Chaque colle comporte une question de cours ainsi qu'un ou plusieurs exercices. Les questions de cours portent sur les éléments précédés d'un astérisque (★) sur le chapitre 14 : Arithmétique dans $\mathbb{Z}$. Les exercices portent sur le chapitre 14 : Arithmétique dans $\mathbb{Z}$.

Chapitre 14 : Arithmétique dans $\mathbb{Z}$.

Anneau euclidien

Relation de divisibilité dans $\mathbb{Z}$. (★) La relation de divisibilité induit une relation d'ordre sur $\mathbb{N}$. Eléments associés. Ensemble $D(a)$ des diviseurs de a, $D^+(a)$ des diviseurs positifs de a. Multiples de a. (★) L'ensemble des multiples de a est un sous-groupe de $\mathbb{Z}$. Générateurs de $a\mathbb{Z}$. a divise b si et seulement si $b\mathbb{Z} \subset a\mathbb{Z}$. (★)Théorème de la division euclidienne. Expression du quotient et du reste à l'aide des parties entières. b divise a ssi $a\%b$ est nul. (★) Les sous-groupes de $\mathbb{Z}$ sont monogènes. $a\mathbb{Z} + b\mathbb{Z}$ est sous-groupe de $\mathbb{Z}$.

Pgcd, ppcm

Le pgcd est défini par $0 \wedge 0 = 0$, sinon $a \wedge b = \max(D^+(a) \cap D^+(b))$ le plus grand diviseur positif commun à a et b. Réduction, si $d = a \wedge b$, il existe des entiers a', b' tels que $a = da'$, $b = db'$ et $a' \wedge b' = 1$. (★) $D(a) \cap D(b + na) = D(a) \cap D(b)$. Algorithme d'Euclide. (★) $D(a) \cap D(b) = D(a \wedge b)$. Homogénéité du pgcd, a divise b si et seulement si $a \wedge b = |a|$. (★) $a\mathbb{Z} + b\mathbb{Z} = (a \wedge b)\mathbb{Z}$. Relation et théorème de Bezout. Algorithme d'Euclide étendu.

Le ppcm est défini par $a \vee 0 = 0$. Si a et b tous deux non nuls, $a \vee b$ est leur grand multiple positif commun. (★) $a\mathbb{Z} \cap b\mathbb{Z} = (a \vee b)\mathbb{Z}$. Homogénétié du ppcm.

Pgcd, ppcm d'une famille fini d'entiers relatifs. Associativité, commutativité. Homogénéité.

Entiers relatifs premiers entre eux

Théorème de Bezout. (★) Lemme de Gauss. (★) Formule des compléments. Résolution d'équations diophantiennes $ax + by = c$. Forme irréductible d'un rationnel. (★) $a \wedge b = 1, a \mid n$ et $b \mid n \Rightarrow (ab) \mid n$. (★) $a \wedge n = 1$ et $b \wedge n = 1 \Rightarrow (ab) \wedge n = 1$. Entiers premiers entre eux dans leur ensemble, deux à deux. La coprimalité deux à deux entraîne la coprimalité dans l'ensemble.

Anneau factoriel

p est dit premier lorsque $|D^+(p)| = 2$. (★) Soit $n \in \mathbb{Z}, |n| \geq 2$, alors n admet un diviseur premier. (★) L'ensemble $\mathcal{P}$ des entiers premiers positifs est infini. $n \in \mathbb{Z}, |n| \geq 2$ est premier ssi $\forall k \in [\![1, |n| - 1]\!], k \wedge n = 1$. Lemme d'Euclide. Si $|n| \geq 2$ est non premier, il admet un diviseur premier p tel que $p \leq \sqrt{n}$. (★) Théorème fondamental de l'arithmétique, existence. (★) Théorème fondamental de l'arithmétique, unicité. Valuation p-adique. $|n| = \prod_{p \in \mathcal{P}} p^{v_p(n)}$. $n \in \mathbb{Z}^*$, $v_p(n) = \max\{k \in \mathbb{N} | p^k \mid n\}$. (★) $v_p(ab) = v_p(a) + v_p(b), v_p(a \wedge b) = \min(v_p(a), v_p(b)), v_p(a \vee b) = \max(v_p(a), v_p(b))$. Indicatrice d'Euler, $\varphi(p^k)$.

Congruences

Relation de congruence modulo n. C'est une relation d'équivalence. $n \mid a \iff a \equiv 0[n]$. (★) Compatibilité avec l'addition et la multiplication. $a \equiv b[n]$ ssi a et b ont même reste dans leur division euclidienne par n. Entier inversible modulo n. (★) a est inversible modulo n ssi $a \wedge n = 1$. Résolution de congruences. (★) Petit théorème de Fermat.

★ ★ ★ ★ ★