Fiche Synthèse - Arithmétique

1 Multiples et diviseurs

a **multiple** de b $\iff$ b **diviseur** de a $\iff$ $\exists q \in \mathbb{Z},\ qb = a$ $\iff$ $a \in b\mathbb{Z}$ $\iff$ $b \in \mathsf{div}(a)$.

$d \mid a$ et $d \mid b, \Rightarrow\ d \mid (au + bv)$ $\quad$ $a \mid b$ et $c \mid d, \Rightarrow ac \mid bd.$ $\quad$ $a \mid b, \Rightarrow a^k \mid b^k$

2 Congruences

$a \equiv b[n]$ $\iff$ $a - b \in n\mathbb{Z}.$

$(a = b[n]$ et $c = d[n]) \Rightarrow (a + c = b + d[n]$ et $ac = bd[n])$ $\quad$ $a = b[n] \Rightarrow a^k = b^k[n]$ $\quad$ $a \equiv b[n] \Leftrightarrow ca \equiv cb[cn].$

Diviseur	**Critère**
n est un multiple de 2	a_0 est un multiple de 2
n est un multiple de 3	la somme des chiffres $\sum_{k=0}^{r} a_k$ est un multiple de 3.
n est un multiple de 4	$10\ a_1 + a_0$ est un multiple de 4 .
n est un multiple de 5	a_0 est un multiple de 5 .
n est un multiple de 9	la somme des chiffres $\sum_{k=0}^{r} a_k$ est un multiple de 9 .
n est un multiple de 11	la somme alternée des chiffres $\sum_{k=0}^{r} a_k(-1)^k$ est un multiple de 11 .

PGCD, PPCM

PGCD = Plus Grand Commun diviseur $\iff$ unique d tel que $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$ $\Rightarrow$ $\exists u, v \in \mathbb{Z},\quad au + bv = d$

PPCM = Plus Petit Multiple Commun $\iff$ unique m tel que $a\mathbb{Z} \cap b\mathbb{Z} = m\mathbb{Z}$ **Coefficients de Bézout**

Lien PGCD-PPCM $(a \wedge b) \cdot (a \vee b) = |ab|$

Pour exercices $d = a \wedge b \iff \begin{cases} \exists a' \in \mathbb{Z}, a = da' \\ \exists b' \in \mathbb{Z}, b = db' \\ a' \wedge b' = 1 \end{cases}$ et $a \vee b = (a \wedge b) \cdot a'b'$

Division euclidienne $\exists!(q, r) \in \mathbb{Z} \times \mathbb{N},\quad a = qb + r \quad 0 \leq r \leq b - 1$

La **DE** conserve le PGCD $\rightarrow$ $a \wedge b = b \wedge r$!

Algorithme d'Euclide $a \wedge b$ est le **dernier reste non nul** de la suite des restes successifs

Algorithme d'Euclide étendu $\rightarrow$ Retrouver les u et v de Bézout

3 Nombres premiers entre eux $\iff$ $a \wedge b = 1$

$\Updownarrow$ **Théorème de Bézout**

$\exists u, v \in \mathbb{Z}, \quad ua + vb = 1$

Lemme de Gauss $a \mid bc$ et $a \wedge b = 1 \quad \Rightarrow \quad a \mid c$

4 Nombres premiers $\iff$ p a exactement 2 diviseurs

Fermat $n^p = n[p]$ et $n \notin p\mathbb{Z} \quad \Rightarrow \quad n^{p-1} = 1[p].$

Thm Fondamental de l'arithmétique $n = \prod_{k=1}^{m} p_k^{\alpha_k}$ où $\alpha_k = v_{p_k}(n) =$ **valuation p_k-adique** de n.