

Arithmétique 2025 normale

EXERCICE 3 : (3 points)

Soient p un nombre premier impair et a un entier premier avec p .

1. Montrer que $a^{\frac{p-1}{2}} \equiv 1 [p]$ ou $a^{\frac{p-1}{2}} \equiv -1 [p]$.
2. On considère dans $\mathbb{Z}$ l'équation : $ax^2 \equiv 1 [p]$. Soit x_0 une solution de cette équation.
 - (a) Montrer que : $x_0^{p-1} \equiv 1 [p]$.
 - (b) En déduire que : $a^{\frac{p-1}{2}} \equiv 1 [p]$.
3. Soit n un entier naturel non nul.
 - (a) Montrer que si p divise $2^{2n+1} - 1$ alors $2^{\frac{p-1}{2}} \equiv 1 [p]$.
 - (b) En déduire que l'équation $(E) : 11x + (2^{2n+1} - 1)y = 1$ admet au moins une solution dans $\mathbb{Z}^2$.
4. On considère dans $\mathbb{Z}$ l'équation $(F) : x^2 + 5x + 2 \equiv 0 [11]$.
 - (a) Montrer que : $(F) \iff 2(2x + 5)^2 \equiv 1 [11]$.
 - (b) En déduire que l'équation (F) n'admet pas de solution dans $\mathbb{Z}$.

Solution :

1. D'après Fermat : $a^{p-1} \equiv 1 [p]$ donc $p | a^{p-1} - 1 = \left(a^{\frac{p-1}{2}} - 1\right) \left(a^{\frac{p-1}{2}} + 1\right)$.

p est impair donc $\frac{p-1}{2} \in \mathbb{N}$ donc $a^{\frac{p-1}{2}} \in \mathbb{N}^*$.

Puisque p est premier, on a : $p | a^{\frac{p-1}{2}} - 1$ ou $p | a^{\frac{p-1}{2}} + 1$. D'où le résultat.

2. (a) Si $p \mid x_0$ alors $p | ax_0^2$ donc $p \mid 1$ (car x_0 est solution de l'équation) donc $p = 1$. Ce qui est absurde car p est premier. Donc p ne divise pas x_0 . Puisque p est premier on a : $p \wedge x_0 = 1$.

D'après Fermat on a le résultat.

(b) On a $ax_0^2 \equiv 1 [p]$, on élève tout à $\frac{p-1}{2}$, donc : $a^{\frac{p-1}{2}} x_0^{p-1} \equiv 1 [p]$.

D'après (a), on obtient le résultat.

3.(a) On a $2^{2n+1} = 2 \times (2^n)^2 \equiv 1 [p]$. Donc pour $a = 2$ (qui est premier avec p car p est impair), on a : $x_0 = 2^n$ est solution de l'équation de la question 2.

D'après 2(b), on a : $a^{\frac{p-1}{2}} \equiv 1 [p]$ avec $a = 2$, d'où le résultat.

(b) Montrons que $(2^{2n+1} - 1) \wedge 11 = 1$. Si $11 \mid (2^{2n+1} - 1)$ alors puisque 11 est premier impair, on peut appliquer le résultat de (a) avec $p = 11$, donc $2^{\frac{11-1}{2}} = 32 \equiv 1 [11]$ ce qui est absurde car $32 \equiv -1 [11]$. Donc 11 ne divise pas $(2^{2n+1} - 1)$.

11 est premier donc $(2^{2n+1} - 1) \wedge 11 = 1$.

Par le théorème de Bézout on a le résultat.

$$4.(a) \ 2(2x+5)^2 - 1 = 2(4x^2 + 25 + 20x) - 1 = 8x^2 + 50 + 40x - 1 = 8x^2 + 49 + 40x \equiv 8x^2 + 40x + 5[11]$$

Et on a $11 \wedge 8 = 1$ donc par Gauss : $11 \mid (x^2 + 5x + 2) \iff 11 \mid 8(x^2 + 5x + 2)$. On donc :

$$(F) \iff 8(x^2 + 5x + 2) \equiv 0[11] \iff 8x^2 + 40x + 16 \equiv 0[11] \iff 8x^2 + 40x + 5 \equiv 0[11]$$

D'où l'équivalence.

(b) $2(2x+5)^2 \equiv 1[11]$ n'admet de solution car sinon d'après 3(a) on aura $2^{\frac{11-1}{2}} = 32 \equiv 1[11]$ ce qui est faux.

D'où (F) n'admet de solution.

