Chapitre 2

Réponse - Technique de preuve

2.1 Preuve : les bases

Ex. 1

a. Règle d'addition
b. Règle de simplification
c. Règle de simplification
d. Syllogisme disjonctif
e. Syllogisme disjonctif
f. Modus ponens
g. Modus tollens
h. Nier l'hypothèse.
i. Affirmer la conclusion.
j. Syllogisme par hypothèse.

Ex. 2

a. Modus ponens
b. Modus tollens
c. Affirmer la conclusion
d. Syllogisme par hypothèse
e. Raisonnement circulaire
f. Affirmer la conclusion
g. Nier l'hypothèse
h. Modus ponens

Ex. 3

Nous allons utiliser les propostions suivantes :

—P : il pleut

—M : le sol est mouillé

—N : il y a des nuages

Nous avons donc (en évitant les si...alors...) :
Preuve : (résolution/réfutation)

$$\begin{array}{r} P \vee N \\ \neg N \vee M \\ \neg M \vee P \\ \neg P \end{array}$$

On peut donc ajouter (en ordre) :

$\neg M$

$\neg N$

P

↯■

Ex. 4

a. Faux, certaines droites de la forme $Ax+By=C$, $A, B, C \in \mathbb{N}$ ne sont pas des fonctions.
Preuve : (contre-exemple)
Si on considère la droite $3x+0y=6$, on obtient une droite verticale en $x=2$ qui n'est pas une fonction.
■
b. Faux, certain(s) nombre(s) premier(s) sont pair(s).
Preuve : (contre-exemple)
2 est un nombre pair et est premier.
■
c. Vrai, Si un triangle a 4 côtés, alors la somme des angles de ce triangle est 180°.
Preuve : (vide)
Un triangle n'a pas 4 côtés, par définition.
■

d. Faux, on a :

$$\begin{aligned}
&\neg\forall x \in \mathbb{N}, (\exists y \in \mathbb{Q}, 6x \times y = 1)\\
&\exists x \in \mathbb{N}, \neg(\exists y \in \mathbb{Q}, x \times y = 1)\\
&\exists x \in \mathbb{N}, \forall y \in \mathbb{Q}, \neg(x \times y = 1)\\
&\exists x \in \mathbb{N}, \forall y \in \mathbb{Q}, x \times y \neq 1
\end{aligned}$$

Preuve : (contre-exemple)
Supposons que $x = 0$, alors $0 \times y = 1$ est fausse pour tout y. ∎

e. Faux, $\exists A, B, AB = BA$.
Preuve : (contre-exemple)
Soit $A = [2]$ et $B = [3]$, on a $AB = BA = [6]$. ∎

f. Faux, $\exists x, y, PPCM(x, y) \neq x \times y$.
Preuve : (contre-exemple)
Supposons que $x = 4$ et $y = 6$. Alors, $PPCM(4, 6) = 12 \neq 4 \times 6 = 24$.
∎

g. Faux, $\exists x, y, PPCM(x, y) = x \times y$.
Preuve : (contre-exemple)
Supposons que $x = 3$ et $y = 5$. Alors, $PPCM(3, 5) = 15 = 3 \times 5$.
∎

h. Vraie, si $n \in \mathbb{N}, n = 2x + 3$, alors $n^2 + 2n \geq 0$.
Preuve : (triviale)

$$\begin{aligned}
n^2 + 2n &\geq n^2 && (n \geq 0)\\
n^2 &\geq 0
\end{aligned}$$

∎

i. Faux, il y a des nombres premiers qui sont la somme de deux carrés.
Preuve : (contre-exemple)
Il y a plusieurs exemples :

$$\begin{aligned}
5 &= 4 + 1\\
13 &= 9 + 4\\
17 &= 16 + 1\\
29 &= 25 + 4\\
37 &= 36 + 1
\end{aligned}$$

∎

j. Faux, Certain nombres qui terminent par 5 sont premiers.
Preuve : (contre-exemple)
5 est un nombre premier qui se termine par 5.
∎

k. Faux, Certains nombres de la forme $n = 2^p - 1$, où p est premier, sont composés.
Preuve : (contre-exemple)
Considérons $n = 2^{11} - 1 = 2047$. Or, $2047 = 23 \times 89$ et n'est pas premier.
∎

l. Vraie, si x est positif et négatif, alors $x^3 - 2x^2 + 8x = 0$
Preuve : (vide)
Il n'y a aucun x qui soit positif et négatif.
∎

2.2 Preuve directe-indirecte-contradiction

Ex. 5

a. Si n est pair, alors n^2 est pair.
Preuve : (directe)
Supposons que $n = 2k, k \in \mathbb{N}$ (n est pair). Alors :

$$\begin{aligned}
n &= 2k\\
n^2 &= (2k)^2\\
n^2 &= 4k^2\\
n^2 &= 2(2k^2), n^2 \text{ est pair.}
\end{aligned}$$

∎

b. Si n^2 est pair, alors n est pair.
Preuve : (indirecte, contraposée)
Supposons que $n = 2k + 1, k \in \mathbb{N}$ (n est impair). Alors :

$$\begin{aligned}
n &= 2k + 1\\
n^2 &= (2k + 1)^2\\
n^2 &= 4k^2 + 4k + 1\\
n^2 &= 2(2k^2 + 2k) + 1, n^2 \text{ est impair.}
\end{aligned}$$

∎

c. Démontrer que 99!100! est un carré parfait.
Preuve : (directe)
Si $n = 99!100!$ alors $\sqrt{n} \in \mathbb{N}$.

$$\begin{aligned}
n &= 99!100!\\
&= 99!100 \cdot 99!\\
&= 99!99! \cdot 10 \cdot 10\\
&= (99!10) \cdot (99!10)\\
&= (99!10)^2
\end{aligned}$$

Donc $\sqrt{n} = 99!100! \in \mathbb{N}$. ∎

d. Si $\sqrt{n} \notin \mathbb{N}$ alors n n'est pas un carré parfait.
Preuve : (contraposée)

Si n est un carré parfait alors $\sqrt{n} \in \mathbb{N}$.
Soit n un carré parfait. Donc, $\exists p \in \mathbb{N}, n = p^2$. On a donc :

$$\begin{aligned}\sqrt{n} &= \sqrt{p^2}\\ &= p\end{aligned}$$

■

e. Si un ensemble S admet une borne supérieure m alors tous les éléments de S sont inférieurs ou égal M.
Preuve : (contraposée)
Si certains éléments de S sont supérieur à m alors m n'Est pas une borne supérieure de S.
Supposons que $s \in S$ est telle que $s > m$. Donc m n'est pas une borne supérieure de S. ■

f. Si n_1 et n_2 sont impairs, alors $n_1 + n_2$ est pair.
Preuve : (directe)
Soit $n_1 = 2k+1, k \in \mathbb{Z}$ et $n_2 = 2l+1, l \in \mathbb{Z}$. Alors, $n_1 + n_2 = 2k+1+2l+1 = 2k+2l+2 = 2(k+l+1)$ qui est pair. ■

g. Soit $f(x) = ax+b, a \in \mathbb{R}^*, b, x_1, x_2 \in \mathbb{R}$. Si $x_1 \neq x_2$ alors $f(x_1) \neq f(x_2)$.
Preuve : (contraposée)
Soit $f(x) = ax+b, a \in \mathbb{R}^*, b, x_1, x_2 \in \mathbb{R}$. Si $f(x_1) = f(x_2)$ alors $x_1 = x_2$.
Supposons que :

$$\begin{aligned}f(x_1) &= f(x_2)\\ ax_1 + b &= ax_2 + b\\ ax_1 &= ax_2\\ x_1 &= x_2\end{aligned}$$

■

h. $n \geq 1 \wedge \exists k \in \mathbb{N}^* n = 2k \leftrightarrow \exists l \in \mathbb{N}^*, 7n+4 = 2k$.
Preuve : (bidirectionnelle)
$\rightarrow$: Si $n = 2k, k \in \mathbb{N}^*$ alors $\exists l \in \mathbb{N}^*, 7n+4 = 2l$.
Soit $n = 2k, k \in \mathbb{N}^*$, alors :

$$\begin{aligned}7n+4 &= 7(2k)+4\\ &= 14k+4\\ &= 2(7k+2), \text{ et } 7n+4 \text{ est pair. OK}\end{aligned}$$

. $\leftarrow$: Si $7n+4 = 2l, l \in \mathbb{N}^*$ alors $\exists k \in \mathbb{N}^*, n = 2k$.
Soit $7n+4 = 2l, l \in \mathbb{N}^*$, alors :

$$\begin{aligned}7n+4 &= 2l\\ 7n &= 2l-4\\ 7n &= 2(l-2)\end{aligned}$$

. Donc $7n$ est pair. Or 7 est impair et le produit de deux nombres impairs donnent un nombre impairs donc n est pair. ■

Ex. 6

a. $3 \mid (n_m n_{m-1} \ldots n_2 n_1 n_0)_2 \leftrightarrow 3 \mid \left(\sum_{\substack{k=0\\k=2s}}^{m} n_k - \sum_{\substack{k=1\\k=2s-1}}^{m} n_k \right)$.
Preuve : (direct double sens)
Soit $(n_m n_{m-1} \ldots n_2 n_1 n_0)_2$ un nombre en base 2. Alors on peut compter :

$$\begin{aligned}&(n_m n_{m-1} \ldots n_2 n_1 n_0)_2\\
&\equiv n_m \times 2^m + n_{m-1} \times 2^{m-1} + \ldots +\\
&\quad n_2 \times 2^2 + n_1 \times 2^1 + n_0 \times 2^0 \mod 3\\
&\equiv \sum_{\substack{k=0\\k=2s}}^{m} n_k 2^k + \sum_{\substack{k=1\\k=2s+1}}^{m} n_k 2^k \mod 3\\
&\equiv \sum_{\substack{k=0\\k=2s}}^{m} n_k 2^{2t} + \sum_{\substack{k=1\\k=2s+1}}^{m} n_k 2 \times 2^{2u} \mod 3\\
&\equiv \sum_{\substack{k=0\\k=2s}}^{m} n_k 4^t + \sum_{\substack{k=1\\k=2s+1}}^{m} n_k 2 \times 4^u \mod 3\\
&\equiv \sum_{\substack{k=0\\k=2s}}^{m} n_k 1^t + \sum_{\substack{k=1\\k=2s+1}}^{m} n_k 2 \times 1^u \mod 3\\
&\equiv \sum_{\substack{k=0\\k=2s}}^{m} n_k + \sum_{\substack{k=1\\k=2s+1}}^{m} n_k 2 \mod 3\\
&\equiv \sum_{\substack{k=0\\k=2s}}^{m} n_k + \sum_{\substack{k=1\\k=2s+1}}^{m} n_k (-1) \mod 3\\
&\equiv \sum_{\substack{k=0\\k=2s}}^{m} n_k - \sum_{\substack{k=1\\k=2s+1}}^{m} n_k \mod 3\end{aligned}$$

$\rightarrow$: Si $3 \mid n_2$ alors $n \mod 3 \equiv 0$ et $3 \mid \sum_{\substack{k=0\\k=2s}}^{m} n_k - \sum_{\substack{k=1\\k=2s+1}}^{m} n_k$ puisque c'est équivalent ($\mod 3$).
$\leftarrow$: Si $3 \mid \sum_{\substack{k=0\\k=2s}}^{m} n_k - \sum_{\substack{k=1\\k=2s+1}}^{m} n_k$ alors $3 \equiv 0 \mod 3$ et $3 \mid n$. ■

b. $9 \mid n \leftrightarrow 9 \mid s, s$ la somme des chiffres qui composent n.
Preuve : (bidirectionnelle)

Soit $n = n_m n_{m-1} ... n_2 n_1 n_0$ un nombre naturel. Alors :

$$\begin{aligned} n &\equiv r \mod 9 \\ n_m 10^m + ... + n_1 10^1 + n_0 10^0 &\equiv r \mod 9 \\ n_m 1^m + ... + n_1 1^1 + n_0 1^0 &\equiv r \mod 9 \\ n_m + n_{m-1} + ... + n_1 + n_0 &\equiv r \mod 9 \end{aligned}$$

$\Rightarrow$ (directe) Si $9 \mid n$, alors $r = 0$ dans l'équation précédente et $9 \mid n_m + n_{m-1} + ... + n_1 + n_0$.
$\Leftarrow$ (indirecte) Si $9 \nmid n_m + n_{m-1} + ... + n_1 + n_0$, alors $r \neq 0$ dans l'équation précédente et $9 \nmid n$.
■

c. Si $a = d \cdot q + r, 0 \leq r < |d|$, alors $PGCD(a, d) \mid r$.
Preuve : (directe)
Soit $a = d \cdot q + r, 0 \leq r < |d|$ et $PGCD(a, d) = p$. Nous avons selon ladéfinition du $PGCD$:

$$PGCD(a, d) \mid a \rightarrow \ \exists k \in \mathbb{Z}, a = kp$$
$$PGCD(a, d) \mid d \rightarrow \ \exists m \in \mathbb{Z}, d = mp$$

En remplaçant :

$$\begin{aligned} a &= d \cdot q + r \\ kp &= mp \cdot q + r \\ kp - mpq &= r \\ p(k - mq) &= r \text{ et } p \mid r. \end{aligned}$$

■

d. Démontrer que $\sum_{k=1}^{n} r^k = \frac{r^{n+1} - r}{r - 1}, r \in \mathbb{R}$.
Preuve : (directe)
Soit $S_n = \sum_{k=1}^{n} r^k$. Alors :

$$\begin{aligned} rS_n &= r \sum_{k=1}^{n} r^k \\ &= \sum_{k=1}^{n} r^{k+1} \\ &= \sum_{k=2}^{n+1} r^k \end{aligned}$$

Donc :

$$\begin{aligned} S_n - rS_n &= \sum_{k=1}^{n} r^k - \sum_{k=2}^{n+1} r^k \\ S_n(1 - r) &= r + \sum_{k=2}^{n} r^k - \sum_{k=2}^{n} r^k - r^{n+1} \\ S_n(1 - r) &= r - r^{n+1} \\ S_n &= \frac{r - r^{n+1}}{1 - r} \\ S_n &= \frac{r^{n+1} - r}{r - 1} \end{aligned}$$

■

e. Démontrer que $\sum_{k=1}^{n} r^k = \frac{r^{n+1} - r}{r - 1}, r \in \mathbb{R}$.
Preuve : (directe)
Soit $S_n = \sum_{k=1}^{n} r^k$. Alors :

$$\begin{aligned} rS_n &= r \sum_{k=1}^{n} r^k \\ &= \sum_{k=1}^{n} r^{k+1} \\ &= \sum_{k=2}^{n+1} r^k \end{aligned}$$

Donc :

$$\begin{aligned} S_n - rS_n &= \sum_{k=1}^{n} r^k - \sum_{k=2}^{n+1} r^k \\ S_n(1 - r) &= r + \sum_{k=2}^{n} r^k - \sum_{k=2}^{n} r^k - r^{n+1} \\ S_n(1 - r) &= r - r^{n+1} \\ S_n &= \frac{r - r^{n+1}}{1 - r} \\ S_n &= \frac{r^{n+1} - r}{r - 1} \end{aligned}$$

■

f. $9 \mid n \leftrightarrow 9 \mid s, s$ la somme des chiffres qui composent n.
Preuve : (bidirectionnelle)
Soit $n = n_m n_{m-1} ... n_2 n_1 n_0$ un nombre naturel. Alors :

$$\begin{aligned} n &\equiv r \mod 9 \\ n_m 10^m + n_{m-1} 10^{m-1} + ... + n_1 10^1 + n_0 10^0 &\equiv r \mod 9 \\ n_m 1^m + n_{m-1} 1^{m-1} + ... + n_1 1^1 + n_0 1^0 &\equiv r \mod 9 \\ n_m + n_{m-1} + ... + n_1 + n_0 &\equiv r \mod 9 \end{aligned}$$

$\Rightarrow$ (directe) Si $9 \mid n$, alors $r = 0$ dans l'équation précédente et $9 \mid n_m + n_{m-1} + ... + n_1 + n_0$.
$\Leftarrow$ (indirecte) Si $9 \not| \ n_m + n_{m-1} + ... + n_1 + n_0$, alors $r \neq 0$ dans l'équation précédente et $9 \not| \ n$.
■

Ex. 7

a. $log_2(10) \notin \mathbb{Q}$.
Preuve : (contradiction)

Supposons le contraire et que $log_2(10) \in \mathbb{Q}$.
Alors : $\exists p, q, PGCD(p,q) = 1, log_2(10) = \frac{p}{q}$.

$$\begin{aligned}\log_2(10) &= \frac{p}{q}\\ 2^{\frac{p}{q}} &= 10\\ \left(2^{\frac{p}{q}}\right)^q &= 10^q\\ 2^p &= 10^q\\ 2^p &= 2^q5^q, ↯\end{aligned}$$

La contradiction est l'unicité de la décomposition de nombre en facteur premier (théorème fondamental de l'arithmétique). ■

b. $\sqrt{2} \in \mathbb{Q}'$.
Preuve : (contradiction)
Supposons le contraire et que $\sqrt{2}\neg \in \mathbb{Q}', \sqrt{2} \in \mathbb{Q}$. Alors, $\exists p, q, PGCD(p,q) = 1$ tel que $\sqrt{2} = \frac{p}{q}$.

$$\begin{aligned}\sqrt{2} &= \frac{p}{q}\\ 2 &= \left(\frac{p}{q}\right)^2\\ 2 &= \frac{p^2}{q^2}\end{aligned}$$

$2q^2 = p^2, p^2$ est pair, et$p$ aussi,$\exists k, p = 2k$.

$$\begin{aligned}2q^2 &= (2k)^2\\ 2q^2 &= 4k\\ q^2 &= 2k, q^2 \text{ est pair,}\\ &PGCD(p,q) \geq 2, ↯(PGCD(p,q) = 1)\end{aligned}$$

■

c. Au moins un nombre d'une suite de nombre réels est plus grand ou égal à la moyenne de cette suite.
Preuve : (contradiction)
Supposons le contraire et que pour une suite de nombre n nombres $x_1, x_2, x_3, ..., x_n$, $\forall k, x_k < \overline{x}$. Nous savons que $\overline{x} = \frac{\sum_{k=1}^{n} x_k}{n}$.
On a donc : $\overline{x} = \frac{\sum_{k=1}^{n} x_k}{n} < \frac{\sum_{k=1}^{n} \overline{x}}{n} = \frac{n\overline{x}}{n} = \overline{x}↯$ ■

d. Si (a,b,c) est un triplet pythagoricien avec $PGCD(a,b) = 1$ alors $PGCD(a,c) = 1$ (et $PGCD(b,c) = 1$).
Preuve : (contradiction)
Supposons le contraire et (a,b,c) est un triplet pythagoricien, $PGCD(a,b) = 1$ mais $PGCD(a,c) = d > 1$. Donc, $\exists p, q, a = pd$ et $c = qd$. Or :

$$\begin{aligned}c^2 &= a^2 + b^2\\ c^2 - a^2 &= b^2\\ (qd)^2 - (pd)^2 &= b^2\\ q^2d^2 - p^2d^2 &= b^2\\ d^2(q^2 - p^2) &= b^2, donc d^2 \mid b^2, d \mid b, ↯\end{aligned}$$

La contradiction est que $PGCD(a,b) = 1$. Nous avons $d \mid b$ et $d \mid a$ (par hypothèse). Cela implique que $PGCD(a,b) \geq d > 1$.
■

Ex. 8

a. Si $\nexists k, n = 5k$ alors $(n \equiv 1 \mod 5 \vee n \equiv 4 \mod 5)$.
Preuve : (cas par cas)
Cas 1 $n = 5k + 1$:

$$\begin{aligned}n^2 &\equiv (5k+1)^2 \mod 5\\ &\equiv 25k^2 + 10k + 1 \mod 5\\ &\equiv 1 + 5(5k^2 + 2k) \mod 5\\ &\equiv 1 \mod 5, \text{OK.}\end{aligned}$$

Cas 2 $n = 5k + 2$:

$$\begin{aligned}n^2 &\equiv (5k+2)^2 \mod 5\\ &\equiv 25k^2 + 20k + 4 \mod 5\\ &\equiv 4 + 5(5k^2 + 4k) \mod 5\\ &\equiv 4 \mod 5, \text{OK.}\end{aligned}$$

Cas 3 $n = 5k + 3$:

$$\begin{aligned}n^2 &\equiv (5k+3)^2 \mod 5\\ &\equiv 25k^2 + 30k + 9 \mod 5\\ &\equiv 4 + 5(5k^2 + 6k + 1) \mod 5\\ &\equiv 4 \mod 5, \text{OK.}\end{aligned}$$

Cas 4 : $n = 5k + 4$:

$$\begin{aligned}n^2 &\equiv (5k+4)^2 \mod 5\\ &\equiv 25k^2 + 40k + 16 \mod 5\\ &\equiv 1 + 5(5k^2 + 8k + 3) \mod 5\\ &\equiv 1 \mod 5, \text{OK.}\end{aligned}$$

■

b. Si $a, b \in \mathbb{R}, |a| + |b| \geq |a + b|$.
Preuve : (cas par cas)

Soit $a, b \in \mathbb{R}$.
Cas 1 - a et b ont le même signe. Om a :$|a+b| = |a| + |b| \leq |a| + |b|$, OK.
Cas 2 - a et b n'ont pas le même signe. On a :$|a+b| = max(|a|,|b|) - min(|a|,|b|) \leq max(|a|,|b|) \leq |a| + |b|$, OK.
■

c. Si la somme des diviseurs de n est $n+1$ alors n est premier.
Preuve : (indirecte)
Supposons que n n'est pas premier, et prouvons que la somme de ses facteurs n'est pas $n+1$.
Cas 1 : $n = 1 : 1 \neq 1+1$, et la somme des diviseurs de n n'est pas $n+1$, OK.
Cas 2 : $n \neq 1 : 1 \mid n$ et $n \mid n$ et $\exists k \neq 0, k \mid n$.
Donc, la somme des facteurs est au moins de $n + 1 + k \neq n+1$, OK.
■

d. Si $n \in \mathbb{N}, (n^2 \mod 4 \equiv 0)$ ou $(n^2 = 1 \mod 4)$
Preuve : (()
cas par cas) Cas 1 : $n = 4k$

$$\begin{aligned} n^2 &\equiv (4k)^2 \mod 4 \\ &\equiv 16k^2 \mod 4 \\ &\equiv 4 \cdot 4k^2 \mod 4 \\ &\equiv 0k^2 \equiv \mod 4 \\ &\equiv 0 \equiv \mod 4, OK. \end{aligned}$$

Cas 2 : $n = 4k+1$

$$\begin{aligned} n^2 &\equiv (4k+1)^2 \mod 4 \\ &\equiv 16k^2 + 8k + 1 \mod 4 \\ &\equiv 4(4k^2 + 2k) + 1 \mod 4 \\ &\equiv 0(4k^2 + 2k) + 1 \equiv \mod 4 \\ &\equiv 1 \equiv \mod 4, OK. \end{aligned}$$

Cas 3 : $n = 4k+2$

$$\begin{aligned} n^2 &\equiv (4k+2)^2 \mod 4 \\ &\equiv 16k^2 + 16k + 4 \mod 4 \\ &\equiv 4(4k^2 + 4k + 1) \mod 4 \\ &\equiv 0(4k^2 + 4k + 1) \equiv \mod 4 \\ &\equiv 0 \equiv \mod 4, OK. \end{aligned}$$

Cas 4 : $n = 4k+3$

$$\begin{aligned} n^2 &\equiv (4k+3)^2 \mod 4 \\ &\equiv 16k^2 + 24k + 9 \mod 4 \\ &\equiv 4(4k^2 + 6k + 2) + 1 \mod 4 \\ &\equiv 0(4k^2 + 6k + 2) + 1 \equiv \mod 4 \\ &\equiv 1 \equiv \mod 4, OK. \end{aligned}$$

■

Ex. 9
Démontrer que dans un triplet pythagoricien primitif (a, b, c), a et b sont de parités différentes.
Preuve : (contradiction)
Soit $(a, b, c), PGCD(a, b) = 1, a^2 + b^2 + c^2$. Supposons que a et b sont de même parité.
Cas 1 : a, b sont pairs (preuve vide)
On a alors $PGCD(a, b) > 1$, OK.
Cas 2 : a, b sont impairs :

$$\begin{aligned} c^2 &= (2p+1)^2 + (2q+1)^2 \mod 4 \\ &= 4p^2 + 4p + 1 + 4q^2 + 4q + 1 \mod 4 \\ &= 4(p^2 + p + q^2 + q) + 2 \mod 4 \\ &= 0(p^2 + p + q^2 + q) + 2 \mod 4 \\ &= 2, ↯ \end{aligned}$$

Voir le numéro **??** **??** ■

a. Démontrer que dans un triplet pythagoricien primitif (a, b, c), c est impair.
Preuve : (directe)
Soit $(a, b, c), PGCD(a, b) = 1, a^2 + b^2 + c^2$. On sait que a, b sont de parités différentes (voir **??**). On peut supposer sans perdre de généralité que a est pair. On a donc $a = 2p, b = 2q + 1$.

$$\begin{aligned} c^2 &= a^2 + b^2 \\ &= (2p)^2 + (2q+1)^2 \\ &= 4p^2 + 4q^2 + 4q + 1 \\ &= 2(2p^2 + 2q^2 + 2q) + 1 \end{aligned}$$

■

Ex. 10 (a, b, c) est un triplet pythagoricien primitif si et seulement s'il existe $m, n \in \mathbb{N}^*, m > n, a = m^2 - n^2, b = 2mn, c = m^2 + n^2, PGCD(m, n) = 1$
Preuve : (bidirectionnelle)

$\Rightarrow$: Si (a, b, c) un triplet pythagoricien primitif, alors $\exists m, n \in \mathbb{N}^*, m > n, a = m^2 - n^2, b = 2mn, c = m^2 + n^2$, $PGCD(m, n) = 1$, m, n de parités différentes.

Soit $(a, b, c), a^2 + b^2 = c^2, PGCD(a, b) = 1$. On sait que a, b sont de parités différentes (voir **?? ??**). On peut supposer sans perdre de généralité que b est pair, $\exists p, b = 2p$ et qu'ainsi a, c sont impairs (voir **?? ??**).

On a donc :

$$\begin{aligned} c^2 &= a^2 + b^2 \\ c^2 - a^2 &= b^2 \\ (c + a)(c - a) &= b^2 \end{aligned}$$

On a que $c + a$ et $c - a$ sont pairs. Donc, $\exists q \in \mathbb{N}, c + a = 2q$ et $\exists r \in \mathbb{N}, c - a = 2r$. Nous avons donc :

$$2p = b$$
$$2q = c + a$$
$$2r = c - a$$

Puisque a, b, c sont relativement premiers, p, q, r sont relativement premiers (sinon, il serait possible de factoriser $2p + 2q = a + b + c$, pareil pour $2p + 2r = -a + b + c$).

On obtient en additionnant :

$$\begin{aligned} c + a + c - a &= 2q + 2r \\ 2c &= 2(q + r) \\ c &= q + r \end{aligned}$$

Et en soustrayant :

$$\begin{aligned} c + a - (c - a) &= 2q - 2r \\ 2a &= 2(q - r) \\ a &= q - r \end{aligned}$$

En remplaçant dans le relation :

$$\begin{aligned} c^2 &= a^2 + b^2 \\ (q + r)^2 &= (q - r)^2 + b^2 \\ q^2 + 2qr + r^2 &= q^2 - 2qr + r^2 + b^2 \\ 4qr &= b^2 \end{aligned}$$

Or, q, r sont relativement premiers, donc il faut que q, r soit des carrés parfaits pour que $4qr$ soit un carré parfait. Posons $q = m^2, r = n^2$. Et ainsi :

$$a = q - r = m^2 - n^2$$
$$b = 2\sqrt{qr} = 2\sqrt{m^2 n^2} = 2mn$$
$$c = q + r = m^2 + n^2.$$

$\Leftarrow$: Si $m, n \in \mathbb{N}^*, m > n, a = m^2 - n^2, b = 2mn, c = m^2 + n^2$ alors $c^2 = a^2 + b^2$ On a donc

$$\begin{aligned} a^2 + b^2 &= (2nm)^2 + (n^2 - m^2)^2 \\ &= 4n^2m^2 + n^4 - 2n^2m^2 + m^4 \\ &= n^4 + 2n^2m^2 + m^4 \\ &= (n^2 + m^2)^2 \\ &= c^2. \text{ OK.} \end{aligned}$$

■

2.3 Preuve d'existence

Ex. 11

a. $\forall n \in \mathbb{N}^*$, il existe un nombre qui a plus de n facteurs premiers.
   Preuve : (constructive)
   Soit $n \in \mathbb{N}^*$ le nombre de facteurs premiers voulus dans notre nombre. Soit $S = \{k \in \mathbb{N}^* \mid k \text{ est premier}\}$ et $|S| = n + 1$.
   Si on considère le produit des $n + 1$ nombre premier qui composent S, on obtient un nombre qui a exactement une fois chacun de ses $n + 1$ facteurs premiers. ■

b. $\forall n \in \mathbb{N}^*$, on peut trouver un nombre premier plus grand que n.
   Preuve : (non constructive)
   Soit $n \in \mathbb{N}^*$ et considérons $n! + 1$. Il y a deux cas à traiter.
   Cas 1 : $n! + 1$ est premier, alors puisque $n! + 1 > n$, le nombre premier plus grand que n existe (on l'a construit), OK. Cas 2 : $n! + 1$ n'est pas premier. Il a donc au moins un facteur. Ce facteur, disons d, est plus grand que n, puisque $\forall k \leq n, k \mid n!$. d est donc un nombre premier plus grand que n, OK.
   ■

c. Il existe une infinité de nombres premiers de la forme $4k + 3$.
   Preuve : (contradiction donc non-constructive)

Supposons le contraire et quil nexiste quun nombre n fini. Soit $S = \{p_1, p_2, ..., p_n\}$ l'ensemble de ces n nombres premiers de la forme $4k+3$.
Considérons $p = 4(p_1 p_2 \cdots p_n) - 1$, ce nombre est de la forme $4k+3$. On remarque qu'aucun des p_i ne divise p. Or, p se décompose en facteurs premiers de la forme $4k+1$ et $4k+3$ $(4k-1)$. Ces facteurs ne peuvent pas tous être de la forme $4k+1$ (puisque $n = 4k-1$ de forme $4k+3$), donc nécessairement, il y un au moins un facteur de $p \notin S$ de la forme $4k+3$, $\lightning S$ était incomplet. ■

2.4 Preuve par récurrence

Ex. 12

a. $6 \mid 2n^3 + 3n^2 + n, n \in \mathbb{N}$.
Preuve : (récurrence)
Notons (juste pour le fun) que :

$$\begin{aligned} 2n^3 + 3n^2 + n &= n(2n^2 + 3n + 1) \\ &= n(2n^2 + 2n + n + 1) \\ &= n(2n(n+1) + n + 1) \\ &= n(n+1)(2n+1) \end{aligned}$$

Comme $\sum_{k=1}^{n} k^2 = \frac{n(n+1)(2n+1)}{6}$ alors $6 \sum_{k=1}^{n} k^2 = n(n+1)(2n+1)$ et $6 \mid 2n^3 + 3n^2 + n$. Ce serait une preuve directe. Par récurrence, on doit plutôt faire ceci :
$n = 0$: $2 \cdot 0 + 2 \cdot 0 + 0 = 0$, $6 \mid 0$. OK.
Supposons que $6 \mid 2n^3 + 3n^2 + n$ et $\exists k \in \mathbb{N}, 6k = 2n^3 + 3n^2 + n$.
Prouvons que $6 \mid 2(n+1)^3 + 3(n+1)^2 + (n+1)$.

$$\begin{aligned} &2(n+1)^3 + 3(n+1)^2 + (n+1) \\ &= 2n^3 + 6n^2 + 6n + 2 + \\ &\quad 3n^2 + 6n + 3 + n + 1 \\ &= 2n^3 + 9n^2 + 13n + 6 \\ &= (2n^3 + 3n^2 + n) + (6n^2 + 12n + 6) \\ &= 6k + 6n^2 + 12n + 6 \\ &= 6(k + n^2 + 2n + 1) \end{aligned}$$

■

b. $3 \mid n^3 - n, n \in \mathbb{N}$.
Preuve : (récurrence)
$n = 1$: $3^3 - 3 = 24$ et $3 \mid 24$. OK.
Supposons que $3 \mid n^3 - n$.
Prouvons que $3 \mid (n+1)^3 - (n+1)$ $(\exists k \in \mathbb{N}^*, 3k = (n+1)^3 - (n+1))$.

$$\begin{aligned} (n+1)^3 - (n+1) &= (n+1)^3 - (n+1) \\ &= n^3 + 3n^2 + 3n + 1 - n - 1 \\ &= n^3 - n + +3n^2 + 3n \\ &= 3k + 3(n^2 + n) \\ &= 3(k + n^2 + n), \end{aligned}$$

et $3 \mid (n+1)^3 - (n+1)$

■

c. $\sum_{k=1}^{n} = \frac{n(n+1)}{2}$.
Preuve : (récurrence)
$n = 1$: $\frac{1 \times 2}{2} = 1$, $\sum_{k=1}^{1} = 1$,OK.
Supposons que $\sum_{k=1}^{n} = \frac{n(n+1)}{2}$.
Prouvons que $\sum_{k=1}^{n+1} = \frac{(n+1)(n+2)}{2}$.

$$\begin{aligned} \sum_{k=1}^{n+1} &= \sum_{k=1}^{n+1} + (n+1) \\ &= \frac{n(n+1)}{2} + (n+1) \\ &= \frac{n(n+1) + 2(n+1)}{2} \\ &= \frac{(n+1)(n+2}{2} \end{aligned}$$

■

d. $5 \mid 6^n + 4$.
Preuve : (récurrence)
$n = 1$: $5^1 + 4 = 10$ et $5 \mid 10$, OK.
Supposons que $5 \mid 6^n + 4$ $(\exists k, 6^n = 5k - 4)$.
Prouvons que $5 \mid 6^{n+1} + 4$

$$\begin{aligned} 6^{n+1} + 4 &= 6 \cdot 6^n + 4 \\ &= 6 \cdot (5k - 4) + 4 \\ &= 6 \cdot 5k - 24 + 4 \\ &= 6 \cdot 5k - 24 + 4 \\ &= 30k - 20 \\ &= 5\,(6k - 4)\,, \text{ et } 5 \parallel n. \end{aligned}$$

■

e. $3 \mid 5^n + 2 \cdot 11^n$.
Preuve : (récurrence)
$n = 1$: $5^1 + 2 \cdot 11^1 = 27$ et $3 \mid 27$, OK.
Supposons que $3 \mid 5^n + 2 \cdot 11^n$ $(\exists k, 3k = 5^n + 2 \cdot 11^n)$,

Prouvons que $3 \mid 5^{n+1} + 2 \cdot 11^{n+1}$

$$\begin{aligned} 5^{n+1} + 2 \cdot 11^{n+1} &= 5^{n+1} + 11 \cdot 2 \cdot 11^{n} \\ &= 5^{n+1} + 11 \cdot (3k - 5^{n}) \\ &= 5 \cdot 5^{n} + 33k - 11 \cdot 5^{n} \\ &= -6 \cdot 5^{n} + 33k \\ &= 3\left(-2 \cdot 5^{n} + 11\right), \text{ et } 3 \parallel n. \end{aligned}$$

■

f. $\sum_{k=0}^{n} 2^k = 2^{n+1} - 1$.
Preuve : (récurrence)

$n = 1$: Supposons que $\sum_{k=0}^{n} 2^k = 2^{n+1} - 1$.

Prouvons que $\sum_{k=0}^{n+1} 2^k = 2^{n+2} - 1$

$$\begin{aligned} \sum_{k=0}^{n+1} 2^k &= \sum_{k=0}^{n} 2^k + 2^{n+1} \\ &= 2^{n+1} - 1 + 2^{n+1} \\ &= 2 \cdot 2^{n+1} - 1 \\ &= 2^{n+2} - 1 \end{aligned}$$

■

g. Démonter que $\sum_{k=1}^{n} \left(\frac{1}{2}\right)^k = 1 - \left(\frac{1}{2}\right)^n$.
Preuve : (récurrence)

$n = 1$: $\sum_{k=1}^{1} \left(\frac{1}{2}\right)^k = \frac{1}{2}$ et $1 - \frac{1}{2} = \frac{1}{2}$,OK.

Supposons que $\sum_{k=1}^{n} \left(\frac{1}{2}\right)^k = 1 - \left(\frac{1}{2}\right)^n$.

Prouvons que $\sum_{k=1}^{n+1} \left(\frac{1}{2}\right)^k = 1 - \left(\frac{1}{2}\right)^{n+1}$

$$\begin{aligned} \sum_{k=1}^{n+1} \left(\frac{1}{2}\right)^k &= \sum_{k=1}^{n} \left(\frac{1}{2}\right)^k + \left(\frac{1}{2}\right)^{n+1} \\ &= 1 - \left(\frac{1}{2}\right)^n + \left(\frac{1}{2}\right)^{n+1} \\ &= 1 - \frac{1}{2^n} + \frac{1}{2^{n+1}} \\ &= 1 - \frac{2-1}{2^{n+1}} \\ &= 1 - \frac{1}{2^{n+1}} \\ &= 1 - \left(\frac{1}{2}\right)^{n+1} \end{aligned}$$

■

h. $\sum_{k=1}^{n} \frac{1}{k(k+1)} = \frac{n}{n+1}$.
Preuve : (récurrence)

$n = 1$: $\sum_{k=1}^{1} \frac{1}{k(k+1)} = \frac{1}{1 \cdot 2} = \frac{1}{2}$ et $\frac{1}{1+1} = \frac{1}{2}$=,OK.

Supposons que $\sum_{k=1}^{n} \frac{1}{k(k+1)} = \frac{n}{n+1}$.

Prouvons que $\sum_{k=1}^{n+1} \frac{1}{k(k+1)} = \frac{n+1}{n+2}$

$$\begin{aligned} \sum_{k=1}^{n+1} \frac{1}{k(k+1)} &= \sum_{k=1}^{n} \frac{1}{k(k+1)} + \frac{1}{(n+1)(n+2)} \\ &= \frac{n}{n+1} + \frac{1}{n+2} \\ &= \frac{n(n+2)+1}{(n+1)(n+2)} \\ &= \frac{n^2+2n+1}{(n+1)(n+2)} \\ &= \frac{(n+1)(n+1}{(n+1)(n+2)} \\ &= \frac{n+1}{n+2} \end{aligned}$$

■

i. $\sum_{k=1}^{n} (-1)^{k-1} k^2 = (-1)^{n-1} \frac{n(n+1)}{2}$.
Preuve : (récurrence)

$n = 1$: $\sum_{k=1}^{1} (-1)^{k-1} 1^2 = 1$ et $\frac{1 \cdot 2}{2} = 1$, OK.

Supposons que :
$\sum_{k=1}^{n} (-1)^{k-1} k^2 = (-1)^{n-1} \frac{n(n+1)}{2}$.

Prouvons que :
$\sum_{k=1}^{n+1} (-1)^{k-1} k^2 = (-1)^{n} \frac{(n+1)(n+2)}{2}$.

$$\begin{aligned} &\sum_{k=1}^{n+1} (-1)^{k-1} k^2 \\ &= \sum_{k=1}^{n+1} (-1)^{k-1} k^2 + (-1)^n (n+1)^2 \\ &= (-1)^{n-1} \frac{n(n+1)}{2} + (-1)^n (n+1)^2 \\ &= (-1)^n (n+1)\left(\frac{-n}{2} + n + 1\right) \\ &= (-1)^n (n+1))\left(\frac{-n+2n+2}{2}\right) \\ &= (-1)^n (n+1)\left(\frac{n+2}{2}\right) \\ &= (-1)^n (\frac{(n+1)(n+2)}{2} \end{aligned}$$

■

j. Démontrer que l'on peut affranchir n'importe quel montant supérieur à 3¢ avec seulement des

timbres de 2¢ et de 5¢.
Preuve : (récurrence)

$n = 4$: on peut faire 4¢ avec 2 timbres de 2¢.
Supposons que l'on peut affranchir n'importe quel montant de n¢.
Prouvons que l'on peut affranchir n'importe quel montant de $n + 1$¢. Pour ce faire nous allons prouver qu'il est possible d'affranchir $(n + 1)$¢ à partir d'un affranchissement de n¢.
Cas 1 : Il y a un 5¢ dans l'affranchissement de n¢, on le remplace par 3×2¢, OK.
Cas 2 : Il n'y a pas de 5¢, il y a au moins 2×2¢. En effet, puisque qu'on a au moins 4¢, un seul 2¢ n'est pas suffisant. On peut donc remplacer ces 2×2¢ par 1×5¢, OK. ■

k. Démontrer que l'on peut affranchir n'importe quel montant supérieur à 11¢ avec seulement des timbres de 3¢ et de 7¢.
Preuve : (récurrence)

$n = 12$: on peut faire 12¢ avec 4 timbres de 3¢.
Supposons que l'on peut affranchir n'importe quel montant de n¢.
Prouvons que l'on peut affranchir n'importe quel montant de $n + 1$¢. Pour ce faire nous allons prouver qu'il est possible d'affranchir $(n + 1)$¢ à partir d'un affranchissement de n¢.
Cas 1 : Il y a 2×3¢ dans l'affranchissement de n¢, on les remplace par 1×7¢, OK.
Cas 2 : Il n'y a pas 2×3¢, il y a au moins 2×7¢. En effet, puisque qu'on a au moins $(12 - 3) = 9$¢, un seul 7¢ n'est pas suffisant. On peut donc remplacer ces 2×7¢ par 5×3¢, OK. ■