Cours groupe C : Théorème d'Euler Fermat

Noé Fisher

4 Janvier 2024

Énoncé

Petit Théorème de Fermat

On considère p un nombre premier, on a alors :

$$\forall a \in \mathbb{Z}, a^p \equiv a \pmod{p},$$

ou encore : $\forall a \in \mathbb{Z}, p \nmid a \implies a^{p-1} \equiv 1 \pmod{p}$.

Exemples

Prérequis

Coefficient binomial

On rappelle que pour deux entiers $0 \leq k \leq n$, on note :

$$\binom{n}{k} = \frac{n!}{k!(n-k)!} = \frac{n(n-1)\dots(n-k+1)}{k!}.$$

(Par convention, on pourra noter $\binom{n}{k} = 0$ si $k > n$.)

On rappelle que ce coefficient, nommé coefficient binomial, est entier et correspond au nombre de façons de choisir k éléments parmi n. (On l'appelle par conséquent "k parmi n".)

Exemples

Pour tout $n \in \mathbb{N}$, on a

$$\binom{n}{0} = \binom{n}{n} = 1,$$

$$\binom{n}{1} = \binom{n}{n-1} = n.$$

Plus généralement, on a pour tout $k \in \{0, 1, \ldots, n\}$,

$$\binom{n}{k} = \binom{n}{n-k}.$$

Prérequis

Formule du binôme de Newton

Soit $(a, b) \in \mathbb{R}^2$ et $n \in \mathbb{N}$, on a alors :

$$a + b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$$

$$(a+b)^n = \binom{n}{0} b^n + \binom{n}{1} ab^{n-1} + \ldots + \binom{n}{n-1} a^{n-1} b + \binom{n}{n} a^n$$

Idée de preuve

On écrit $(a+b)^n = \underbrace{(a+b)(a+b)\dots(a+b)}_{n \text{ fois}}$.

Soit $k \in \{0, 1, \dots, n\}$, si on développe le produit et qu'on regarde le facteur devant a^k, on trouve qu'il faut choisir k fois a parmi les n paires $\{a, b\}$.
Ce faisant on multiplie aussi $n-k$ fois par b, et il y a exactement "k parmi n" termes vérifiant cette condition, d'où l'on obtient $\binom{n}{k} a^k b^{n-k}$.

Lemme 1

Soit p un nombre premier, on a alors pour tout $k \in \{1, \ldots, p-1\}$:

$$p \mid \binom{p}{k}.$$

Ce qui est équivalent à $\binom{p}{k} \equiv 0 \pmod{p}$.

Démonstration

- On utilise la formule $\binom{p}{k} = \frac{p!}{k!(p-k)!}$. p étant premier, et comme $k < p$, $p - k < p$, les entiers $k!$ et $(p-k)!$ sont premiers avec p. En revanche $p \mid p!$, ce qui conclut.
- On aurait aussi pu utiliser la formule $\binom{p}{k} \cdot k = p \cdot \binom{p-1}{k-1}$, remarquer que p divise le terme de droite donc celui de gauche et que $k \wedge p = 1$ car $k < p$.

Lemme 2 : Morphisme de Frobenius

On travaille modulo p un nombre premier, et on considère la fonction $f_p : x \mapsto x^p$. On a :

- $\forall (a, b) \in \mathbb{Z}^2, f_p(a \cdot b) = f_p(a) \cdot f_p(b)$,
- $\forall (a, b) \in \mathbb{Z}^2, f_p(a + b) \equiv f_p(a) + f_p(b) \pmod{p}$,

Preuve

Soit $(a, b) \in \mathbb{Z}^2$, par le binôme de Newton :

$$(a+b)^p = \underbrace{\binom{p}{0}}_{=1} b^p + \underbrace{\binom{p}{1}}_{\equiv 0 \,(\mathrm{mod}\, p)} ab^{p-1} + \underbrace{\ldots}_{\equiv 0 \,(\mathrm{mod}\, p)} + \underbrace{\binom{p}{p-1}}_{\equiv 0 \,(\mathrm{mod}\, p)} ab^{p-1} + \underbrace{\binom{p}{p}}_{=1} a^p$$

$$(a+b)^p \equiv b_p + 0 + \ldots + 0 + a^p \equiv a^p + b^p \pmod{p}$$

Preuve du petit théorème de Fermat

On commence par le montrer pour $a \in \mathbb{N}$ par récurrence :

• Initialisation :

$0^p = 0 \equiv 0 \pmod{p}$

• Hérédité :

Soit $a \in \mathbb{N}$, on suppose que $a^p \equiv a \pmod{p}$, alors :

$(a+1)^p \equiv a^p + 1^p \equiv a + 1 \pmod{p}$ d'après le lemme précédent.

Pour généraliser à $a \in \mathbb{Z}$, il suffit de remarquer que $(-1)^p \equiv -1 \pmod{p}$. (Si $p > 2$, p est impair car premier, et pour 2 : $(-1)^2 \equiv 1 \equiv -1 \pmod{2}$.)

Entiers inversibles modulo n

Définition

Soit $n \in \mathbb{N}^*$, avec $n \geq 2$. On dit qu'un entier $a \in \mathbb{Z}$ est **inversible** modulo n si et seulement si il existe $b \in \mathbb{Z}$ tel que $a \cdot b \equiv 1 \pmod{n}$.

Remarque : Si a est inversible, et que deux entiers $(x, y) \in \mathbb{Z}^2$ vérifient $a \cdot b \equiv a \cdot c \pmod{n}$, alors $x \equiv y \pmod{n}$.
Il suffit en effet de multiplier les deux cotés de l'égalité par b tel que $a \cdot b \equiv 1 \pmod{n}$.
En particulier, tous les entiers b tels que $a \cdot b \equiv 1 \pmod{n}$ ont le même reste modulo n, on pourra noter ce reste a^{-1}.

Propriétés

- On a l'équivalence :

  a est inversible modulo n ssi a et b sont premiers entre eux.

  Preuve : par exemple en utilisant le théorème de Bézout.
- Si a et b sont deux entiers inversibles modulo n, alors $a \cdot b$ est aussi inversible modulo n.
  Il suffit d'utiliser l'implication $a \wedge n = b \wedge n = 1 \implies ab \wedge n = 1$.
- Attention, en revanche, si a et b sont inversibles, $a + b$ ne sont pas nécessairement inversibles.
  (Il suffit de prendre $b = -a$ pour s'en convaincre.)

Fonction indicatrice d'Euler

Définition

Soit $n \in \mathbb{N}^*$, on considère $\mathcal{P}_n = \{a \in [\![0, n-1]\!] \mid a \wedge n = 1\}$, c'est-à-dire l'ensemble des entiers strictement positifs inférieurs à n et premiers avec n ou encore (si $n \neq 1$) l'ensemble des restes possibles modulo n des entiers inversibles modulo n.

On pose alors $\boxed{\varphi(n) = \mathrm{card}(\mathcal{P}_n)}$.

On appelle la fonction φ fonction indicatrice d'Euler (elle est définie sur $\mathbb{N}^*$).

Propriétés

- $\varphi(1) = 1$
- si p est premier, $\varphi(p) = p - 1$
- si $a, b \in \mathbb{N}^*$ sont premiers entre eux, alors $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$
- pour $k \in \mathbb{N}^*$ et p premier, $\varphi(p^k) = (p-1)p^{k-1}$
- par conséquent, on a que si n admet comme décomposition en facteurs premiers $n = \prod_{j=1}^{m} p_j^{\alpha_j}$, alors $\varphi(n) = \prod_{j=1}^{m} (p_j - 1)p_j^{\alpha_j - 1} = n \cdot \prod_{j=1}^{m} \left(1 - \frac{1}{p_j}\right)$.

Théorème d'Euler-Fermat

Soit $n \geq 2$ un entier, et $a \in \mathbb{Z}$ tels que a et n sont premiers entre eux, alors :

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

En prenant n un nombre premier, ce théorème implique le théorème de Fermat.

Preuve

L'idée va être de considérer le produit de tous les restes d'entiers inversibles modulo n.
On note de nouveau $\mathcal{P}_n = \{a \in [\![0, n-1]\!] \mid a \wedge n = 1\}$.
On remarque alors que pour $a \in \mathcal{P}_n$, la fonction

$$g_a : \begin{cases} \mathcal{P}_n & \to \mathcal{P}_n \\ x & \mapsto ax \end{cases}$$

est bijective. (On a $g_a \circ g_{a^{-1}} = g_{a^{-1}} \circ g_a = \mathrm{Id}_{\mathcal{P}_n}$.)

Preuve

On numérote les éléments de $\mathcal{P}_n$, $x_1, x_2, \ldots, x_m$. Ainsi,

$$A = \prod_{x \in \mathcal{P}_n} x = x_1 \cdot x_2 \cdot \ldots \cdot x_m$$

$$A \equiv \prod_{x \in \mathcal{P}_n} g_a(x) \equiv (ax_1) \cdot (ax_2) \cdot \ldots \cdot (ax_m) \equiv a^m \cdot A \pmod{n}$$

Or A est inversible modulo n en tant que produit d'entiers inversibles modulo n, d'où $a^m \equiv 1 \pmod{n}$.
De plus, m est exactement le nombre d'éléments de $\mathcal{P}_n$, c'est-à-dire $\varphi(n)$.

Définition

Soit a et $n \geq 2$ deux entiers premiers entre eux.
D'après le théorème d'Euler-Fermat, on sait qu'il existe au moins un entier $b \in \mathbb{N}^*$ tels que $a^b \equiv 1 \pmod{n}$.
On note alors **ordre (multiplicatif)** de a modulo n le plus petit entier strictement positif satisfaisant cette condition.
Par la suite, on le notera $\omega_n(a)$.

Proposition

On considère toujours, a et $n \geq 2$ des entiers premiers entre eux, on a alors l'équivalence $a^b \equiv 1 \pmod{n} \iff \omega_n(a) \mid b$.

En particulier, on en déduit que $\omega_n(a) \mid \varphi(n)$.

Remarque

Attention, en général, on n'a pas nécessairement $\omega_n(a) = \varphi(n)$.
Il faut donc bien distinguer ces ceux notions.