Arithmétique.

L'arithmétique est la branche des mathématiques qui s'intéresse aux nombres ($\alpha\rho\iota\theta\mu o\varsigma$ ou arithmos en grec signifie nombre). Elle est prolongée par la théorie des nombres (il n'y a pas de consensus sur où s'arrête précisément l'arithmétique et où commence précisément la théorie des nombres, mais en général quand on utilise des outils d'algèbre ou d'analyse (voir articles 9 et 10) on parle de théorie des nombres et sinon on parle d'arithmétique).

I) Plus grand commun diviseur et plus petit commun multiple.

Dans les articles précédents, on démontrait des "énoncés". On va désormais être plus précis : on peut démontrer une proposition, un lemme, un théorème ou un corollaire.
Un théorème est un énoncé très important, une proposition un énoncé moins important (mais important quand même, sinon on ne se fatiguerait pas à le démontrer), un lemme est un énoncé qui va servir à démontrer un théorème et un corollaire est un énoncé qui va se démontrer grâce à un théorème.
Certains manuels scolaires désignent des énoncés comme étant des "propriétés", mais dans les cursus universitaires et le monde de la recherche on ne démontre jamais une "propriété" (vous pouvez remplacer vos "propriétés" par des propositions, ou des lemmes si elles servent à démontrer un théorème).

Commençons par un lemme très important.

Lemme : Toute partie non vide de $\mathbb{N}$ admet un plus petit élément (c'est-à-dire que si $A \subset \mathbb{N}$ n'est pas vide alors il existe $n \in A$ tel que pour tout $a \in A$ $n \leq a$).

Dém : Soit $A \subset \mathbb{N}$. On veut montrer que si A est non vide alors A admet un plus petit élément.
Démontrons la contraposée (cf. article 3. Contraposition et absurde) :
Si A n'admet pas de plus petit élément alors A est vide.
Supposons que pour tout $n \in A$ il existe $m \in A$ tel que $m < n$. Montrons par récurrence forte sur $k \in \mathbb{N}$ que $k \notin A$ (k n'appartient pas à A).
$0 \notin A$ car pour tout $m \in \mathbb{N}$ $0 \leq m$ donc en particulier pour tout $m \in A$ $0 \leq m$.

Supposons que pour tout $l \leq k$ $l \notin A$.
Pour tout $m \in A$ $k+1 \leq m$ (car sinon $m \in \{0, \ldots, k\}$) donc $k+1 \notin A$.
Ainsi, pour tout $k \in \mathbb{N}$, $k \notin A$, donc A est vide.

Remarque : Le plus petit élément est unique, car si a_1 et a_2 sont des plus petits éléments de A alors $a_1 \leq a_2$ (car a_1 plus petit élément de A et $a_2 \in A$) et $a_2 \leq a_1$ (car a_2 plus petit élément de A et $a_1 \in A$) donc $a_1 = a_2$.

Déf : $a \in \mathbb{N}$ est divisible par $b \in \mathbb{N}$ s'il existe $c \in \mathbb{N}$ tel que $a = b \times c$. On dit aussi que a est un multiple de b ou que b divise a. On note ceci $b \mid a$ (lire "b divise a").

Remarques : Si $b \mid a$ et si $a \neq 0$ alors $b \leq a$. En effet on a alors $a = b \times c$ avec $c \geq 1$ (on est juste en train de dire que $b, 2b, 3b$ etc sont supérieurs à b).
Le seul entier divisible par 0 est 0 et 0 est divisible par tous les entiers (car pour tout $c \in \mathbb{N}$ $0 \times c = 0$).
Tous les entiers sont divisibles par 1 (car pour tout $c \in \mathbb{N}$ $1 \times c = c$) et 1 n'est divisible que par 1.

Thm : Soient $a \in \mathbb{N}$ et $b \in \mathbb{N} \setminus \{0\}$. Il existe un unique couple d'entiers naturels (q, r) tel que $r < b$ et $a = qb + r$ (division euclidienne de a par b).

Dém : Démontrons tout d'abord l'unicité : si (q, r) et (p, s) conviennent, alors $qb+r = pb+s$ et $r < b$, $s < b$, donc $(q-p)b = s-r$ donc $s-r$ est un multiple de b donc $s-r = 0$ ou $b \leq s-r$ or $s-r \leq s < b$ (voir inégalités ci-dessus) donc $s-r = 0$ donc $(q-p)b = 0$ or $b \neq 0$ donc $q-p = 0$: ainsi $r = s$ et $q = p$.

Si $a < b$ alors $q = 0$ et $r = a$ conviennent. Sinon, $a - b \geq 0$ donc $0 \notin A = \{n \in \mathbb{N}, a - nb < 0\} \subset \mathbb{N}$ qui est non vide car $a + 1 \in A$ (car $a + 1 > a$ et $b \geq 1$ (car $b \in \mathbb{N} \setminus \{0\}$)) donc, avec le lemme précédent, il existe un plus petit élément n de A. $a - nb < 0$ (car $n \in A$) et $a - (n-1)b \geq 0$ (car $n - 1 < n$ donc $n - 1 \notin A$ car n est le plus petit élément de A). Posons $q = n - 1$ et $r = a - qb$. $q \in \mathbb{N}$, $r \in \mathbb{N}$ et $r < b$.

On peut désormais définir le plus grand commun diviseur de deux entiers :

Déf : Le plus grand commun diviseur de $a \in \mathbb{N}$ et de $b \in \mathbb{N}$, noté $\text{pgcd}(a, b)$, est l'entier $d \in \mathbb{N}$ qui vérifie $d \mid a$, $d \mid b$ et si $c \mid a$ et $c \mid b$ alors $c \mid d$.

Pour que cette définition soit correcte, il faut et il suffit qu'il existe un unique entier d vérifiant ces propriétés (s'il n'y en a pas on est en train de donner un nom à quelque chose qui n'existe pas et s'il y en a plusieurs notre définition est ambigüe car elle désigne plusieurs entiers et pas un seul).

Montrons que cette définition est correcte.

Commençons par l'unicité :
Si d_1 et d_2 vérifient les propriétés de pgcd de a et de b alors, comme $d_1 \mid a$ et $d_1 \mid b$ on a $d_1 \mid d_2$ et comme $d_2 \mid a$ et $d_2 \mid b$ on a $d_2 \mid d_1$.
Si $d_1 = 0$ alors comme $d_1 \mid d_2$ on a $d_2 = 0$. De même, si $d_2 = 0$ alors $d_1 = 0$.
Si $d_1 \neq 0$ et $d_2 \neq 0$ alors on a $d_1 \leq d_2$ et $d_1 \geq d_2$ (car $d_1 \mid d_2$ et $d_2 \mid d_1$) donc on a $d_1 = d_2$.
On a prouvé l'unicité du pgcd par disjonction de cas.

Montrons à présent l'existence du pgcd.
On remarque que si $\text{pgcd}(a, b)$ existe alors $\text{pgcd}(b, a)$ aussi et $\text{pgcd}(a, b) = \text{pgcd}(b, a)$ (cf. la définition du pgcd (cf signifie confer c'est-à-dire allez voir)).
On peut donc supposer $b \geq a$ (quitte à échanger a et b).
Si $a = 0$ alors $b \mid a$ et $b \mid b$ et si $c \mid a$ et $c \mid b$ alors $c \mid b$ donc $b = \text{pgcd}(a, b)$.
Sinon, effectuons la division euclidienne de b par a : soient $q_0, r_0 \in \mathbb{N}$ tels que $b = q_0 a + r_0$ et $0 \leq r_0 < a$. Montrons que si $\text{pgcd}(r_0, a)$ existe alors $\text{pgcd}(a, b)$ existe et $\text{pgcd}(r_0, a) = \text{pgcd}(a, b)$.
$\text{pgcd}(r_0, a)$ divise r_0 et a donc divise $b = q_0 a + r_0$ et a.
Si c divise a et b alors c divise $r_0 = b - q_0 a$ et a donc divise $\text{pgcd}(r_0, a)$.
Ainsi $\text{pgcd}(r_0, a) = \text{pgcd}(a, b)$.
Le raisonnement qu'on a mené sur a et b peut être mené sur r_0 et a :
Si $r_0 = 0$ alors $a = \text{pgcd}(r_0, a) = \text{pgcd}(a, b)$.
Sinon on effectue la division euclidienne de a par r_0 : on a $q_1, r_1 \in \mathbb{N}$ tels que $a = q_1 r_0 + r_1$ et $0 \leq r_1 < r_0$; on a que si $\text{pgcd}(r_1, r_0)$ existe alors $\text{pgcd}(r_0, a)$ et $\text{pgcd}(a, b)$ existent et $\text{pgcd}(r_1, r_0) = \text{pgcd}(r_0, a) = \text{pgcd}(a, b)$.
Montrons par récurrence qu'on peut construire une suite (q_n, r_n) telle que pour tout $n \geq 1$ si $r_n \neq 0$ on a $r_{n-1} = q_{n+1} r_n + r_{n+1}$ et $r_{n+1} < r_n$, si $r_n = 0$ on a $q_{n+1} = 0$ et $r_{n+1} = 0$.
On a déjà construit (q_0, r_0) et (q_1, r_1).
Si on a déjà construit $(q_0, r_0), \ldots, (q_n, r_n)$ alors on construit (q_{n+1}, r_{n+1}) comme suit : si $r_n = 0$ alors on pose $q_{n+1} = 0$ et $r_{n+1} = 0$, sinon on effectue la divi-

sion euclidienne de r_{n-1} par r_n : il existe un unique couple d'entiers naturels (q_{n+1}, r_{n+1}) tel que $r_{n-1} = q_{n+1}r_n + r_{n+1}$ et $r_{n+1} < r_n$.
En appliquant le lemme montré plus haut à l'ensemble des r_n non nuls (qui est non vide car on a supposé que r_0 est non nul) on obtient qu'il existe $m \in \mathbb{N}$ tel que r_m est non nul et pour tout r_n non nul, $r_m < r_n$. r_{m+1} est donc nul (car avec la construction faite plus haut si r_{m+1} est non nul alors $r_{m+1} < r_m$ ce qui contredit $r_m < r_{m+1}$).
En faisant les mêmes raisonnements que plus haut, on a que si r_m existe alors $r_m = \text{pgcd}(r_{m+1}, r_m) = \text{pgcd}(r_m, r_{m-1}) = \cdots = \text{pgcd}(r_1, r_0) = \text{pgcd}(r_0, a) = \text{pgcd}(a, b)$. Or r_m existe donc $\text{pgcd}(a, b)$ existe.

Déf : Soit $n \in \mathbb{N} \setminus \{0, 1\}$. Soient $a_1, \ldots, a_n \in \mathbb{N}$. Le plus grand commun diviseur de $a_1, \ldots, a_n$, noté $\text{pgcd}(a_1, \ldots, a_n)$, est l'entier $d \in \mathbb{N}$ qui vérifie $d \mid a_1$, ..., $d \mid a_n$ et si $c \mid a_1$, ..., $c \mid a_n$ alors $c \mid d$.

Exercice : Montrer que cette définition est correcte.
Pour l'existence pour $n > 2$ on pourra vérifier que $\text{pgcd}(\text{pgcd}(a_1, ..., a_{n-1}), a_n)$ vérifie les hypothèses de $\text{pgcd}(a_1, ..., a_n)$.

Démontrons à présent une proposition bien utile.

Prop : Soient $a, b \in \mathbb{N}$. Soit $c \in \mathbb{N} \setminus \{0\}$. $\text{pgcd}(ca, cb) = c\ \text{pgcd}(a, b)$.

Dém : Notons $d = \text{pgcd}(a, b)$. $d \mid a$ et $d \mid b$ donc $cd \mid ca$ et $cd \mid cb$.
Ainsi, $cd \mid \text{pgcd}(ca, cb)$. $c \mid ca$ et $c \mid cb$ donc $c \mid \text{pgcd}(ca, cb)$. Soit $e \in \mathbb{N}$ tel que $\text{pgcd}(ca, cb) = ce$.
Soient $a', b' \in \mathbb{N}$ tels que $ca = \text{pgcd}(ca, cb)a'$ et $cb = \text{pgcd}(ca, cb)b'$.
$ca = cea'$ et $cb = ceb'$. En simplifiant on a :
$a = ea'$ et $b = eb'$ donc e divise a et b donc e divise $d = \text{pgcd}(a, b)$.
Ainsi $\text{pgcd}(ca, cb) = ce \mid cd$ or on avait $cd \mid \text{pgcd}(ca, cb)$ d'où l'égalité.

Définissons à présent le plus petit commun multiple de deux entiers.

Déf : Le plus petit commun multiple de $a \in \mathbb{N}$ et de $b \in \mathbb{N}$, noté $\text{ppcm}(a, b)$, est l'entier $m \in \mathbb{N}$ qui vérifie $a \mid m$, $b \mid m$ et si $a \mid c$ et $b \mid c$ alors $m \mid c$.

Montrons que cette définition est correcte.

Commençons par l'unicité :
Si m_1 et m_2 vérifient les propriétés de ppcm de a et de b alors, comme $a \mid m_1$ et $b \mid m_1$ on a $m_2 \mid m_1$ et comme $a \mid m_2$ et $b \mid m_2$ on a $m_1 \mid m_2$.
Si $m_1 = 0$ alors comme $m_1 \mid m_2$ on a $m_2 = 0$. De même, si $m_2 = 0$ alors $m_1 = 0$.
Si $m_1 \neq 0$ et $m_2 \neq 0$ alors on a $m_1 \leq m_2$ et $m_1 \geq m_2$ (car $m_1 \mid m_2$ et $m_2 \mid m_1$) donc on a $m_1 = m_2$.
On a prouvé l'unicité du ppcm par disjonction de cas.

Montrons à présent l'existence du ppcm.
Si $a = 0$ alors $a \mid a$, $b \mid a$ et si $a \mid c$ et $b \mid c$ alors $a \mid c$, donc $a = \text{ppcm}(a, b)$.
Sinon :
$\text{pgcd}(a, b) \mid a$ donc il existe $c \in \mathbb{N}$ tel que $a = c\ \text{pgcd}(a, b)$.
$\text{pgcd}(a, b) \mid b$ donc il existe $d \in \mathbb{N}$ tel que $b = d\ \text{pgcd}(a, b)$.
$cb = cd\ \text{pgcd}(a, b) = ad$ donc cb est un multiple de b et est un multiple de a.
Si $a \mid e$ et $b \mid e$ alors $cb \mid ce$ et $cb = da \mid de$ donc :
$cb \mid \text{pgcd}(ce, de) = e\ \text{pgcd}(c, d) = e$ car $\text{pgcd}(c, d) = 1$ car $\text{pgcd}(a, b) = \text{pgcd}(c\text{pgcd}(a, b), d\text{pgcd}(a, b)) = \text{pgcd}(a, b)\ \text{pgcd}(c, d)$ donc $\text{pgcd}(c, d) = 0$ ou 1 et $\text{pgcd}(c, d) \neq 0$ car $c \neq 0$ (car $a \neq 0$).
On a donc $cb = \text{ppcm}(a, b)$.

Remarque : On a montré que $\text{ppcm}(a, b) = \frac{ab}{\text{pgcd}(a,b)}$.

Déf : Soit $n \in \mathbb{N} \setminus \{0, 1\}$. Soient $a_1, \ldots, a_n \in \mathbb{N}$. Le plus petit commun multiple de $a_1, \ldots, a_n$, noté $\text{ppcm}(a_1, \ldots, a_n)$, est l'entier $m \in \mathbb{N}$ qui vérifie $a_1 \mid m$, ..., $a_n \mid m$ et si $a_1 \mid c$, ..., $a_n \mid c$ alors $m \mid c$.

Exercice : Montrer que cette définition est correcte.
Pour l'existence pour $n > 2$ on pourra vérifier que $\text{ppcm}(\text{ppcm}(a_1, ..., a_{n-1}), a_n)$ vérifie les hypothèses de $\text{ppcm}(a_1, ..., a_n)$.

Démontrons une proposition analogue à celle démontrée plus haut.

Prop : Soient $a, b \in \mathbb{N}$. Soit $c \in \mathbb{N} \setminus \{0\}$. $\text{ppcm}(ca, cb) = c\ \text{ppcm}(a, b)$.

Dém : $\text{ppcm}(ca, cb) = \frac{cacb}{\text{pgcd}(ca,cb)} = \frac{cacb}{c\text{pgcd}(a,b)} = c\frac{ab}{\text{pgcd}(a,b)} = c\text{ppcm}(a, b)$.

II) Lemme de Gauss et théorème d'unicité de la décomposition en facteurs premiers.

Déf : Soit $n \in \mathbb{N} \setminus \{0, 1\}$. On dit que $a_1, \ldots, a_n$ sont premiers entre eux si $\text{pgcd}(a_1, \ldots, a_n) = 1$.

Démontrons le lemme de Gauss (mathématicien de la première moitié du XIXe siècle) puis deux autres lemmes qui en découlent.

Lemme de Gauss : Si a et b sont premiers entre eux et si $a|bc$ alors $a|c$.

Dém : $a \mid ac$ et $a \mid bc$ donc $a \mid \text{pgcd}(ac, bc) = \text{pgcd}(a, b)c = c$ car $\text{pgcd}(a, b) = 1$.

Lemme : Si a et b sont premiers entre eux tels que $a|c$ et $b|c$ alors $ab|c$.

Dém : $b \mid c$ donc il existe $d \in \mathbb{N}$ tel que $c = bd$. $a \mid c = bd$ et a et b sont premiers entre eux donc, avec le lemme précédent, $a \mid d$ donc il existe $e \in \mathbb{N}$ tel que $d = ae$ donc $c = bd = bae = abe$ donc $ab \mid c$.

Lemme : Soit p un nombre premier. Soit $n \in \mathbb{N}\setminus\{0\}$. Soient $a_1, \ldots, a_n \in \mathbb{N}$. Si $p \mid a_1 \times \cdots \times a_n$ alors $p \mid a_1$ ou ... ou $p \mid a_n$.

Exercice : Démontrer ce lemme en utilisant le lemme de Gauss et le fait que si p est un nombre premier et $c \in \mathbb{N}$ alors $\text{pgcd}(p, c) = 1$ ou p (cette dernière affirmation se démontre aisément avec la définition de nombre premier (cf. l'article 2)).

Notation : On note $\min(x_1, \ldots, x_n)$ le minimum des entiers $x_1, \ldots, x_n$, c'est-à-dire le plus petit d'entre eux. On note $\max(x_1, \ldots, x_n)$ le maximum des entiers $x_1, \ldots, x_n$, c'est-à-dire le plus grand d'entre eux.

Dans l'article 2 on avait montré l'existence de la décomposition en facteurs premiers ; montrons-en à présent l'unicité.

Thm : Soient $m, n \in \mathbb{N} \setminus \{0\}$. Soient $p_1 \leq \cdots \leq p_m$, $q_1 \leq \cdots \leq q_n$ des nombres premiers. Si $p_1 \times \cdots \times p_m = q_1 \times \cdots \times q_n$ alors $m = n$, $p_1 = q_1, \ldots, p_m = q_m$. C'est l'unicité de la décomposition en facteurs pre-

miers.

Dém : Raisonnons par récurrence sur $\max(m,n)$.

Si $\max(m,n)=1$ alors on a $m=1$ et $n=1$ donc $m=n$ et $p_1=q_1$.

Supposons le résultat établi pour k.
Soient $m,n\in\mathbb{N}\setminus\{0\}$ tels que $\max(m,n)=k+1$.
Si $p_1<q_1$ alors $p_1\notin\{q_1,\dots,q_n\}$ or $p_1\mid q_1\times\cdots\times q_n$ donc avec le lemme précédent $p_1\mid q_1$ ou ... ou $p_1\mid q_n$ (car p_1 premier) donc $p_1=q_1$ ou ... ou $p_1=q_n$ (car $q_1,\dots,q_n$ premiers et $p_1\neq 1$) ce qui contredit $p_1\notin\{q_1,\dots,q_n\}$. (En d'autres mots, $p_1<q_1$ implique $p_1\notin\{q_1,\dots,q_n\}$ et $p_1\in\{q_1,\dots,q_n\}$ proposition toujours fausse, d'où $p_1\geq q_1$)
Si $q_1<p_1$ alors $q_1\notin\{p_1,\dots,p_m\}$ or $q_1\mid p_1\times\cdots\times p_m$ donc avec le lemme précédent $q_1\mid p_1$ ou ... ou $q_1\mid p_m$ (car q_1 premier) donc $q_1=p_1$ ou ... ou $q_1=p_m$ (car $p_1,\dots,p_m$ premiers et $q_1\neq 1$) ce qui contredit $q_1\notin\{p_1,\dots,p_m\}$. Ainsi $p_1=q_1$. On a donc $p_2\times\cdots\times p_m=q_2\times\cdots\times q_n$ donc, comme à gauche on a $m-1$ termes et à droite $n-1$ termes et que $\max(m-1,n-1)=\max(m,n)-1=k$, par hypothèse de récurrence $m=n$ et $p_2=q_2$, ..., $p_m=q_m$.

Notation : Si $x\in\mathbb{R}$ et $n\in\mathbb{N}\setminus\{0\}$ on note $x^n=x\times\cdots\times x$ n fois ($x^1=x, x^2=x\times x, x^3=x\times x\times x$ etc). Si $x\in\mathbb{R}$ on note $x^0=1$.
x^n se prononce "x puissance n"(et on dit souvent "x au carré "plutôt que "x puissance 2"et "x au cube "plutôt que "x puissance 3").

Puisqu'on a établi l'unicité de la décomposition en facteurs premiers, on peut définir correctement la valuation p-adique d'un entier naturel non nul :

Déf : Soit p un nombre premier. Soit $n\in\mathbb{N}\setminus\{0,1\}$. La valuation p-adique de n est la puissance à laquelle apparaît p dans la décomposition en facteurs premiers de n, c'est-à-dire que si $n=p_1^{a_1}\times\cdots\times p_m^{a_m}$ avec $p_1,\dots,p_m$ des nombres premiers distincts (c'est-à-dire tous différents les uns des autres), alors si $p=p_i$ la valuation p-adique de n est a_i et si $p\notin\{p_1,\dots,p_m\}$ (c'est-à-dire p différent de tous les p_i) alors la valuation p-adique de n est nulle (car $p^0=1$). La valuation p-adique de 1 est nulle. La valuation p-adique de n est notée $v_p(n)$.

Exemples : $v_2(2) = 1$ et pour tout p premier différent de $2, v_2(p) = 0$.
$12 = 2^2 \times 3$ donc $v_2(12) = 2, v_3(12) = 1$ et pour tout p premier différent de 2 et de 3, $v_p(12) = 0$.

Remarque : Si pour tous les nombres premiers p $v_p(n) = v_p(m)$ alors $n = m$ (cf. la décomposition en facteurs premiers).

Prop : Soient $a, b \in \mathbb{N} \setminus \{0\}$. Soit p premier. $v_p(ab) = v_p(a) + v_p(b)$.

Dém : Si $a = 1$ alors $v_p(a) = 0$ et on a bien $v_p(ab) = v_p(b) = v_p(a) + v_p(b)$.
Si $b = 1$ alors $v_p(b) = 0$ et on a bien $v_p(ab) = v_p(a) = v_p(a) + v_p(b)$.
Si $a \neq 1$ et $b \neq 1$, on les décompose en facteurs premiers :
$a = p_1^{v_{p_1}(a)} \times \cdots \times p_m^{v_{p_m}(a)}$ et $b = p_1^{v_{p_1}(b)} \times \cdots \times p_m^{v_{p_m}(b)}$ (les valuations p-adiques peuvent être nulles parce qu'on a mis tous les facteurs premiers de a et de b)
$ab = p_1^{v_{p_1}(a)} \times p_1^{v_{p_1}(b)} \times \cdots \times p_m^{v_{p_m}(a)} \times p_m^{v_{p_m}(b)} = p_1^{v_{p_1}(a)+v_{p_1}(b)} \times \cdots \times p_m^{v_{p_m}(a)+v_{p_m}(b)}$
donc $v_{p_1}(ab) = v_{p_1}(a) + v_{p_1}(b), \ldots, v_{p_m}(ab) = v_{p_m}(a) + v_{p_m}(b)$, et pour tout p premier qui n'appartient pas à $\{p_1, \ldots, p_m\}$ on a : $v_p(ab) = 0 = 0 + 0 = v_p(a) + v_p(b)$.

Prop : Soient $a, b \in \mathbb{N} \setminus \{0\}$. $a \mid b$ si et seulement si pour tout nombre premier p $v_p(a) \leq v_p(b)$.

Dém : Supposons que $a \mid b$.
Il existe $c \in \mathbb{N} \setminus \{0\}$ tel que $b = ac$. Soit p premier.
D'après la proposition précédente, $v_p(b) = v_p(a) + v_p(c) \geq v_p(a)$ (car $v_p(c) \in \mathbb{N}$ (cf. la définition de la valuation p-adique) donc $v_p(c) \geq 0$).
Supposons que pour tout nombre premier p $v_p(a) \leq v_p(b)$.
Si $a = b$ on a bien $a \mid b$. Sinon :
Soient $p_1, \ldots, p_m$ les nombres premiers p tels que $v_p(a) < v_p(b)$ (il n'y en a qu'un nombre fini car $v_p(a) \neq 0$ ou $v_p(b) \neq 0$ que pour un nombre fini de p)

$$b = a \times p_1^{v_{p_1}(b)-v_{p_1}(a)} \times \cdots \times p_m^{v_{p_m}(b)-v_{p_m}(a)}$$

(cf. les décompositions en facteurs premiers de a et de b)
donc $a \mid b$.

Prop : Soient $x_1, \ldots, x_n \in \mathbb{N}$. Soit p premier. $v_p(\text{pgcd}(x_1, \ldots, x_n)) = \min(v_p(x_1), \ldots, v_p(x_n))$.

Dém : Soit d le nombre tel que pour tout p premier $v_p(d) = \min(v_p(x_1), \ldots, v_p(x_n))$ (un tel nombre existe car il n'y a qu'un nombre fini de p pour lesquels $v_p(x_1) \neq 0$ et si $v_p(x_1) = 0$ alors $\min(v_p(x_1), \ldots, v_p(x_n)) = 0$). D'après la proposition précédente, $d \mid x_1, \ldots, d \mid x_n$.
Soit c tel que $c \mid x_1, \ldots, c \mid x_n$. D'après la proposition précédente, pour tout p premier : $v_p(c) \leq v_p(x_1), \ldots, v_p(c) \leq v_p(x_n)$ donc $v_p(c) \leq \min(v_p(x_1), \ldots, v_p(x_n)) = v_p(d)$.
D'après la proposition précédente, on a donc $c \mid d$.
d est donc le plus grand commun diviseur de $x_1, \ldots, x_n$.

Prop : Soient $x_1, \ldots, x_n \in \mathbb{N}$. Soit p premier. $v_p(\text{ppcm}(x_1, \ldots, x_n)) = \max(v_p(x_1), \ldots, v_p(x_n))$.

Dém : Soit m le nombre tel que pour tout p premier $v_p(m) = \max(v_p(x_1), \ldots, v_p(x_n))$ (un tel nombre existe car il n'y a qu'un nombre fini de p pour lesquels $v_p(x_1) \neq 0$ ou ... ou $v_p(x_n) \neq 0$ et si $v_p(x_1) = 0, \ldots, v_p(x_n) = 0$ alors $\max(v_p(x_1), \ldots, v_p(x_n)) = 0$). D'après une proposition plus haut, $x_1 \mid m, \ldots, x_n \mid m$.
Soit c tel que $x_1 \mid c, \ldots, x_n \mid c$. D'après une proposition plus haut, pour tout p premier : $v_p(x_1) \leq v_p(c), \ldots, v_p(x_n) \leq v_p(c)$ donc $v_p(c) \geq \max(v_p(x_1), \ldots, v_p(x_n)) = v_p(m)$.
D'après une proposition plus haut, on a donc $m \mid c$.
m est donc le plus petit commun multiple de $x_1, \ldots, x_n$.

Prop : Soient $x_1, \ldots, x_n, a_1, \ldots, a_n \in \mathbb{N}$. Si $\text{pgcd}(x_1, \ldots, x_n) = 1$ alors $\text{pgcd}(x_1^{a_1}, \ldots, x_n^{a_n}) = 1$.

Dém : D'après la remarque plus haut, il suffit de montrer que pour tout nombre premier p, $v_p(\text{pgcd}(x_1^{a_1}, \ldots, x_n^{a_n})) = 0$.
Soit p un nombre premier. D'après une proposition plus haut :
$v_p(\text{pgcd}(x_1^{a_1}, \ldots, x_n^{a_n}))) = \min(v_p(x_1^{a_1}), \ldots, v_p(x_n^{a_n})) = \min(a_1 v_p(x_1), \ldots, a_n v_p(x_n))$
(cf. la définition de puissance et la proposition plus haut selon laquelle la valuation p-adique d'un produit est la somme des valuations p-adiques)
or $0 = v_p(1) = v_p(\text{pgcd}(x_1, \ldots, x_n)) = \min(v_p(x_1), \ldots, v_p(x_n))$ donc il existe $i \in \{1, \ldots, n\}$ tel que $v_p(x_i) = 0$ donc $a_i v_p(x_i) = 0$
donc $v_p(\text{pgcd}(x_1^{a_1}, \ldots, x_n^{a_n}))) = 0$.

III) Triplets pythagoriciens et cas $n = 3$ et $n = 4$ du grand théorème de Fermat.

En géométrie, le théorème de Pythagore stipule que si x, y, z sont les longueurs des côtés d'un triangle rectangle, avec z la longueur de l'hypoténuse, alors $x^2 + y^2 = z^2$ (voir l'article 7. Géométrie). La réciproque du théorème de Pythagore stipule que si x, y, z sont les longueurs des côtés d'un triangle et vérifient $x^2 + y^2 = z^2$ alors ce triangle est rectangle et son hypoténuse est le côté de longueur z. On peut se demander quels triplets d'entiers naturels non nuls (x, y, z) vérifient l'équation $x^2 + y^2 = z^2$ (ce qui revient à se demander quels sont les triangles rectangles dont les longueurs des côtés sont des entiers). On appelle de tels triplets des "triplets pythagoriciens".

Exo : Résolution de l'équation de Pythagore $x^2+y^2 = z^2$ avec $x, y, z \in \mathbb{N}\setminus\{0\}$.

1) Montrer que (x, y, z) est solution si et seulement si, en notant $d = \text{pgcd}(x, y, z)$, $(\frac{x}{d}, \frac{y}{d}, \frac{z}{d})$ est solution. Remarquer que $\text{pgcd}(\frac{x}{d}, \frac{y}{d}, \frac{z}{d}) = 1$.

2) Soit (x, y, z) une solution de pgcd 1. Déterminer le reste dans la division euclidienne de z^2 par 4 (en considérant les différentes possibilités pour ceux de x^2 et y^2) et en déduire que z est impair, x ou y est pair et l'autre est impair.

3) Soit (x, y, z) une solution de pgcd 1. Si x est pair et y est impair, montrer que $\text{pgcd}(\frac{z-y}{2}, \frac{z+y}{2}) = 1$. En déduire, puisque $(z-y)(z+y) = z^2-y^2 = x^2$, que $\frac{z-y}{2}$ et $\frac{z+y}{2}$ sont des carrés d'entiers, puis une expression de x, y et z.

4) Donner toutes les solutions de l'équation $x^2 + y^2 = z^2$ dans $\mathbb{N} \setminus \{0\}$.

Cet exercice et les suivants seront corrigés dans l'article 5 bis. Si vous bloquez sur une question n'hésitez pas à la sauter pour faire les autres questions (quitte à réessayer plus tard, souvent la nuit porte conseil).

Remarque : Si $x, y, z \in \mathbb{Z} \setminus \{0\}$ vérifient $x^2+y^2 = z^2$, en remplaçant x par $-x$ ou y par $-y$ ou z par $-z$ on a encore $x^2+y^2 = z^2$ et $x, y, z \in \mathbb{Z} \setminus \{0\}$. En changeant les signes qu'il faut, on se ramène à $x, y, z \in \mathbb{N} \setminus \{0\}$, et l'exercice précédent nous donne donc tous les $x, y, z \in \mathbb{Z} \setminus \{0\}$ qui vérifient $x^2+y^2 = z^2$ en changeant des signes (explicitez ces solutions).

Une question que l'on peut naturellement se poser est de savoir s'il existe $x, y, z \in \mathbb{Z} \setminus \{0\}$ tels que $x^3 + y^3 = z^3$ ou $x^4 + y^4 = z^4$ etc. Pierre de Fermat (1601-1665) a énoncé la conjecture suivante (appelée grand théorème de Fermat ou dernier théorème de Fermat) : pour tout $n \geq 3$, il n'existe pas $x, y, z \in \mathbb{Z} \setminus \{0\}$ tels que $x^n + y^n = z^n$. Andrew Wiles (1953-) l'a démontrée en 1995 grâce à des mathématiques très sophistiquées (le documentaire [Fermat's Last Theorem](http ://topdocumentaryfilms.com/fermats-last-theorem/) présente l'aventure de la preuve au grand public). Les cas $n = 3$ et $n = 4$ sont faciles à montrer et font l'objet des exercices suivants. Ensuite il suffit de montrer le résultat pour $n \geq 5$ premier (prouvez-le ! ce sera corrigé dans l'article 5 bis, tout comme les exercices suivants), c'est ce qu'a fait Wiles (je dis "il suffit"mais c'est très difficile (sinon le grand théorème de Fermat n'aurait pas attendu plus de 300 ans avant d'être prouvé)).

Pour le cas $n = 4$ on montre même qu'il n'y a pas de solution dans $\mathbb{Z} \setminus \{0\}$ à $x^4 + y^4 = z^2$ (ce qui implique le cas $n = 4$ en prenant z un carré d'entier).

Il suffit de montrer qu'il n'y a pas de solution dans $\mathbb{N} \setminus \{0\}$ car les exposants (4,4 et 2) sont pairs (c'est-à-dire divisibles par 2 ; comme dans la remarque plus haut, on peut changer les signes de x, y, z pour avoir des entiers positifs).

Exo : Il n'y a pas de solution dans $\mathbb{N} \setminus \{0\}$ à $x^4 + y^4 = z^2$.

1) Se ramener à x, y, z de pgcd 1.

Indication : en notant d le pgcd de x, y, z, montrer que $\frac{x}{d}, \frac{y}{d}, \frac{z}{d^2}$ sont de pgcd 1.

2) Vérifier que si x, y, z est solution de $x^4 + y^4 = z^2$ et de pgcd 1 alors (x^2, y^2, z) est un triplet pythagoricien et en déduire qu'il existe $u, v \in \mathbb{N} \setminus \{0\}$ de pgcd 1 tels que $x^2 = 2uv, y^2 = u^2 - v^2$ et $z = u^2 + v^2$ (quitte à échanger x et y).

Indication : dans la preuve de l'exercice sur les triplets pythagoriciens, vous devriez avoir trouvé de tels u, v mais sans avoir prouvé qu'ils sont de pgcd 1 ; en revanche vous devriez avoir prouvé que $u^2 = \frac{z-y}{2}$, $v^2 = \frac{z+y}{2}$ et $\text{pgcd}(\frac{z-y}{2}, \frac{z+y}{2}) = 1$, et vous devriez pouvoir en déduire que $\text{pgcd}(u, v) = 1$.

3) Montrer que u est impair et que v est pair puis en déduire que u est un carré d'entier et que v est le produit de 2 et d'un carré d'entier.

4) Vérifier que (v, y, u) est un triplet pythagoricien de pgcd 1 et, en utilisant les questions précédentes, en déduire qu'il existe $x', y', z' \in \mathbb{N} \setminus \{0\}$ tels que $x'^4 + y'^4 = z'^2$ et $z' < z$.

5) Utiliser le fait que toute partie non vide de $\mathbb{N}$ admet un plus petit élément pour conclure.

Prop : Il n'y a pas de solution dans $\mathbb{Z} \setminus \{0\}$ à $x^3 + y^3 = z^3$.

Je connais deux preuves de cette proposition ; l'une n'utilise que des outils arithmétiques mais est assez fastidieuse (voir :
http ://fermatslasttheorem.blogspot.com/2005/05/fermats-last-theorem-proof-for-n3.html pour cette preuve) et l'autre utilise des nombres complexes ; cette dernière preuve sera faite dans l'article 19 Théorie des nombres.

Clémentine Lemarié–Rieusset