Les questions de cours portent sur les éléments entre accolades et en gras. On attend une maîtrise de l'*ensemble* des notions du programme de colle.

Chapitre 13 : Arithmétique dans $\mathbb{Z}$.

Anneau euclidien $\mathbb{Z}$.

Relation de divisibilité. Elle induit une relation d'ordre sur $\mathbb{N}$. Eléments associés. Ensemble des diviseurs d'un entier relatif. L'ensemble des multiples de a, $a\mathbb{Z}$ est un sous-groupe de $\mathbb{Z}$. a divise b ssi $b\mathbb{Z} \subset a\mathbb{Z}$. [**Théorème de la division euclidienne :** $\forall (a,b) \in \mathbb{Z} \times \mathbb{Z}^*, \exists ! (q,r) \in \mathbb{Z} \times [\![0, |b|-1]\!], a = bq + r$]. Expressions du quotient et du reste à l'aide de la partie entière. [**Caractérisation des sous-groupes de $\mathbb{Z}$: $G \subset \mathbb{Z}$ est un sous-groupe de $(\mathbb{Z}, +)$ si et seulement s'il existe $n \in \mathbb{N}$ tel que $G = n\mathbb{Z}$.**] Exemple des sous-groupes $a\mathbb{Z} + b\mathbb{Z}$ et $a\mathbb{Z} \cap b\mathbb{Z}$.

Pgcd, ppcm de deux entiers relatifs.

Définition du pgcd : $a \wedge b$ est l'unique générateur positif du sous-groupe $a\mathbb{Z} + b\mathbb{Z}$. [**Dans le cas $(a,b) \neq (0,0)$, $a \wedge b$ est le plus grand diviseur positif commun à a et b**]. Réduction : $\forall (a,b) \in \mathbb{Z}^2, \exists (a', b') \in \mathbb{Z}^2, a = (a \wedge b)a', b = (a \wedge b)b', a' \wedge b' = 1$. Propriétés : $a \wedge b = b \wedge a = |a| \wedge |b| = a \wedge (b + na)$. Si b non nul et r le reste dans la division de a par b, $a \wedge b = b \wedge r$. L'ensemble des diviseurs communs à a et b est l'ensemble des diviseurs de $a \wedge b$. Algorithme d'Euclide. Homogénéité positive du pgcd. Relation de Bezout, théorème de Bezout, algorithme d'Euclide étendu pour déterminer une relation de Bezout. Définiton du ppcm : $a \vee b$ est l'unique générateur positif du sous-groupe $a\mathbb{Z} \cap b\mathbb{Z}$. Dans le cas $a \neq 0, b \neq 0$, c'est le plus petit multiple positif commun à a et b. Homogénétié positive du ppcm. Extensions à une famille finie d'entiers relatifs.

Entiers relatifs premiers entre eux.

Notions d'entiers premiers entre eux. Lemme de Gauss : Soit $(a,b,c) \in \mathbb{Z}^3$ tel que a divise bc et a premier avec b, alors a divise c. [**Relation entre pgcd et ppcm :** $\forall (a,b) \in \mathbb{Z}^2, (a \wedge b)(a \vee b) = |ab|$.] Résolution d'équations diophantiennes. Ecriture sous forme irréductible d'un rationnel. Soit $(a,b,n) \in \mathbb{Z}^3$ tel que $a \wedge b = 1$, a divise n et b divise n, alors ab divise n. Soit $(a,b,n) \in \mathbb{Z}^3$ tel que $a \wedge n = 1$ et $b \wedge n = 1$, alors $ab \wedge n = 1$. Famille d'entiers premiers entre eux deux à deux, premiers entre eux dans leur ensemble. La coprimalité deux à deux entraîne la coprimalité dans l'ensemble.

Anneau factoriel

Notion d'entier premier. Notation $\mathcal{P}$ des entiers naturels premiers. [**Soit $n \in \mathbb{Z}$ tel que $|n| \geq 2$, alors n admet un diviseur premier**]. L'ensemble $\mathcal{P}$ est infini. Soit $n \in \mathbb{Z}$ tel que $|n| \geq 2$, alors n est premier ssi $\forall k \in [\![1, |n|-1]\!], k \wedge n = 1$. Deux entiers naturels premiers distincts sont premiers entre eux. Lemme d'Euclide : soit $(a,b) \in \mathbb{Z}^2$ et $p \in \mathcal{P}$ tel que p divise ab, alors p divise a ou p divise b. Tout entier non premier possède un diviseur premier inférieur ou égal à $\sqrt{|n|}$. Notion de famille à support fini. [**Théorème fondamental de l'arithmétique :** $\forall n \in \mathbb{Z}^*, \exists ! (u, (\alpha_p)_{p \in \mathcal{P}}) \in \{-1,1\} \times \mathbb{N}^{(\mathcal{P})}, n = u \prod_{p \in \mathcal{P}} p^{\alpha_p}$]. Valuation p-adique d'un entier non nul. Valuation p-adique du produit, du pgcd, du ppcm de deux entiers relatifs non nuls. Indicatrice d'Euler d'un entier premier, d'une puissance d'un entier premier.

Arithmétique modulaire

n désigne un entier naturel non nul. Relation de congruence modulo n. Compatibilité avec l'addition et le produit. Inversibilité modulo n. Pour tout a dans $\mathbb{Z}$, a est inversible modulo n si et seulement si a est premier avec n. Résolution d'équation modulaires. [**Petit théorème de Fermat : soit $a \in \mathbb{Z}, p \in \mathcal{P}$ tel que $a \wedge p = 1$. Alors $a^{p-1} \equiv 1 [p]$.**]

★ ★ ★ ★ ★