Programme interrogations orales n°7

Du 13 au 17 Novembre

Arithmétique

Capacités attendues

Divisibilité dans $\mathbb{Z}$ Connaitre les définitions de diviseur et multiple d'un entier. Savoir caractériser des couples d'entiers associés. Maîtriser la notion de division euclidienne de d'un entier relatif par un entier naturel non nul
Maîtriser la définition de relation de congruence entre deux entiers et savoir les manipuler (somme, produit).

PGCD et PPCM Connaitre la définition du PGCD de deux entiers (plus grand diviseur commun, notation $a \wedge b$) et savoir le déterminer au moyen de l'algorithme d'Euclide. Maîtriser les propriétés du PGCD. Savoir utiliser la propriété "Les diviseurs communs de deux entiers sont les diviseurs de leur PGCD".

Maîtriser la notion de relation de Bézout associée à deux entiers et savoir déterminer un couple de coefficients de Bézout par l'algorithme d'Euclide étendu.

Connaitre la définition du PPCM de deux entiers (plus petit multiple commun, notation $a \vee b$. Savoir déterminer le PPCM de deux entiers à l'aide de leur PGCD. Maîtriser les propriétés du PGCD. Savoir utiliser la propriété "Les multiples communs de deux entiers sont les multiples de leur PPCM".

Entiers premiers entre eux Maîtriser la notion de couple d'entiers premiers entre eux et savoir les caractériser par le théorème de Bézout. Savoir définir la notion de forme irréductible d'un rationnel. Si a et b sont premiers avec n alors ab est premier avec n.

Savoir définir la notion d'entier inversible modulo n, savoir caractériser les entiers inversibles modulo n et savoir les utiliser pour résoudre une congruence modulo n.

Maîtriser le lemme de Gauss. Si a et b sont premiers entre eux et divisent n alors ab divise n.

Savoir définir le PGCD d'un nombre fini d'entiers, la notion de relation de Bézout associée. Maîtriser la notion d'entiers premiers entre eux dans leur ensemble et préciser le lien avec la notion d'entiers premiers entre eux deux à deux.

Nombres premiers Maîtriser la définition de nombre premier et savoir que l'ensemble des nombres premiers est infini. Savoir utiliser le critère "Tout entier $n \geqslant 2$ non premier admet un diviseur premier d tel que $2 \leqslant d \leqslant \sqrt{n}$" pour déterminer si un entier est premier ou non. Savoir mettre en oeuvre le crible d'Eratosthène.

Maîtriser le petit théorème de Fermat.

Maîtriser le théorème d'existence et unicité de la décomposition d'un entier supérieur ou égal à 2 en produit de facteurs premiers. Savoir définir la notion de valuation p-adique d'un entier pour p premier. Savoir exprimer la valuation p-adique d'un produit. Savoir caractériser la divisibilité entre deux entiers en termes de valuations p-adiques. Savoir exprimer le PGCD et le PPCM de deux entiers à l'aide des valuations p-adiques de ces entiers.

Questions de cours

- Énoncer le théorème de division euclidienne et les deux versions du petit théorème de Fermat.
- Déterminer le PGCD de deux entiers (choisis par l'examinateur) et en déterminer deux coefficients de Bézout grâce à l'algorithme d'Euclide étendu.
- Énoncer le théorème de Bézout puis démontrer que si $a \wedge n = 1$ et $b \wedge n = 1$ alors $ab \wedge n = 1$.
- Énoncer le lemme de Gauss puis démontrer que si $a|n$ et $b|n$ avec $a \wedge b = 1$ alors $ab|n$.
- Si $a \wedge b = 1$, montrer que $a \vee b = ab$ puis démontrer la formule donnant $(a \wedge b)(a \vee b)$ dans le cas général.
- Résoudre l'équation diophantienne $6u + 15v = -3$.
- Donner la définition d'entier inversible modulo n et démontrer que a est inversible modulo n si et seulement si $a \wedge n = 1$.
- Démontrer le petit théorème de Fermat (facultatif).

Exercices

Les exercices pourront porter sur l'intégralité du chapitre Arithmétique et en particulier sur la bonne maîtrise des théorèmes de Bézout et Gauss.