DM 10 : un corrigé

Problème 1 : Nombres parfaits pairs

1°) $k-1 \geq 1$, donc $n = 2^{k-1}(2^k-1)$ est pair.
2^k-1 est premier, donc l'écriture $n = 2^{k-1}(2^k-1)$ est la décomposition de n en produit de nombres premiers. Ainsi, l'ensemble des diviseurs de n est égal à
$\{2^h \ / \ 0 \leq h \leq k-1\} \cup \{(2^k-1)2^h \ / \ 0 \leq h \leq k-1\}$. On en déduit que la somme des diviseurs de n vaut $S = \Big(\sum_{h=0}^{k-1} 2^h\Big)(1+(2^k-1)) = 2^k \dfrac{2^k-1}{2-1} = 2n$, donc n est parfait et pair.

2°) $\diamond$ Pour tout $k \in \mathbb{N}$, $0 = 0 \times k$, donc k divise 0. Ainsi la somme des diviseurs dans $\mathbb{N}$ de 0 est infinie et 0 n'est pas parfait. Ainsi $n \geq 2$, puis en décomposant n en produit de facteurs premiers, on obtient $n = 2^{k-1}m$, où $m = \displaystyle\prod_{p \in \mathbb{P}\setminus\{2\}} p^{v_p(n)}$ est impair. $k \geq 2$ car n est supposé pair.
$\diamond$ Notons D l'ensemble des diviseurs dans $\mathbb{N}$ de m.
D'après le cours, $D = \Big\{ \displaystyle\prod_{p \in \mathbb{P}\setminus\{2\}} p^{w_p} / \ \forall p \in \mathbb{P}\setminus\{2\},\ w_p \leq v_p(m)\Big\}$ et l'ensemble des diviseurs de n est égal à $\Big\{2^h \displaystyle\prod_{p \in \mathbb{P}\setminus\{2\}} p^{w_p} / \ 0 \leq h \leq k-1 \text{ et } \forall p \in \mathbb{P}\setminus\{2\},\ w_p \leq v_p(m)\Big\}$.
Ainsi, l'ensemble des diviseurs de n est égal à $\{2^h d \ / \ d \in D \text{ et } 0 \leq h \leq k-1\}$.
On en déduit que $S(n) = \displaystyle\sum_{h=0}^{k-1} \Big(\sum_{d \in D} 2^h d\Big) = \sum_{h=0}^{k-1} \Big(\sum_{d \in D} d\Big) 2^h = \Big(\sum_{d \in D} d\Big) \sum_{h=0}^{k-1} 2^h$, ainsi $S(n) = S(m)\dfrac{2^k-1}{2-1} = (2^k-1)S(m)$.

3°) On a donc $S(m)(2^k-1) = S(n) = 2n = 2^k m$ car n est supposé parfait. Ainsi $2^k-1 \mid 2^k m$, or $2^k-(2^k-1) = 1$, donc d'après l'identité de Bezout, 2^k et 2^k-1 sont premiers entre eux. Alors d'après le théorème de Gauss, $2^k-1 \mid m$, ce qui permet de conclure.

4°) $\diamond$ $1+m+M = 1+m+\dfrac{m}{2^k-1} = 1+\dfrac{2^k m}{2^k-1} = 1+S(m)$.

$\diamond$ On a $m = M(2^k - 1)$, donc $1 \leq M < m$. Si $M \neq 1$, alors 1, M et m sont trois diviseurs de m deux à deux distincts, donc $S(m) \geq 1 + m + M = 1 + S(m)$, ce qui est faux. Ainsi, $M = 1$, puis $m = 2^k - 1$ et $n = 2^{k-1}(2^k - 1)$.
De plus, $S(m) = m + M = m + 1$, or $S(1) = 1$, donc $m \neq 1$.
Alors le fait que $S(m) = m + 1$ signifie que 1 et m sont les seuls diviseurs dans $\mathbb{N}$ de m, ce qui prouve que m est premier.
On a ainsi montré que tout entier pair et parfait est de la forme $2^{k-1}(2^k - 1)$ avec $k \geq 2$ et $2^k - 1$ premier. La réciproque correspond à la première question.

Remarque culturelle : La question 1 est un résultat d'Euclide (IIIième siècle avant J.-C.), la réciproque est due à Euler (18ième siècle). On ne sait presque rien au sujet des nombres parfaits impairs, on ne sait même pas s'il en existe.

Problème 2 : confluence

1°)

- Soit $x \in E$. Prenons $p = 0$ et $x_0 = x$. Alors on a bien $x_0 = x$, $x_p = x$ et pour tout $i \in \mathbb{N}_0 = \emptyset$, $x_{i-1} \longrightarrow x_i$, donc $x \longrightarrow^* x$, ce qui prouve que $\longrightarrow^*$ est réflexive.
- Soit $x, y \in E$ tels que $x \longrightarrow^* y$. il existe $p \in \mathbb{N}$ et $x_0, \ldots, x_p \in E$ tels que $x_0 = x$, $x_p = y$ et, pour tout $i \in \mathbb{N}_p$, $x_{i-1} \longrightarrow x_i$.
  Pour tout $i \in \{0, \ldots, p\}$, posons $y_i = x_{p-i}$. Ainsi, $y_0 = y$, $y_p = x$ et, pour tout $i \in \mathbb{N}_p$, $y_{i-1} = x_{p-i+1} \longrightarrow x_{p-i} = y_i$, car la relation $\longrightarrow$ est supposée symétrique.
  Ceci démontre que $y \longrightarrow^* x$, donc la relation $\longrightarrow^*$ est symétrique.
- Soit $x, y, z \in E$ tels que $x \longrightarrow y$ et $y \longrightarrow z$.
  Il existe $p, q \in \mathbb{N}$ et $x_0, \ldots, x_p, y_0, \ldots, y_q \in E$ tels que $x_0 = x$, $x_p = y = y_0$, $y_q = z$, pour tout $i \in \mathbb{N}_p$, $x_{i-1} \longrightarrow x_i$ et, pour tout $i \in \mathbb{N}_q$, $y_{i-1} \longrightarrow y_i$.
  Pour tout $i \in \{p+1, \ldots, p+q\}$, posons $x_i = y_{i-p}$. Ainsi, $x_0 = x$, $x_{p+q} = y_q = z$ et pour tout $i \in \mathbb{N}_{p+q}$, $x_{i-1} \longrightarrow x_i$ (c'est notamment vrai pour $i = p + 1$ car $x_p = y = y_0$). Ceci démontre que $x \longrightarrow^* z$, donc $\longrightarrow^*$ est transitive.

En conclusion, on a montré que $\longrightarrow^*$ est une relation d'équivalence.
On remarque que, même lorsque $\longrightarrow$ n'est pas symétrique, $\longrightarrow^*$ reste réflexive et transitive.

2°) Soit $x, y \in \mathbb{Z}$. Montrons que $x \longrightarrow^* y$ si et seulement si $x \equiv y\ [p]$.
Supposons que $x \longrightarrow^* y$. Il existe $q \in \mathbb{N}$ et $x_0, \ldots, x_q \in E$ tels que $x_0 = x$, $x_q = y$ et, pour tout $i \in \mathbb{N}_q$, $|x_{i-1} - x_i| = p$. Alors, pour tout $i \in \mathbb{N}_p$, $x_{i-1} \equiv x_i\ [p]$, donc par transitivité de la relation de congruence, $x = x_0 \equiv x_p = y\ [p]$.
Réciproquement, supposons que $x \equiv y\ [p]$. Sans perte de généralité, on peut supposer que $x < y$ (car d'après la question précédente, la relation $\longrightarrow^*$ est symétrique). Alors il existe $q \in \mathbb{N}$ tel que $y = x + pq$. Posons, pour tout $i \in \{0, \ldots, q\}$, $x_i = x + iq$. Ainsi, $x_0 = x$, $x_q = y$ et, pour tout $i \in \mathbb{N}_q$, $|x_{i-1} - x_i| = p$. Donc $x \longrightarrow^* y$.
Ceci démontre que $\longrightarrow^*$ est la relation de congruence modulo p.

3°) Notons $\longrightarrow^{+*} = (\longrightarrow^+)^*$. Il s'agit de montrer que $\longrightarrow^{+*} = \longrightarrow^*$.
Pour tout $x, y \in E$, on a $x \longrightarrow^+ y \Longrightarrow x \longrightarrow y$: on en déduit aisément que

$x \longrightarrow^{+*} y \Longrightarrow x \longrightarrow^{*} y$.
Réciproquement, soit $x, y \in E$ tels que $x \longrightarrow^{*} y$. Notons A l'ensemble des entiers $p \in \mathbb{N}$ tels qu'il existe $x_0, \ldots, x_p \in E$ vérifiant $x_0 = x$, $x_p = y$ et, pour tout $i \in \mathbb{N}_p$, $x_{i-1} \longrightarrow x_i$. Par hypothèse, A est un ensemble non vide inclus dans $\mathbb{N}$, donc d'après le cours, il possède un minimum que l'on notera m. Par définition de m, il existe $x_0, \ldots, x_m \in E$ vérifiant $x_0 = x$, $x_m = y$ et, pour tout $i \in \mathbb{N}_m$, $x_{i-1} \longrightarrow x_i$.
Soit $i \in \mathbb{N}_m$ (donc $m \geq i \geq 1$). Supposons que $x_{i-1} = x_i$. Posons, pour tout $j \in \{0, \ldots, i-1\}$, $y_j = x_j$ et pour tout $j \in \{i, \ldots, m-1\}$, $y_j = x_{j+1}$. Alors $y_0 = x_0 = x$, $y_{m-1} = x_m = y$ et, pour tout $j \in \mathbb{N}_{m-1}$, $y_{j-1} \longrightarrow y_j$, même lorsque $j = i$, car $y_{i-1} = x_{i-1} = x_i \longrightarrow x_{i+1} = y_i$. On en déduit que $m - 1 \in A$ ce qui contredit la définition de m.
Ainsi, pour tout $i \in \mathbb{N}_m$, $x_{i-1} \neq x_i$, donc $x_{i-1} \longrightarrow^{+} x_i$, ce qui prouve que $x \longrightarrow^{+*} y$.

4°) La relation $\longrightarrow^{*}$ étant toujours réflexive et transitive, c'est une relation d'ordre si et seulement si elle est antisymétrique.
Montrons que la condition nécessaire et suffisante pour que $\longrightarrow^{*}$ soit une relation d'ordre est l'absence de cycles, c'est-à-dire qu'il n'existe pas $p \in \mathbb{N}^*$ et $x_0, \ldots, x_p \in E$ tels que, pour tout $i \in \mathbb{N}_p$, $x_{i-1} \longrightarrow^{+} x_i$ et $x_p = x_0$. Notons (C) cette dernière condition.
$\diamond$ Supposons que (C) n'est pas vérifiée. Alors il existe $p \in \mathbb{N}^*$ et $x_0, \ldots, x_p \in E$ tels que, pour tout $i \in \mathbb{N}_p$, $x_{i-1} \longrightarrow^{+} x_i$ et $x_p = x_0$. Dans ces conditions, $x_0 \longrightarrow^{*} x_1$ et $x_1 \longrightarrow^{*} x_p = x_0$, mais $x_0 \neq x_1$, donc $\longrightarrow^{*}$ n'est pas une relation d'ordre.
$\diamond$ Réciproquement, supposons que $\longrightarrow^{*}$ n'est pas une relation d'ordre. Alors il existe $x, y \in E$ tels que $x \neq y$, $x \longrightarrow^{*} y$ et $y \longrightarrow^{*} x$.
D'après la question précédente, Il existe $p, q \in \mathbb{N}$ et $x_0, \ldots, x_p, y_0, \ldots, y_q \in E$ tels que $x_0 = x$, $x_p = y$, $y_0 = y$, $y_q = x$, pour tout $i \in \mathbb{N}_p$, $x_{i-1} \longrightarrow^{+} x_i$ et, pour tout $i \in \mathbb{N}_q$, $y_{i-1} \longrightarrow^{+} y_i$. Alors la suite $x = x_0, \ldots, x_p = y = y_0, y_1, \ldots, y_q = x$ constitue un cycle ($p \geq 1$ car $x \neq y$), ce qui prouve $\neg(C)$.

5°)
$\diamond$ Supposons que $\longrightarrow$ est confluente. Soit $x, y_1, y_2 \in E$ tels que $x \longrightarrow y_1$ et $x \longrightarrow y_2$. Il est alors clair que $x \longrightarrow^{*} y_1$ et $x \longrightarrow^{*} y_2$, or $\longrightarrow$ est confluente, donc il existe $z \in E$ tel que $y_1 \longrightarrow^{*} z$ et $y_2 \longrightarrow^{*} z$. Ceci prouve que $\longrightarrow$ est localement confluente.
$\diamond$ Pour montrer que la réciproque est fausse, il est suffisant de construire un contre-exemple. Prenons pour E un ensemble constitué de 4 éléments distincts notés A, B, C et D. Sur E, considérons la relation $\longrightarrow$ définie par le schéma suivant :

$$A \longleftarrow B \longleftrightarrow C \longrightarrow D.$$

La relation $\longrightarrow$ est localement confluente car les seuls triplets (x, y_1, y_2) tels que $y_1 \neq y_2$, $x \longrightarrow y_1$ et $x \longrightarrow y_2$ sont (B, A, C), (B, C, A), (C, B, D) et (C, D, B). Pour les deux premiers triplets, on remarque que $A \longrightarrow^{*} A$ et $C \longrightarrow^{*} A$ et pour les deux derniers triplets, on remarque que $D \longrightarrow^{*} D$ et $B \longrightarrow^{*} D$, donc la relation $\longrightarrow$ est localement confluente.
Cependant $B \longrightarrow^{*} A$ et $B \longrightarrow^{*} D$, mais s'il existe $z \in E$ tel que $A \longrightarrow^{*} z$ et $D \longrightarrow^{*} z$, alors $A = z = D$, ce qui est faux. Ainsi, la relation $\longrightarrow$ n'est pas confluente.

6°)
◇ Supposons que $\leq$ n'est pas un ordre, alors $\geq = \longrightarrow^*$ n'est pas un ordre, donc d'après la question 4, il existe $p \in \mathbb{N}^*$ et $x_0, \ldots, x_p \in E$ tels que, pour tout $i \in \mathbb{N}_p$, $x_{i-1} \longrightarrow^+ x_i$ et $x_p = x_0$.
Pour tout $n \in \mathbb{N}$, en notant i le reste de la division euclidienne de n par p, posons $x_n = x_i$. Ainsi, la suite $(x_n)_{n\in\mathbb{N}}$ est p-périodique.
Soit $n \in \mathbb{N}$. Notons à nouveau i le reste de la division euclidienne de n par p.
Si $i < p-1$, $x_n = x_i \longrightarrow x_{i+1} = x_{n+1}$.
Si $i = p-1$, $x_n = x_{p-1} \longrightarrow x_p = x_0 = x_{n+1}$.
Ainsi, pour tout $n \in \mathbb{N}$, $x_n \longrightarrow x_{n+1}$, ce qui est impossible.
On a montré que $\leq$ est une relation d'ordre sur E.
◇ Soit A une partie non vide de E. Supposons que A ne possède pas d'élément minimal.
$A \neq \emptyset$, donc il existe $x_0 \in A$.
x_0 n'est pas minimal, donc il existe $x_1 \in A$ tel que $x_1 < x_0$.
Soit $n \in \mathbb{N}$. Supposons construits $x_0, \ldots, x_n \in A$ tels que $x_n < x_{n-1} < \cdots < x_0$.
x_n n'est pas minimal dans A, donc il existe $x_{n+1} \in A$ tel que $x_{n+1} < x_n$.
On construit ainsi par récurrence une suite $(x_n)_{n\in\mathbb{N}}$ d'éléments de E telle que, pour tout $n \in \mathbb{N}$, $x_{n+1} < x_n$, donc telle que $x_n \longrightarrow^* x_{n+1}$ avec $x_n \neq x_{n+1}$.
Pour tout $n \in \mathbb{N}$, il existe $p_n \in \mathbb{N}^*$ et $y_{n,0}, \ldots, y_{n,p_n} \in E$ tels que $y_{n,0} = x_n$, $y_{n,p_n} = x_{n+1}$ et, pour tout $i \in \mathbb{N}_{p_n}$, $y_{n,i-1} \longrightarrow y_{n,i}$.
En renommant $(z_n)_{n\in\mathbb{N}}$ la suite $y_{0,0}, \ldots, y_{0,p_0}, y_{1,1}, \ldots, y_{1,p_1}, \ldots, y_{k,1}, \ldots, y_{k,p_k}, \ldots$, on a construit une suite (z_n) d'éléments de E telle que, pour tout $n \in \mathbb{N}$, $z_n \longrightarrow z_{n+1}$, ce qui est impossible.
Ainsi, A admet nécessairement un élément minimal.
◇ Montrons que c'est faux en construisant un contre-exemple.
Prenons $E = \{0, 1\}$ et choisissons pour $\longrightarrow$ la relation vide sur E : pour tout $x, y \in E$, $\neg(x \longrightarrow y)$.
Alors $\longrightarrow$ est bien noethérienne, mais E, qui est non vide, ne possède pas de minimum, car $\neg(0 \leq 1)$ et $\neg(1 \leq 0)$.

7°) Raisonnons par l'absurde en supposant que $A = \{x \in E/\ \neg(P(x))\} \neq \emptyset$.
Alors A possède un élément minimal, noté m. On a $\neg(P(m))$, donc d'après l'hypothèse de l'énoncé, il existe $y \in E$ tel que $m \longrightarrow y$ et $\neg(P(y))$.
Si $y = m$, alors en posant pour tout $n \in \mathbb{N}$, $x_n = m$, on aurait, pour tout $n \in \mathbb{N}$, $x_n \longrightarrow x_{n+1}$, ce qui est impossible. Ainsi $y \neq m$ et $y \leq m$.
On en déduit que $y < m$ et $y \in A$ (car $\neg(P(y))$), ce qui contredit la minimalité de m.
Ainsi $A = \emptyset$, ce qui prouve que $P(x)$ est vrai pour tout $x \in E$.

8°) Pour tout $x \in E$, notons $P(x)$ le prédicat suivant : pour tout $y_1, y_2 \in E$ tel que $x \longrightarrow^* y_1$ et $x \longrightarrow^* y_2$, il existe $z \in E$ tel que $y_1 \longrightarrow^* z$ et $y_2 \longrightarrow^* z$.
Nous allons montrer que $P(x)$ est vrai pour tout $x \in E$ en utilisant le principe de pseudo-récurrence de la question précédente : soit $x \in E$. On suppose que $P(y)$ est vraie pour tout $y \in E$ tel que $x \longrightarrow y$ et l'on doit montrer $P(x)$.
Soit $y_1, y_2 \in E$ tel que $x \longrightarrow^* y_1$ et $x \longrightarrow^* y_2$.

◇ Si $y_1 = x$, en posant $z = y_2$, on a bien $y_1 = x \longrightarrow^* y_2 = z$ et $y_2 \longrightarrow^* y_2 = z$.
On raisonne de même si $y_2 = x$.
◇ On peut donc supposer que $y_1 \neq x$ et que $y_2 \neq x$.
Alors il existe $z_1, z_2 \in E$ tels que $x \longrightarrow z_1 \longrightarrow^* y_1$ et $x \longrightarrow z_2 \longrightarrow^* y_2$.

La démonstration s'appuie sur la figure suivante :

$$\begin{array}{ccccc} x & \longrightarrow & z_1 & \longrightarrow^* & y_1 \\ \downarrow & & \downarrow_* & & \downarrow_* \\ z_2 & \longrightarrow^* & z' & \longrightarrow^* & z'' \\ & \searrow^* & & & \downarrow_* \\ & & y_2 & \longrightarrow^* & z''' \end{array}$$

Par hypothèse, $\longrightarrow$ est localement confluente, donc il existe $z' \in E$ tel que $z_1 \longrightarrow^* z'$ et $z_2 \longrightarrow^* z'$.
$x \longrightarrow z_1$, donc $P(z_1)$ est vraie. Or $z_1 \longrightarrow^* y_1$ et $z_1 \longrightarrow^* z'$, donc il existe $z'' \in E$ tel que $y_1 \longrightarrow^* z''$ et $z' \longrightarrow^* z''$.
De même, $x \longrightarrow z_2$, donc $P(z_2)$ est vraie. Or $z_2 \longrightarrow^* z' \longrightarrow^* z''$ et $z_2 \longrightarrow^* y_2$, donc d'après la transitivité de $\longrightarrow^*$, il existe $z''' \in E$ tel que $y_2 \longrightarrow^* z''$ et $z'' \longrightarrow^* z'''$.
Ainsi, $y_1 \longrightarrow^* z'' \longrightarrow^* z'''$ et $y_2 \longrightarrow^* z'''$, ce qu'il fallait démontrer.

Remarque culturelle : En informatique, la notion de confluence intervient dans l'étude des systèmes de réécritures. La confluence locale est une propriété a priori plus faible que la confluence mais qui a l'avantage d'être décidable. Le lemme de Newman, que l'on vient de démontrer, dit que dans le cas d'un système de réécriture noethérien, la confluence coïncide avec la confluence locale et est donc décidable.

Problème 3 : Les valeurs absolues de $\mathbb{Q}$

1°) Il est clair que V_0 est positive et qu'elle ne s'annule qu'en 0.
Soient $x, y \in \mathbb{Q}$. Si $x = 0$ ou $y = 0$, on a $xy = 0$ donc $V_0(xy) = 0 = V_0(x)V_0(y)$.
Si $x \neq 0$ et $y \neq 0$, on a $xy \neq 0$ donc $V_0(xy) = 1 = V_0(x)V_0(y)$.
Soient $x, y \in \mathbb{Q}$. Si $x = 0$ et $y = 0$, on a $V_0(x + y) = 0 = V_0(x) + V_0(y)$.
Si $x \neq 0$ ou $y \neq 0$, on a $V_0(x + y) \leq 1 \leq V_0(x) + V_0(y)$.
En conclusion, la valeur absolue triviale V_0 est bien une valeur absolue sur $\mathbb{Q}$.

2°) Pour $n \in \mathbb{N}^*$, notons $R(n)$ l'assertion suivante :
— pour tout $x_1, \ldots, x_n \in \mathbb{Q}$, $V(x_1 \times \cdots \times x_n) = V(x_1) \times \cdots \times V(x_n)$;
— pour tout $x \in \mathbb{Q}$, $V(x^n) = V(x)^n$;
— pour tout $x_1, \ldots, x_n \in \mathbb{Q}$, $V(x_1 + \cdots + x_n) \leq V(x_1) + \cdots + V(x_n)$.
◇ Lorsque $n = 1$, $R(1)$ est évidente.
◇ Soit $n \geq 2$. Supposons $R(n-1)$ et montrons $R(n)$. Soit $x_1, \ldots, x_n \in \mathbb{Q}$ et $x \in \mathbb{Q}$.
$V(x_1 \times \cdots \times x_n) = V(x_1 \times \cdots \times x_{n-1})V(x_n)$ d'après la multiplicativité de V, donc d'après $R(n-1)$, $V(x_1 \times \cdots \times x_n) = V(x_1) \times \cdots \times V(x_n)$.
En particulier lorsque pour tout $i \in \mathbb{N}_n$, $x_i = x$, on en déduit que $V(x^n) = V(x)^n$.

$V(x_1+\cdots+x_n)=V([x_1+\cdots+x_{n-1}]+x_n)\leq V(x_1+\cdots+x_{n-1})+V(x_n)$ d'après l'inégalité triangulaire, donc d'après $R(n-1)$, $V(x_1+\cdots+x_n)\leq V(x_1)+\cdots+V(x_n)$. Ainsi, d'après le principe de récurrence, pour tout $n\in\mathbb{N}^*$, $R(n)$ est prouvée.

3°)

— On a $V(1)=V(1^2)=V(1)^2$ et comme $V(1)\neq 0$, cela implique que $V(1)=1$.

— On a $1=V(1)=V((-1)^2)=V(-1)^2$ et comme $V(-1)\geq 0$, il vient $V(-1)=1$. Ainsi, pour tout $x\in\mathbb{Q}$, on a bien $V(-x)=V(-1\times x)=V(-1)V(x)=1\times V(x)=V(x)$.

— Pour tout $x\in\mathbb{Q}^*$, on a $V(x^{-1})V(x)=V(x^{-1}x)=V(1)=1$, donc $\forall x\in\mathbb{Q}^*,\ \ V(x^{-1})=V(x)^{-1}$.

4°)

◇ Si $n\in\mathbb{N}^*$, le théorème fondamental de l'arithmétique permet d'écrire de manière unique n sous la forme $n=\prod_{q\in\mathbb{P}}q^{w_q}$, où $(w_q)_{q\in\mathbb{P}}$ est une famille presque nulle d'entiers naturels. Il est alors clair que selon la définition de l'énoncé, on a $w_p=v_p(n)$.
On pourra donc écrire, pour tout $n\in\mathbb{N}^*$, $n=\prod_{q\in\mathbb{P}}q^{v_q(n)}$.
Si $n,m\in\mathbb{N}^*$, on a $\prod_{q\in\mathbb{P}}q^{v_q(nm)}=nm=\Big(\prod_{q\in\mathbb{P}}q^{v_q(n)}\Big)\times\Big(\prod_{q\in\mathbb{P}}q^{v_q(m)}\Big)=\prod_{q\in\mathbb{P}}q^{v_q(n)+v_q(m)}$, donc d'après l'unicité d'une telle écriture, $v_p(nm)=v_p(n)+v_p(m)$, pour tout $n,m\in\mathbb{N}^*$.
Si maintenant $n,m\in\mathbb{Z}^*$, alors
$v_p(nm)=v_p(|nm|)=v_p(|n|\times|m|)=v_p(|n|)+v_p(|m|)=v_p(n)+v_p(m)$.

◇ L'énoncé nous demande de montrer que la quantité $v_p(a)-v_p(b)$ ne dépend que de $\frac{a}{b}$: Soit $r\in\mathbb{Q}^*$. Supposons que $r=\frac{a}{b}=\frac{c}{d}$ où $a,c\in\mathbb{Z}^*$ et $b,d\in\mathbb{N}^*$.
Alors $ad=cb$, donc $v_p(ad)=v_p(cb)$, puis d'après le point précédent,
$v_p(a)+v_p(d)=v_p(c)+v_p(b)$, donc $v_p(a)-v_p(b)=v_p(c)-v_p(d)$, ce qu'il fallait démontrer.
De plus lorsque $r\in\mathbb{Z}^*$, $r=\frac{r}{1}$, donc $v_p(r)-v_p(1)=v_p(r)$. Ainsi, la définition
"$v_p\Big(\frac{a}{b}\Big)=v_p(a)-v_p(b)$" est correcte et elle prolonge bien l'application v_p déjà définie sur $\mathbb{Z}^*$ en une application de $\mathbb{Q}^*$ dans $\mathbb{Z}$.

◇ Soit $r,s\in\mathbb{Q}^*$. Notons $r=\frac{a}{b}$ et $s=\frac{c}{d}$, où $a,c\in\mathbb{Z}^*$ et $b,d\in\mathbb{N}^*$. Alors $rs=\frac{ac}{bd}$, donc
$$\begin{aligned}v_p(rs)&=v_p(ac)-v_p(bd)=v_p(a)+v_p(c)-(v_p(b)+v_p(d))\\&=(v_p(a)-v_p(b))+(v_p(c)-v_p(d))=v_p(r)+v_p(s).\end{aligned}$$

◇ Commençons par montrer la propriété relative à $v_p(r+s)$ lorsque $r,s\in\mathbb{Z}^*$:
Soit $n,m\in\mathbb{Z}^*$ tels que $n+m\neq 0$.
Sans perte de généralité, on peut supposer que $v_p(n)\leq v_p(m)$.
Notons s_n,s_m et s_{n+m} les signes de n,m et $n+m$. Alors
$|n+m|=s_{n+m}(n+m)=s_{n+m}(s_n|n|+s_m|m|)$,
donc en notant $\sigma=s_{n+m}s_n$ et $\sigma'=s_{n+m}s_m$,
$|n+m|=\sigma\prod_{q\in\mathbb{P}}q^{v_q(n)}+\sigma'\prod_{q\in\mathbb{P}}q^{v_q(m)}=p^{v_p(n)}\Big(\sigma\prod_{\substack{q\in\mathbb{P}\\q\neq p}}q^{v_q(n)}+\sigma' p^{v_p(m)-v_p(n)}\prod_{\substack{q\in\mathbb{P}\\q\neq p}}q^{v_q(m)}\Big)$, donc
$p^{v_p(n)}$ divise $|n+m|$, ce qui prouve que $v_p(n+m)\geq v_p(n)=\min(v_p(n),v_p(m))$.

Supposons de plus que $v_p(n) < v_p(m)$: posons $a = \sigma \prod_{\substack{q\in\mathbb{P}\\ q\neq p}} q^{v_q(n)} + \sigma' p^{v_p(m)-v_p(n)} \prod_{\substack{q\in\mathbb{P}\\ q\neq p}} q^{v_q(m)}$.
$v_p(m) - v_p(n) \geq 1$, donc p divise $\sigma' p^{v_p(m)-v_p(n)} \prod_{\substack{q\in\mathbb{P}\\ q\neq p}} q^{v_q(m)}$, or p ne divise pas $\sigma \prod_{\substack{q\in\mathbb{P}\\ q\neq p}} q^{v_q(n)}$, donc p ne divise pas a. Ainsi, lorsque $v_p(n) \neq v_p(m)$,
on a montré que $v_p(n+m) = \min(v_p(n), v_p(m))$.

$\diamond$ Soit $r, s \in \mathbb{Q}^*$. Notons à nouveau $r = \frac{a}{b}$ et $s = \frac{c}{d}$, où $a, c \in \mathbb{Z}^*$ et $b, d \in \mathbb{N}^*$. $r + s = \dfrac{ad+cb}{bd}$, donc $v_p(r+s) = v_p(ad+cb) - v_p(bd)$. D'après le point précédent, $v_p(r+s) \geq \min(v_p(ad), v_p(cb)) - v_p(bd) = \min(v_p(a)+v_p(d), v_p(c)+v_p(b)) - v_p(b) - v_p(d)$, donc $v_p(r+s) \geq \min(v_p(a) - v_p(b), v_p(c) - v_p(d)) = \min(v_p(r), v_p(s))$.
De plus, si $v_p(r) \neq v_p(s)$, alors $v_p(a) - v_p(b) \neq v_p(c) - v_p(d)$, donc $v_p(ad) \neq v_p(bc)$, donc d'après le cas d'égalité dans $\mathbb{Z}^*$, on obtient que $v_p(r+s) = \min(v_p(r), v_p(s))$.

5°) Soit $\alpha \in \mathbb{R}_+^*$.

Il est clair que $(|\cdot|_p)^\alpha$ est positive et qu'elle ne s'annule qu'en 0.

Soient $r, s \in \mathbb{Q}^*$. On a $|rs|_p = p^{-v_p(rs)} = p^{-v_p(r)-v_p(s)} = p^{-v_p(r)} p^{-v_p(s)} = |r|_p |s|_p$ donc $(|rs|_p)^\alpha = (|r|_p)^\alpha (|s|_p)^\alpha$. La multiplicativité est donc établie, car c'est clair lorsque $r = 0$ ou $s = 0$.

Soient $r, s \in \mathbb{Q}^*$ tels que $r + s \neq 0$. On a $|r+s|_p = p^{-v_p(r+s)}$. Or on sait que $v_p(r+s) \geq \min\{v_p(r), v_p(s)\}$, donc $|r+s|_p \leq p^{-\min\{v_p(r), v_p(s)\}}$, c'est-à-dire $|r+s|_p \leq p^{\max\{-v_p(r), -v_p(s)\}}$ ou encore $|r+s|_p \leq \max\{p^{-v_p(r)}, p^{-v_p(r)}\}$. On a donc $|r+s|_p \leq \max\{|r|_p, |s|_p\}$. En élevant à la puissance α (qui est strictement positive), on obtient $(|r+s|_p)^\alpha \leq \max\{(|r|_p)^\alpha, (|s|_p)^\alpha\}$. A fortiori, on a l'inégalité triangulaire $(|r+s|_p)^\alpha \leq (|r|_p)^\alpha + (|s|_p)^\alpha$.

En conclusion, pour tout $\alpha \in \mathbb{R}_+^*$, l'application $(|\cdot|_p)^\alpha$ est une valeur absolue sur $\mathbb{Q}$.

Remarque culturelle : Dans le cas de la valeur absolue p-adique $|\cdot|_p$, l'inégalité triangulaire classique découle d'une inégalité plus forte : $\forall r, s \in \mathbb{Q},\ |r+s|_p \leq \max\{|r|_p, |s|_p\}$ que l'on appelle l'inégalité ultramétrique.
Ce caractère ultramétrique confère à la topologie issue de la valeur absolue p-adique des propriétés très riches qui permettent de faire de l'analyse sur les corps p-adiques $\mathbb{Q}_p$ (qui sont des complétés de $\mathbb{Q}$, différents de $\mathbb{R}$).

6°) a) Par l'absurde : on suppose que $\forall p \in \mathbb{P},\ V(p) \geq 1$.
Comme $\forall n \in \mathbb{N},\ V(n) \leq 1$, on a $\forall p \in \mathbb{P},\ V(p) = 1$.
Pour tout entier $n \in \mathbb{N} \setminus \{0, 1\}$ dont la décomposition primaire est $n = {p_1}^{\alpha_1} \cdots {p_k}^{\alpha_k}$, on a alors $V(n) = V({p_1}^{\alpha_1} \cdots {p_k}^{\alpha_k}) = V(p_1)^{\alpha_1} \cdots V(p_k)^{\alpha_k} = 1$. Rappelons que l'on sait déjà que $V(1) = 1$. Donc $\forall n \in \mathbb{N}^*,\ V(n) = 1$.
Comme V est paire, il s'ensuit que $\forall n \in \mathbb{Z}^*,\ V(n) = 1$.
Pour tout nombre rationnel non nul $r = \frac{a}{b}$, on a donc $V(r) = V(\frac{a}{b}) = \frac{V(a)}{V(b)} = \frac{1}{1} = 1$.
Autrement dit, V est la valeur absolue triviale, ce qui est contraire aux hypothèses.
En conclusion, il existe un nombre premier p tel que $V(p) < 1$.

6°) b)
◇ Soit $k \in \mathbb{N}^*$.
Comme p et q sont deux nombres premiers distincts, les entiers p^k et q^k sont premiers entre eux. Le théorème de Bézout dit en conséquence qu'il existe $u, v \in \mathbb{Z}$ tels que $up^k + vq^k = 1$.
Il est clair que u et v sont non nuls.
D'une part, on a $V(up^k + vq^k) = V(1) = 1$. D'autre part,
$V(up^k + vq^k) \leq V(up^k) + V(vq^k) = V(u)V(p)^k + V(v)V(q)^k \leq 1 \times V(p)^k + 1 \times V(q)^k$
où l'on a utilisé l'inégalité triangulaire, la multiplicativité
et l'hypothèse $\forall n \in \mathbb{N},\ V(n) \leq 1$.
En combinant ces résultats, on obtient $V(p)^k + V(q)^k \geq 1$.

◇ Par l'absurde : on suppose que $V(q) \neq 1$, c'est-à-dire $V(q) < 1$. En passant à la limite ($k \longrightarrow +\infty$) dans la relation $V(p)^k + V(q)^k \geq 1$, il vient $0 \geq 1$. Absurde !
Donc $V(q) = 1$.

6°) c) On a vu aux questions précédentes que $V(p) < 1$ et $\forall q \in \mathbb{P} \setminus \{p\},\ V(q) = 1$.
Par conséquent, pour tout $n \in \mathbb{N}^*$, on a
$$V(n) = V\Big(p^{v_p(n)} \prod_{q \in \mathbb{P}\setminus\{p\}} q^{v_q(n)}\Big) = V(p)^{v_p(n)} \prod_{q \in \mathbb{P}\setminus\{p\}} V(q)^{v_q(n)} = V(p)^{v_p(n)},$$
c'est-à-dire $V(n) = e^{v_p(n)\ln(V(p))} = (e^{\ln p})^{-v_p(n)\alpha}$, où $\alpha = -\dfrac{\ln V(p)}{\ln p}$.
Ainsi, $V(n) = (p^{-v_p(n)})^{\alpha}$.
Comme $V(p) < 1$, on a bien $\alpha > 0$.
Comme V est paire, il s'ensuit que $\forall n \in \mathbb{Z}^*,\ V(n) = (p^{-v_p(n)})^{\alpha}$.
Pour $r = \frac{a}{b} \in \mathbb{Q}^*$, on a donc $V(r) = V(\frac{a}{b}) = \frac{V(a)}{V(b)} = (p^{-v_p(a)+v_p(b)})^{\alpha} = (p^{-v_p(r)})^{\alpha}$.
En conclusion, il existe $\alpha \in \mathbb{R}_+^*$ tel que $V = (|\cdot|_p)^{\alpha}$.

7°) Soit $\alpha \in]0, 1]$.
L'application $|\cdot|^{\alpha}$ hérite la positivité, la séparation et la multiplicativité des propriétés de la valeur absolue classique et des puissances.
Reste l'inégalité triangulaire. Soient $r, s \in \mathbb{Q}$. On a $|r + s| \leq |r| + |s|$
donc $|r + s|^{\alpha} \leq (|r| + |s|)^{\alpha}$. Il suffit donc de prouver que $(|r| + |s|)^{\alpha} \leq |r|^{\alpha} + |s|^{\alpha}$.
On pose $a = |s|$ et on introduit la fonction $f : \mathbb{R}_+ \longrightarrow \mathbb{R}$ définie par
$\forall x \in \mathbb{R}_+,\ f(x) = (x + a)^{\alpha} - x^{\alpha} - a^{\alpha}$. La fonction f est dérivable sur $\mathbb{R}_+^*$
et $\forall x \in \mathbb{R}_+^*,\ f'(x) = \alpha(x + a)^{\alpha-1} - \alpha x^{\alpha-1} \leq 0$ car $0 < \alpha \leq 1$. La fonction f est donc décroissante sur $\mathbb{R}_+^*$ et continue sur $\mathbb{R}_+$, donc elle est décroissante sur $\mathbb{R}_+$.
Comme $f(0) = 0$, on en déduit que $\forall x \in \mathbb{R}_+,\ f(x) \leq 0$, c'est-à-dire
$\forall x \in \mathbb{R}_+,\ (x + a)^{\alpha} \leq x^{\alpha} + a^{\alpha}$. Pour $x = |r|$, on a donc $(|r| + |s|)^{\alpha} \leq |r|^{\alpha} + |s|^{\alpha}$. On peut ainsi conclure que $|r + s|^{\alpha} \leq |r|^{\alpha} + |s|^{\alpha}$, ce qui prouve que $|\cdot|^{\alpha}$ satisfait l'inégalité triangulaire.

8°) a)
◇ On pose $p = \lfloor k \log_b a \rfloor$. On a

$$\begin{aligned}
\sum_{j=0}^{p} b_{k,j}\, b^j &= \sum_{j=0}^{p} \left(\lfloor a^k b^{-j} \rfloor - b \lfloor a^k b^{-j-1} \rfloor\right) b^j \\
&= \sum_{j=0}^{p} \lfloor a^k b^{-j} \rfloor\, b^j - \sum_{j=0}^{p} \lfloor a^k b^{-j-1} \rfloor\, b^{j+1} \\
&= \sum_{j=0}^{p} \lfloor a^k b^{-j} \rfloor\, b^j - \sum_{i=1}^{p+1} \lfloor a^k b^{-i} \rfloor\, b^i \qquad \text{en posant } i = j+1 \\
&= \lfloor a^k b^{-0} \rfloor\, b^0 - \lfloor a^k b^{-p-1} \rfloor\, b^{p+1} \\
&= \quad a^k \quad - \quad 0
\end{aligned}$$

où la dernière égalité découle du fait que $a^k \in \mathbb{N}$ et $0 \leq a^k b^{-p-1} < 1$ car $p+1 > k \log_b a$.

Donc $a^k = \displaystyle\sum_{j=0}^{\lfloor k \log_b a \rfloor} b_{k,j}\, b^j$.

$\diamond$ Soit $j \in \mathbb{N}$. Comme $\forall x \in \mathbb{R},\ x - 1 < \lfloor x \rfloor \leq x$, on a $a^k b^{-j} - 1 < \left\lfloor a^k b^{-j} \right\rfloor \leq a^k b^{-j}$ et $-a^k b^{-j} \leq -b \left\lfloor a^k b^{-j-1} \right\rfloor < -a^k b^{-j} + b$. En additionnant ces deux encadrements, on obtient $-1 < \left\lfloor a^k b^{-j} \right\rfloor - b \left\lfloor a^k b^{-j-1} \right\rfloor < b$, c'est-à-dire $-1 < b_{k,j} < b$, et comme $b_{k,j} \in \mathbb{Z}$, on en déduit que $b_{k,j} \in [\![0, b-1]\!]$.

C'est deux points prouvent que la décomposition de a^k en base b s'écrit bien $a^k = \displaystyle\sum_{j=0}^{\lfloor k \log_b a \rfloor} b_{k,j}\, b^j$.

8°) b)

Pour tout $k \in \mathbb{N}^*$, on a

$$\begin{aligned}
V(a)^k &= V(a^k) \qquad \text{par multiplicativité} \\
&= V\Big(\sum_{j=0}^{\lfloor k \log_b a \rfloor} b_{k,j}\, b^j \Big) \qquad \text{d'après } \mathbf{a)} \\
&\leq \sum_{j=0}^{\lfloor k \log_b a \rfloor} V(b_{k,j}\, b^j) \qquad \text{par inégalité triangulaire} \\
&= \sum_{j=0}^{\lfloor k \log_b a \rfloor} V(b_{k,j})\, V(b)^j \qquad \text{par multiplicativité} \\
&\leq \sum_{j=0}^{\lfloor k \log_b a \rfloor} M_b\, V(b)^j \qquad \text{car } \forall j \in \mathbb{N},\ b_{k,j} \in [\![0, b-1]\!] \\
&= M_b \sum_{j=0}^{\lfloor k \log_b a \rfloor} V(b)^j.
\end{aligned}$$

On distingue alors deux cas.

Si $V(b) \leq 1$, on a, pour tout $k \in \mathbb{N}^*$,

$V(a)^k \leq M_b \sum_{j=0}^{\lfloor k \log_b a \rfloor} 1^j = M_b\,(1 + \lfloor k \log_b a \rfloor) \leq M_b\,(1 + k \log_b a)$,
donc si $V(b) \leq 1$, on a $\forall k \in \mathbb{N}^*,\ V(a)^k \leq M_b\,(1 + k \log_b a)$.
Si $V(b) > 1$, on peut utiliser la formule de sommation d'une suite géométrique, ce qui donne pour tout $k \in \mathbb{N}^*$,
$V(a)^k \leq M_b \dfrac{V(b)^{\lfloor k \log_b a \rfloor + 1} - 1}{V(b) - 1} \leq M_b \dfrac{V(b)^{\lfloor k \log_b a \rfloor + 1}}{V(b) - 1} \leq M_b \dfrac{V(b)^{k \log_b a + 1}}{V(b) - 1}$,
donc si $V(b) > 1$, on a $\forall k \in \mathbb{N}^*,\ V(a)^k \leq \dfrac{M_b\,V(b)}{V(b) - 1}\,V(b)^{k \log_b a}$.

9°) a) Par l'absurde : on suppose qu'il existe $b \in \mathbb{N} \setminus \{0, 1\}$ tel que $V(b) \leq 1$.
On peut alors appliquer la première inégalité de la question précédente avec $a = n_0$, ce qui donne $V(n_0)^k \leq M_b\,(1 + k \log_b n_0)$ ou encore $1 \leq \dfrac{M_b\,(1 + k \log_b n_0)}{V(n_0)^k}$.
En passant à la limite ($k \longrightarrow +\infty$) dans cette inégalité, on obtient, d'après les croissances comparées, $1 \leq 0$. C'est absurde.
On en conclut que $\forall n \in \mathbb{N} \setminus \{0, 1\},\ V(n) > 1$.

9°) b) On sait que $V(n) > 1$ d'après la question précédente. Cela nous permet d'appliquer la seconde inégalité de la question 8.b avec $a = n$ et $b = m$. On a, pour tout $k \in \mathbb{N}^*$, $V(n)^k \leq \dfrac{M_m\,V(m)}{V(m) - 1}\,V(m)^{k \log_m n}$, c'est-à-dire $V(n) \leq \left(\dfrac{M_m\,V(m)}{V(m) - 1}\right)^{1/k} V(m)^{\log_m n}$.
En passant à la limite ($k \longrightarrow +\infty$) dans cette inégalité, on obtient $V(n) \leq V(m)^{\log_m n}$, c'est-à-dire $V(n)^{1/\ln n} \leq V(m)^{1/\ln m}$.
En échangeant n et m, on obtient $V(m)^{1/\ln m} \leq V(n)^{1/\ln n}$, donc $V(n)^{1/\ln n} = V(m)^{1/\ln m}$.

9°) c) La question précédente nous dit que la suite $(V(n)^{1/\ln n})_{n \geq 2}$ est constante, c'est-à-dire $\forall n \in \mathbb{N} \setminus \{0, 1\},\ V(n)^{1/\ln n} = V(2)^{1/\ln 2}$. Comme $V(2) > 1$, on peut écrire $V(2)^{1/\ln 2} = e^{\alpha}$ où $\alpha > 0$. D'où $\forall n \in \mathbb{N} \setminus \{0, 1\},\ V(n)^{1/\ln n} = e^{\alpha}$, c'est-à-dire
$\forall n \in \mathbb{N} \setminus \{0, 1\},\ V(n) = e^{\alpha \ln n}$ ou encore $\forall n \in \mathbb{N} \setminus \{0, 1\},\ V(n) = n^{\alpha}$.
Comme $V(0) = 0$ et $V(1) = 1$, on a $\forall n \in \mathbb{N},\ V(n) = n^{\alpha}$.
Comme V est paire, il s'ensuit que $\forall n \in \mathbb{Z},\ V(n) = |n|^{\alpha}$.
Pour $r = \frac{a}{b} \in \mathbb{Q}$, on a donc $V(r) = V(\frac{a}{b}) = \frac{V(a)}{V(b)} = (\frac{|a|}{|b|})^{\alpha} = (|\frac{a}{b}|)^{\alpha} = |r|^{\alpha}$.
Donc il existe $\alpha > 0$ tel que $V = |\cdot|^{\alpha}$.
De plus, $2^{\alpha} = V(2) = V(1 + 1) \leq V(1) + V(1) = 2$, donc $\alpha \ln 2 \leq \ln 2$, or $\ln 2 > 0$, donc $\alpha \leq 1$.

10°) D'après les questions précédentes, les valeurs absolues non triviales sur $\mathbb{Q}$ sont exactement les $(|\ .\ |_p)^{\alpha}$ avec $\alpha > 0$ et les $|\ .\ |^{\alpha}$ avec $0 < \alpha \leq 1$.