Corrigé de la Série 1

1.1. Ensembles, nombres naturels et nombres premiers

1. (a) Soit l'ensemble $E := \{1, 2, 3\}$. Enumerez tous les ss-ensembles de E. Montrez qu'il y en a 8.

(b) Soit un ensemble E avec n éléments. Montrez que le nombre de ss-ensembles de E est 2^n.

(a) La collection de tous les ss-esnsembles d'un ensemble E est un ensemble dénoté par $\mathcal{P}(E)$. On a $\mathcal{P}(\{1,2,3\}) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1,2\}, \{1,3\}, \{2,3\}, \{1,2,3\}\}$.

(b) On peut remarquer, que former un sous-ensemble de E est un choix à faire sur chaque élément de E de le prendre ou non. Si E a n éléments, il s'agit donc de décider pour chaque élément de le prendre ou non. Il y a donc deux choix possibles par élément, d'où le nombre de choix possibles au total (donc le nombre de sous-ensembles de E) est 2^n.

2. Soient E un ensemble et $A, B, C \in \mathcal{P}(E)$. Soit l'affirmation:

$$\text{Si } A \cap B = A \cap C \text{ et si } A \cup B = A \cup C, \quad \text{alors } B = C.$$

Mettez les phrases suivantes dans un ordre qui démontre cette affirmation:

(*a*) Comme $x \notin A$, on doit avoir $x \in C$.

(*b*) On a donc $x \in C$ dans les deux cas.

(*c*) Par symétrie, il suffit de montrer $B \subset C$.

(*d*) $x \notin A$. Alors, $x \in A \cup B = A \cup C$.

(*e*) Soit $x \in B$. On distingue alors deux cas.

(*f*) $x \in A$. Alors, $x \in A \cap B = A \cap C$ et donc, $x \in C$.

L'ordre correcte est (c)-(e)-(f)-(d)-(a)-(b). Avec plus de détails, on trouve la pruev suivante:

(c) Par symétrie, il suffit de montrer $B \subset C$. (on peut ensuite montrer que $C \subset B$ en utilisant le même argument qui va suivre, après avoir renversé les rôles de B et de C).

(e) Soit $x \in B$. On distingue alors deux cas:

(f) (Premier cas) $x \in A$. Alors, $x \in A \cap B = A \cap C$ (par hypothèse) et alors $x \in C$.

(d) (Deuxième cas) $x \notin A$. Alors, $x \in A \cup B = A \cup C$ (à nouveau par hypothèse).

(a) Comme $x \notin A$, on doit avoir $x \in C$.

(b) On a donc $x \in C$ dans les deux cas (puisque forcément, $x \in A$ ou $x \notin A$).

□

3. Soient E, F, G des ensembles. Montrer que
(a) $E \setminus (F \cap G) = (E \setminus F) \cup (E \setminus G)$.
(b) $E \setminus (F \cup G) = (E \setminus F) \cap (E \setminus G)$.

(a)

$$\begin{aligned} E \setminus (F \cap G) &= \{x \in E : x \notin F \cap G\} \\ &= \{x \in E : \neg(x \in G \text{ et } x \in F)\} \\ &= \{x \in E : x \notin F \text{ ou } x \notin G\} = \{x \in E : x \in E \setminus F \text{ ou } x \in E \setminus G\} \\ &= (E \setminus F) \cup (E \setminus G). \end{aligned}$$

(b)

$$\begin{aligned} E \setminus (F \cup G) &= \{x \in E : x \notin F \cup G\} \\ &= \{x \in E : \neg(x \in G \text{ ou } x \in F)\} \\ &= \{x \in E : x \notin F \text{ et } x \notin G\} = \{x \in E : x \in E \setminus F \text{ et } x \in E \setminus G\} \\ &= (E \setminus F) \cap (E \setminus G). \end{aligned}$$

4. Vrai ou faux?
(a) $\{\emptyset, \{\emptyset\}\} \subset \mathcal{P}(\mathcal{P}(\mathbb{N}))$.
(b) $\{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\} \subset \mathcal{P}(\mathcal{P}(\mathcal{P}(\mathbb{N})))$.
(c) Chaque élément de $\{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}$ en est un sous-ensemble.
(d) Chaque sous-ensemble de $\{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}$ en est un élément.

(a) Vrai, car $\emptyset \subset \mathbb{N}$, donc $\emptyset \in \mathcal{P}(\mathbb{N})$, donc $\{\emptyset\} \subset \mathcal{P}(\mathbb{N})$ et $\{\emptyset\} \in \mathcal{P}(\mathcal{P}(\mathbb{N}))$. Comme $\emptyset \in \mathcal{P}(\mathcal{P}(\mathbb{N}))$ aussi, on a $\{\emptyset, \{\emptyset\}\} \subset \mathcal{P}(\mathcal{P}(\mathbb{N}))$.

(b) On vient de voir que $\{\emptyset, \{\emptyset\}\} \subset \mathcal{P}(\mathcal{P}(\mathbb{N}))$. Donc $\{\emptyset, \{\emptyset\}\} \in \mathcal{P}(\mathcal{P}(\mathcal{P}(\mathbb{N})))$.
Comme $\emptyset \subset \mathcal{P}(\mathbb{N})$ on a $\emptyset \in \mathcal{P}(\mathcal{P}(\mathbb{N}))$, donc $\{\emptyset\} \subset \mathcal{P}(\mathcal{P}(\mathbb{N}))$, donc $\{\emptyset\} \in \mathcal{P}(\mathcal{P}(\mathcal{P}(\mathbb{N})))$.
Comme $\emptyset \subset \mathcal{P}(\mathcal{P}(\mathbb{N}))$ on a $\emptyset \in \mathcal{P}(\mathcal{P}(\mathcal{P}(\mathbb{N})))$.
Ainsi, $\{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\} \subset \mathcal{P}(\mathcal{P}(\mathcal{P}(\mathbb{N})))$ est vraie.

(c) Vrai, car $\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\} \in \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}$.

(d) Faux: $\{\{\emptyset\}\} \notin \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}$.

5. Soit un nombre naturel n. Montrez, que si tous les nombres premiers p avec $p^2 \leq n$ ne divisent pas n, alors n est premier.

On peut montrer la contraposée: "Si $n \in \mathbb{N}$ n'est pas premier alors n possède un facteur premier p tel que $p^2 \leq n$."
En effet, par le théorème fondamental de l'arithmétique,

$$n = p_1^{n_1} p_2^{n_2} \dots p_f^{n_f}$$

où $n_1 + n_2 + \ldots + n_f \geq 2$ si n n'est pas premier. On a donc

$$p_1^2 \leq p_1^{n_1+n_2+\ldots+n_f} \leq p_1^{n_1} p_2^{n_2} \ldots p_f^{n_f} = n.$$

Ainsi, le plus petit facteur premier de n, à savoir p_1 est tel que $p_1^2 \leq n$.

6. Soit $p \geq 5$ un nombre premier. Montrez que $p^2 - 1$ est un multiple de 24.
(Indication: écrire $p^2 - 1$ comme $(p-1)(p+1)$. Que peut-on dire alors des trois nombres $p-1, p, p+1$?)

On a $p^2 - 1 = (p+1)(p-1)$. Puisque p est premier et supérieur à 5, $p-1$ et $p+1$ sont deux nombres pairs successifs. L'un d'entre eux est donc divisible par 4 et l'autre par 2. Leur produit se divise donc par 8. De plus, $p-1$, p, $p+1$ sont trois nombres naturels successifs et l'un d'entre eux est donc divisible par 3. Comme p est premier, soit $p-1$ soit $p+1$ est divisible par 3. On en conclut, que le produit $(p-1)(p+1)$ est divisible par $2 \times 3 \times 4$, i.e. par 24.

7. Montrez que pour tout $2 \leq n \in \mathbb{N}$, aucun nombre entre $n! + 2$ et $n! + n$ n'est premier.

Si $m \in \mathbb{N}$ est tel que $n! + 2 \leq m \leq n! + n$ on peut écrire $m = n! + d$ avec $2 \leq d \leq n$. d divise alors clairement $n!$, puisque cette dernière n'est autre que le produit des nombres entre 2 et n. On a donc $n! = dq$ avec $q \in \mathbb{N}^*$. Donc, $m = n! + d = dq + d = d(q+1)$, ce qui montre que m n'est pas premier.

8. Montrez que si $a, n \geq 2$ sont des nombres naturels tels que $a^n - 1$ est premier, alors $a = 2$ et n est premier.
(Indication: que vaut $1 + a + \ldots + a^{n-1}$ multiplié par $(a-1)$é?)

On peut écrire $a^n - 1 = (a-1)(a^{n-1} + \ldots + a + 1)$. Si $a > 2$, on aurait que $a - 1$ comme diviseur de $a^n - 1$, qui est pourtant premier. D'où $a = 2$.
Si n n'est pas premier, on a $n = mq$ et $a^n - 1 = a^{mq} - 1 = (a^m)^q - 1 = (a^m - 1)((a^m)^{q-1} + \ldots + 1)$ et $(a^m - 1)$ serait un diviseur de $a^n - 1$, encore une contradiction.

Problèmes supplémentaires

(PS1) Montrer qu'il existe un nombre infini de nombres premiers.

Soit $\{p_1, p_2, \ldots, p_n\}$ l'énumération des n premiers nombres premiers. Le nombre $m = p_1 p_2 \ldots p_n + 1$ est certainement plus grand que tous les p_k, $k = 1, \ldots, n$. De plus, on voit qu'aucun des premiers dans $\{p_1, p_2, \ldots, p_n\}$ ne divise m. Par le théorème fondamental de l'arithmétique il se décompose en produit de facteurs premiers. On a deux possibilités:

(a) m est un nombre premier. Dans ce cas, puisque $m \notin \{p_1, p_2, \ldots, p_n\}$, il existe au moins $n+1$ nombres premiers.

(b) m n'est pas premiers. Dans ce cas il doit exister un nombre premier p qui divise m. Mais $p \notin \{p_1, p_2, \ldots, p_n\}$ et il existe aussi au moins $n+1$ nombres premiers.

Cet argument étant valable pour tout $n \in \mathbb{N}^*$, on en conclut qu'il n'existe pas de liste finie et exhaustive de tous les nombres premiers. Il y en a donc une infinité.

(PS2) Montrez que si $n \geq 5$ n'est pas premier, alors n divise $(n-1)!$.

On va distinguer deux cas:

(a) n est un carré. On peut donc écrire $n = m^2$. Puisque $n \geq 5$ on doit avoir $m < \frac{n}{2}$, car sinon, $n = m^2 \geq \frac{n^2}{4}$, ce qui impliquerait $n(4-n) \geq 0$, i.e. $n \leq 4$. On a alors que $2 \leq m < 2m < n$ et m apparaît comme facteur d'au moins deux nombres dans $2, 3, \ldots, n-1$. Donc $n = m^2$ divise $(n-1)!$.

(b) n n'est pas un carré. Dans ce cas, et puisque n n'est pas premier, on peut écrire $n = pm$, avec p le plus petit facteur premier de n. Ainsi, $2 \leq p < m < n-1$ et p ainsi que m apparaissent dans la liste $2, \ldots, m-1$. $n = pm$ divise alors $(n-1)!$.