

SEMAINE 12 DU 18/12/2023

1 PROGRAMME OFFICIEL

a) Divisibilité et division euclidienne	
Divisibilité dans \mathbf{Z} , diviseurs, multiples. Théorème de la division euclidienne.	Caractérisation des couples d'entiers associés.
b) PGCD et algorithme d'Euclide	
PGCD de deux entiers naturels dont l'un au moins est non nul. Algorithme d'Euclide. Extension au cas de deux entiers relatifs. Relation de Bezout. PPCM.	Notation $a \wedge b$. Le PGCD de a et b est défini comme étant le plus grand élément (pour l'ordre naturel dans \mathbf{N}) de l'ensemble des diviseurs communs à a et b . L'ensemble des diviseurs communs à a et b est égal à l'ensemble des diviseurs de $a \wedge b$. $a \wedge b$ est le plus grand élément (au sens de la divisibilité) de l'ensemble des diviseurs communs à a et b . Pour $k \in \mathbf{N}^*$, PGCD de ka et kb . Détermination d'un couple de Bezout par l'algorithme d'Euclide étendu. Notation $a \vee b$.
c) Entiers premiers entre eux	
Couples d'entiers premiers entre eux. Théorème de Bézout. Lemme de Gauss. Si a et b premiers entre eux divisent n , alors ab divise n . Si a et b sont premiers à n , alors ab est premier à n . PGCD d'un nombre fini d'entiers, relation de Bezout. Entiers premiers entre eux dans leur ensemble, premiers entre eux deux à deux.	Forme irréductible d'un rationnel.

d) Nombres premiers

Nombre premier. L'ensemble des nombres premiers est infini. Existence et unicité de la décomposition d'un entier naturel non nul en produit de nombres premiers. Pour p premier, valuation p -adique. Valuation p -adique d'un produit.	Crible d'Eratosthène. Notation $v_p(n)$. Caractérisation de la divisibilité en termes de valuations p -adiques. Extension du PGCD et du PPCM à l'aide des valuations p -adiques.
---	--

e) Congruences

Relation de congruence modulo un entier sur \mathbf{Z} . Opérations sur les congruences : somme, produit. Utilisation d'un inverse modulo n pour résoudre une congruence modulo n . Petit théorème de Fermat.	Notation $a \equiv b [n]$. Les anneaux $\mathbf{Z}/n\mathbf{Z}$ sont hors programme.
--	--

2 EXERCICES À SAVOIR REFAIRE

Et preuves sur lesquelles insister davantage.

- 1) Lemme de Gauss (avec Bezout ou valuation p -adiques).
- 2) Si $a|c$ et $a'|c$ avec $a \wedge a' = 1$, alors $aa'|c$ (avec Bezout ou valuation p -adiques).
- 3) Résolution d'une équation du type $5x + 7y = 1$ sur \mathbf{Z} .
- 4) CCINP 86
 - (a) Soit $(a, b, p) \in \mathbf{Z}^3$. Prouver que : si $p \wedge a = 1$ et $p \wedge b = 1$, alors $p \wedge (ab) = 1$.
 - (b) Soit p un nombre premier.
 - i. Prouver que $\forall k \in \llbracket 1, p-1 \rrbracket$, p divise $\binom{p}{k}k!$, puis en déduire que p divise $\binom{p}{k}$.
 - ii. Prouver que: $\forall n \in \mathbf{N}$, $n^p \equiv n \pmod{p}$. *Indication*: procéder par récurrence.
 - iii. En déduire, pour tout entier naturel n , que :

$$p \text{ ne divise pas } n \implies n^{p-1} \equiv 1 \pmod{p}.$$

- 5) CCINP 94
 - (a) Énoncer le théorème de Bézout dans \mathbf{Z} .
 - (b) Soit a et b deux entiers naturels premiers entre eux.
Soit $c \in \mathbf{N}$. Prouver que: $(a|c \text{ et } b|c) \iff ab|c$.
 - (c) On considère le système (S) : $\begin{cases} x \equiv 6 & [17] \\ x \equiv 4 & [15] \end{cases}$ dans lequel l'inconnue x appartient à \mathbf{Z} .
 - i. Déterminer une solution particulière x_0 de (S) dans \mathbf{Z} .
 - ii. *Déduire des questions précédentes* la résolution dans \mathbf{Z} du système (S) .