Rappels arithmétiques

blogdemaths.wordpress.com

1 Ordre d'un élément

Proposition. *Soit a et p deux entiers premiers entre eux. Il existe un plus petit entier $m > 0$ tel que :*

$$a^m \equiv 1 \mod [p]$$

L'entier m s'appelle l'ordre de a modulo p.

Démonstration. On commence par montrer qu'il existe au moins un entier n tel que $a^n \equiv 1 \mod [p]$. Si on considère la suite $(a^k \mod [p])$ des puissances de a modulo p, on a une infinité de nombres qui ne peuvent prendre qu'un nombre fini de valeurs (1, 2, 3, ..., $p-1$). D'après le principe des tiroirs, il existe deux de ces nombres qui doivent être égaux :

$$a^r \equiv a^s \mod [p] \text{ avec } r > s$$

Comme a est premier avec p, il admet un inverse modulo p, ce qui revient à dire qu'on peut simplifier par a à gauche et à droite. On en déduit donc que :

$$a^{r-s} \equiv 1 \mod [p]$$

avec $r - s > 0$. En posant $n = r - s$, on a donc bien $n > 0$ et $a^n \equiv 1 \mod [p]$. Ainsi, l'ensemble

$$\{n > 0 \mid a^n \equiv 1 \mod [p]\}$$

est un sous-ensemble de $\mathbb{N}$ non vide, donc il admet un plus petit élément $m > 0$. □

Proposition. *Soit a et p deux entiers premiers entre eux. Soit m l'ordre de a modulo p. Si m' est tel que :*

$$a^{m'} \equiv 1 \mod [p]$$

alors m divise m'.

Démonstration. Soit $m' = mq + r$ (avec $0 \leqslant r < m$) la division euclidienne de m' par m. On a :

$$a^r = a^{m'-mq} = a^{m'}(a^m)^q \equiv 1 \times 1^q = 1 \mod [p]$$

On ne peut donc pas avoir $r > 0$ car le fait que $r < m$ contredirait la définition même de l'ordre d'un élément (qui est, rappelons-le, le plus petit entier $m > 0$ tel que $a^m \equiv 1 \mod [p]$). Ainsi, $r = 0$, et donc $m' = mq$, ce qui veut bien dire que m divise m'. □

2 Carrés modulo p

On dit qu'un entier a est un carré modulo p s'il existe un entier x tel que :

$$a \equiv x^2 \mod [p]$$

Proposition. *Soit $p > 2$ un nombre premier et a un nombre premier avec p. Si a est un carré modulo p, alors :*

$$a^{\frac{p-1}{2}} \equiv 1 \mod [p]$$

Démonstration. Par hypothèse, il existe un entier x tel que $a \equiv x^2 \mod [p]$. En prenant cette relation à la puissance $\frac{p-1}{2}$, on obtient :

$$a^{\frac{p-1}{2}} \equiv (x^2)^{\frac{p-1}{2}} = x^{p-1} \mod [p]$$

Or, d'après le petit théorème de Fermat, on a $x^{p-1} \equiv 1 \mod [p]$, d'où le résultat. □

Proposition. *Réciproquement, si $p > 2$ est premier et si a est tel que :*

$$a^{\frac{p-1}{2}} \equiv 1 \mod [p]$$

alors a est un carré modulo p.

Démonstration. Comme le groupe $(\mathbb{Z}/p\mathbb{Z})^*$ est cyclique, donc si on note g un de ses générateurs, on sait qu'il existe un entier k tel que $a \equiv g^k \mod [p]$. En prenant cette relation à la puissance $\frac{p-1}{2}$, on trouve :

$$a^{\frac{p-1}{2}} \equiv g^{k\frac{p-1}{2}} \mod [p]$$

ce qui entraîne que $1 \equiv g^{k\frac{p-1}{2}} \mod [p]$. Mais, puisque g est un générateur, on sait que son ordre est $p-1$. D'après une proposition précédente, on en déduit que $p-1$ divise $k\frac{p-1}{2}$:

$$\exists t \in \mathbb{Z},\ k\frac{p-1}{2} = t(p-1) \iff \frac{k}{2} = t$$

Ainsi, $\frac{k}{2}$ est un entier. Nous en déduisons alors que :

$$a \equiv g^k = (g^{\frac{k}{2}})^2 \mod [p]$$

et donc a est bien un carré modulo p. □

Théorème. *Si p est de la forme $8m+1$ alors 2 est un carré modulo p.*

Démonstration. D'après la proposition précédente, il suffit de prouver que $2^{\frac{p-1}{2}} \equiv 1 \mod [p]$. Pour cela, on va calculer de deux façons différentes (modulo p) le produit :

$$N = 2 \times 4 \times 6 \times \cdots \times (p-1)$$

Tout d'abord, on remarque que :

$$N = (2 \times 1) \times (2 \times 2) \times \cdots \times (2 \times \frac{p-1}{2}) = 2^{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)!$$

D'autre part, comme $p - 1 = 8m$, on a :

$$\begin{aligned}
N &= \underbrace{[2 \times 4 \times 6 \times \cdots \times 4m]}_{2m \text{ facteurs}} \times \underbrace{[(4m+2) \times (4m+4) \times \cdots \times (8m-2) \times 8m]}_{2m \text{ facteurs}} \\
&\equiv [2 \times 4 \times 6 \times \cdots \times 4m] \times \left[(4m+2-p) \times (4m+4-p) \times \cdots \times (8m-2-p) \times (8m-p)\right] \mod [p] \\
&\equiv [2 \times 4 \times 6 \times \cdots \times 4m] \times [(-(4m-1)) \times (-(4m-3)) \times \cdots \times (-3) \times (-1)] \mod [p] \\
&\equiv (-1) \times 2 \times (-3) \times 4 \times \cdots \times (-(4m-1)) \times 4m \mod [p] \\
&\equiv (-1)^{2m}(4m)! \mod [p] \\
&\equiv (4m)! \mod [p]
\end{aligned}$$

Comme $4m = \frac{p-1}{2}$, nous voyons que $N \equiv \left(\frac{p-1}{2}\right)! \mod [p]$. Puisque nous avions aussi vu que $N = 2^{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)!$, on en déduit :

$$2^{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)! \equiv \left(\frac{p-1}{2}\right)! \mod [p]$$

et donc en simplifiant par $\left(\frac{p-1}{2}\right)!$ (qui est bien premier avec p), on obtient :

$$2^{\frac{p-1}{2}} \equiv 1 \mod [p]$$

CQFD !

□