DÉMONSTRATIONS D'ARITHMÉTIQUE

D1 (Théorème de la division euclidienne)
Données a, b entiers, $b > 0$ (donc $b \geqslant 1$).

1) ANALYSE
Si le couple (q, r) existe, $0 \leqslant r = a - bq < b,$ donc $bq \leqslant a < b(q+1)),$ d'où
$q \leqslant \dfrac{a}{b} < q + 1$ et q est la partie entière de a/b et $r = a - bq$: fin de l'analyse.

2) SYNTHESE
Soit $q = E\left(\dfrac{a}{b}\right)$ et $r = a - bq$; alors $a = bq + r$ et $q \leqslant \dfrac{a}{b} < q + 1$ d'où
$0 \leqslant r = a - bq < b$; fin de la synthèse.

D2 (Théorème des sous-groupes de $\mathbb{Z}$)
Soit G un sous-groupe additif de $\mathbb{Z}$; on vérifie déjà que si a appartient à G, alors $a\mathbb{Z} \subset G$; en effet, par récurrence sur n on montre que na appartient à G pour tout naturel n (stabilité pour $+$), puis comme $-a$ appartient à $G,$ que na appartient à G pour tout n entier négatif.
Si $G = \{0\},\ G = 0\mathbb{Z}$; supposons donc $G \neq \{0\}$.
Comme $x \in G \Rightarrow -x \in G,\ G \cap \mathbb{N}^*$ est non vide et possède un plus petit élément a ; d'après ce que nous venons de voir $a\mathbb{Z} \subset G$, et montrons l'inclusion réciproque.
Soit x un élément de G ; effectuons la division euclidienne de x par a ; $x = aq + r$; comme x et a appartiennent à $G,\ r = x - aq$ appartient à G et vérifie $0 \leqslant r < a$; a étant le minimum de $G \cap \mathbb{N}^*,$ la seule possibilité est $r = 0$; donc $x = aq$ et $x \in aZ.$
Conclusion : $G = a\mathbb{Z}.$

D3 (Théorème de la décomposition d'un entier dans une base)
Soit b entier $\geqslant 2;$

On va montrer par récurrence sur n que si
$b^n \leqslant a < b^{n+1}$ alors $\exists!(r_0, r_1, \ldots, r_n) \in [|0, b-1|]^{n+1}/$

$$\boxed{a = r_0 + r_1 b + r_2 b^2 + \ldots + r_n b^n} \text{ avec } r_n \neq 0$$

Cas $n = 0$; alors si $1 \leqslant a < b,\ a = r_0,$ avec $r_0 \neq 0.$

HR : si $b^n \leqslant a < b^{n+1}$ alors $\exists!(r_0, r_1, \ldots, r_n) \in [|0, b-1|]^{n+1}/$

$$\boxed{a = r_0 + r_1 b + r_2 b^2 + \ldots + r_n b^n} \text{ avec } r_n \neq 0$$

Soit maintenant a tel que $b^{n+1} \leqslant a < b^{n+2}$

S'il existe $(r_0, r_1, \ldots, r_n) \in [|0, b-1|]^{n+1}$ tel que $a = r_0 + r_1 b + r_2 b^2 + \ldots + r_n b^n \ + r_{n+1} b^{n+1} = r_0 + b(r_1 + r_2 b + \ldots + r_{n+1} b^n),\ r_0$ est forcément le reste de la division euclidienne de a par b, d'où son unicité;

Effectuons donc la division euclidienne de a par b : $a = bq + r_0$.

Comme $0 \leqslant a - bq \leqslant b - 1$, on a : $a - b + 1 \leqslant bq \leqslant a$, donc $b^{n+1} - b + 1 \leqslant bq < b^{n+2}$, donc $b^n - 1 + 1/b \leqslant q < b^{n+1}$, d'où $b^n - 1 \leqslant q < b^{n+1}$; on peut donc appliquer l'H.R. à q : $\exists!(r_1, r_2, \ldots, r_{n+1}) \in [|0, b-1|]^{n+1}/$

$$\boxed{q = r_1 + r_2 b + \ldots + r_{n+1} b^n} \text{ avec } r_{n+1} \neq 0$$

alors $a = bq + r_0 = r_0 + r_1 b + r_2 b^2 + \ldots + r_{n+} b^{n+1}$avec $r_{n+1} \neq 0$ et $(r_0, r_1, \ldots, r_{n+1})$ unique : CQAR.

D5

Soit a, b entiers ; les divisions euclidiennes de a et b par n s'écrivent $a = qn + r$ et $b = q'n + r'$.

alors, comme $a - b = n(q' - q) + r - r'$, on a $a \equiv b\ \ [n]$ ssi n divise $r - r'$, ssi $r = r'$ (car r et r' sont entre 0 et $n - 1$).

D6,7 : tableau

D8 (Théorème de Bézout)

LEMME : si G_1 et G_2 sont deux sous-groupes de $\mathbb{Z}$, $G_1 + G_2$ aussi.

Voir tableau pour la démo.

Sens "trivial" du théorème.

Si $au + bv = 1$

Soit d un diviseur commun > 0 à a et b ; alors d divise $au + bv$, donc 1, donc $d = 1$ et a et b sont premiers entre eux.

Sens non trivial.

Si a et b sont premiers entre eux ; $a\mathbb{Z}$ et $b\mathbb{Z}$ étant des sous-groupes de $\mathbb{Z}$, $a\mathbb{Z} + b\mathbb{Z}$ aussi d'après le lemme ; d'après le théorème des sous-groupes, il existe un naturel c tel que $a\mathbb{Z} + b\mathbb{Z} = c\mathbb{Z}$.

Comme $a = a.1 + b.0$ appartient à $a\mathbb{Z} + b\mathbb{Z}$, $a \in c\mathbb{Z}$, donc c divise a ; de même, il divise b, donc, comme a et b sont premiers entre eux, $c = 1$; mais alors 1 appartient à $a\mathbb{Z} + b\mathbb{Z}$, donc il existe u et v tels que $au + bv = 1$.

D9 (Théorème de Gauss)

Si a divise bc ($bc = ka$) et a est premier avec b ; d'après Bézout il existe u et v tels que $au + bv = 1;$

on écrit alors $c = acu + bcv = acu + kav = a(cu + kv)$ donc a divise c.

D10 :

En effet, $c = ka,$ et b divise ka avec b premier avec a ; donc (Gauss) b divise k , d'où ab divise c.

D11 :tableau

D12 (Caractérisations du pgcd).

1$\Rightarrow$ 2

d est le pgcd de a et $b,$ donc d divise a et $b, a/d = q, b/d = q'$.

soit δ un diviseur de q et q' ; alors δd est un diviseur de $a = qd$ et $b = q'd,$ donc $\delta d \leqslant d$ d'où $\delta \leqslant 1;$ comme $\delta > 0,$ $\delta = 1,$ donc q et q' sont bien premiers entre eux.

2$\Rightarrow$ 3

on sait que q et q' sont premiers entre eux, donc d'après Bézout, il existe u et v tels que $qu + q'v = 1$; en multipliant par d, on obtient $d = au + bv$; donc $d \in a\mathbb{Z} + b\mathbb{Z}$, d'où $\boxed{d\mathbb{Z} \subset a\mathbb{Z} + b\mathbb{Z}}$ (car $a\mathbb{Z} + b\mathbb{Z}$ est un sous-groupe de $\mathbb{Z}$).

Maintenant, si x appartient à $a\mathbb{Z} + b\mathbb{Z}$, c'est un multiple de d puisque a et b sont des multiples de $d.$ Donc x appartient à $d\mathbb{Z}$ *et* $\boxed{a\mathbb{Z} + b\mathbb{Z} \subset d\mathbb{Z}}$.

3$\Rightarrow$ 4

On sait que $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$ et supposons que d' divise a et $b.$ Comme d appartient à $d\mathbb{Z}$, donc à $a\mathbb{Z} + b\mathbb{Z}$, d est un multilpe de $d',$ donc d' divise $d.$

Supposons que d' divise $d,$ l'hypothèse $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$ montre que a et b appartiennent à $d\mathbb{Z}$ donc que d divise a et $b.$ par transitivité, d' divise donc a et $b.$

4$\Rightarrow$ 1

H : pour tout $d' > 0,\quad d'$divise a et b ssi d'divise d

En prenant $d' = d,$ on obtient que d divise a et b. Si maintenant d' divise a et $b,$ il divise d donc il est $\leqslant d$ (ici, tout est >1) , d'où 1.

D13 (Algorithme d'Euclide basique)

PGCD(a,b) =PGCD$(\min(a,b),|a-b|)$??

Si $a \leqslant b$ cela s'écrit PGCD(a,b) =PGCD$(a,b-a)$ et cela provient de ce que les

diviseurs communs à a et b sont les mêmes que les diviseurs communs à a et à $b-a$; l'autre cas s'obtient en échangeant a et b.

Posons maintenant $\begin{cases} a_0 = a \\ b_0 = b \end{cases}$ et $\begin{cases} a_{n+1} = \min(a_n,b_n) \\ b_{n+1} = |a_n - b_n| \end{cases}$; d'après ce qui précède, on a PGCD(a_n,b_n) =PGCD(a,b) pour tout n.

Supposons que $a_n \neq b_n$, et non nuls, par exemple $0 < a_n < b_n$; alors $\max(a_{n+1}$ $b_{n+1}) = \max(a_n,b_n-a_n) < b_n = \max(a_n,b_n)$ (idem pour l'autre cas).

Si on avait constamment $a_n \neq b_n$, et non nuls, alors $(\max(a_n,b_n))$ serait une suite

strictement décroissante d'entiers >0 : c'est absurde ; il existe donc un n pour lequel $a_n = b_n$ et alors PGCD$(a,b) = a_n$.

D14 (Algorithme d'Euclide par division euclidienne)

PGCD(a,b) =PGCD$\big(b,\text{reste}(a,b)\big)$??

Cela vient de ce que reste$(a,b) = a - bq$ et que les diviseurs communs à a et b sont les mêmes que ceux communs à a et $a-bq$.

Si on pose $\begin{cases} a_0 = a \\ b_0 = b \end{cases}$ et $\begin{cases} a_{n+1} = b_n \\ b_{n+1} = \text{reste}(a_n,b_n) \end{cases}$, d'après ce qui précède, on a PGCD(a_n,b_n) =PGCD(a,b) pour tout n.

Si b_n est non nul (donc >0) alors par définition du reste de la division euclidienne, $b_{n+1} < b_n$; si b_n était constamment non nul, la suite (b_n) serait une suite strictement décroissante d'entiers >0 : absurde : il existe donc un n pour lequel $b_n = 0$ et alors PGCD$(a,b) = a_n$.

D15:

D16 (Caractérisations du PPCM)

1$\Rightarrow$ 2

$m =$ PGCD(a,b) ; $a\mathbb{Z} \cap b\mathbb{Z}$ est un sous-groupe de $\mathbb{Z}$ (intersection de 2 sous-groupes) et m est son plus petit élément strictement >0 ; on a vu dans D2 qu'alors $a\mathbb{Z} \cap b\mathbb{Z} = n\mathbb{Z}$.

$2 \Leftrightarrow 3$ est évident, c'est une simple traduction (car m' est mutiple de a et b ssi m' appartient à $a\mathbb{Z} \cap b\mathbb{Z}$)

$3 \Rightarrow 1$ vient de ce qu'un multilple positif d'un nombre positif est plus grand que celui-ci.

D17 (Relation entre le PGCD et le PPCM)

Soient maintenant $a, b > 0$ $d =$PGCD(a,b) et $m =$PPCM(a,b)

1er cas : $d = 1$; a et b sont premiers entre eux, et a et b divisent m ; donc d'après D10 ab divise m ; mais comme m divise ab (car il divise tout multiple commun à a et b) $ab = m$, CQFD

cas général :

$$\text{PGCD}(a,b) \times \text{PPCM}(a,b) = d.\text{PGCD}(\frac{a}{d}, \frac{b}{d}) \times d.\text{PPCM}(\frac{a}{d}, \frac{b}{d}) = d^2 \frac{a}{d} \frac{b}{d} = ab.$$

D19 (critère d'Eratosthène)

Lemme :

si $n = dd'$, alors $d \leqslant \sqrt{n} \Leftrightarrow \frac{n}{d'} \leqslant \sqrt{n} \Leftrightarrow \frac{n}{\sqrt{n}} \leqslant d' \Leftrightarrow d' \geqslant \sqrt{n}$.

Supposons donc que $n \geqslant 2$ ne possède pas de diviseur premier dans $[2, \sqrt{n}]$; alors tout entier $\geqslant 2$ ayant un diviseur premier, il ne possède pas de diviseur tout court dans $[2, \sqrt{n}]$; mais d'après le lemme, il n'en possède pas non plus dans $[\sqrt{n}, n/2]$, donc dans $[\sqrt{n}, n-1]$: il est donc premier.

D20

Montrons par récurrence sur k que la liste L_k est croissante, que les k premiers termes de la liste L_k sont les k premiers nombres premiers et que les autres termes sont tous ceux entre 2 et n qui ne sont pas divisibles par les $k-1$ premiers nombres premiers.

C'est bon pour $k = 1$, et supposons que ce soit bon pour un certain k ; dans L_{k+1} on a ôté tous les multiples du k-ième terme de L_k ; les k premiers termes de L_{k+1} sont toujours premiers et le $k+1$ ième l'est également car il n'est mutiple d'aucun des k premiers nombres premiers, et c'est le plus petit à avoir cette propriété. Les termes restant sont tous ceux entre 2 et n qui ne sont pas divisibles par les $k-1$ premiers nombres premiers, et non plus par le k*ième* puis qu'on a ôté ses multilples , CQAR.

Considérons la dernière liste L_k dont le $k-1$ ième terme est $\leqslant \sqrt{n}$; ses $k-1$ premiers termes sont les nombres premiers $\leqslant \sqrt{n}$, et les autres sont tous ceux entre 2 et

n qui ne sont pas divisibles par ceux-ci. D'après le lemme ci-dessus, ce sont les nombres premiers entre 1 et n restant.

D21

Preuve du LEMME : soit un nombre premier p divisant un produit de nombres premiers $p_1 p_2 \ldots p_k$. S'il n'est pas égal à p_1, il est premier avec lui, donc (Gauss) il divise $p_2 \ldots p_k$; s'il n'est pas égal à p_2, il divise $p_3 \ldots p_k$ etc... Enfin, s'il n'est égal ni à p_1, ni à p_{k-1}, alors il divise p_k donc il lui est égal *CQFD*.

Supposons donc qu'un entier se décompose de deux façons en produit de facteurs premiers ; on est donc en présence de deux listes croissantes de nombre premiers dont les produits sont égaux ; tout nombre d'une des listes divise le produit des éléments de l'autre, donc doit se retrouver dans l'autre liste (y compris s'il y a des répétitions) ; les deux listes sont donc égales.