PROGRAMME DE COLLE
ARITHMÉTIQUE DANS $\mathbb{Z}$

§ 1 DÉROULEMENT DE LA COLLE

La colle comporte deux phases.

(1) Rédaction d'une question de cours **(8 points • 20 minutes maximum)** : la colle débute par une des questions de cours listées dessous.

(2) Résolution d'exercices proposés par l'examinateur **(12 points)** : la colle se poursuit avec des exercices que vous ne connaissez pas à l'avance et que vous résoudrez au tableau, sans temps de préparation sur feuille.

§ 2 PROGRAMME

Chapitre 12 • Arithmétiques dans $\mathbb{Z}$ [PDF]

- Relation binaire sur un ensemble
- Divisibilité et division euclidienne
- PGCD et algorithme d'Euclide
- Entiers premiers entre eux
- Nombres premiers
- Congruences

§ 3 À VENIR

Chapitre 13 • Calcul matriciel et systèmes linéaires

§ 4 QUESTIONS DE COURS

Q1 — Définition d'une relation binaire réflexive (resp. symétrique, antisymétrique, transitive) [C12.3]. Définition d'une relation d'équivalence [C12.6]. Définition d'une classe d'équivalence [C12.8]. Les classes d'équivalence forment une partition [C12.11, énoncé formalisé et démonstration].

Q2 — Définition de la divisibilité dans $\mathbb{Z}$ [C12.14]. Division euclidienne dans $\mathbb{Z}$ [C12.19, énoncé formalisé et démonstration].

Q3 — Définition du PGCD de deux entiers naturels non nul [C12.25]. Lemme clé pour l'algorithme d'Euclide [C12.29, énoncé et démonstration]. Calcul du PGCD de deux entiers naturels non nuls a et b <u>donnés par l'interrogateur</u>, en exécutant l'algorithme d'Euclide.

Q4 — Algorithme d'Euclide [C12.30, énoncé et démonstration]. Détermination d'une relation de Bézout pour deux entiers naturels non nuls a et b <u>donnés par l'interrogateur</u>, en « remontant » l'algorithme d'Euclide.

Q5 — Relation de Bézout [C12.39, énoncé]. Lien fondamental entre PGCD et PPCM [C12.43, énoncé et démonstration dans le cas où $(a, b) \in \mathbb{N}^* \times \mathbb{N}^*$].

Q6 — Définition de deux entiers premiers entre eux [C12.46]. Théorème de Bézout [C12.48, énoncé et démonstration].

Q7 — Lemme de Gauß [C12.51, énoncé et démonstration]. Si des entiers a et b sont premiers entre eux, alors, pour tout $(m, n) \in \mathbb{N}^* \times \mathbb{N}^*$, a^m et b^n sont premiers entre eux [C12.50, démonstration].

Q8 — Définition d'un nombre premier [C12.53]. Crible d'Eratosthène [C12.57, énoncé et démonstration].

Q9 — L'ensemble des nombres premiers est infini [C12.61, énoncé et démonstration]. Pierre angulaire pour l'unicité dans le théorème fondamental de l'arithmétique [C12.63, énoncé et démonstration].

Q10 — Théorème fondamental de l'arithmétique [C12.64, énoncé intégral du polycopié et démonstration de l'existence].

Q11 — Définition de la valuation p-adique d'un entier [C12.68]. Valuation p-adique et décomposition en produit de facteurs premiers [C12.72, énoncé]. Valuation p-adique d'un produit [C12.74, énoncé et démonstration].

Q12 — Définition de la relation de congruence modulo n [C12.79]. Caractérisation de la relation de congruence par les restes [C12.81, énoncé et démonstration]. Critère de divisibilité par 9 [C12.85, énoncé et démonstration].

Q13 — Inversibilité et inverse modulo n [C12.86, énoncé et démonstration]. Résolution d'une équation de la forme $ax + b = c\ [n]$ d'inconnue $x \in \mathbb{Z}$ où a, b, c, n sont des entiers <u>donnés par l'interrogateur</u>.

Q14 — Si p est premier alors, pour tout $k \in [\![1, p-1]\!]$, $\binom{p}{k}$ est divisible par p [C12.88, démonstration]. Petit théorème de Fermat [C12.90, énoncé et démonstration].

§ 5 Après la colle

Vous repartirez avec les énoncés des exercices que vous a proposés l'examinateur. Vous collerez cet énoncé sur une feuille simple et vous en rédigerez une solution soignée que vous me remettrez sans faute à la fin du TD du lundi suivant votre colle.