

II. Lemmes de Gauss :

On note $\left(\frac{a}{p}\right)$ la valeur de $a^{\frac{p-1}{2}}$ dans $\mathbb{Z}/p\mathbb{Z}$.

Dans la division de n par p , on appelle reste minimal, l'unique nombre r tel que : $n = pq + r$ où $-\frac{1}{2}p < r < \frac{1}{2}p$; exemple : le reste minimal de la division de 50 par 11 est -5 ($50 = 5 \times 11 - 5$, $-\frac{1}{2}11 < -5 < \frac{1}{2}11$).

1°). Si $a \neq 0$ et $a < p$, on pose : $k.a = p.q_k + r_k$ (r_k reste minimal).

Montrer que si $k \in [1, \frac{p-1}{2}]$: $r_k = r_{k'}$ $\Rightarrow k = k'$

et $r_k + r_{k'} = 0$ impossible.

(i.e. : $r : k \rightarrow |r_k|$ est une injection).

En déduire le lemme de Gauss : les restes minimaux de chacun des produits $1 \times a, 2 \times a, \dots, \frac{1}{2}(p-1)a$ ont pour valeur absolue les nombres : $1, 2, \dots, \frac{p-1}{2}$.

2°) En utilisant les relations du 1°, montrer que :

$\left(\frac{p-1}{2}\right)! a^{\frac{p-1}{2}} \equiv (-1)^u \left(\frac{p-1}{2}\right)! [p]$ où u désigne le nombre de restes négatifs. En déduire le deuxième lemme de Gauss : $\left(\frac{a}{p}\right) = (-1)^u$.

3°) Etude de $\left(\frac{2}{p}\right)$:

a) Exemple : si $p = 41$, et $k \in [1, \frac{p-1}{2}]$, donner les valeurs de k telles que les restes minimaux des termes $2k$ sont négatifs.

b) Dans le cas général, montrer qu'il y a autant de restes négatifs qu'il y a de nombres impairs inférieurs à $\frac{p}{2}$.

c) En déduire que si $p = 8h \pm 1$ alors $\left(\frac{2}{p}\right) = 1$

et que si $p = 8h \pm 3$ alors $\left(\frac{2}{p}\right) = -1$.

(Résultats que l'on peut mettre sous la forme : $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$)

4°) En admettant la loi de réciprocité quadratique :

$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}$ si p et q sont des nombres premiers impairs,

préciser si : i) 5 est un carré dans $\mathbb{Z}/1987\mathbb{Z}$

ii) -1459 est un carré dans $\mathbb{Z}/22366891\mathbb{Z}$

(1987 et 22366891 sont des nombres premiers)