C1 : Nombres Réels

DM 1 : $\sqrt{2} \notin \mathbb{Q}$.

DM 2 : Rela° $\mid$ sur $\mathbb{N}$: $\mathcal{R}$ ordre & non totale

DM 3 : M est maximum.

DM 4 : CBI

DM 5 : CSBI

DM 6 : $\mathbb{R}$ archimédien, $\forall x \in \mathbb{R}, \exists n \in \mathbb{N}, n > x$.

DM 7 : $\mathbb{E}(x) \leq x < \mathbb{E}(x) + 1$

DM 8 : intervalles de $\mathbb{R}$.

DM 9 : $\mathbb{Q}$ est dense ds $\mathbb{R}$.

DM 10 : CBSI

C2 : Suites

DM 1 : si suite CV sa lim est uniq.

DM 2 : $\lim U_n = \ell \iff \lim U_n - \ell = 0$

DM 3 : $\lim \frac{1}{U_n} = \frac{1}{\ell}$, $\ell \in \mathbb{R}$

DM 4 : Tte suite CV est bornée.

DM 5 : $\lim U_n = +\infty$; $V_n \geq U_n \Rightarrow \lim V_n = +\infty$.

DM 6 : TDG

DM 7 : Tte suite ↘ & minorée est CV.

DM 8 : Tte suite & ↗ majorée ~~est~~ → $+\infty$.

DM 9 : Si (U_n) & (V_n) adjacentes alors CV vers m lim.

DM 10 : Si $\varphi : \mathbb{N} \to \mathbb{N}$, st ↗ alors $\forall n \in \mathbb{N}, \varphi(n) \geq n$.

DM 11 : Si $\lim U_{2n} = \lim U_{2n+1} = \ell$ alors $\lim U_n = \ell$

DM 12 : TBW tte suite bornée admt ss-suite CV.

C3 : Arithmétique

DM 1 : $\exists q, r \in \mathbb{Z}$, $a = bq + r$, $0 \leq r < b$

DM 2 : $a \wedge b = b \wedge r$ (PAE)

DM 3 : si $d \mid a$, $d \mid b \Rightarrow d \mid a \wedge b$ (DM 9 $a \mid c$, $b \mid c \Rightarrow a \vee b \mid c$)

DM 4 : LDG : si $a \mid bc$ & $a \wedge b = 1 \Rightarrow a \mid c = 1$

DM 5 : $d = a \wedge b \iff a = da'$, $b = db'$; $a' \wedge b' = 1$

DM 6 : $ka \wedge kb = |k| (a \wedge b)$

DM 7 : (ED) $ax + by = c$

DM 8 : $(a \wedge b)(a \vee b) = |ab|$

DM 10 : Tt entier ≥ 2 admt divis° q est nbr premier.

DM 11 : $\exists$ ∞té nbr premiers.

DM 12 : p : np ; si $p \mid ab \iff p \mid a$ ou $p \mid b$.

DM 13 : p : np, $a \in \mathbb{Z}$: soit $p \mid a$ soit p & a st premiers e/x.

DM 14 : pptés calculs n Congruences.

DM 15 : $ax \equiv b \, [n]$ < DM 7 >

DM 16 : PTF.

S

C1 : Nombres Réels

est relaᵗ° ordre & elle est

Pptés $\mathbb{R}$: 1) $(\mathbb{R}, +, \times)$ commutatif 2) Relaᵗ° $\leq$ sur $\mathbb{R}$ TOTALE.
3) TFL : $\forall x \in \mathbb{R}, \exists n \in \mathbb{N}, n > x$ 4) Tte partie de $\mathbb{R}$ non-vide & maj admet borne sup.

- Majorant : $\exists M \in \mathbb{R}, \forall x \in A, x \leq M$.
- minorant : $\exists m \in \mathbb{R}, \forall x \in A, x \geq m$.
- Maximum : $\exists M \in \mathbb{R}, M \in A, \forall x \in A, x \leq M$.
- minimum : $\exists m \in \mathbb{R}, m \in A, \forall x \in A, x \geq m$.
- Borne sup : si $x \in A$, $x \leq \sup A$ & $\forall y < \sup A, \exists x \in A, y < x$.
- Borne inf : si $x \in A$, $x \geq \inf A$ & $\forall y > \inf A, \exists x \in A, y > x$.

$||x| - |y|| \leq |x \pm y| \leq |x| + |y|$

CSBS : $\sup A$ est majorant de A. $\exists (x_n)_{n \in \mathbb{N}}$ d'élts A q CV vers $\sup A$.

CSBI : $\inf A$ est minorant de A. $\exists (x_n)_{n \in \mathbb{N}}$ d'élts A q CV vers $\inf A$.

$\mathbb{Q}$ est dense ds $\mathbb{R}$. $\mathbb{Q}$ ne vérifie pas ppté borne sup.

C2 : Les Suites

CV vers l : $\forall \varepsilon > 0, \exists N \in \mathbb{N}, \forall n \in \mathbb{N}, |U_n - l| \leq \varepsilon$.

$+\infty$: $\forall A > 0, \exists N \in \mathbb{N}, \forall n \in \mathbb{N}, U_n \geq A$.

$-\infty$: $\forall A > 0, \exists N \in \mathbb{N}, \forall n \in \mathbb{N}, U_n \leq A$.

$\lim U_n = l \iff \lim (U_n - l) = 0$ & $\lim U_n = l \Rightarrow \lim |U_n| = |l|$ & $\lim \frac{1}{U_n} = \frac{1}{l}$

- Tte suite CV est bornée.
- $\lim \frac{U_{n+1}}{U_n} = l < 1 \Rightarrow \lim U_n = 0$.   - $U_n = \frac{\mathbb{E}(a 10^n)}{10^n}$ approx nbre décim.
- Tte suite ↗ & majorée est CV. - Tte suite ↘ & minorée : CV
- Tte suite ↗ & non-maj $\longrightarrow +\infty$ - Tte suite ↘ & CV vers 0 est : ⊕.

TBW : Tte suite bornée admet sous-suite CV.
(voir TH $U_{\varphi(n)}$)   ↪ $\forall \varepsilon > 0, \exists x \in A, \exists x > \sup A - \varepsilon$.

DM 1 $\sqrt{2} \notin \mathbb{Q}$. (?!) $\sqrt{2} = \frac{p}{q}$ $\mathbb{Z}$ / $\mathbb{N}^*$ → premiers entre eux

$2q^2 = p^2 \Rightarrow p$: entier pair. $p = 2p' \Rightarrow 2q^2 = 4p'^2$ & $q^2 = 2p'^2$
↪ cela prouve que $2 | q^2 \Rightarrow 2 | p$. On a prvé $2 \div p$ & q. (?!)

DM 2 Relaᵗ° $|$ sur $\mathbb{N}$: $\longleftrightarrow$ ordre & non-totale.
$a, b \in \mathbb{Z}$, $a | b$ ssi $a | b$ $\exists k \in \mathbb{Z}$, $b = ka$.
✓ Réflexivité ($a|a \to a = 1 \times a$) ✓ Antisymétriq (cas a...) ✓ Transitivité.

DM 3 M est un maximum ; M & M' : 2 maxima de A.
$M \leq M'$ car M' est majorant de A, $M' \in A$. $M' \leq M$ car M est majorant de A, $M \in A$. $\Rightarrow M = M'$.

DM 4 CBI ; Mq $\inf A$ ✓ ⓘ ⓘⓘ → ⓘ ✓ car $\inf A$ est minorant de A
→ si $y > \inf A$ alors y n'est pas minorant de A, on a $\exists x \in A, x < y$.
Soit $\alpha \in \mathbb{R}$, ⓘ $\forall x \in A$ ⓘⓘ $\forall y > \alpha, \exists x \in A, y > x$.
Mq $\alpha = \inf A$: α minorant d'après ⓘ.
D+, si $y > \alpha$ alors ⓘⓘ $\Rightarrow y$ n'est pas minorant A. Dc α est bien + grd minorants de A.

DM 5 CSBI ; $\inf A$ ✓ ⓘ, d'après ⓘⓘ CBI.
$\forall n \in \mathbb{N}^*, \exists x_n \in A, x_n < \inf A + \frac{1}{n}$.
D'où $\inf A \leq x_n \leq \inf A + \frac{1}{n}$. D'où $\lim x_n = \inf A$ **TDG**

DM 6 $\mathbb{R}$ archimédien, $\forall x \in \mathbb{R}, \exists n \in \mathbb{N}, n > x$.
↪ suffit mq pie $\mathbb{N}$ n'est pas majorée ds $\mathbb{R}$.
(?!) elle est majorée, ĉ elle est non-vide, elle admet borne sup M.
ie $\forall n \in \mathbb{N}, n \leq M$, a fortiori $\forall n \in \mathbb{N}, n+1 \leq M$ où $n \leq M-1$
$M-1$ est majorant de pie $\mathbb{N}$.

DM 7 $\mathbb{E}(x) \leq x < \mathbb{E}(x) + 1$ ie $\forall x \in \mathbb{R}$, $\mathbb{E}(x)$ + grd entier $\mathbb{Z} \leq n$.
Ⓐ SppS $x \geq 0$ par TFL, $\exists n \in \mathbb{N}, n > x$.
Ens : $K = \{k \in \mathbb{N}, k \leq x\}$ dc fini car $\forall k \in K$, $0 \leq k < n$.
Dc admt + grd élt $k_{max} = \max K$. On a alors $k_{max} \leq x$
car $k_{max} \in K$, $k_{max} + 1 > x$ car $k_{max} + 1 \notin K$.
(?!) $k \leq x < k+1$ & $l \leq x < l+1$, entiers $\mathbb{Z}$, dc $k \leq x < l+1 \to k < l+1$.
Puis $l < k+1$. Dc $l-1 < k < l+1$. MS il n'y a qu'un seul entier compris strictement entre $l-1$ & $l+1$, c'est l : $k = l$.

DM 8 / intervalles de $\mathbb{R}$

DM 9 / $\mathbb{Q}$ est dense ds $\mathbb{R}$.

1) $\forall$ intervalle contient 1 rationnel
2) $\forall$ intervalle contient 1 irrationnel
3) $\forall$ intervalle contient ∞té rationnel / irrationnel

1) Mq $\forall a,b \in \mathbb{R}$, $a<b \Rightarrow \exists x \in \mathbb{Q}$, $a<x<b$.
Soit $x = \frac{p}{q}$, $p \in \mathbb{Z}$, $q \in \mathbb{N}^*$, $aq<p<bq$. cela revient à trouver $q \in \mathbb{N} \mid]qa,qb[$ contienne entier p.
Il suffit longueur $qb-qa = q(b-a)$ dépasse strict 1 $\Leftrightarrow q > \frac{1}{b-a}$.
D'après TFE, $\exists$ entier q, $q > \frac{1}{b-a}$ car on a $b-a>0 \Rightarrow q \in \mathbb{N}^*$.
On pose $p = E(aq)+1$ alors $p-1 \leq aq < p$.
Soit $a < \frac{p}{q}$ & $\frac{p}{q} - \frac{1}{q} \leq a$. Dc $\frac{p}{q} \leq a + \frac{1}{q} < b \Rightarrow \frac{p}{q} \in]a,b[$.

2) $a<b \Rightarrow \exists x \in \mathbb{Q}$, $a<x<b$; couple $(a-\sqrt{2}, b-\sqrt{2}) \Rightarrow \exists$ rationnelle r ds $]a-\sqrt{2}, b-\sqrt{2}[$ & par translation $r+\sqrt{2} \in]a,b[$. Or $r+\sqrt{2}$ est irrationnel.
Si $a<b$, $]a,b[$ contient aussi irrationnel.

3) ∞ ratio, irratio ds $\forall$ intervalle $]a,b[$. Pr $N \geq 1$, l'ens de N intervalles ouverts
$]a, a+\frac{b-a}{N}[$, $]a+\frac{b-a}{N}, a+\frac{k(b-a)}{N}[$, $]a+\frac{(N-1)(b-a)}{N}, b[$.
Chq intvll contient ratio & irratio de $]a,b[$, il y a N ratio, N irrationnels.

DM 10 CBSI $\exists (x_n)_{n \in \mathbb{N}}$, SppS $\alpha \in \mathbb{R}$ est minorant de A.
Mq $\alpha = \inf A$. suite élts (x_n) de A CV vers α.
D'après CBI, il suffit mq $\forall y > \alpha$, $\exists x \in A$, $y > x$.
Soit $y>\alpha$, on pose $\varepsilon = \frac{y-\alpha}{2}$ car (x_n) CV vers α,
$\exists N \in \mathbb{N}$, $\forall n \geq N$, $|x_n - \alpha| \leq \varepsilon$.
Or $x_n \in A$; $x_n - \alpha \leq \varepsilon$ soit $x_n \leq \alpha+\varepsilon = \frac{y+\alpha}{2} < y$ car $y>\alpha$.

C2 : Si suite CV sa lim est uniq. ?!

DM1 SppS (U_n) admt 2 lim distinctes $\ell \neq \ell'$.
Soit $\varepsilon = \frac{|\ell-\ell'|}{3} > 0$ car $\ell \neq \ell'$ & (U_n) CV vers ℓ ;
$\exists N \in \mathbb{N}$, $\forall n \geq N$, $|U_n - \ell| \leq \varepsilon$. $\rightarrow$ Pr $K = \max(N, N_1)$
$\exists N_1 \in \mathbb{N}$, $\forall n \geq N_1$, $|U_n - \ell'| \leq \varepsilon$.
$\Rightarrow 3\varepsilon = |\ell-\ell'| = |\ell - U_n + U_n - \ell'| \leq |\ell-U_n| + |U_n + \ell'| \leq 2\varepsilon$.
Dc $\varepsilon \leq 0$?!

DM2 $\lim U_n = \ell \Leftrightarrow \lim U_n - \ell = 0$
$\forall \varepsilon>0, \exists N \in \mathbb{N}, \forall n \geq N, |U_n - \ell| \leq \varepsilon$.
$\forall \varepsilon>0, \exists N \in \mathbb{N}, \forall n \geq N, |U_n - \ell - 0| \leq \varepsilon$.
soit $\varepsilon>0$ alors $\exists N \in \mathbb{N}, \forall n \geq N, |U_n - \ell| \leq \varepsilon$.
cq, $\forall n \geq N$, $\big||U_n| - |\ell|\big| \leq |U_n - \ell| \leq \varepsilon$

DM3 $\lim \frac{1}{U_n} = \frac{1}{\ell}$, $\ell \in \mathbb{R}$ <SAD>

DM4 Tte suite CV est bornée.
(U_n) CV vers $\ell \in \mathbb{R}$ alors $\exists N \in \mathbb{N}$, $|U_n - \ell| \leq 1$.
cq, $|U_n| = |U_n - \ell + \ell| \leq |U_n - \ell| + |\ell| \leq |\ell| + 1$.
D+ car $\{|U_0|, \dots, |U_{n-1}|\}$ est fini ; on définit $M = \max\{|U_0|, \dots |U_{n-1}|\}$
ainsi, $\forall n \in \mathbb{N}$, $|U_n| \leq \max(M, |\ell|+1)$.

DM5 $\lim U_n = +\infty$; $V_n \geq U_n \Rightarrow \lim V_n = +\infty$.
$\exists N \in \mathbb{N}$, $U_n \geq A$, soit $A>0$; ainsi pr m̂ rg $\forall n \geq N$, $V_n \geq U_n \geq A$.

DM6 TDG ; soit $\varepsilon>0$,
$\exists N_1 \in \mathbb{N}, \forall n \geq N_1$, $\ell-\varepsilon \leq V_n \leq \ell+\varepsilon$ par transitivité.
$\exists N_2 \in \mathbb{N}, \forall n \geq N_2$, $\ell-\varepsilon \leq W_n \leq \ell+\varepsilon$
ainsi $n = \max(N_1, N_2)$ on a : $\ell-\varepsilon \leq V_n \leq U_n \leq W_n \leq \ell+\varepsilon$ $\Rightarrow \ell-\varepsilon \leq U_n \leq \ell+\varepsilon$

DM 7 Tte suite ↘ & minorée est CV. — A est pie de $\mathbb{R}$ minorée

Soit $A = \{U_n, n \in \mathbb{N}\}$ & U_n ↘ & minorée. A non vide. Elle admet borne inf $\ell = \inf A$. Mq (U_n) CV vers ℓ.

Soit $\varepsilon > 0$, par CBI, $\exists \mathcal{N} \in \mathbb{N}$, $U_{\mathcal{N}} < \ell + \varepsilon$ $\quad (\ell + \varepsilon > U_{\mathcal{N}})$

Ainsi ĉ U_n ↘, on a $\forall n \geqslant \mathcal{N}$, $U_n \leqslant U_{\mathcal{N}} < \ell + \varepsilon$.

ĉ ℓ est minorant de A, alors $\forall n \in \mathbb{N}$, $U_n \geqslant \ell > \ell - \varepsilon$.

is $\forall n \geqslant \mathcal{N}$, $\ell - \varepsilon \leqslant U_n \leqslant \ell + \varepsilon$.

DM 7' Tte suite ↗ & non-maj ⟶ $+\infty$.

Soit $A > 0$, ĉ A n'est pas majorant de (U_n) alors $\exists \mathcal{N} \in \mathbb{N}$, $U_n > A$.

Or (U_n) ↗, dc $\forall n \geqslant \mathcal{N}$, $U_n \geqslant U_{\mathcal{N}} > A$.

DM 8 Tte suite ↘ & CV vers 0 est ⊕. ?!

(U_n) ↘ vers 0 ?!, SppS (U_n) ⊖ alors $\exists \mathcal{N} \in \mathbb{N}$, $U_{\mathcal{N}} < 0$.

ĉ (U_n) ↘ alors $\forall n \geqslant \mathcal{N}$, $U_n \geqslant U_{\mathcal{N}} < 0$. En passant à lim, on a $0 \leqslant U_{\mathcal{N}}$. ?!

DM 9 Si (U_n) & (V_n) adjcts alors CV vers m̂ lim.

→ ĉ U_n ↗ ; $-U_n$ ↘ Dc $V_n - U_n$ ↘ or $\lim V_n - U_n = 0$. lemme.

$\forall n \in \mathbb{N}$, $V_n - U_n \geqslant 0$. Ainsi $\forall n \in \mathbb{N}$, $U_0 \leqslant U_n \leqslant V_n \leqslant V_0$.

Dc $\ell' - \ell = \lim V_n - U_n = 0$ d'où $\ell' = \ell$.

DM 10 Si $\varphi : \mathbb{N} \to \mathbb{N}$, ST ↗ alors $\forall n \in \mathbb{N}$, $\varphi(n) \geqslant n$.

$\varepsilon > 0$, $\exists \mathcal{N} \in \mathbb{N}$, $\forall n \geqslant \mathcal{N} \Rightarrow |U_n - \ell| \leqslant \varepsilon$. Mq pr $n \in \mathbb{N}$

- $\varphi(0) \geqslant 0$ car $\varphi(0) \in \mathbb{N}$.
- SppS $\varphi(n) \geqslant n$ pr cert n tq $n \geqslant 0$

$\varphi(n+1) > \varphi(n)$ car $\varphi(n)$ ↗ ST

$\varphi(n+1) \geqslant \varphi(n) + 1$ car $\varphi \in \mathbb{N}$

$\varphi(n+1) \geqslant n + 1$ par HDR

$\Rightarrow \varphi(n) \geqslant n \Rightarrow$ si $n \geqslant \mathcal{N} \Rightarrow \varphi(n) \geqslant \mathcal{N} \Rightarrow |U_{\varphi(n)} - \ell| \leqslant \varepsilon$

DM 11 Si $\lim U_{2n} = \lim U_{2n+1} = \ell$ alors $\lim U_n = \ell$.

Soit $\varepsilon > 0$,

$$\begin{cases} \exists \mathcal{N}_1 \in \mathbb{N}, \forall n \geqslant \mathcal{N}_1, |U_{2n} - \ell| \leqslant \varepsilon & (1) \\ \exists \mathcal{N}_2 \in \mathbb{N}, \forall n \geqslant \mathcal{N}_2, |U_{2n+1} - \ell| \leqslant \varepsilon & (2) \end{cases}$$

On pose $k = \max(2\mathcal{N}_1, 2\mathcal{N}_2 + 1)$ ainsi pr $n \geqslant k$; on a :

- $n = 2p$ de $p \in \mathbb{N} \Rightarrow n \geqslant k \geqslant 2\mathcal{N}_1 \Rightarrow p \geqslant \mathcal{N}_1$

$\overset{(1)}{\Rightarrow} |U_n - \ell| \Rightarrow |U_{2p} - \ell| \leqslant \varepsilon$.

- $n = 2q+1$ de $q \in \mathbb{N} \Rightarrow n \geqslant k \geqslant 2\mathcal{N}_2 + 1 \Rightarrow q \geqslant \mathcal{N}_2$

$\overset{(2)}{\Rightarrow} |U_n - \ell| \Rightarrow |U_{2q+1} - \ell| \leqslant \varepsilon$ Ds ts cas $|U_n - \ell| \leqslant \varepsilon$

DM 12 TBW Tte suite bornée admet ss-suite CV. $\boxed{\text{DICHOTOMIE}}$

→ ens val^{rs} ds $[a, b]$, posons $a = a_0$, $b = b_0$, $\varphi(0) = 0$.

· Au −, 1 ds 2 intrvlls $\left[a_0, \frac{a_0 + b_0}{2}\right]$ ou $\left[\frac{a_0 + b_0}{2}, b_0\right]$ contient U_n pr ∞té indices n.

· on note $[a_1, b_1]$, $\varphi(1) > \varphi(0)$, un entier, $U_{\varphi(1)} \in [a_1, b_1]$.

· en itérant constrctn $\forall n \in \mathbb{N}$, ∀ intrvll $[a_n, b_n]$ de lg^r $\frac{b-a}{2^n}$ & un entier $\varphi(n) > \varphi(n-1)$ / $U_{\varphi(n)} \in [a_n, b_n]$.

On note a_n ↗, b_n ↘ ĉ $\lim b_n - a_n = 0 = \lim \frac{b-a}{2^n} = 0$.

Adjcts dc CV vers m̂ lim. TDG ; $\lim U_{\varphi(n)} = 0$

Ch 3 : Arithmétique

- $b | a$ si $\exists q \in \mathbb{Z}$, $a = bq$.
  - $\forall a \in \mathbb{Z}$, $a | 0$ & $1 | a$ - $a | b$ & $b | a \Rightarrow b = \pm a$
  - $a | b$ & $b | c \Rightarrow a \,|\, \lambda b + \mu c$ $\forall \lambda, \mu \in \mathbb{Z}$.
  - si $b | a$ & $a \neq 0$ alors $|b| \leq |a|$.

DE $\exists q, r \in \mathbb{Z}$, $a = bq + r$ et $0 \leq r < b$.

pgcd $a, b \in \mathbb{Z} \setminus \{0,0\}$: le + grd entier q ÷ à la fois a & b : pgcd.

- $a \wedge b = 1 \iff$ a et b sont premiers entre eux.
- $a \wedge b = b \wedge r$

TB $au + bv = a \wedge b$ (u, v ne st pas uniqs)

$\Rightarrow$ si $d | a$ et $d | b$ alors $d \,|\, a \wedge b$.

$\Rightarrow$ $au + bv = 1 \iff$ a et b premiers entre eux.

LDG si $a | bc$ & $a \wedge b = 1 \Rightarrow a | c$.

- $d = a \wedge b \iff a = da'$, $b = db'$, $a' \wedge b' = 1$

Homog. pgcd : $ka \wedge kb = |k| . a \wedge b$

ED $ax + by = c$; $d = a \wedge b$; $a' \wedge b' = 1$ | $a = da'$, $b = db'$

1) (ED) a soluθs si $d | c$.   k parcourant $\mathbb{Z}$.
2) Dans ce cas, $\exists$ ∞té soluθs entières, $(x, y) = (x_0 - b'k, y_0 + a'k)$

- ppcm(a, b) est + entier entier divisible par a & b.
- $(a \wedge b)(a \vee b) = |a| . |b|$

- si $a | c$ & $b | c$ alors $a \vee b \,|\, c$.
- Nbr premier p est entier ≥ 2 dt seuls diviseurs positifs $\{1, p\}$.
- Tt entier $n \geq 2$ admt ÷r q est nbr premier.
- $\exists$ ∞té nbrs premiers.

LE Soit p nbr premier, si $p | ab$ alors $p | a$ ou $p | b$.

- Si p nbp, $a \in \mathbb{Z}$, alors soit $p | a$ soit p et a st premiers entre eux.
- Décomp fctrs premiers $n \geq 2$: $n = p_1^{a_1} \times \dots \times p_r^{a_r}$.
- Soit $\begin{cases} a = p_1^{\alpha_1} \times \dots \times p_k^{\alpha_p} \\ b = p_1^{\beta_1} \times \dots \times p_k^{\beta_p} \end{cases} \Rightarrow$
  1) $a | b \iff \forall 1 \leq i \leq k$; $\alpha_i \leq \beta_i$
  2) $a \wedge b = p_1^{\min(\alpha_1, \beta_1)} \times \dots \times p_k^{\min(\alpha_p, \beta_p)}$
  3) $a \vee b = p_1^{\max(\alpha_1, \beta_1)} \times \dots \times p_k^{\max(\alpha_p, \beta_p)}$

Congru $n \geq 2$, $a \equiv b\ [n] \iff n \,|\, b - a$ ou $\exists k \in \mathbb{Z}$, $a = b + kn$.

- Relaθ $\equiv [n]$: relaθ équivlce.
  - Réflex ($a \equiv a\ [n]$) - Symétr ($a \equiv b\ [n] \to b \equiv a\ [n]$) - Trans $a \equiv b\ [n]$, $b \equiv c\ [n] \Rightarrow a \equiv c\ [n]$.

EC soit $a \in \mathbb{Z}^*$, $b \in \mathbb{Z}$, $n \geq 2$ fixés. $d = a \wedge n$.

$n = dn'$, $a = da' \Rightarrow n' \wedge a' = 1$.

(EC) $ax \equiv b\ [n]$ d'inc. $x \in \mathbb{Z} \iff \exists k \in \mathbb{Z}$, $ax - kn = b$

1) (EC) soluθs ssi $d | b$.
2) Dans ce cas, soluθs so forme $x = x_0 + ln' \iff x \equiv x_0\ [n']$

- **Inverse a [n] :** $aa' \equiv 1\ [n]$ $\Leftrightarrow$ $a \in \mathbb{Z}^*$, $n \geq 2$, $a \wedge n = 1$; $\exists!\, a'$
  ↳ si $b \in \mathbb{Z}$, $ax \equiv b\ [n] \iff x \equiv a'b\ [n]$

PTF si p nbp, $a^p \equiv a\ [p]$ **Coro** Si $p \nmid a \Rightarrow a^{p-1} \equiv 1\ [p]$

- p divise $\binom{p}{k}$, $1 \leq k \leq p-1$ [illegible]

cl 3 : $a \in \mathbb{Z}$, $b \in \mathbb{N} \setminus \{0\}$.

DM 1 $\exists\, q, r \in \mathbb{Z}$, $a = bq + r$, $0 \leq r < b$

(∃) Soit $\mathcal{N} = \{m \in \mathbb{N} \mid bm \leq a\}$. → ens (NV) car $m = 0 \in \mathcal{N}$.
$\forall\, m \in \mathcal{N}$, on a $m \leq a$. Dc nbr fini élts de $\mathcal{N}$: $q = \max \mathcal{N}$.
Alors $qb \leq a$ car $q \in \mathcal{N}$ & $(q+1)b > a$ car $q+1 \notin \mathcal{N}$.
Dc $qb \leq a < (q+1)b = qb + b$; définit $r = a - qb$; r vérifie $0 \leq r = a - qb < b$.
(∃!) Sibi q', r' ; soit 2 entiers vérif^t CI Th. D'abord $a = bq + r = bq' + r'$
Dc $b(q - q') = r - r'$. + D $0 \leq r' < b$ & $0 \leq r < b$.
Dc $-b \leq r' - r < b$. MS $r' - r = b(q - q')$. Dc $-b \leq b(q-q') < b$.
On pt ÷ par $b > 0$ → $-1 \leq q - q' < 1$; ĉ $q - q'$ est un entier.
⇒ $q - q' = 0$ ⇒ $q = q'$. De m̂ $\forall$ $r - r' = b(q - q')$ ⇒ $r = r'$.

DM 2 $a \wedge b = b \wedge r$. (?AE).

Mq divisrs a & b st m̂s q b & r.
Soit d, dvsr a & b : $d \mid b$ dc $d \mid bq$; $d \mid a$ dc $d \mid a - bq = r$.
Soit d, dvsr b & r : $d \mid bq + r = a$.

?AE On souhaite calculer pgcd $a, b \in \mathbb{N}^*$. Sibi $a \geq b$.
On calcule DE successives, le pgcd sera le dernier reste non nul.
- division de a p b, $a = bq_1 + r_1$. D lem, $a \wedge b = b \wedge r_1$ et si $r_1 = 0$ alors $a \wedge b = b$ sinon on continue :
- $b = r_1 q_2 + r_2$; $a \wedge b = b \wedge r_1 = r_1 \wedge r_2$
- $r_1 = r_2 q_3 + r_3$; $a \wedge b = r_2 \wedge r_3$.
- $r_{k-2} = r_{k-1} q_k + r_k$; $a \wedge b = r_{k-1} \wedge r_k$
- $r_{k-1} = r_k q_k + 0$; $a \wedge b = r_k \wedge 0$.

ĉ chq étape, reste + ptt quotient, on sait q $0 \leq r_{i+1} \leq r_i$. Ainsi ?AE finit car sûr to get reste non nul ; restes forment suite ↘ entiers positifs non nuls $b > r_1 > r_2 > \dots \geq 0$.

DM 3 si $d \mid a$, $d \mid b$ ⇒ $d \mid a \wedge b$.

D'après (TB), $\exists\, u, v \in \mathbb{Z}$, $a \wedge b = au + bv$.
Ainsi si $d \mid a$ & $d \mid b$ ⇒ $d \mid au + bv = a \wedge b$.

DM 4 LDG : si $a \mid bc$ & $a \wedge b = 1$ alors $a \mid c$.

$a \wedge b = 1$, $\exists\, u, v \in \mathbb{Z}$, $au + bv = 1$.
On multiplie par $acu + bcv = c$ Mais $a \mid acu$ & par H, $a \mid bcv$ dc $a \mid acu + bcv$.

DM 5 $d = a \wedge b$ ⟺ $a = da'$, $b = db'$; $a' \wedge b' = 1$.

(⇒) on a $a = da'$, $b = db'$. d est dvsr de a & b. D'après (TB), $\exists\, u, v \in \mathbb{Z} \mid au + bv = d$. Alors $da'u + db'v = d$, dc $a'u + b'v = 1$. D'après caractéris$^\circ$ (np) ⟷ v, $a' \wedge b' = 1$.
(⟸) ĉ $d \mid a$ & $d \mid b$ alors $d \mid a \wedge b$ d'apr avnt, or $\exists\, u, v \in \mathbb{Z} \mid a'u + b'v = 1$
D'où $da'u + db'v = d$; sibi $au + bv = d$ dc $a \wedge b \mid d$.
Or d, $a \wedge b \in \mathbb{N}^*$; d'où $a \wedge b$.

DM 6 $ka \wedge kb = |k| \, (a \wedge b)$.

Sibi $k \in \mathbb{N}^*$, on pose $d = a \wedge b$. Alors $\exists\, a', b' \in \mathbb{Z}$, $\left| \begin{array}{l} a = da' \\ b = db' \\ a' \wedge b' = 1 \end{array} \right.$
Alors $ka = (kd)a'$ & $kb = (kd)b'$ & tjrs $a' \wedge b' = 1$.
Dc $ka \wedge kb = kd = k(a \wedge b)$.

DM 7 (ED) $ax + by = c$; 1) $d \mid a$, $d \mid b$ dc $d \mid ax + by = c$. (ED) a solu$^\circ$s ssi
2) sibi $d \mid c$; ie $c = dc'$, $c' \in \mathbb{Z}$.
d'après (TB), $\exists\, u, v \in \mathbb{Z} \mid au + bv = d$.
En multipliant par c', on a $a(uc') + b(vc') = dc' = c$.
En notant $\left| \begin{array}{l} x_0 = uc' \\ y_0 = vc' \end{array} \right.$ → on a obtenu une solu$^\circ$ part.
Ds la suite Démo, nos alls réaliser Raisonn^t Analyse / Synthèse.

DM 7 suite.

Analyse Soit (x,y) sol° (ED) $\begin{cases} ax+by=c \\ ax_0+by_0=c \end{cases}$ dc $a(x-x_0)+b(y-y_0)=0$
$a(x-x_0)=b(y_0-y)$

où $\cancel{d}a'(x-x_0)=\cancel{d}b'(y_0-y)$ (*)

Ainsi $a' \mid b'(y_0-y)$ ET $a'\wedge b'=1 \Rightarrow a' \mid y_0-y$. LDG

Ainsi $\exists k \in \mathbb{Z}$, $y_0-y=ka'$.

Ainsi (*) s'écrit $a'(x-x_0)=-b'ka' \Rightarrow x-x_0=-b'k$.

Ainsi $(x,y)=(x_0-b'k\ ;\ y_0+a'k)$ $\forall k\in\mathbb{Z}$.

Synthèse On vérifie récipmqt q tt $(x,y)=(x_0-b'k,\ y_0+a'k)$ $\forall k\in\mathbb{Z}$ est bien sol° de (ED).

On calcule
$$ax+by=a(x_0-b'k)+b(y_0+a'k)$$
$$ax+by=(ax_0+by_0)-ab'k+ba'k$$
$$ax+by=c-da'b'k+da'b'k$$
$$ax+by=c$$

DM 8 $(a\wedge b)(a\vee b)=|ab|$.

Sibi $a>0$, $b>0$; on pose $d=a\wedge b$. $\left|\begin{array}{l} a=da' \\ b=b'd \end{array}\right.$ et $a'\wedge b'=1$

On pose $m=da'b'$. Alors $md=d^2a'b'=(da')(db')=ab$.

m est un multiple commun à a & b pcq $m=da'b'=ab'=ab$.

Il reste à mq m est + petit multiple commun. Si m est un ôtre mcS à a & b alors $m=ka=lb$. Ainsi $kda'=ldb'$.

Soit $ka'=lb'$. Ainsi $a' \mid b'l$ et $a'\wedge b'=1$ dc $a' \mid l'$ LDG

Fin^t, $a'b=m \mid lb=m$.

DM 11 $\exists$ ∞té nbr premiers

Par l'absurde, ?!, sibi nbr fini (np) ≥ 2. On définit $N=p_1\ldots p_m+1$. D'après Lem, N admet un fact^r premier. À cet$_1$ indice p_i de $1\leq i\leq m$ Alors $P \mid N$ et $p_i \mid p_1\ldots p_m$.

Dc $p_i \mid N-p_1\ldots p_m+1$ ainsi : $p_i=1$ $\boxed{c?!c}$

DM 10 Tout entier ≥ 2 admet divis^r q est nbr premier.

Soit $\mathcal{D}$: ens divisrs de n q st ≥ 2 : $\mathcal{D}=\{k\geq 2 \mid k \mid n\}$.

- Ens $\mathcal{D}$: NV car $n\in\mathcal{D}$, notons $p=\min\mathcal{D}$.
- Sibi ?! que p n'est pas np alors p admet un diviseur q, $1<q<p$ MS q est aussi divis^r n & dc $q\in\mathcal{D}$ & $q<p$.

$\Rightarrow \boxed{c!!c}$ car p est le minimum. Ccl : p est np. ĉ $p\in\mathcal{D}$. $p \mid n$.

DM 12 p : np ; si $p \mid ab \iff p \mid a$ ou $p \mid b$.

Si p ne divise pas a alors p & a st premiers entre eux (en effet ÷rs de p st 1 & p) ms sl 1 divise aussi a, dc $a\wedge p=1$. Ainsi p LDG $\rightarrow p \mid b$.

DM 13 Si p : np ; $a\in\mathbb{Z}$ soit $p \mid a$ soit p & a st premiers entre eux.

$a\wedge p \mid p$ & p : np d'où $a\wedge p=1$ soit $a\wedge p=p$ & alors $p \mid a$.

DM 14 Pptés calculs & Congruences.

1) (i) $a\equiv a\,[n]$ car $n \mid 0$ (ii) $n \mid b-a \iff n \mid a-b$.
(iii) si $n \mid b-a$ & $n \mid c-b$ alors $n \mid b-a+c-b=c-a \Rightarrow n \mid c-a \Rightarrow a\equiv c\,[n]$

2) Somme

3) Produit si $b-a=kn$ & $d-c=ln$ alors $bd=(a+kn)(c+ln)$
$bd=ac+n(al+kc+kln)$ Dc si $a\equiv b\,[n]$ & $c\equiv d\,[n] \Rightarrow ac\equiv bd\,[n]$

DM 15 $ax\equiv b\,[n]$ <SAD> <DM (ED) 7>.

DM 16

$\binom{p}{k}=\dfrac{p!}{k!(p-k)!}$; dc $p \mid p!=\binom{p}{k}\cdot k!\,(p-k)!$ ←

ĉ $p\nmid k!$ et $p\nmid(p-k)!$ LEu $\rightarrow p \mid \binom{p}{k}$. Mq (pr) $\forall a\geq 0$.

- $a=0$ alors $0\equiv 0\,[p]$
- on fixe $a\geq 0$, sibi $a^p\equiv a\,[n]$. Calculons $(a+1)^p$ de FFBN

$(a+1)^p=a^p+\binom{p}{p-1}a^{p-1}+\ldots+\binom{p}{1}+1$. Réduisons mtn $[p]$

$(a+1)^p=a^p+\binom{p}{p-1}a^{p-1}+\ldots+\binom{p}{1}+1\ [p]\equiv a^p+1\ [p]$ ĝ Lemme
$\equiv a+1\ [p]$ HDR

$\Rightarrow$ PTF mq ĝ (pr) $\forall a\geq 0$; m̂ cas $a<0$