Ex0538 - 7

p premier $\geqslant 3$

Montrer que pour k non divisible par $p-1$ on a :

$1^k + 2^k + \dots + (p-1)^k$ divisible par p

Plaçons-nous dans le corps $\mathbb{F}_p$ $\left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)$

Considérons φ le morphisme de groupe de $\mathbb{F}_p^*$ dans $\mathbb{F}_p^*$

défini par : $\varphi : a \longrightarrow a^k$

NB : on peut se limiter à $k \leq p-2$ à cause du théorème de Fermat.

1er cas : $\operatorname{Ker} \varphi = \{1\}$

dans ce cas φ est bijectif

Il y a égalité des ensembles $\{1^k, 2^k, \dots, (p-1)^k\}$

et $\{1, 2, \dots, p-1\}$

Or ces éléments sont les racines du polynôme $X^{p-1} - 1$

la somme des racines est nulle et donc

$1^k + 2^k + \dots + (p-1)^k = 0$ dans $\mathbb{F}_p$

donc $1^k + 2^k + \dots + (p-1)^k$ est divisible par p dans $\mathbb{N}$.

$\rightarrow$

2ème cas : $\operatorname{Ker} \varphi = G$ avec $\operatorname{Card}(G) = q > 1$

q divise $p-1$ car G est un sous-groupe du groupe multiplicatif $\mathbb{F}_p^*$

Montrons aussi que $q < p-1$

En effet si q était égal à $p-1$ on aurait

$$1^k = 1 \qquad 2^k = 1 \qquad \dots \qquad (p-1)^k = 1$$

en vertu du théorème de Fermat

et on aurait donc $1^k + 2^k + \dots + (p-1)^k = p-1 = -1 \neq 0$

Donc on a $1 < q < p-1$ et q divise $p-1$

Soit $H = \operatorname{Im}(\varphi)$ avec $\operatorname{Card}(H) = r$

on a évidemment $qr = p-1$

De plus G et H sont deux sous-groupes cycliques de $\mathbb{F}_p^*$ car $\mathbb{F}_p^*$ lui-même est cyclique.

$$G = \{ b, b^2, \dots, b^{q-1}, b^q = 1 \}$$

$$H = \{ c, c^2, \dots, c^{r-1}, c^r = 1 \}$$

Par ailleurs $\mathbb{F}_p^*$ est la réunion de q classes d'équivalence

$$(x \mathcal{R} y \iff x y^{-1} \in H)$$

Ces classes d'équivalence sont : $H_0 = H = \{c, c^2, \dots, c^r = 1\}$

$H_1 = \{bc, bc^2, \dots, bc^r = b\}$

$H_2 = \{b^2c, b^2c^2, \dots, b^2c^r = b^2\}$

$H_{q-1} = \{b^{q-1}c, b^{q-1}c^2, \dots, b^{q-1}c^r = b^{q-1}\}$

soit S_i la somme des éléments de H_i

$$S_i = b^i c + b^i c^2 + \cdots + b^i c^{r-1} + b^i c^r$$

$$= b^i (1 + c + \cdots + c^{r-1}) = b^i \frac{c^r - 1}{c-1} = b^i \frac{1-1}{c-1} = 0$$

Donc $1^k + \cdots + (p-1)^k = \sum_{i=0}^{q-1} S_i = 0$

c.q.f.d