Correction

Question 1 : Une relation R sur un ensemble E est dite bien fondée si et seulement si il n'existe pas de suite infinie strictement décroissante d'élément de E.

Question 2 :
a)

- Une relation $R \in A \times B$ est dite injective si et seulement si : $\forall x, y, z \in A \times A \times B, R(x, z) \& R(y, z) \Rightarrow x = y$
- Une relation $R \in A \times B$ est dite surjective si et seulement si : $\forall y \in B, \exists x \in A, R(x, y)$

(autre version acceptée : dans le cas des fonctions/applications)

- Une application $f : A \to B$ est dite injective si et seulement si : $\forall x, y \in A : f(x) = f(y) \Rightarrow x = y$
- Une application $f : A \to B$ est dite surjective si et seulement si : $\forall y \in B, \exists x \in A, f(x) = y$

b)

- f n'est pas injective. En effet, on a $f(2, 3) = 5 = f(3, 2)$ mais $(3, 2) \neq (2, 3)$.
- f est surjective. Prouvons le. Soit $n \in \mathbb{N}$, on a $f(0, n) = 0 + n = n$, donc il existe un antécédent à n : $(0, n)$.

Question 3 :
a) Montrons que R est réflexive, symétrique et transitive.

Preuve de la réflexivité.
Soit $x \in E$, montrons que xRx. On a : $g(x) = g(x)$,
donc, par définition de R, xRx.

Preuve de la symétrie.
Soient $x, y \in E$ tels que xRy. Montrons que yRx.
On a xRy, et donc $g(x) = g(y)$, par définition.
Donc $g(y) = g(x)$, et donc yRx par définition

Preuve de la transitivité.
Soient $x, y, z \in E^3$ tels que xRy et yRx. Montrons que xRy.
On a xRy. Par définition de R, on a alors $g(x) = g(y)$.
On a yRz. Par définition de R, on a alors $g(y) = g(z)$.
Donc $g(x) = g(y) = g(z)$, donc $g(x) = g(z)$,
et donc xRz, par définition.

b) Si g est injective alors $R = Id_E$. En effet, supposons g injective et montrons $R = Id_E$.
Montrons que $Id_E \subseteq R$.
Soient $x, y \in Id_E$.
Par définition de Id_E, on a $x = y$.
Par réflexivité de R, on a $(x, x) \in R$.
Donc $(x, y) \in R$
Montrons $R \subseteq Id_E$.
Soient $(x, y) \in R$.
Par définition de R, on a $g(x) = g(y)$.
Par injectivité de g, on a donc $x = y$.
De plus, par définition de Id_E, on a $(x, x) \in Id_E$
Or $x = y$, donc $(x, x) = (x, y)$, donc $x, y \in Id_E$.

Question 4 :

(voir court pour les définitions)

- E n'a pas d'élément maximal. Pour tout $k \in E$, $2k \in E$ et $k \| 2k$, donc pour tout élément k de E, il existe un élément k' strictement plus grand.
- La borne inférieur de a, b est $pgcd(a, b)$.
- Le maximum de A est 24, car 24 est divisible par 4,6, 8 et 24.

Question 5 :

$f0 = a^1 = a$ et pour tout entier n, $f(n+1) = a^{2^{n+1}} = a^{2^n \times 2} = (a^{2^n})^2 = (f(n)^2)$

Question 6 :
a) Montrons cette égalité par double inclusion.

Preuve de $\mathcal{P}(A \cap B) \subseteq \mathcal{P}(A) \cap \mathcal{P}(B)$
Soit $X \in \mathcal{P}(A \cap B)$. Alors, $X \subseteq A \cap B$.
Or : $A \cap B \subseteq A$ et $A \cap B \subseteq B$.
Donc $X \subseteq A$ et $X \subseteq B$.
Donc $X \in \mathcal{P}(A)$ et $X \in \mathcal{P}(B)$.
Donc $X \in \mathcal{P}(A) \cap \mathcal{P}(B)$.

Preuve de $\mathcal{P}(A) \cap \mathcal{P}(B) \subseteq \mathcal{P}(A \cap B)$ Soit $X \in \mathcal{P}(A) \cap \mathcal{P}(B)$.
Alors $X \in \mathcal{P}(A)$ et $X \in \mathcal{P}(B)$.
Donc $X \subseteq A$ et $X \subseteq B$.
Donc $X \subseteq A \cap B$.
Donc $X \in \mathcal{P}(A \cap B)$
b) Cette égalité est fausse. Montrons un contre-exemple.
Prenons $A = \{0, 1\}$ et $B = \{0, 2\}$.
Alors : $\mathcal{P}(A) = \{\emptyset, \{0\}, \{1\}, \{0, 1\}\}$ et $\mathcal{P}(B) = \{\emptyset, \{0\}, \{2\}, \{0, 2\}\}$, et donc $\mathcal{P}(A) \cup \mathcal{P}(B) = \mathcal{P}(A) = \{\emptyset, \{0\}, \{1\}, \{2\}, \{0, 1\}, \{0, 2\}\}$.
De plus $A \cup B = \{0, 1, 2\}$, d'où $\mathcal{P}(A \cup B) = \{\emptyset, \{0\}, \{1\}, \{2\}, \{1, 2\}, \{0, 2\}, \{0, 1\}, \{0, 1, 2\}\}$.
Ainsi, on a $\mathcal{P}(A \cup B) \neq \mathcal{P}(A) \cup \mathcal{P}(B)$.

Question 7 :

Posons, pour tout élément N de $\mathcal{N}$, la propriété P suivante : $P(N) = \forall M \in \mathcal{N}, Add(N, M) = Add(M, N)$. Montrons P par induction structurelle.

Cas de Base : montrons $P(Z)$
On veut montrer : $\forall M \in \mathcal{N}, Add(Z, M) = Add(M, Z)$.
Montrons ceci par induction structurelle sur M.

— Cas de base.
  On a bien $Add(Z, Z) = Add(Z, Z)$
— Cas inductif. Soit $M \in \mathcal{N}$ tel que $Add(Z, M) = Add(M, Z)$, montrons que $Add(Z, S(M)) = Add(S(M), Z)$.
  On a

$$\begin{aligned} Add(Z, S(M)) &= S(Add(Z, M)) \text{ par définition de } Add \\ &= S(Add(M, Z)) \text{ par hypothèse d'induction} \\ &= S(M) \text{ par définition de } Add \end{aligned}$$

  et $Add(Z, S(M)) = S(M)$ par définition. Donc, on a bien $Add(Z, S(M)) = Add(S(M), Z)$.

On a donc montré : $\forall M \in \mathcal{N}, Add(Z, M) = Add(M, Z)$. D'où $P(Z)$.

Cas inductif. Soit $N \in \mathcal{N}$*, tel que* $P(N)$*. Montrons* $P(S(N))$*.*
On veut montrer : $\forall M \in \mathcal{M} : Add(M, S(N)) = Add(S(N), M)$. Procédons par induction structurelle sur M.

— Cas de Base. Plus haut on a montré : $\forall M \in \mathcal{N}, Add(Z, M) = Add(M, Z)$. Appliqué à $S(N)$, on obtient $Add(Z, S(N)) = Add(S(N), Z)$. Le cas de base est donc vérifié.
— Cas d'induction. Soit $M \in \mathcal{N}$ tel que $Add(M, S(N)) = Add(S(N), M)$, montrons $Add(S(M), S(N)) = Add(S(N), S(M))$.
  On a

$$\begin{aligned} Add(S(M), S(N)) &= S(Add(S(M), N)) \\ &= S(Add(N, S(M))) \text{ par } P(N) \\ &= S(S(Add(N, M))) \\ &= S(S(Add(M, N))) \text{ par } P(N) \\ &= S(Add(M, S(N))) \\ &= S(Add(S(N), M)) \text{ par hypothèse d'induction sur } M \\ &= Add(S(N), S(M)). \end{aligned}$$

  Le cas d'induction est donc vérifié. D'où $P(S(N))$.