Niveau : 1 **Jaune**

Le petit théorème de Fermat et ses généralisations

1 Le petit théorème de Fermat

Soit p un nombre premier. Nous notons $\mathbb{Z}/p\mathbb{Z}$ l'anneau des classes résiduelles modulo p, qui dans ce cas (p premier) est un corps. Le groupe multiplicatif des éléments inversibles est donc :

$$(\mathbb{Z}/p\mathbb{Z})^* = \mathbb{Z}/p\mathbb{Z} \setminus \{0\}.$$

Le petit théorème de Fermat concerne dans un premier temps les éléments inversibles de ce corps, c'est-à-dire les classes non nulles. Un élément inversible est donc représenté par un entier qui n'est pas un multiple de p.

Théorème 1.1 (Petit théorème de Fermat) *Pour tout entier a premier avec p (de manière équivalente non multiple de p) on a la relation :*

$$a^{p-1} \equiv 1 \quad (p).$$

Une conséquence capitale de ce théorème pour le calcul des puissances modulo p, est qu'on peut diminuer la taille des exposants dans les calculs :

Théorème 1.2 *Pour tout entier a premier avec p et pour tout exposant entier d on a la relation :*

$$a^d \mod p = a^{d \mod p-1} \mod p.$$

Il est facile maintenant de donner une version du petit théorème de Fermat valable pour tout entier (y compris pour les multiples de p).

Théorème 1.3 *Pour tout entier a on a la relation :*

$$a^p \equiv a \quad (p).$$

2 généralisation

Soit maintenant un entier $n > 1$ quelconque. On étudie l'anneau $\mathbb{Z}/n\mathbb{Z}$ des classes résiduelles modulo n. Nous noterons $(\mathbb{Z}/n\mathbb{Z})^*$ son sous-groupe multiplicatif des éléments inversibles. L'ordre de ce

sous-groupe (son nombre d'éléments) est $\Phi(n)$ où Φ est la fonction indicatrice d'Euler. Un résultat classique sur les groupes permet d'énoncer alors :

Théorème 2.1 *Pour tout entier a premier avec n on a la relation :*

$$a^{\Phi(n)} \equiv 1 \quad (n).$$

Ce théorème appliqué au cas précédent où n est un nombre premier p redonne le petit théorème de Fermat.

3 Cas où n est un produit de deux nombres premiers

Le cas où $n = pq$ est un produit de deux grands nombres premiers p et q est important en cryptographie, puisqu'il permet de traiter le cas du système RSA. Dans ce cas la fonction d'Euler est :

$$\Phi(n) = (p-1)(q-1).$$

On a donc tout de suite en conséquence du théorème précédent :

Théorème 3.1 *Pour tout entier a premier avec p et avec q et tout entier k on a la relation :*

$$a^{k(p-1)(q-1)+1} \equiv a \quad (n).$$

Il se trouve que dans ce cas particulier ce théorème reste vrai pour tout entier a, même s'il n'est pas premier avec pq.

Théorème 3.2 *Pour tout entier a et tout entier k on a la relation :*

$$a^{k(p-1)(q-1)+1} \equiv a \quad (n).$$

Cette dernière relation est très importante pour le système RSA, puisqu'elle permet de montrer comment se calcule le déchiffrement d'un texte chiffré.