

II. 1°). si $\pi_k = \pi_{k'} \Rightarrow ka = ka' [p] \Rightarrow p | (k - k')a$.

Or: $0 < a < p$ donc, $p | (k - k')$ mais $|k - k'| < p \Rightarrow \underline{k = k'}$. (3)

si $\pi_k + \pi_{k'} = 0$, alors $(k + k')a = 0 [p] \Rightarrow p | (k + k')$

donc: $k + k' = p$, mais: $k \leq \frac{p-1}{2} \Rightarrow k + k' \leq p-1$ impossible
 $k' \leq \frac{p-1}{2}$ (3)

Donc: $\pi: k \rightarrow |\pi_k|$ injection de $[1, \frac{p-1}{2}]$ dans l'ensemble des restes en valeurs absolues: mais: $|\pi_k| < \frac{p}{2} \Leftrightarrow |\pi_k| \leq \frac{p-1}{2}$; d'autre part, aucun reste n'est nul, donc π est une bijection de $[1, \frac{p-1}{2}]$ sur lui-même; on obtient ainsi le 1^{er} lemme de Gauss. (3)

$$2^\circ). (1 \times a) \times (2 \times a) \times \dots \times \left(\frac{p-1}{2} \times a\right) \equiv \pi_1 \times \dots \times \pi_{\frac{p-1}{2}} [p]$$

$$\left(\frac{p-1}{2}\right)! \cdot a^{\frac{p-1}{2}} \equiv \left(\frac{p-1}{2}\right)! (-1)^u \text{ où } u \text{ est le nombre de restes négatifs.}$$

Comme p est premier, $\left(\frac{p-1}{2}\right)!$ et p sont étrangers, donc, on peut diviser par $\left(\frac{p-1}{2}\right)!$ dans $\mathbb{Z}/p\mathbb{Z}$ d'où le 2^e lemme de Gauss: $\left(\frac{a}{p}\right) = (-1)^u$ (3)

3°) soit $p = 41$, $k \in [1, 20]$: $\pi_k > 0 \Leftrightarrow 2k \leq 20 \Leftrightarrow k \leq 10$.

$\pi_k < 0 \Leftrightarrow 2k > 20 \Leftrightarrow k \in [11, 20]$. (3)

Et dans ce dernier cas; on a: $2k = 41 + \pi_k \Leftrightarrow \pi_k = -(41 - 2k)$.

$41 - 2k$ est un nombre impair positif, inférieur à $\frac{1}{2}(41)$ car $|\pi_k| < \frac{1}{2}41$

b). si $2k \leq \frac{p-1}{2}$, $\pi_k = 2k > 0$, si $2k > \frac{p-1}{2}$, on a: $2k = p + \pi_k$.

Donc, on a autant de restes négatifs que de nombres $-\pi_k = p - 2k$ où: (6)

$0 < -\pi_k < \frac{p}{2}$: i.e. on a autant de restes négatifs que de nombres impairs $< \frac{1}{2}p$.

c) $p = 8h \pm 1$: $\frac{p}{2} = 4h \pm \frac{1}{2}$.

nombre de nombres impairs: il faut résoudre: $1 \leq 2h-1 \leq 4h-1 \Leftrightarrow h \in [1, 2h]$

On a donc $2h$ nombres impairs donc: $\left(\frac{2}{p}\right) = 1$

$p = 8h \pm 3$: $\frac{p}{2} = 4h \pm \frac{3}{2}$. (5)

$\frac{p}{2} = 4h - \frac{3}{2}$, il faut résoudre: $1 \leq 2h-1 \leq 4h-2 \Leftrightarrow h \in [1, 2h-1] \Rightarrow \left(\frac{2}{p}\right) = -1$.

$\frac{p}{2} = 4h + \frac{3}{2} \Leftrightarrow h \in [1, 2h+1]$

4°). i) On a: $\left(\frac{5}{1987}\right) \cdot \left(\frac{1987}{5}\right) = (-1)^{993-2} = 1$; il suffit de connaître: $\frac{1987}{5}$

Or: $\left(\frac{1987}{5}\right) = \left(\frac{2}{5}\right) = -1$ donc, 5 n'est pas un carré dans $\mathbb{Z}/1987\mathbb{Z}$ (3)

ii) On pose $p = 22366891$: $\left(-\frac{1459}{p}\right) = \left(-\frac{1}{p}\right) \left(\frac{1459}{p}\right)$ or: $p = 3 + 4h$ donc,

grâce au I. 5°a) $\left(-\frac{1}{p}\right) = -1$.

1459 est premier, donc: $\left(\frac{1459}{p}\right) \cdot \left(\frac{p}{1459}\right) = (-1)$ car $\frac{p-1}{2}$ impair et $\frac{1459-1}{2}$ impair.

$p \equiv 421 [1459] \Rightarrow \left(-\frac{1459}{p}\right) = \left(\frac{421}{1459}\right) = \left(\frac{1459}{421}\right) = \left(\frac{196}{421}\right) = 1$ car $196 = 14^2$. (8)

Donc: 1459 est un carré dans $\mathbb{Z}/p\mathbb{Z}$.