Chap 10 : Arithmétique sur $\mathbb{Z}$

I. Divisibilité

p divise n ($p \mid n$) s'il existe $k \in \mathbb{Z}$ tel que $n = kp$

La relation de divisibilité est une relation d'ordre sur $\mathbb{Z}$

$b \mid a$ *ssi* le reste de la div. euclid. de a par b est nul

$b \mid a, b \mid c \Rightarrow b \mid (ja + kc)$

$(a,b) \in \mathbb{Z}^2$, $(q,r) \in \mathbb{N}^2$ tq $a = bq + r$ et $r \in [\![0, b-1]\!]$ $\quad \{div\,communs\,à\ a\,et\,b\} = \{div\,communs\,à\ b\,et\,r\}$

Preuves : combinaison linéaire

$\forall (a,b) \in (\mathbb{N}^*)^2, \exists! d \in \mathbb{N}^*$ tel que $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$ $\quad d = \text{pgcd}(a,b) = a \wedge b$

Théorème de Bezout : $\forall (a,b) \in (\mathbb{N}^*)^2$, $\exists (u,v) \in \mathbb{Z}^2$ tels que $\text{pgcd}(a,b) = au + bv$

$D \mid a, D \mid b, \exists (u,v) \in \mathbb{Z}^2, D = au + bv \Leftrightarrow D = \text{pgcd}(a,b)$

a, b sont premiers entre eux si $a \wedge b = 1$ (On a dans ce cas la réciproque du thm de Bezout)

Lemme de Gauss : $\begin{cases} a \wedge b = 1 \\ a \mid bc \end{cases} \Rightarrow a \mid c$

Preuve : $a\mathbb{Z} + b\mathbb{Z}$ idéal de $\mathbb{Z} \Rightarrow d\mathbb{Z}$ $\quad a \in d\mathbb{Z}\ b \in d\mathbb{Z}\ d = au + bv$ $\quad D \mid a, D \mid b \Rightarrow D \mid d$

$\begin{cases} a \mid c \\ b \mid c \\ a \wedge b = 1 \end{cases} \Rightarrow ab \mid c$ (Idem pour les produits plus grands)

$\forall (a,b) \in (\mathbb{N}^*)^2, \exists! m \in \mathbb{N}^*$, $a\mathbb{Z} \cap b\mathbb{Z} = m\mathbb{Z} = \{\text{multiples communs à } a \text{ et } b\}$ $\quad m = ppcm(a,b) = a \vee b$

$a \times b = (a \wedge b)(a \vee b)$

Preuve : $a = da_0, b = db_0$ $\quad m_0 = da_0 b_0$ $\quad a_0 \wedge b_0 = 1$

$m = a \vee b$ $\quad m = ka, b \mid m \Leftrightarrow db_0 \mid kda_0 \Leftrightarrow b_0 \mid k \Rightarrow k = b_0 j$

$m = (ab_0) j = m_0 j$ $\quad$ Comme m_0 multiple de $(a_0 d) = a$ et de $(b_0 d) = b, m_0 \mid m \Rightarrow m_0 = ppcm(a,b)$

$(a \wedge b) \wedge c = a \wedge (b \wedge c) = a \wedge b \wedge c$ est l'unique $d \in \mathbb{N}^*$ tel que $a\mathbb{Z} + b\mathbb{Z} + c\mathbb{Z} = d\mathbb{Z}$ (idem ppcm)

/!\ (a,b,c) premiers entre eux dans leur ensemble ($\Leftrightarrow a \wedge b \wedge c = 1$)

$\neq (a,b,c)$ premiers entre eux deux à deux ($\Leftrightarrow a \wedge b = a \wedge c = b \wedge c = 1$)

II. Nombres premiers

$p \in \mathbb{Z}^* \setminus \{-1,+1\}$ est premier si les seuls diviseurs de p sont :

Les inversibles $\{+1;-1\}$

Les nombres associés à p $\{+p,-p\}$

$p \in \mathbb{N}^*$ premier $\Leftrightarrow \forall j \in \mathbb{N}^*, j \wedge p = 1$ ou $p \mid j$

Tout nombre $n \geq 2$ admet un diviseur premier

Preuve : {diviseurs >1 de n} partie non vide de $\mathbb{N}$ ➔ minorée. Le minorant est premier

Il existe une infinité de nombres premiers

Preuve : par l'absurde : $m = \prod_{j=1}^{N} p_j + 1 \quad p_k \mid m \quad p_k \mid \prod_{j=1}^{N} p_j \Rightarrow p_k \mid m - \prod_{j=1}^{N} p_j \Leftrightarrow p_k \mid 1$

Tout entier s'écrit de manière unique sous la forme d'un produit de nombres premiers (à l'ordre près des facteurs)

Preuve : récurrence forte sur n>1. Si n pas premier, admet 1 diviseur premier ➔ puissance +1

$$n = \prod_{j=1}^{R} p_j^{\alpha_j} \qquad m = \prod_{k=1}^{R} p_j^{\beta_j} \qquad \Rightarrow a \wedge b = \prod_{k=1}^{R} p_k^{\min(\alpha_j,\beta_j)} \qquad a \wedge b = \prod_{k=1}^{R} p_k^{\max(\alpha_j,\beta_j)}$$

III. Congruences et $\mathbb{Z}/n\mathbb{Z}$

$n \in \mathbb{N}, n > 1$

j est congru à k modulo n ($j \equiv k[n]$) si $\exists p \in \mathbb{Z} / k = l + pn$

La congruence est une relation d'équivalence, compatible avec $+$ et $\times$

$\bar{k}$ est la classe d'équivalence de k. $\mathbb{Z}/n\mathbb{Z} = \{\bar{k}, k \in [\![0, n-1]\!]\}$

$\text{card}\, \mathbb{Z}/n\mathbb{Z} = n$

On définit des lci $+$ et $\times$: $\mathbb{Z}/n\mathbb{Z}$ est un anneau commutatif

$x \in \mathbb{Z}/n\mathbb{Z} \qquad x \in \left(\mathbb{Z}/n\mathbb{Z}\right)^* \; ssi \; k \wedge n = 1$

n premier $\Leftrightarrow \mathbb{Z}/n\mathbb{Z}$ est un corps

Preuve : Bezout

Tout anneau intègre de cardinal fini est un corps

Lemme chinois : Si $n \wedge p = 1$, alors $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ est isomorphe à $\mathbb{Z}/np\mathbb{Z}$