# Petit théorème de Fermat

Anca Nitulescu
anca.nitulescu@ens.fr

Ecole Normale Supérieure, Paris

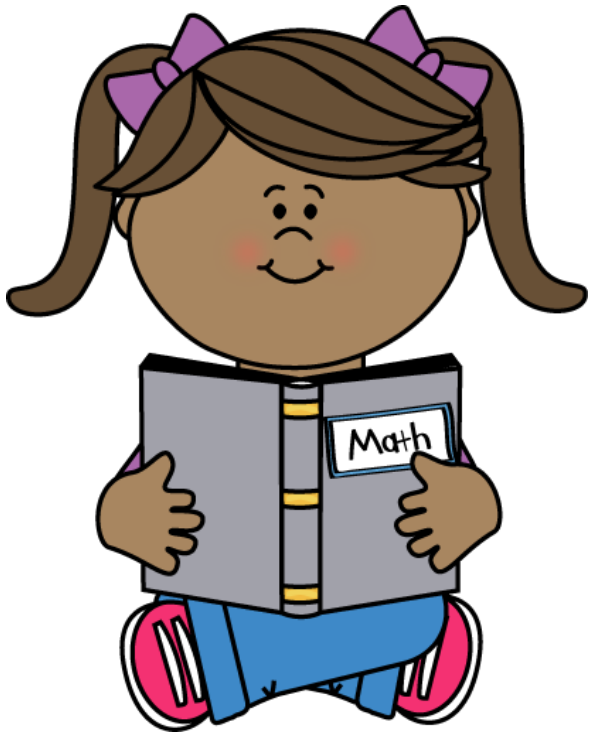
12 octobre 2016

# Arithmétique modulaire

## Arithmétique modulaire

Notation : $\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}_n$

- $(\mathbb{Z}_n, +) =$ **groupe additif abélien.**
- $(\mathbb{Z}_n, +, \cdot) =$ **anneau commutatif.**
- $(\mathbb{Z}_p^\star, \cdot) =$ **groupe multiplicatif.**
- $(\mathbb{Z}_p, +, \cdot) =$ **corps commutatif.**



# Arithmétique modulaire

- $(\mathbb{Z}_n, +)$ forme un **groupe additif commutatif d'ordre** $n$.
- $(\mathbb{Z}_n, +, \cdot)$ forme un **anneau commutatif**.
- **Inverse modulaire** de $a$ dans $\mathbb{Z}_n$ : entier $b = a^{-1}$ tel que

$$a \times b = 1 \mod n$$

- $\mathbb{Z}_n^\star =$ l'ensemble des éléments inversibles modulo $n$.

**Attention !**

$\mathbb{Z}_n^\star \neq \mathbb{Z}_n \setminus \{0\}$ pour $n$ **composé**
$\mathbb{Z}_p^\star = \mathbb{Z}_p \setminus \{0\}$ pour $p$ **prime**

# Critère d'inversibilité

## Les entiers inversibles modulo $n$

$x \in \mathbb{Z}_n^\star$ est inversibles modulo $n$ si et seulement si $\text{pgcd}(x, n) = 1$.
*Preuve* : T. Bézout.

## Calcul de l'inverse modulaire

Trouver $x^{-1} \mod n$

- Il existe $u$ et $v$ tels que $xu + nv = \text{pgcd}(x, n) = 1$
- Trouver l'inverse d'un élément revient à calculer $u$.
- L'algorithme d'Euclid étendu calcule des coeficients $(u, v)$

# Fonction d'Euler

## Définition

- $\varphi(n)$ est le nombre d'entiers de $[1, n]$ qui sont premiers avec $n$.
- $\varphi(n)$ désigne l'ordre du groupe multiplicatif $\mathbb{Z}_n^\star$

## Propriétés

Si $p, q$ sont deux nombres premiers distinctes :

- $\varphi(p) = p - 1$
- $\varphi(pq) = \varphi(p)\varphi(q)$

# Exponentiation modulaire

## Théorème de Lagrange

Si $\mathbb{G}$ est un groupe multiplicatif d'ordre $n$, alors :

$$\forall g \in \mathbb{G} \quad g^n = e$$

## Théorème d'Euler

Pour tout entier $n$ et tout $a \in \mathbb{Z}_n^\star$, on a

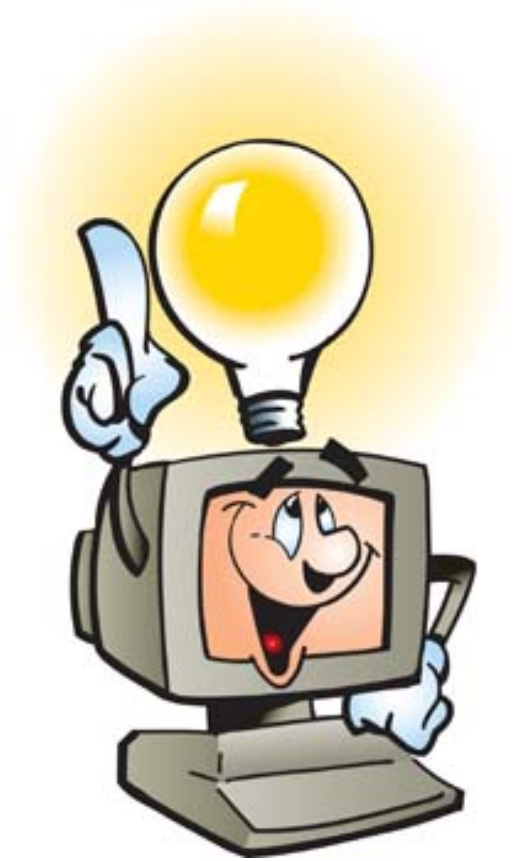
$$a^{\varphi(n)} = 1 \mod n$$

## Petit théorème de Fermat

Pour $p$ premier et tout entier $a$ on a

$$a^p = a \mod p$$

# Exponentiation modulaire



## Ordre du groupe $\mathbb{Z}_n^\star$

- $|\mathbb{Z}_n^\star| = \varphi(n) \quad \Rightarrow \quad a^{\varphi(n)} = 1 \ (mod\ n)$
- $|\mathbb{Z}_p^\star| = \varphi(p) = p-1 \Rightarrow \ a^{p-1} = 1 \ (mod\ n)$

## Règles

- Dans une exponentiation modulaire (modulo un entier $n$), les exposants doivent être pris modulo $\varphi(n)$.
- Effectuer les réduction modulaires au fur et à mesure.