Programme de colle – MP 1

EDL (fin)

Extrait du programme officiel :

Contenus	Capacités & commentaires
b) Solutions d'une équation différentielle linéaire	
Exemples d'équations différentielles linéaires scalaires d'ordre 1 ou 2 non résolues : $a(x)y' + b(x)y = c(x), \quad a(x)y'' + b(x)y' + c(x)y = d(x)$.	Les étudiants doivent savoir exploiter la recherche de solutions développables en série entière.
f) Équations différentielles scalaires du second ordre	
Adaptation de la méthode de variation des constantes aux équations scalaires du second ordre.	
Wronskien de deux solutions d'une équation scalaire homogène d'ordre 2.	Définition et calcul. Cas d'une équation $x'' + q(t)x = 0$.

Révisions d'arithmétique sur $\mathbb{Z}$ (MPSI)

Voir programme page suivante.

Groupes monogènes, $\mathbb{Z}/n\mathbb{Z}$

Extrait du programme officiel :

Contenus	Capacités & commentaires
Groupes et sous-groupes	
Sous-groupe engendré par une partie.	
Groupes monogènes et cycliques	
Groupe $(\mathbb{Z}/n\mathbb{Z}, +)$. Générateurs de $\mathbb{Z}/n\mathbb{Z}$.	
Groupe monogène, groupe cyclique.	Groupe des racines n-ièmes de l'unité.
Tout groupe monogène infini est isomorphe à $(\mathbb{Z}, +)$. Tout groupe monogène fini de cardinal n est isomorphe à $(\mathbb{Z}/n\mathbb{Z}, +)$.	
Ordre d'un élément dans un groupe	
Élément d'ordre fini d'un groupe, ordre d'un tel élément.	Si x est d'ordre fini, l'ordre de x est le cardinal du sous-groupe de G engendré par x.
Si x est d'ordre fini d et si e désigne le neutre de G, alors, pour n dans $\mathbb{Z}$, on a $x^n = e \iff d \mid n$.	
L'ordre d'un élément d'un groupe fini divise le cardinal du groupe.	La démonstration n'est exigible que pour G commutatif.
L'anneau $\mathbb{Z}/n\mathbb{Z}$	
Anneau $\mathbb{Z}/n\mathbb{Z}$.	
Inversibles de $\mathbb{Z}/n\mathbb{Z}$.	L'anneau $\mathbb{Z}/n\mathbb{Z}$ est un corps si et seulement si n est premier.
Théorème chinois : si m et n sont deux entiers premiers entre eux, isomorphisme naturel de $\mathbb{Z}/mn\mathbb{Z}$ sur $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$.	Application aux systèmes de congruences.
Indicatrice d'Euler φ. Calcul de $\varphi(n)$ à l'aide de la décomposition de n en facteurs premiers.	⇆ I : calcul de $\varphi(n)$ à l'aide d'une méthode de crible.
Théorème d'Euler.	Lien avec le petit théorème de Fermat étudié en première année.
	⇆ I : codage RSA.

Questions de cours :

(i) Générateurs du groupe $(\mathbb{Z}/n\mathbb{Z}, +)$, inversibles de l'anneau $(\mathbb{Z}/n\mathbb{Z}, +, \times)$.

(ii) Si $(G, *)$ est un groupe fini de neutre e, tous ses éléments sont d'ordre fini, leur ordre divise $|G|$ (cas commutatif) et pour tout $a \in G$, $a^{|G|} = e$.

(iii) Si p est premier et $k \in \mathbb{N}^*$, calcul de $\varphi\left(p^k\right)$, d'où une expression de $\varphi(n)$ à l'aide de ses diviseurs premiers. Théorème d'Euler, d'où le petit théorème de Fermat.

(iv) **Théorème de Lagrange**

Soit $(G, *)$ un groupe fini, H un sous-groupe de G.

(a) Montrer que la relation définie par $x\mathcal{R}y \iff x^{-1} * y \in H$ est une relation d'équivalence sur G.

(b) Vérifier que les classes d'équivalence ont toutes le même cardinal.

(c) Démontrer le théorème de Lagrange : $|H|$ divise $|G|$.

(d) En déduire que l'ordre de tout élément de G divise l'ordre de G.

(v) **CCINP 31** :

(a) Déterminer une primitive de $x \longmapsto \cos^4 x$.

(b) Résoudre sur $\mathbb{R}$ l'équation différentielle : $y'' + y = \cos^3 x$ en utilisant la méthode de variation des constantes.

(vi) **CCINP 32** : Soit l'équation différentielle : $x(x-1)y'' + 3xy' + y = 0$.

(a) Trouver les solutions de cette équation différentielle développables en série entière sur un intervalle $]-r, r[$ de $\mathbb{R}$, avec $r > 0$.
Déterminer la somme des séries entières obtenues.

(b) Est-ce que toutes les solutions de $x(x-1)y'' + 3xy' + y = 0$ sur $]0, 1[$ sont les restrictions d'une fonction développable en série entière sur $]-1, 1[$?

(vii) **CCINP 66** : On note p un entier naturel supérieur ou égal à 2.

On considère dans $\mathbb{Z}$ la relation d'équivalence $\mathcal{R}$ définie par : $x\,\mathcal{R}\,y \overset{\text{déf.}}{\iff} \exists k \in \mathbb{Z}$ tel que $x - y = kp$.

On note $\mathbb{Z}/p\mathbb{Z}$ l'ensemble des classes d'équivalence pour cette relation $\mathcal{R}$.

(a) Quelle est la classe d'équivalence de 0 ? Quelle est celle de p ?

(b) Donner soigneusement la définition de l'addition usuelle et de la multiplication usuelle dans $\mathbb{Z}/p\mathbb{Z}$. On justifiera que ces définitions sont cohérentes.

(c) On admet que, muni de ces opérations, $\mathbb{Z}/p\mathbb{Z}$ est un anneau.
Démontrer que $\mathbb{Z}/p\mathbb{Z}$ est un corps si et seulement si p est premier.

(viii) **CCINP 42** : On considère les deux équations différentielles suivantes :

$$2xy' - 3y = 0 \qquad (H)$$

$$2xy' - 3y = \sqrt{x} \qquad (E)$$

(a) Résoudre l'équation (H) sur l'intervalle $]0, +\infty[$.

(b) Résoudre l'équation (E) sur l'intervalle $]0, +\infty[$.

(c) L'équation (E) admet-elle des solutions sur l'intervalle $[0, +\infty[$?

(ix) **CCINP 86** : Petit théorème de Fermat

(a) Soit $(a, b, p) \in \mathbb{Z}^3$. 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 $\forall k \in [\![1, p-1]\!]$, p divise $\binom{p}{k} k!$ puis en déduire que p divise $\binom{p}{k}$.

ii. Prouver que : $\forall n \in \mathbb{N}$, $n^p \equiv n \ [p]$.
Indication : procéder par récurrence.

iii. En déduire, pour tout entier naturel n, que : p ne divise pas $n \implies n^{p-1} \equiv 1 \ [p]$.

(x) **CCINP 94** :

(a) Énoncer le théorème de Bézout dans $\mathbb{Z}$.

(b) Soit a et b deux entiers naturels premiers entre eux. Soit $c \in \mathbb{N}$. Prouver que : $(a|c$ et $b|c) \iff ab|c$.

(c) On considère le système (S) : $\begin{cases} x & \equiv & 6 & \mod(17) \\ x & \equiv & 4 & \mod(15) \end{cases}$ dans lequel l'inconnue x appartient à $\mathbb{Z}$.

i. Déterminer une solution particulière x_0 de (S) dans $\mathbb{Z}$.

ii. *Déduire des questions précédentes* la résolution dans $\mathbb{Z}$ du système (S).

Programme de MPSI

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.	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. Notation $a \wedge b$.
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.
Extension au cas de deux entiers relatifs.	
Relation de Bézout.	L'algorithme d'Euclide fournit une relation de Bézout. $\leftrightarrows$ I : algorithme d'Euclide étendu. L'étude des idéaux de $\mathbb{Z}$ est hors programme.
PPCM.	Notation $a \vee b$. Lien avec le PGCD.
c) Entiers premiers entre eux	
Couple d'entiers premiers entre eux. Théorème de Bézout. Lemme de Gauß. 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	
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.	$\leftrightarrows$ I : crible d'Eratosthène.
Pour p premier, valuation p-adique.	Notation $v_p(n)$. Caractérisation de la divisibilité en termes de valuations p-adiques. Expressions du PGCD et du PPCM à l'aide des valuations p-adiques.
e) Congruences	
Relation de congruence modulo un entier sur $\mathbb{Z}$. Opérations sur les congruences : somme, produit. Petit théorème de Fermat.	Notation $a \equiv b\ [n]$. Les anneaux $\mathbb{Z}/n\mathbb{Z}$ sont hors programme.