i\text{-}1)$$

où le symbole $\prod_{i=1}^{i=r}$ renvoie au produit pour tous les entiers *i* compris entre 1 et *r*, et $\prod_{ti \geq 1}$ au produit pour tous les entiers *i* compris entre 1 et *r* et tels que $t_i \geq 1$ (si aucun *i* ne vérifie $t_i \geq 1$, ce produit vaut 1).

En décomposant chaque facteur du type $p_i^{si+ti-1}$ en produit : $p_i^{si-1} \times p_i^{ti}$, puis en simplifiant l'expression obtenue, il vient :

$$(\prod_{i=1}^{i=r} p_i^{si-1}) \times (\prod_{ti \geq 1} p_i) \times (\prod_{ti=0} (p_i\text{-}1)) = 1.$$

Ces trois facteurs sont des entiers positifs (le premier l'est parce qu'on suppose $s_i \geq 1$) : leur produit vaut 1 si, et seulement si, ils valent tous 1.

En particulier, il est nécessaire (mais pas suffisant) qu'on ait

$$\prod_{ti \geq 1} p_i = 1.$$

Ce produit est un produit d'entiers strictement supérieurs à 1 (le plus petit nombre premier est 2), avec autant de facteurs qu'il y a d'entiers i compris entre 1 et r tels que : $t_i \geq 1$.

Ce produit ne peut valoir 1 que s'il n'est formé d'aucun facteur, c'est-à-dire s'il n'existe aucun entier i compris entre 1 et r tel que $t_i \geq 1$.

Donc pour tout entier i compris entre 1 et r,

$$t_i = 0$$

et w, qui s'écrit $\prod_{i=1}^{i=r} p_i^{ti}$, vaut 1.

On a : $A = A'$, et p est premier avec A.

Nous avons donc démontré que pour avoir $\varphi(D) = \varphi(A)$, avec $D = p \times A$, il est nécessaire que p et A soient premiers entre eux.

Il est alors facile de calculer

$$\varphi(D) = \varphi(p \times A),$$

qui vaut (d'après le théorème 2) :

$$\varphi(p) \times \varphi(A).$$

L'égalité $\varphi(D) = \varphi(A)$ s'écrit alors : $\varphi(p) = 1$.

L'entier p est alors tel qu'il n'existe qu'un nombre inférieur à p et premier avec p (il s'agit alors de 1).

Or les entiers p et p-1 sont premiers entre eux pour $p \geq 2$ (si un entier divise simultanément p et p-1, il divise leur différence qui vaut 1 : cet entier vaut 1).

Parmi les entiers inférieurs à p et premiers avec p, il y a donc toujours 1 et p-1 ; pour que $\varphi(p)$ vaille 1 (avec $p \geq 2$), il est donc nécessaire que 1 et p-1 soient le même entier, c'est-à-dire que p vaille 2.

Réciproquement, on a bien :

$$\varphi(2) = 1.$$

Le seul cas où $\varphi(D) = \varphi(A)$, avec $D = p \times A$, est donc le cas où p vaut 2 et où A est premier avec 2, c'est-à-dire impair. D est alors réfractaire si, et seulement si, A l'est.

Dans tous les autres cas (c'est-à-dire quand p est supérieur ou égal à 3 ou, si p vaut 2, quand A est pair), $\varphi(D)$ est strictement supérieur à $\varphi(A)$ et D ne peut pas être réfractaire.

THÉOREME 5 :

Dans tout anneau $\mathbb{Z}/D\mathbb{Z}$, la classe d'équivalence de représentant n est inversible si, et seulement si, n est premier avec D.

Démonstration :
n est inversible dans $\mathbb{Z}/D\mathbb{Z}$ si, et seulement si, il existe un entier j tel que $j \times n \equiv 1 \pmod{D}$. Cela équivaut à :

il existe un entier m tel que $1 = j \times n + m \times d$, soit n premier avec D (égalité de Bezout).

Sommaire des notations et définitions utilisées

Première partie : démonstration directe

A : diviseur de 10^q-1, qui s'écrit en base 10 sous la forme $a_1a_2\ldots a_q$.
$\mathbf{0,}\boldsymbol{a_1a_2\ldots a_q}$: nombre rationnel $0,a_1a_2\ldots a_qa_1a_2\ldots a_qa_1a_2\ldots a_q\ldots$ de période $a_1a_2\ldots a_q$.
F : une permutation circulaire de *A* ;
$F = a_i\ldots a_qa_1\ldots a_{i-1}$.

Deuxième partie : réciproque

D : un entier non nul *q*-permutable, qui s'écrit en base 10 sous la forme $d_1d_2\ldots d_q$.
$\boldsymbol{X_i}$: l'entier $d_1d_2\ldots d_i$ formé par les *i* premiers chiffres de *D*.
X : le nombre rationnel $0,\boldsymbol{d_1d_2\ldots d_q}$, dont la période est *D*.
p/k : l'écriture de *X* comme fraction irréductible (*p* et *k* sont premiers entre eux).
A : l'entier *D*/*p*, dont on démontre qu'il est diviseur de 10^q-1. Son écriture en base 10 est $a_1a_2\ldots a_q$.

Troisième partie : élargissement du sujet

Ensemble des occurrences

D : un entier quelconque.
occurrence d'un entier *D* : un entier *q* tel que *D* soit *q*-permutable.
ensemble des occurrences de *D* : ensemble, noté *E*, des entiers *q* tels que *D* est *q*-permutable.
PGCD de deux entiers *a* et *b* : le plus grand des entiers qui sont diviseurs à la fois de *a* et de *b*. Si le PGCD (Plus Grand Commun Diviseur) de *a* et de *b* vaut 1, on dit que *a* et *b* sont premiers entre eux, ou que *a* est premier avec *b*. Cette définition du PGCD de deux entiers s'étend au PGCD de plusieurs entiers.
irréductible : nombre tel qu'il n'existe aucun entier *p* supérieur ou égal à 2 qui soit diviseur de chacun de ses chiffres.
Autres définitions équivalentes : entier dont les chiffres sont premiers dans leur ensemble, ou entier dont le PGCD des chiffres vaut 1.
Z/*D*Z : anneau présenté avant l'annexe.
ordre : voir le théorème 3.
φ : indicatrice d'Euler ; φ(*n*) représente le nombre d'éléments inversibles de Z/*D*Z, c'est-à-dire le nombre d'entiers compris entre 1 et *n* et premiers avec *n*.
Pour le calcul de φ(*n*), voir le théorème 2.

Entiers réfractaires

b : base considérée.
(Z/*D*Z**)*** : ensemble des éléments inversibles de l'anneau Z/*D*Z.
générateur d'un groupe *E* : élément *g* de *E* tel que pour tout élément *a* de *E* il existe un entier *n* tel que $a = g^n$. L'ordre de *g* est le nombre d'éléments de *E*.
G : ensemble des puissances successives de *b* dans Z/*D*Z.