Colle 18 : Arithmétique et Dérivation

Résultats et preuves à connaître

Proposition 1 Croissance des pentes

Soit $f : I \to \mathbb{R}$. Pour tout $a \in I$ on note

$$\tau_a : \begin{cases} I \setminus \{a\} & \to & \mathbb{R} \\ x & \mapsto & \frac{f(x)-f(a)}{x-a} \end{cases}$$

La fonction f est convexe sur I si et seulement si, pour tout $a \in I$, τ_a est croissante.

Proposition 2 Caractérisation des fonctions convexes dérivables et deux fois dérivables

Soit $f : I \to \mathbb{R}$ une fonction dérivable. La fonction f est convexe sur I si et seulement si f' est croissante sur I.
Et dans le cas où f est deux fois dérivable, f est convexe ssi $f'' \geq 0$

Proposition 3 Algorithme d'Euclide

- Si r est le reste de la division euclidienne de a par b alors

$$\mathscr{D}(a) \cap \mathscr{D}(b) = \mathscr{D}(b) \cap \mathscr{D}(r)$$

- le pgcd de a et b est le dernier reste non nul de l'algorithme d'Euclide et $\mathscr{D}(a) \cap \mathscr{D}(b) = \mathscr{D}(a \wedge b)$

Proposition 4 Coefficients de Bezout

Soient $(a,b) \in \mathbb{Z}^2$. Il existe $(u,v) \in \mathbb{Z}^2$ tel que

$$au + bv = a \wedge b$$

u et v sont appelés **coefficients de Bezout** de a et b.

Proposition 5 Conséquence

Soient $(a,b) \in \mathbb{Z}^2$

$$a\mathbb{Z} + b\mathbb{Z} = (a \wedge b)\mathbb{Z}$$

Proposition 6 Théorème de Gauss

Soient $(a,b,c) \in \mathbb{Z}^3$.

$$a \wedge b = 1 \quad \text{et} \quad a \,|\, bc \Longrightarrow a \,|\, c$$

Proposition 7 Conséquences

- $a \wedge b = 1$ et $a \wedge c = 1 \iff a \wedge (bc) = 1$
- $a \wedge b = 1 \Longrightarrow \forall (m,n) \in \mathbb{N}^2, a^m \wedge b^n = 1$
- Un produit de facteurs est premier avec a ssi chacun des facteurs est premier avec a.
- $a \wedge b = 1, a \,|\, c$ et $b \,|\, c \Longrightarrow ab \,|\, c$.

Proposition 8 Calcul du PPCM

- Si $a \wedge b = 1$ alors $a \vee b = |ab|$.
- Si $d = a \wedge b$, comme $a = da'$ et $b = db'$ avec $a' \wedge b' = 1$, alors

$$a \vee b = d\,|a'b'| \quad \text{et} \quad (a \wedge b)(a \vee b) = |ab|$$

Proposition 9 Équation diophantienne $ax + by = c$

Soient $(a,b,c) \in \mathbb{Z}^3$.
On cherche les couples $(x,y) \in \mathbb{Z}^2$ solution de l'équation

$$ax + by = c$$

Si $a \wedge b$ ne divise pas c, l'équation n'a pas de solution.
(à savoir démontrer) Sinon la solution générale de l'équation est la somme d'une solution particulière (obtenue par remontée de l'algorithme d'Euclide du calcul de $a \wedge b$) et de la solution générale de l'équation homogène associée $ax + by = 0$.
On ne demandera pas de démonstration, mais de savoir appliquer la méthode pour résoudre une telle équation diophantienne sur un exemple précis.

Définition 1

Soit $(a_k)_{1 \leqslant k \leqslant p}$ une famille d'entiers ($p \geqslant 2$) non tous nuls. L'ensemble des diviseurs communs à $a_1, a_2 \dots a_p$ admet un plus grand élément appelé **plus grand commun diviseur** de la famille $(a_k)_{1 \leqslant k \leqslant p}$ et est noté $a_1 \wedge a_2 \wedge \cdots \wedge a_p$.

Le PGCD est commutatif et associatif, de plus, $\bigcap_{i=1}^{p} \mathcal{D}(a_i) = \mathcal{D}(\wedge_{i=1}^{p} a_i)$

Si $a_1 = a_2 = \cdots = a_p = 0$, on pose $a_1 \wedge a_2 \wedge \cdots \wedge a_p = 0$.

Proposition 10 Coefficients de Bézout

Il existe une famille d'entiers relatifs $(u_k)_{1 \leqslant k \leqslant p}$ tels que

$$\sum_{k=1}^{p} u_k a_k = \bigwedge_{k=1}^{p} a_k$$

À savoir faire

- ☐ Calculer le PGCD de deux entiers et déterminer les coefficients de Bézout pour ces deux entiers
- ☐ Calculer le PGCD, le PPCM de p entiers.
- ☐ Résoudre une équation diophantienne de la forme $ax + by = c$
- ☐ Faire des calculs modulo n.
- ☐ Penser à calculer une quantité modulo n pour montrer qu'elle est multiple de n.
- ☐ Tout sur les fonctions dérivables/convexes

Ce qu'en dit le programme

C - Convexité

CONTENUS	CAPACITÉS & COMMENTAIRES
a) Généralités : Programme de la semaine 18	
b) Fonctions convexes dérivables, deux fois dérivables	
Caractérisation des fonctions convexes dérivables. Position du graphe d'une fonction convexe dérivable par rapport à ses tangentes. Caractérisation des fonctions convexes deux fois dérivables.	

Arithmétique dans l'ensemble des entiers relatifs

L'objectif de cette section est d'étudier les propriétés de la divisibilité des entiers et des congruences. L'approche préconisée reste élémentaire en ce qu'elle ne fait pas appel au langage des structures algébriques.

CONTENUS	CAPACITÉS & COMMENTAIRES
a) Divisibilité et division euclidienne	
Divisibilité dans $\mathbb{Z}$, 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.	Notation $a \wedge b$. Le PGCD de a et b est défini comme étant le plus grand élément (pour l'ordre naturel dans $\mathbb{N}$) de l'ensemble des diviseurs communs à a et b.
Algorithme d'Euclide.	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 $k \in \mathbb{N}^*$, PGCD de ka et kb.
Extension au cas de deux entiers relatifs. Relation de Bézout.	Détermination d'un couple de Bézout par l'algorithme d'Euclide étendu.
PPCM.	Notation $a \vee b$.

CONTENUS	CAPACITÉS & COMMENTAIRES
c) Entiers premiers entre eux	
Couple d'entiers premiers entre eux. Théorème de Bézout. Lemme de Gauss. Si a et b sont premiers entre eux et 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 Bézout. Entiers premiers entre eux dans leur ensemble, premiers entre eux deux à deux.	Forme irréductible d'un rationnel.
d) Nombres premiers La semaine prochaine	
e) Congruences	
Relation de congruence modulo un entier sur $\mathbb{Z}$. 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 $\mathbb{Z}/n\mathbb{Z}$ sont hors programme.