# ORDRE MULTIPLICATIF & PETIT THÉORÈME DE FERMAT

## Itération et ordre

Pour $a$ et $n$ des entiers on cherche à calculer $a^k \pmod n$ pour $k$ parcourant $\mathbb{N}$.

**Exemple 1.**
Pour $n = 6$ :

— Si $a = 5$ alors on a $1, 5, 1, 5, 1 \ldots$.

— Si $a = 2$ alors on a $1, 2, 4, 2, 4, 2, 4, 2 \ldots$

Il semblerait qu'on finisse par boucler. Il est déjà possible d'intuiter deux cas. Le premier est celui où comme pour $5$ on retombera sur $1$ et la suite des puissances sera bien périodique. Le second est celuiqui comme pour $2$ on ne retombera pas sur $1$ et la suite sera seulement périodique à partir d'un certain rang. Formalisons un peu :

**Lemme 2.**
Il existe $i$ et $\ell$ tels que $a^{i+\ell} = a^i \pmod n$ et alors pour tout $j \geqslant i$ on a $a^{j+\ell} = a^j \pmod n$.
**Démonstration**. Par principe des tiroirs, les chaussettes étant les $a^k$ et les tiroirs les valeurs modulos $n$. Pour la seconde proposition on a $a^{j+\ell} = a^{j-i}a^{i+\ell} = a^{j-i}a^i = a^j \pmod n$. □

Formalisons maintenant la distinction des deux cas précédents :

**Lemme 3.**
Si $a$ est premier avec $n$, alors pour le $\ell$ précédent on a $a^\ell = 1 \pmod n$.
**Démonstration**. En effet si $a$ est premier avec $n$ alors $a$ est inversible modulo $n$ et donc $a^\ell = (a^{-1})^i a^{i+\ell} = 1 \pmod n$. □

Ce cas est très agréable puisqu'une fois $\ell$ déterminé, on n'a pas de $i$ inconnu parasitant nos calculs. Dans ce cas les $a^k$ forment une suite périodique dans $\mathbb{Z}/n\mathbb{Z}$.

**Lemme 4.**
Soit $(x_i)_{i\in\mathbb{N}}$ une suite périodique. La période minimale $T_0$ est telle que toute période $T$ de $(x_i)_{i\in\mathbb{N}}$ est un multiple de $T_0$.
**Démonstration**. En effet posons la division euclidienne $T = qT_0 + r$ où $r < T_0$ alors pour tout $i$, $x_{r+i} = x_{qT_0+r+i} = x_{T+i} = x_i$ donc ou bien $r$ est une période $< T_0$, absurde par définition, ou bien $r = 0$. Ainsi $T = qT_0$. □

**Définition 5** (Ordre multiplicatif)**.**
Si $a$ est premier avec $n$ on définit $o_n(a)$ l'ordre de $a$ modulo $n$, la période minimale de la suite $a^n$ dans $\mathbb{Z}/n\mathbb{Z}$.
Ainsi, pour tout $q \in \mathbb{N}$, on l'équivalence $a^q = 1 \pmod p \iff o_n(a) \mid q$.

**Remarque 6** (Stratégie pour trouver l'ordre)**.**
Pour trouver l'ordre de $a$ modulo $n$ il suffit de trouver un $q$ relativement petit tel que $a^q = 1 \pmod n$ et ensuite regarder les diviseurs de $q$. Parmi le lemme suivant on trouvera $o_n(a)$parmi eux.

**Remarque 7** (Quand $\gcd(a,n) \neq 1$)**.**
L'ordre de $a$ modulo $n$ n'est défini que lorsque $a$ est premier avec $n$. Dans le cas contraire, la suite n'est que périodique à partir d'un certain rang $i$, à priori inconnu. En fait on peut déterminer ce $i$ avec un peu d'effort et en utilisant le théorème des restes chinois. Toutefois, pour diverses raisons, cela nous est rarement utile.

## Petit théorème de Fermat

La remarque 6 nous pousse à chercher des $q$ très simples à calculer en fonction de $n$. Comme dit précédemment, le cas le plus favorable est celui où $a$ est premier avec $n$. Supposons donc que $n$ est premier de sorte que tous les éléments de $\mathbb{Z}/n\mathbb{Z}$ soit inversibles sauf $0$. Dans le reste de cette partie on notera $p$ pour désigner un nombre premier qui jouera le même rôle que $n$ précédemment.

**Exemple 8.**
Pour $p = 7$ :

— Pour $a = 2$ on a $2, 4, -1, -2, -4, 1$ donc $o_7(2) = 6$.

— Pour $a = 5$ on a $5, 4, -1, -5, -4, 1$ donc $o_7(5) = 6$.

— Pour $a = 4$, on calcule $o_7(4) = 3$.

Pour $p = 11$ :

— Pour $a = 2$ on calcule $o_{11}(2) = 10$.

— Pour $a = 4$ on calcule $o_{11}(4) = 5$.

— Pour $a = 10$ on calcule $o_{11}(10) = 2$.

On remarque que dans tous les cas $o_p(a) \mid p-1$. Il est donc naturel de vouloir montrer que $a^{p-1} = 1 \pmod p$.

**Théorème 9** (Petit théorème de Fermat)**.**
Soit $p$ un nombre premier. Pour tout $a$ non-divisible par $p$, $o_p(a) \mid p-1$,
de sorte que pour $a$ non-divisible par $p$, on a

$$a^{p-1} = 1 \pmod p,$$

de sorte que pour $a \in \mathbb{Z}$ on a

$$a^p = a \pmod p.$$

**Démonstration**. Soit $a$ non-divisible par $p$. Regardons

$$A = \{1, a^1, a^2, \ldots, a^{o_p(a)-1}\}$$

on a $\mathrm{Card}(A) = o_p(a)$. Par définition de $o_p(a)$ tous les éléments de $A$ ont une valeur différente modulo $p$.
Ou bien $o_p(a) = p-1$, ou bien on dispose de $b_1$ non-divisible par $p$ tel que $b_1$ a une valeur différente de tous les éléments de $A$ modulo $p$. Soit

$$A_1 = \{b_1, ab_1, a^2b_1, \ldots a^{o_p(a)-1}b_1\}.$$

Mais alors les éléments de $A$ et de $A_1$ ont tous une valeur différente modulo $p$. En effet on aurait sinon $a^u = a^v b_1 \pmod p$ et alors $b_1 = a^{u-v} \pmod p$, absurde par définition de $b_1$.
$\mathrm{Card}(A \cup A_1) = 2o_p(a)$. On peut maintenant prendre $b_2$ qui a une valeur différente de tous les éléments de $A$ et $A_1$ modulo $p$. De manière similaire avec $A_2 = \{b_2, ab_2, a^2b_2, \dots a^{o_p(a)-1}b_2\}$ on peut continuer le raisonnement. A la fin, quand on aura épuisé toutes les valeurs possibles modulo $p$ (sauf $0$) on aura

$$p - 1 = \mathrm{Card}((\mathbb{Z}/p\mathbb{Z})^*) = \mathrm{Card}(A \cup A_1 \cup A_2 \cdots A_{m-1}) = mo_p(a)$$

et ainsi $o_p(a) \mid p - 1$. □

**Remarque 10** (L'erreur préférée des élèves)**.**
Comme illustré dans 8, on a seulement $o_p(a) \mid p - 1$ et nullement en général $o_p(a) = p - 1$. Si vous écrivez (ou pensez) que le théorème de Fermat est la seconde chose, la POFM vous retrouvera.

**Remarque 11** (Une heureuse erreur)**.**
Il est toutefois possible de s'intéresser au cas spécifique où $o_p(a) = p - 1$ (ce qui n'arrive pas tout le temps) Dans ce cas, tous les éléments de $(\mathbb{Z}/p\mathbb{Z})^*$ peuvent s'écrire comme une puissance de $a$. On discute de cas dans l'annexe sur les racines primitives.

**Remarque 12** (Une autre preuve)**.**
Il existe une preuve astucieuse et très courte à ce théorème, présentée en annexes.
La preuve présentée supra est plus simple, naturelle, et générale, bien qu'elle soit un peu plus longue.

## Théorème & indicatrice d'Euler

Revenons au cas où $n$ est non-premier. Il est possible de regarder fixement dans les yeux la preuve précédente et de se demander comment l'adapter au le cas général. Une bonne raison pour laquelle cela serait possible est que l'apparation du $p - 1$ est tardive, et qu'il intervient comme une contrainte donnée par le problème et non comme un paramètre initial.
Finalement, la seule chose qui change pour $n$ quelconque est le nombre de valeurs différentes inversibles modulo $n$ .

**Théorème 13.**
On note $\varphi(n)$ le nombre de valeurs inversibles modulo $n$. Pour $a$ premier avec $n$, $o_n(a) \mid \varphi(n)$ ce qui équivaut à dire

$$a^{\varphi(n)} = 1 \pmod n.$$

**Démonstration**. Strictement la même que pour le théorème de Fermat, en remplaçant "non-divisible par $p$" par "premier avec $n$". □

Reste maintenant à calculer $\varphi(n)$.

**Exemple 14** (A la main)**.**
Que vaut $\varphi(n)$ pour $n$ valant successivement $4, 5, 8$ et $24$ ?

**Proposition 15** (Expression de $\varphi(n)$)**.**
Pour $n > 0$ :

$$\varphi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right)$$

où les $p$ sont premiers.
Une autre manière de le dire est que $n = \prod_i p_i^{\alpha_i}$,

$$\varphi(n) = \prod_i (p_i - 1) p_i^{\alpha_i - 1}.$$

**Démonstration**. D'abord $\varphi(n)$ est le nombre d'entiers entre $0$ et $n-1$ premiers avec $n$.
Par ailleurs $\mathcal{P}$ l'ensemble des premiers divisant $n$ de sorte que $\gcd(a,n) = 1$ ssi pour tout $p \in \mathcal{P}$, $p \nmid a$.
Calculons la probibilité que $d \mid a$ où $a$ est choisi uniformément dans $[\![0, n-1]\!]$ et $d \mid n$ : les multiples de $d$ sont $0, d, \ldots, n-d$, et ainsi la probibilité est de $\frac{1}{d}$. Mais alors les évènements $(p \mid a)$ sont indépendants et ainsi l'évènement $\gcd(a,n) = 1$ a la probibilité $\prod_{p \in \mathcal{P}} \left(1 - \frac{1}{p}\right)$ d'où l'expression de $\varphi(n)$. □

**Exemple 16** (Sans les mains)**.**
Que vaut $\varphi(n)$ pour $n$ valant $100$, $1024$ et $2025$ ?

**Proposition 17.**
Avec la seconde expression de $\varphi$ il est clair que pour $n$ et $m$ premiers entre eux on a

$$\varphi(nm) = \varphi(n)\varphi(m)$$

.

**Remarque 18** (Ordre de grandeur de $\varphi(n)$, pour la culture)**.**
Dans un sens très précis de "en moyenne" et "ordre de grandeur" que nous ne détaillerons pas ici, et avec des outils plus avancés on trouve qu'en moyenne l'ordre de grandeur de $\varphi(n)$ est de $\frac{6n}{\pi^2}$.
Il faut toutefois se rendre compte que la taille de $\varphi(n)$ est assez variable.
Il est clair que pour $p$ premier $\frac{\varphi(p)}{p} \to 1$ quand $p \to \infty$.
Mais on peut aussi trouver une suite de $n_i$ pour laquelle $\frac{\varphi(n_i)}{n_i} \to 0$.
Il est donc quelque peu illusoire d'espérer utiliser la valeur $\frac{6n}{\pi^2}$ donnée précédemment.

## Exercices

**Exercice 1**
Démontrer, pour tout entier $n \geq 0$, que 7 divise $3^{12n+1} + 2^{6n+2}$.

**Exercice 2**
Montrez que pour tout $n$, $42 \mid n^7 - n$.

**Exercice 3**
Soit $n \in \mathbb{N}^*$ impair. Montrer que $n \mid 2^{n!} - 1$.

**Exercice 4**
Soient $p, q$ premiers tels que $q \mid 1 + p + ... + p^{p-1}$. Montrer que $q \equiv 1 \pmod{p}$.

**Exercice 5**
Soit $k \geq 1$ un entier premier avec 6. Démontrer qu'il existe un entier $n \geq 0$ pour lequel $k$ divise $2^n + 3^n + 6^n - 1$.

**Exercice 6**
Montrez que pour $n \geqslant 2$, et $a$ impair on a $a^{2^{n-2}} = 1 \pmod{2^n}$.

**Exercice 7**
Soit $n$ un entier. Dénombrer les $a \in [\![1, n]\!]$ tels que $a^n = 0 \pmod{n}$.

**Exercice 8**
Soit $p > 3$ premier. Trouver un $k > 0$ tel que $1^k 2^k + 2^k 3^k + 3^k 4^k + \cdots (p-2)^k (p-1)^k = 2 \pmod{p}$.

**Exercice 9**
Soit $d$ divisant $n$, que vaut $\mathrm{Card}\{k \in [\![1, n]\!] : \gcd k, n = d\}$ ? En déduire la valeur de $\sum_{d|n} \varphi(d)$.

## Solutions

**Solution de l'exercice 1**
Le petit théorème de Fermat indique directement que

$$3^{12n+1} + 2^{6n+2} \equiv 3 \times (3^6)^{2n} + 4 \times (2^6)^n \equiv 3 \times 1^{2n} + 4 \times 1^n \equiv 3 + 4 \equiv 0 \pmod 7.$$

**Solution de l'exercice 2**
On a $7 \mid n^7 - n$ par Fermat. On utilise Fermat pour $n = 2$ et $3$ en faisant la disjonction de cas $0$ et le reste et ceci conclut.

**Solution de l'exercice 3**
Puisque $2$ est premier avec $n$, soit $\omega$ l'ordre de $2$ modulo $n$. Par définition, on sait que $\varphi(n) \leqslant n$, donc que $\varphi(n)$ divise $n!$. Ainsi, puisque $\omega$ divise $\varphi(n)$, il divise $n!$ également. Ainsi, si l'on pose $k = n!/\omega$, et puisque $n$ est premier avec $2$, on constate que

$$2^{n!} - 1 \equiv (2^\omega)^k - 1 \equiv 1^k - 1 \equiv 0 \pmod n.$$

**Solution de l'exercice 4**
Si $q \mid p^{p-1} + p^{p-2} + \ldots + p + 1$ alors

$$q \mid (p^{p-1} + p^{p-2} + \ldots + p + 1)(p-1) = p^p - 1$$

On a donc l'ordre $\omega$ de $p$ modulo $q$ qui divise $p$, et deux cas sont possibles :
Si $\omega = 1$ alors il vient que $p \equiv 1 \pmod q$ et donc $p^{p-1} + p^{p-2} + \ldots + p + 1 \equiv p \pmod q$ et donc $p = q$, mais alors $q \mid 1$, absurde.
Si $\omega = p$ alors par le petit théorème de Fermat on a $p$ qui divise $q - 1$.

**Solution de l'exercice 5**
L'idée est de remarquer que $1/6 + 1/3 + 1/2 = 1$. Idéalement, on souhaiterait donc choisir $n = -1$, mais on ne peut pas procéder brutalement ainsi. À la place, on va l'entier $n = \varphi(k) - 1$. En effet, on constate alors que

$$6(2^n + 3^n + 6^n - 1) \equiv 3 \times 2^{\varphi(k)} + 2 \times 3^{\varphi(k)} + 6^{\varphi(k)} - 6 \equiv 3 + 2 + 1 - 6 \equiv 0 \pmod n,$$

et puisque $k$ est premier avec $6$, on en conclut que $k$ divise bien $2^n + 3^n + 6^n - 1$.

**Solution de l'exercice 6**
On ne peut pas appliquer Euler-Fermat, puisque $\varphi(2^n) = 2^{n-1}$. On doit revenir vers de méthode plus classique. Essayons une récurrence.
L'initialisation est faite pour $2^3 = 8$.
Pour l'hérédite on a $a^{2^{n-2}} = q2^n + 1 \implies a^{2^{n-1}} = (q2^n + 1)^2 = q^{2^{2n}} + q^{n+1} + 1$.

**Solution de l'exercice 7**
C'est la même méthode que pour trouver l'expression de $\varphi(n)$ ; on obtient $n \prod_{p \mid n} \frac{1}{p}$ .

**Solution de l'exercice 8**
De imaginons qu'on puisse prendre $k = -1$, avec l'identité $\frac{1}{n(n+1)} = \frac{1}{n} - \frac{1}{n+1}$ on aurait une somme téléscopique qui fonctionne. Pour contourner $k > 0$, on peut prendre $k = p-2$ puisque $a^{p-2}a = 1 \pmod p$ donc $a^{p-2} = a^{-1} \pmod p$.

**Solution de l'exercice 9**
On trouve $\varphi(\frac{n}{d})$. En regroupant les nombres de $1, n$ par gcd on trouve que la somme vaut $n$.

## Annexe : Preuve alternative pour Euler-Fermat

**Proposition 19.**
Soit $a \in (\mathbb{Z}/p\mathbb{Z})^*$, l'application $x \mapsto ax$ est une bijection de $(\mathbb{Z}/p\mathbb{Z})^*$.
**Démonstration**. En effet, $ax \in (\mathbb{Z}/p\mathbb{Z})^*$, l'application est clairement injective, et $(\mathbb{Z}/p\mathbb{Z})^*$ est un ensemble fini. □

**Théorème 20.**
(Petit théorème de Fermat) Pour $a \in (\mathbb{Z}/p\mathbb{Z})^*$, on a $a^{p-1} = 1$.
**Démonstration**. En effet $\prod_{x\in(\mathbb{Z}/p\mathbb{Z})^*} x \neq 0$ et par ailleurs

$$\prod_{x\in(\mathbb{Z}/p\mathbb{Z})^*} x = \prod_{x\in(\mathbb{Z}/p\mathbb{Z})^*} ax = a^{p-1} \prod_{x\in(\mathbb{Z}/p\mathbb{Z})^*} x.$$

□

**Remarque 21.**
La même preuve s'adapte bien pour le théorème d'Euler.

## Annexe : Sur les racines primitives

**Théorème 22.**
Soit $p$ premier, il existe $a$ tel que $o_p(a) = p - 1$.

Faisons la preuve en quelques étapes :

**Lemme 23.**
Si l'ordre de $a$ est $u$ et l'ordre de $b$ est $v$ avec $u$ et $v$ premier entre alors $ab$ est d'ordre $uv$.
**Démonstration**. On note $\omega$ l'ordre de $ab$, pour $m$ le ppcm de $\omega$ et $u$ on a $(ab)^m = 1$ d'une part et $(ab)^m = b^m$ d'autre part. Ainsi $v \mid m$ et donc comme $u$ et $v$ sont premiers entre eux $v \mid \omega$.
De manière similaire on montre que $u \mid \omega$ et ainsi $uv \mid \omega$. Comme $\omega \mid uv$ on a bien $\omega = uv$. □

**Lemme 24.**
Un polynôme de degré $d$ a au plus $d$ racines dans $\mathbb{Z}/p\mathbb{Z}$.
Attention, ce lemme n'est plus vrai dans $\mathbb{Z}/n\mathbb{Z}$.
Le résultat se montre de la même manière que pour les polynômes sur les réels, par soucis de concision nous l'admettons.

**Démonstration**. Soit $a$ l'élément dont l'ordre est le plus grand parmi les éléments de $(\mathbb{Z}/p\mathbb{Z})^*$ et notons $\omega$ cet ordre. Pour $b \in (\mathbb{Z}/p\mathbb{Z})^*$ d'ordre $t$ et $g = \gcd(\omega, t)$ alors $b^g$ est d'ordre $t/g$ premier avec $\omega$ donc il existe un élément d'ordre $\omega\frac{t}{g}$ d'après le lemme 23.
Par maximalité de $\omega$ on a ainsi $t = g$ et donc $t \mid \omega$. Ainsi $b^\omega = 1$.
Tous les éléments de $(\mathbb{Z}/p\mathbb{Z})^*$ sont donc racines de $X^\omega - 1$ d'où par le lemme 24, $\omega \geqslant p - 1$, mais alors comme $\omega \mid p - 1$ on a $\omega = p - 1$. □