Arithmétique

Nombre de pages: 5

a | b Relations

Relation de divisibilité

$(a,b) \in \mathbb{Z}^2$ $\quad a|b \iff \exists k \in \mathbb{Z},\ b = ka$

- $[a|b \wedge b|a] \iff |a| = |b|$, $\quad a|1 \iff |a| = 1$
- réflexive, transitive, antisymétrique sur $\mathbb{N}$: relation d'ordre sur $\mathbb{N}$
- $[c \neq 0 \wedge ac|bc] \Rightarrow a|b$
- $[a|b \wedge a|c] \Rightarrow \forall (u,v) \in \mathbb{Z}^2,\ a|(ub+vc)$

Relation de congruence

$(a,b) \in \mathbb{Z}^2$, $m \in \mathbb{N}^*$ $\quad a \equiv b\ [m] \iff m|(b-a)$

- réflexive, transitive, symétrique : relation d'équivalence (m classes)
- $a \equiv b\ [m] \Rightarrow \forall n \in \mathbb{N}^*,\ an \equiv bn\ [mn]$
- $\begin{cases} a_1 \equiv b_1\ [m] \\ a_2 \equiv b_2\ [m] \end{cases} \Rightarrow \begin{cases} k_1 a_1 + k_2 a_2 \equiv k_2 b_1 + k_2 b_2\ [m] \\ a_1 a_2 \equiv b_1 b_2\ [m] \\ a_1^k \equiv a_2^k\ [m] \end{cases}$

- Montrer que deux quantités sont égales : se divise l'une l'autre puis étude de signe
- a infiniment divisible par b ($\forall n,\ b^n | a$) $\Rightarrow a = 0$

Racines rationnelles

Division euclidienne (DE)

$a \in \mathbb{Z}$, $b \in \mathbb{N}^*$ $\quad \exists ! (q,r) \in \mathbb{Z} \times [\![0;b[\![$, $a = qb + r$

↳ Existence

- Si $a \geq 0$, on pose $A := \{k \in \mathbb{N},\ kb \leq a\}$
A non vide ($0 \in A$) et majoré par a donc admet un maximum q. Donc $q+1 \notin A$.

$qb \leq a < (q+1)b$ donc $0 \leq \underbrace{a - qb}_{:=r} < b$

On a bien $a = qb + r$.

- Si $a < 0$, il existe $(q,r) \in \mathbb{Z} \times [\![0;b[\![$, $-a = qb + r$
Si $r = 0$, $a = (-q)b + 0$ ponctionne.
Sinon, $a = (-q-1)b + (b-r)$ ponctionne.

Unicité On se munit de (q_1, r_1) et (q_2, r_2) satisfaisant toutes les hypothèses.

$a = q_1 b + r_1 = q_2 b + r_2$ donc $b\,|q_1 - q_2| = |r_2 - r_1| < b$

Donc $q_1 = q_2$, donc $r_1 = r_2$.

▶ Se munir d'une DE pertinente

Plus grand diviseur commun (PGCD)

$(a,b) \in \mathbb{Z}^2$. $\exists ! \, p \in \mathbb{N}$,
- $p|a$ et $p|b$
- $\forall q \in \mathbb{Z}$, $[q|a \wedge q|b] \Rightarrow q|p$

↳ Existence $a \wedge b = b \wedge a = |a| \wedge |b|$: on suppose $a \geq b \geq 0$

Récurrence forte sur $a+b$. H_0 vraie ($p=0$ vérifie toute les hypothèses). Soit $n \in \mathbb{N}$. Si $a+b = n+1$, $a \geq b$ et H_i vraie pour tout $i \leq n$:
- Soit $b=0$: $p=a$ ponctionne
- Soit $b>0$: on se munit de $p = (a-b) \wedge b$ qui existe par hypothèse. p ponctionne

Unicité p_1 et p_2 vérifiant les hypothèses se divisent l'un l'autre donc sont égaux.

▶ Raisonner par récurrence sur $a+b$

▶ $a \wedge 0 = |a|$, $a \wedge 1 = 1$

▶ $a \wedge b = 0 \iff [a=0 \wedge b=0]$

▶ $(ka) \wedge (kb) = |k| (a \wedge b)$

▶ $a \wedge b = a \wedge (b+ka)$ $\forall k \in \mathbb{Z}$ (perturbation)

Algorithme d'Euclide

Utiliser $a \wedge b = b \wedge (a \bmod b)$ .. successivement. Le premier terme est strictement décroissant à partir de la deuxième itération, d'où la terminaison.

Exemple : $147 \wedge 105 = 105 \wedge 42 = 42 \wedge 21 = 21 \wedge 0 = 21$

Entiers premiers entre eux $a \wedge b = 1$

▶ $\begin{cases} a \wedge b = 1 \\ a \wedge c = 1 \end{cases} \Rightarrow \begin{cases} a \wedge (bc) = 1 \\ \forall (n,m) \in \mathbb{N}^2, \ a^n \wedge b^m = 1 \end{cases}$

▶ $\begin{cases} [a|c \ \wedge \ b|c] \\ a \wedge b = 1 \end{cases} \Rightarrow ab|c$

▶ Se munir de a', b' tels que $a = (a \wedge b)a'$ et $b = (a \wedge b)b'$. On a donc :
$a \wedge b = (a'(a \wedge b)) \wedge (b'(a \wedge b)) = (a \wedge b)(a' \wedge b')$
Donc si $(a,b) \neq (0,0)$, $a \wedge b \neq 0$ et donc $a' \wedge b' = 1$

Lemme de Gauss $[a|bc \ \wedge \ a \wedge b = 1] \Rightarrow a|c$

↳ $a|bc$ donc $\exists w \in \mathbb{Z}$, $bc = wa$
$a \wedge b = 1$ donc $\exists (u,v) \in \mathbb{Z}^2$, $1 = ua + vb$ (Bézout)
$c = c(ua + vb) = auc + v'wa = a(\underbrace{uc + vw}_{\in \mathbb{Z}})$

Forme irréductible

$r \in \mathbb{Q}$. $\exists ! (p,q) \in \mathbb{Z} \times \mathbb{N}^*$, $[p \wedge q = 1 \ \wedge \ r = \frac{p}{q}]$

↳ Existence Soit $(p,q) \in \mathbb{Z} \times \mathbb{N}^*$ tel que $r = \frac{p}{q}$,
$s := p \wedge q$, $(a,b) \in \mathbb{Z} \times \mathbb{N}^*$ tel que
$p = sa$, $q = sb$. Alors $r = \frac{p}{q} = \frac{sa}{sb} = \frac{a}{b}$.

Unicité Soient (a_1, b_1) et (a_2, b_2) satisfaisant les hypothèses. Alors $a_1 b_2 = a_2 b_1$
Donc $a_1 | a_2 b_1$ donc (Gauss) $a_1 | a_2$. De même $a_2 | a_1$, et de même signe, donc $a_1 = a_2$ et $b_1 = b_2$

▶ Racines rationnelles d'un polynôme :
$0 = \sum_{k=0}^{n} a_k \left(\frac{p}{q}\right)^k \Rightarrow q | a_n$ et $p | a_0$

Relation de Bézout

$(a,b) \in \mathbb{Z}^2 \quad \exists (u,v) \in \mathbb{Z}^2, \quad ua+vb = a \wedge b$

↳ On se ramène à $(a,b) \in \mathbb{N}^2$. Récurrence forte sur $a+b$. H_0 vraie : $(0,0)$ ponctionne. Soit $n \in \mathbb{N}$. Si $a+b = n+1$, $a \geq b$, H_i vraie pour tout $i \leq n$:
- Si $b=0$: $(1,0)$ ponctionne $(a \wedge b = a)$
- Sinon $a \wedge b = (a-b) \wedge b$ donc un couple ponctionne par hypothèse

▶ Peut s'obtenir par remontée de l'algorithme d'Euclide. L'ensemble des solutions s'obtient par théorème de superposition et Gauss.

▶ Se munir de (u,v) tel que $ua+vb = a \wedge b$

Théorème de Bézout

$a \wedge b = 1 \iff \exists (u,v) \in \mathbb{Z}^2, \ ua+bv = 1$

↳ $\Rightarrow$ donné par relation de Bézout

$\Leftarrow$ $a \wedge b$ divise a et b donc $ua+bv = 1$
donc $a \wedge b = 1$

Plus petit commun multiple (PPCM)

$(a,b) \in \mathbb{Z}^2$ $\quad \exists ! \, p \in \mathbb{N}$
- $a|p$ et $b|p$
- $\forall q \in \mathbb{Z}$, $[a|q \wedge b|q] \Rightarrow p|q$

↳ Existence Si a ou b est nul, $p=0$. Sinon, on se ramène à $(a,b) \in \mathbb{N}^{*2}$.
On pose $X = \{n \in \mathbb{N}^*, \ a|n \text{ et } b|n\}$.
X est non vide ($ab \neq 0 \in X$) donc admet un minimum p qui convient. En effet, soit $q \in \mathbb{Z}$ tel que $a|q$ et $b|q$, (s,r) le résultat de la DE de q par p.

$a|q$, $a|p$ donc $a|q-sp=r$, de même $b|r$
Si $r \in \mathbb{N}^*$, $r \in X$ mais $r < p$ mq. donc $r=0$

Unicité p_1 et p_2 vérifiant les hypothèses se divisent l'un l'autre donc sont égaux

- $a \vee 0 = 0$, $\quad a \vee 1 = |a|$
- $a \vee b = 0 \iff [a=0 \ \vee \ b=0]$
- $(ka) \vee (kb) = |k| (a \vee b)$
- $(a \wedge b)(a \vee b) = |ab|$

↳ $(a,b) \in \mathbb{Z}^*$ (cas a ou b nul évident)
$(a',b') \in \mathbb{Z}^*$ $\quad a = (a \wedge b) a'$, $\quad b = (a \wedge b) b'$ i.e $a' \wedge b' = 1$
On a $a' \vee b' = |a'b'|$: $a' \mid |ab|$, $b' \mid |ab|$, et si $q \in \mathbb{Z}$ multiple de a' et b', $a'b' | q$ donc $|a'b'| | q$.

$$(a \wedge b)(a \vee b) = (a \wedge b)^2 (a' \wedge b')(a' \vee b') = (a \wedge b)^2 |a'b'|$$
$$= |a'(a \wedge b) \cdot b'(a \wedge b)| = |ab|$$

a | b

Généralisation

$n \in \mathbb{N}$, $I = [\![1, n]\!]$, $a \in \mathbb{Z}^I$

PGCD $\exists ! \, p \in \mathbb{N}$,
- $\forall i \in I$, $p \mid a_i$
- $\forall q \in \mathbb{Z}$, $[\forall i \in I, q \mid a_i] \Rightarrow q \mid p$

Deux à deux premiers entre eux

$(i,j) \in I^2 \quad i \neq j \Rightarrow a_i \wedge a_j = 1$

Premiers entre eux dans leur ensemble

$$\bigwedge_{i \in I} a_i = 1$$

Théorème de Bézout étendu

$$\bigwedge_{i \in I} a_i = 1 \iff \exists u \in \mathbb{Z}^I, \sum_{i \in I} u_i a_i = 1$$

$\Leftarrow$ $\bigwedge_{i \in I} a_i$ divise $\sum_{i \in I} u_i a_i$ donc divise 1 donc est égal 1.

$\Rightarrow$ Récurrence avec théorème de Bézout

Nombre premier entier $p \geq 2$ n'admettant que 1 et p comme diviseurs positifs.

▶ $p \in \mathbb{P}$, $n \in \mathbb{Z}$. $p \wedge n | p$ donc
- soit $p \wedge n = 1$
- soit $p \wedge n = p$ donc $p | n$

▶ $(a,b) \in \mathbb{Z}^2$. $p | ab \Rightarrow [p|a \text{ ou } p|b]$

↳ Soit $p|a$ soit $p \wedge a = 1$ donc (Gauss) $p|b$

▶ Tout $n \geq 2$ admet un diviseur premier.

↳ $X := \{k \in \mathbb{N}, k|n\}$ est non vide ($n \in X$) donc admet un minimum p. Soit k un diviseur de p. k est non nul, car sinon $p = 0$ (ms). Si $k \geq 2$, $k \in X$ car $k|p$ donc $k|n$. Donc $k \geq p$. Donc $k = p$. Donc p est premier.

▶ Tout $n \geq 2$ non premier s'écrit $n = ab$ avec $a \geq 2$ et $b \geq 2$. (utile pour l'absurde)

Infinité de nombres premiers

Supposons qu'il en existe un nombre fini n. Soit $N := \prod_{i=1}^{n} p_i + 1 \geq 2$. N admet un diviseur premier. Donc il existe $i_0 \in [\![1;n]\!]$ tel que $p_{i_0} | N$. Or $p_{i_0} | \prod_{i=1}^{n} p_i$. Donc $p_{i_0} | 1$. Donc $p_{i_0} = 1$, d'où la contradiction.

a | b

Petit théorème de Fermat

$p \in \mathcal{P}$, $m \in \mathbb{Z}$ $\qquad p \nmid m \Rightarrow m^{p-1} \equiv 1 \ [p]$

↳ $\forall (a,b) \in \mathbb{Z}^2$, $(a+b)^p = a^p + b^p + p\left(\underbrace{\sum_{k=1}^{p-1} \frac{(p-1)!}{k!(p-k)!} a^k b^{p-k}}_{\in \mathbb{Z}}\right)$

$\equiv a^p + b^p \ [p]$

$H_n := "n^p \equiv n \ [p]"$. H_0 vraie. Soit $n \in \mathbb{N}$. Si H_n vraie, $(n+1)^p \equiv n^p + 1 \equiv n+1 \ [p]$ par hypothèse. Donc H_{n+1}.
Soit $m \in \mathbb{Z}_-^*$. $0 \equiv (-m+m)^p \equiv (-m)^p + m^p \equiv -m + m^p \ [p]$
donc $m^p \equiv m \ [p]$.

Soit $m \in \mathbb{Z}$ tel que $p \nmid m$, i.e. $p \wedge m = 1$ car $p \in \mathcal{P}$.
$p \mid m(m^{p-1} - 1)$ donc (Gauss) $p \mid (m^{p-1} - 1)$, i.e. $m^{p-1} \equiv 1 \ [p]$

Décomposition en produit de facteurs premiers

$n \in \mathbb{Z}^*$. $\exists ! (u, r, p, \alpha) \in \{-1;1\} \times \mathbb{N} \times \mathcal{P}^{[\![1;r]\!]} \times \mathbb{N}^{*\,[\![1;r]\!]}$

$n = u \prod_{i=1}^{r} p_i^{\alpha_i}$ où les p_i sont distincts

↳ Existence Récurrence sur $n \in \mathbb{N}^*$ avec $u = 1$, puis extension à $\mathbb{Z}^*$ avec $u = -1$. H_1 vraie (produit vide).
Soit $n \in \mathbb{N}^*$. Si H_i vraie $\forall i \leq n$, soit $n+1$ est premier, soit il s'écrit $n+1 = ab$ avec $a, b \in [\![2; n]\!]$, d'où le résultat par hypothèse.

Unicité Fastidieuse

Valuations

$n \in \mathbb{Z}^*$, $p \in \mathcal{P}$. $\mathrm{Val}_p(n) = \max\{\alpha \in \mathbb{N},\ p^\alpha \mid n\}$

▶ $(n_1, n_2) \in \mathbb{Z}^{*2}$. $\quad n_1 \mid n_2 \iff \forall p \in \mathcal{P},\ \mathrm{Val}_p(n_1) \leq \mathrm{Val}_p(n_2)$

$\forall p \in \mathcal{P}$, $\begin{cases} \mathrm{Val}_p(n_1 \wedge n_2) = \min(\mathrm{Val}_p(n_1), \mathrm{Val}_p(n_2)) \\ \mathrm{Val}_p(n_1 \vee n_2) = \max(\mathrm{Val}_p(n_1), \mathrm{Val}_p(n_2)) \end{cases}$