Corrigé succinct du Partiel MEV 204. 2024.

Ex 1 : ① et ② voir cours

③ . On a une identité de Bezout :

$$5a - 14b = 1$$, d'où $\mathrm{pgcd}(a,b) = 1$

Ex 2 :

① p est premier et $\neq 2$; $p = 2k+1$;

$(p-1) = 2k$; $(p+1) = 2(k+1)$; $k, k+1$ sont deux entiers consécutifs, l'un des deux est pair ; On a donc : 4 divise $p-1$ ou 4 divise $p+1$; ce qui donne : en conclusion

$2 \times 4 \mid (p-1)(p+1)$; $2 \mid p^2+1$

16 divise $(p^4-1) = (p-1)(p+1)(p^2+1)$.

② On a par le corollaire du th du petit Fermat : (5 et 3 sont des nombres premiers).

$$5 \mid p^{5-1} - 1 = p^4 - 1 \quad \text{et} \quad 3 \mid p^{3-1} - 1 = (p^2-1),$$

ou encore : $3 \mid (p^2-1)(p^2+1) = p^4-1$.

③ $240 = 16 \times 5 \times 3$. ; ~~On conclut~~ ces trois nombres sont premiers entre eux. et chacun divise p^4-1

On conclut que le produit 240 divise p^4-1

Ex3 : Soit ℓ un entier qui appartient à $[N+2, N+n]$; $\ell = N+k$; avec k un entier $2 \leq k \leq n$;

$k \mid N = n!$ et $k \mid k \Rightarrow k \mid N+k = \ell$.

et ℓ n'est pas premier.

Ex4 ①

$$520 = 1 \times 325 + 195$$
$$325 = 1 \times 195 + 130$$
$$195 = 1 \times 130 + 65$$
$$130 = 2 \times 65 + 0.$$

② $m = 65$

③
$$65 = 195 - 1 \times 130$$
$$= 195 - 1(325 - 1 \times 195)$$
$$= 195 \times 2 - 325$$
$$= (520 - 1 \times 325) \times 2 - 325$$
$$= 520 \times 2 - 3 \times 325.$$

Ex5 - $a^5 = 1$ donc $a^6 = a$

$a^3 b = b a^3$, on compose par a^3 (à gauche)

$ab = a^6 b = (a^3 b) a^3 = (b a^3) a^3 = b a^6 = ba$

Ex 6

(1) Soit n un nombre premier, supposons que n divise $q^k = q \cdot q^{(k-1)}$, d'après le lemme d'euclide, n divise l'un des deux, si n ne divise pas q, alors il divise q^{k-1} et on recommence. Finalement on aura : $n \mid q$.

Soit d un diviseur positif commun à p et à q^k ; si $d \neq 1$, il existe un diviseur premier n de d ; $n \mid p$ et $n \mid q^k \Rightarrow n \mid p$ et $n \mid q$. Absurde car $\text{pgcd}(p, q) = 1$, donc $d = 1$ et $\text{pgcd}(p, q^k) = 1$

(2) On a : $a_n \left(\frac{p}{q}\right)^n + a_{n-1}\left(\frac{p}{q}\right)^{n-1} + \cdots + a_0 = 0$

On multiplie le tout par q^n, on obtient :

$$a_n p^n + \underbrace{a_{n-1} p^{n-1} q + a_{n-2} p^{n-2} q^2 + \cdots + a_1 p \cdot q^{n-1} + a_0 q^n}_{\text{multiple de } q} = 0$$

$\Rightarrow q \mid a_n p^n$; comme $\text{pgcd}(q, p^n) = 1$ (question 1, (p et q jouent un rôle symétrique)) d'après Gauss : $q \mid a_n$.

(3) On applique le même raisonnement et on obtient : $p \mid a_0$.

(4)

(4) $a_0 = -2$; $a_n = a_3 = 1$;

$q \mid 1 \Rightarrow q = 1 \quad (q > 0)$.

$p \mid -2 \Rightarrow p \in \{-1, -2, 1, 2\}$.

les solutions rationnelles possibles sont :

$\{-1, -2, 1, 2\}$; on les teste toutes et on trouve

une unique solution rationelle : $x = 2$

EX 7 : Montrons d'abord que :

si $M \in M_n(\mathbb{Z})$; $\det M \in \mathbb{Z}$.

Par récurrence sur n ; pour $n = 2$; $\begin{vmatrix} a & b \\ c & d \end{vmatrix} = ad - bc \in \mathbb{Z}$

supposons que $\det M_n \in \mathbb{Z}$ pour n donné quelconque

soit M_{n+1} = matrice de taille $(n+1)$; on développe

le det suivant la première ligne :

on obtient $\det M_{n+1} = a_{11} \det M_1 + a_{12} \det M_2 + \cdots + (-1)^{n+2} \det M_{n+1}$

chaque matrice M_i est de taille n et à coefficients entiers

son det est un entier (hypothèse de récurrence).

Finalement : $\det M_{n+1} \in \mathbb{Z}$.

Revenons à notre exercice. $M = (a_{ij})$; $a_{ij} \in \{-1, 1\}$.

$\det M$ = det de la matrice obtenue en faisant les changement suivant :

$C_1 \longrightarrow C_1$

$C_2 \longrightarrow C_1 + C_2$

$\vdots$

$C_n \longrightarrow C_1 + C_n$.

les colonnes $C_1 + C_i$: ~~ne contient que~~
formée d'element $\in \{0, 2, -2\}$.
donc : des multiples de 2.

On a : $\det M = \begin{vmatrix} C_1 & C_2 & C_3 & \cdots & C_n \end{vmatrix}$

$$= \underbrace{2 \times \cdots 2}_{(n-1) \text{ fois}} \begin{vmatrix} C_1 & \frac{C_2 + C_1}{2} & \frac{C_3 + C_1}{2} & \cdots & \frac{C_n + C_1}{2} \end{vmatrix}$$

$$= 2^{n-1} \begin{vmatrix} \underbrace{C_1 \quad \frac{C_2 + C_1}{2} \quad \cdots \quad \frac{C_n + C_1}{2}}_{\in M_n(\mathbb{Z})} \end{vmatrix}$$

On a donc : 2^{n-1} divise $\det M$