NOMBRES ET STRUCTURES ALGÉBRIQUES USUELLES (R)

1. Ensembles et applications

1.1.

Exercice 1.1.1. **F**
Si $f \in \mathcal{F}(E, F)$, montrer les équivalences :

(i) f est surjective
(ii) $\forall y \in F, f(f^{-1}(\{y\})) = \{y\}$
(iii) $\forall Y \in \mathcal{P}(F), f(f^{-1}(Y)) = Y$
(iv) Le seul $Y \in \mathcal{P}(F)$ tel que $f^{-1}(Y) = \emptyset$ est $\emptyset$

($\mathcal{P}(F)$ désigne l'ensemble des parties de F).
Trouver un énoncé analogue en remplaçant (i) par f injective.

Exercice 1.1.2. **F C**
Soient $f : E \to F$, $h : E \to G$ deux applications.
Montrer que pour qu'il existe une application $g : F \to G$ telle que $h = g \circ f$, il faut et il suffit que :

$$\forall (x, y) \in E^2,\ f(x) = f(y) \Rightarrow h(x) = h(y).$$

À quelle condition g est-elle uniquement déterminée ?

Exercice 1.1.3. **F**
Soient $f : E \to F$, $g : F \to G$, $h : G \to E$ trois applications.
Montrer que si $g \circ f$ et $h \circ g$ sont bijectives alors, f, g et h sont bijectives.

Exercice 1.1.4. **D**
Soit $E = [0, 1] \times [0, 1]$: montrer que, si l'on munit E de l'ordre lexicographique, toute partie non vide admet une borne supérieure.
Ce résultat subsiste-t-il si on prend $E = [0, 1] \times]0, 1]$?

Exercice 1.1.5. **F**
L'application définie par

$$f : (x, y) \in \mathbb{R}^2 \mapsto (x, xy - y^3) \in \mathbb{R}^2$$

est elle injective, surjective ?

EXERCICE 1.1.6. **F**
Soient E, F, G 3 ensembles, $f \in \mathcal{F}(E,F)$ et $g \in \mathcal{F}(E,G)$. On définit $h \in \mathcal{F}(E, F\times G)$ par $h(x) = (f(x), g(x))$.
Si f et g sont injectives, qu'en est-il de h ?
Si f et g sont surjectives, qu'en est-il de h ?

---

2. ENTIERS NATURELS, DÉNOMBREMENTS

2.1.

EXERCICE 2.1.1. **I**
Soit P_n le nombre de partitions sur un ensemble fini de cardinal n ; montrer que :

$$P_{n+1} = \sum_{k=0}^{n} \binom{n}{k} P_k.$$

EXERCICE 2.1.2. **F C**
En écrivant que $(1+x)^n(1+x)^p = (1+x)^{n+p}$, montrer que, si $k \leqslant \inf(n,p)$ alors :

$$\binom{n+p}{k} = \binom{n}{k} + \binom{n}{k-1}\binom{p}{1} + \cdots + \binom{n}{k-h}\binom{p}{h} + \cdots + \binom{p}{k}.$$

EXERCICE 2.1.3. **D C**
Soit p_n le nombre de permutations σ de $[1,n]$ telles que, $\forall k \in [1,n], \sigma_k \neq k$ (σ est un *dérangement*).

(1) Montrer que : $n! = p_n + \binom{n}{1}p_{n-1} + \cdots + \binom{n}{n-2}p_2 + 1$
(évaluer de 2 manières le nombre de permutations de $[1,n]$).
(2) Montrer les 2 relations :

$$2^p\binom{n}{p} = \binom{n}{0}\binom{n}{p} + \binom{n}{1}\binom{n-1}{p-1} + \cdots + \binom{n}{p}\binom{n-p}{0} \tag{1}$$

$$0 = \binom{n}{0}\binom{n}{p} - \binom{n}{1}\binom{n-1}{p-1} + \cdots + (-1)^p\binom{n}{p}\binom{n-p}{0}. \tag{2}$$

(3) Montrer que : $p_n = n! - \binom{n}{1}(n-1)! + \cdots + (-1)^k\binom{n}{k}(n-k)! + \cdots + (-1)^n$; trouver un équivalent de p_n quand $n \to +\infty$.

EXERCICE 2.1.4. **F**
Soient n et p 2 entiers non nuls tels que $n \geqslant p$.
Quel est le nombre d'applications strictement croissantes de $[\![1,p]\!]$ dans $[\![1,n]\!]$?

EXERCICE 2.1.5. **I**
Déterminer le nombre de solutions dans $\mathbb{N}^3$ du système :

$$\begin{cases} x+y+z &= n \\ x &\leqslant y+z \\ y &\leqslant z+x \\ z &\leqslant x+y \end{cases}$$

où n est un entier donné.

EXERCICE 2.1.6. **I**
Soit E un ensemble fini à n éléments, calculer le cardinal des ensembles suivants :

(1) $F = \{(A,B) \in \mathcal{P}(E)^2 \mid A \cup B = E,\ A \cap B = \emptyset\}$.
(2) $G_A = \{B \in \mathcal{P}(E) \mid A \cup B = E\}$ où A est une partie de E contenant p éléments.
(3) $H = \{(A,B) \in \mathcal{P}(E)^2 \mid A \cup B = E\}$.

EXERCICE 2.1.7. **D C**
Soient $n \leqslant p$ 2 entiers, on note $S_{p,n}$ le nombre de surjections d'un ensemble à p éléments dans un ensemble à n éléments.

(1) Calculer $S_{n+1,n}$ et $S_{p,2}$.
(2) Montrer que :

$$\forall (n,p) \in (\mathbb{N}^*)^2,\ n^p = \sum_{i=1}^{n} \binom{n}{i} S_{p,i}.$$

EXERCICE 2.1.8. **I**

Soient $(n,p) \in (\mathbb{N}^*)^2$ et $a_1, \ldots, a_p$ p entiers tels que $\sum_{i=1}^{p} a_i = n$.
Déterminer le nombre d'applications de $[\![1,n]\!]$ dans $[\![1,p]\!]$ telles que, pour tout $i \in [\![1,p]\!]$, i ait exactement a_i antécédents.

EXERCICE 2.1.9. **I**
Soit E un ensemble à np éléments (où n et p sont 2 entiers naturels non nuls), on note $P_{n,p}$ le nombre de partitions de E en n parties à p éléments.
Montrer que :

$$P_{n,p} = \frac{1}{n}\binom{np}{p} P_{n-1,p}.$$

En déduire l'expression de $P_{n,p}$.

---

3. Structures algébriques usuelles

3.1. Groupes et anneaux.

Exercice 3.1.1. **F**
Soit G un groupe abélien et $A \subset G$ une partie non vide de G stable.

(1) On désigne par A^* l'ensemble des éléments de G qui s'écrivent xy^{-1} où $(x, y) \in A^2$. Prouver que A^* est un sous-groupe de G.
(2) Lorsque G est fini, montrer que A est un sous-groupe de G, comparer alors A et A^*.

Exercice 3.1.2. **I**
Soit G un groupe, A et B 2 sous-groupes de G et $P = AB = \{ab, a \in A, b \in B\}$
Montrer que P est un sous-groupe de G ssi $AB = BA$.

Exercice 3.1.3. **I**
Si A et B sont 2 sous-groupes de G et si $A \cup B$ est un sous-groupe de G, alors montrer que $A \subset B$ ou $B \subset A$.

Exercice 3.1.4. **D**
Soit l'anneau $\mathbb{Z}[\sqrt{13}] = \{x + \sqrt{13}y, (x, y) \in \mathbb{Z}^2\}$.

(1) Chercher le groupe U des éléments inversibles de l'anneau $\mathbb{Z}[\sqrt{13}]$ (on montrera que $18+5\sqrt{13}$ est le plus petit élément de U strictement supérieur à 1, puis on conclura que $U = \{\pm(18 + 5\sqrt{13})^n, n \in \mathbb{Z}\}$ en faisant intervenir $N(x + y\sqrt{13}) = x^2 - 13y^2$).
(2) Montrer que 2, $3 - \sqrt{13}$ et $-3 - \sqrt{13}$ sont irréductibles (i.e. si on a l'implication $(a = rs \Rightarrow r$ ou s sont inversibles) alors a est irréductible). Trouver un élément qui admet plusieurs décompositions en produit d'éléments irréductibles.

Exercice 3.1.5. **I**
Soit B un anneau intègre et A un sous-anneau de B. On suppose que pour tout x de B, il existe un polynôme normalisé P dans $A[X]$ tel que $P(x) = 0$.
Montrer l'équivalence : A corps ssi B corps.

3.2. Arithmétique dans $\mathbb{Z}$.

Exercice 3.2.1. **F**
Soit $(a, b) \in \mathbb{N}^{*2}$; $a > b$ trouver l'ensemble des $(x, y) \in \mathbb{N}^{*2}$ tels que : $x^2 - y^2 = a^2b^2$ (a et b premiers).
Applications : $(a, b) = (7, 2)$; $(a, b) = (11, 5)$.

EXERCICE 3.2.2. **F**
Si $a \wedge b = 1$ montrer que :

$$(a+b) \wedge ab = 1 \ ; \ (a+b) \wedge (a^2 - ab + b^2) = \begin{cases} 1 \\ 3 \end{cases} ; (a^2+b^2) \wedge ab = 1 \ ; \ (2a+b) \wedge (5a+2b) = 1.$$

EXERCICE 3.2.3. **F**
On pose $d = a \wedge b$, $m = a \vee b$; trouver tous les couples (a, b) vérifiant l'une des propriétés :

$$8m = 105d + 30$$
$$m = 30, \ a^2 + b^2 = 325$$
$$m = d^2, \ m + d = 156$$

EXERCICE 3.2.4. **F**

(1) Trouver tous les triplets $(a, b, c) \in \mathbb{N}^3$ tels que a, b, c soient premiers et les trois termes consécutifs d'une suite arithmétique de raison 10.
(2) Soit $E = \{(u, v, w) \in \mathbb{Z}^3 \ ; 3u + 13v + 23w = 0\}$
   (*i*) Si $(v, w) \in \mathbb{Z}^2$, montrer que : $13v + 23w \equiv 0[3] \Leftrightarrow v \equiv w[3]$.
   (*ii*) En déduire que : $E = \{(-13k - 23k' - 12r, 3k + r, 3k' + r), (k, k') \in \mathbb{Z}^2, r \in \{0, 1, 2\}\}$.

EXERCICE 3.2.5. **D**
Soit n un entier naturel tel que 24 divise $n + 1$.
Montrer que 24 divise la somme des diviseurs de n.

EXERCICE 3.2.6. **D C**
On veut montrer que si $\frac{p}{q} \in \mathbb{Q}$ et si $0 < \frac{p}{q} < 1$ alors il existe $n \in \mathbb{N}$, $n \geqslant 2$ et il existe des a_i uniques, dans $\mathbb{N}$ tels que $0 \leqslant a_i \leqslant i - 1$ vérifiant :

$$\frac{p}{q} = \frac{a_2}{2!} + \frac{a_3}{3!} + \cdots + \frac{a_n}{n!}$$

(1) Chercher cette décomposition si $(p, q) \in \{(3, 8), (5, 7), (13, 21)\}$.
(2) Montrer que $n \leqslant q$, calculer n si $q = 84$.
(3) Prouver la propriété demandée et écrire un algorithme de décomposition.

EXERCICE 3.2.7. **F C**
Montrer qu'il existe des intervalles de $\mathbb{N}$ de longueur aussi grande que possible ne contenant aucun nombre premier.

EXERCICE 3.2.8. **F**
Soit $(a, b) \in \mathbb{Z} \times \mathbb{N}^*$.

(1) Résoudre dans $\mathbb{Z}$ les équations $E\left(\frac{a+x}{b}\right) = E\left(\frac{a}{b}\right)$, $E\left(\frac{a+x}{b}\right) = E\left(\frac{a}{b}\right) + 1$.

(2) Simplifier
$$E\left(\frac{a}{b}\right)+E\left(\frac{a+1}{b}\right)+\cdots+E\left(\frac{a+b-1}{b}\right).$$

Exercice 3.2.9. **I**
Trouver les entiers p et q sachant que le produit des diviseurs de $n=3^p5^q$ vaut 45^{42}.

Exercice 3.2.10. **D**
Soit $p\in\mathbb{N}$ tel que 2^p-1 soit un nombre premier.

(1) Montrer que p est premier.
(2) Montrer que $n=2^{p-1}(2^p-1)$ est parfait (i.e. n est égal à la somme de ses diviseurs stricts).
(3) Montrer que tout nombre parfait pair est de la forme $2^{p-1}(2^p-1)$ (p premier).

Exercice 3.2.11. **D**

(1) Montrer qu'il existe une infinité de nombres premiers de la forme $4k+3$.
(2) Montrer qu'il existe une infinité de nombres premiers de la forme $6k+5$.

Exercice 3.2.12. **I**
Soit $\mathcal{P}=\{p_1<p_2<\ldots<p_n<\ldots\}$ l'ensemble des nombres premiers.

(1) Montrer que $p_{n+1}\leqslant p_1p_2\ldots p_n+1$.
(2) En déduire que $p_n\leqslant 2^{2^n}$.
(3) Soit $x\geqslant 1$, on note $\pi(x)=\mathrm{Card}(\mathcal{P}\cap[1,x])$.
Montrer que, pour x assez grand, $\ln(\ln x)\leqslant\pi(x)\leqslant x$ (on utilisera et démontrera l'inégalité $e^{e^{n-1}}\geqslant 2^{2^n}$ pour $n\geqslant 3$).

Exercice 3.2.13. **D**

(1) Montrer qu'il existe une et une seule application $d:\mathbb{N}^*\to\mathbb{Z}$ telle que
- $d(p)=1$ pour tout nombre premier p,
- $\forall(u,v)\in(\mathbb{N}^*)^2$, $d(uv)=ud(v)+vd(u)$.

(2) Résoudre l'équation $d(n)=n$.

---

1. Indications :

Indication 1.1.1 On montre que $(i)\Rightarrow(ii)\Rightarrow(iii)\Rightarrow(iv)\Rightarrow(i)$.
La version f injective sera (i) f injective. (ii) $\forall x\in E$, $f^{-1}(\{f(x)\})=\{x\}$. (iii) $\forall X\subset E$, $f^{-1}(f(X))=X$. (iv) Le seul X de $\mathcal{P}(E)$ tel que $f(X)=f(E)$ est E.

Indication 1.1.2 On définit g sur $f(E)$ par $g(z)=h(x)$ pour $z=f(x)$, réciproque immédiate.
g est déterminé de façon unique ssi (f est surjective ou $\mathrm{Card}\,G=1$).

Indication 1.1.3 Il suffit d'utiliser les implications $g\circ f$ bijective $\Rightarrow$ g surjective et $h\circ g$ bijective $\Rightarrow$ g injective.

Indication 1.1.4 Si $A \subset E$: $A \neq \emptyset$, poser $\alpha = \sup\{x \mid (x,y) \in A\}$ et $\beta = \sup\{y, (\alpha, y) \in A\}$ si ce dernier ensemble est non vide, dans ce cas $(\alpha, \beta) = \sup A$, sinon montrer que $(\alpha, 0) = \sup A$. Si $E = [0,1]\times]0,1]$, la propriété ne subsiste pas (regarder le deuxième cas).

Indication 1.1.5 f est surjective, non injective.

Indication 1.1.6 h est injective mais non surjective en général (prendre un contre-exemple).

Indication 2.1.1 Si $x \in E$, poser A_x le seul ensemble d'une partition de E qui contient x et, si $\mathrm{Card}(A_x) = n - k + 1$, dénombrer les possibilités de construire une partition de E à partir de A_x.

Indication 2.1.2 Il suffit d'écrire l'égalité des coefficients de x^k.

Indication 2.1.3

(1) Poser $\mathfrak{S}_{n,h}$ ensemble des permutations laissant exactement h éléments invariants et réaliser ainsi une partition de $\mathfrak{S}_n$.
(2) Écrire $2^p = (1+1)^p$ et $0^p = (1-1)^p$.
(3) Raisonner par récurrence sur n en utilisant la relation du (2), on trouve ensuite que $p_n \sim n!/e$.

Indication 2.1.4 Le nombre cherché vaut $\binom{n}{p}$ (établir une bijection de l'ensemble des applications strictement croissantes de $[\![1,p]\!]$ dans $[\![1,n]\!]$ sur l'ensemble des parties à p éléments de $[\![1,n]\!]$).

Indication 2.1.5 Remplacer z par $n - x - y$ et discuter selon la parité de n.

Indication 2.1.6 $\mathrm{Card}\, F = 2^n$, $\mathrm{Card}\, G_A = 2^p$ et $\mathrm{Card}(H) = 3^n$.

Indication 2.1.7

(1) $S_{n+1,n} = n\binom{n+1}{2}(n-1)! = \frac{n(n+1)!}{2}$, $S_{p,2} = 2^p - 2$.
(2) Écrire que $\mathcal{F}(E,F) = \bigcup_{i\in[\![1,n]\!]}\{f \in \mathcal{F}(E,F) \mid \mathrm{Card}\, f(E) = i\}$ puis $\{f \in \mathcal{F}(E,F) \mid \mathrm{Card}\, f(E) = i\} = \bigcup_{\mathrm{Card}\, A=i}\{f \in \mathcal{F}(E,F) \mid f(E) = A\}$.

Indication 2.1.8 Le nombre cherché vaut $\binom{n}{a_1}\binom{n-a_1}{a_2}\binom{n-a_1-a_2}{a_3}\dots\binom{n-a_1-\dots-a_p}{a_p} = \frac{n!}{a_1!\dots a_p!}$.

Indication 2.1.9 Il y a $P_{n-1,p}$ partitions de E qui contiennent une partie X à p éléments, on dénombre les choix pour X et on enlève les redondances. $P_{n,p} = \frac{(np)!}{n!(p!)^n}$.

Indication 3.1.1

(1) Si xy^{-1} et zt^{-1} sont deux éléments de A^* alors $(xy^{-1})(zt^{-1})^{-1} = xt(yz)^{-1}$.
(2) Montrer que, pour $x \in G$, $\exists N \in \mathbb{N}^*$ tel que $x^N = e$. On trouve $A = A^*$.

Indication 3.1.2 Utiliser l'équivalence

$$AB = BA \Leftrightarrow \forall (a,b) \in A\times B, \begin{cases} (\exists (a',b') \in A\times B \ : ab = b'a') \\ \text{ et } \\ (\exists (a",b") \in A\times B \ : ba = a"b") \end{cases}.$$

Indication 3.1.3 Montrer que, s'il existe $x \in A \setminus B$ alors $B \subset A$ (considérer les xy où $y \in B$).

Indication 3.1.4
Considérer l'application N : $\mathbb{Z}[\sqrt{13}] \to \mathbb{Z}$ définie par $N(x + y\sqrt{13}) = x^2 - 13y^2$;

(1) Montrer que les éléments inversibles de $\mathbb{Z}[\sqrt{13}]$ vérifient $x^2 - 13y^2 = \pm 1$, puis que si $\alpha = x + y\sqrt{13}$ est inversible et supérieur à 1, alors $x > 0$ et $y > 0$ et que $18 + 5\sqrt{13}$ est le plus petit élément de $U > 1$. Montrer alors que $U \cap [1, +\infty[= \{(18+5\sqrt{13})^n,\ n \in \mathbb{N}\}$ et conclure.
(2) Utiliser N, remarquer enfin que $4 = 2.2 = (3 - \sqrt{13}).(-3 - \sqrt{13})$.

Indication 3.1.5 $\Rightarrow$ Écrire $x^n + a_{n-1}x^{n-1} + \dots + a_0 = 0$ avec a_0 non nul.
$\Leftarrow$ Reprendre le polynôme écrit ci-dessus avec $x = a^{-1}$ et multiplier par a^{n-1}.

Indication 3.2.1 Factoriser et se ramener à étudier 4 cas. On trouve si $(a,b)=(7,2)$ alors $x=50$, $y=48$, si $(a,b)=(11,5)$ alors $x=1512, y=1511$; $x=305, y=300$; $x=143, y=132$; $x=73, y=48$ (cas non triviaux).

Indication 3.2.2 $(a+b)\wedge a=(a+b)\wedge b=1$ puis on écrit $a^2-ab+b^2=(a+b)^2-3ab$, $a^2+b^2=(a+b)^2-2ab$ et pour la dernière, on utilise Bézout.

Indication 3.2.3 Si $8m=105d+30$ alors $m=30(1+7k)$, $d=2(1+8k)$ et l'ensemble des solutions est donné par $\{(6,10),(10,6),(2,30),(30,2)\}$.
Si $m=30$, $a^2+b^2=325$ on trouve : $(a,b)\in\{(10,15),(15,10)\}$.
Enfin, pour $m=d^2$, $m+d=156$, les couples (a,b) solutions sont : $(36,48)$ et $(48,36)$.

Indication 3.2.4

(1) $a=3, b=13, c=23$ est la seule solution.
(2) (i) Se placer dans $\mathbb{Z}/3\mathbb{Z}$, (ii) $\dot{v}=\dot{w}=r$.

Indication 3.2.5 Soit $n=24k-1=pq$ alors montrer que $p\neq q$, poser $p=24k-1-h$ et $q=\frac{24k-1}{24k-1-h}$ et montrer que $(p+q)p^2\equiv 0\ [24]$ puis regrouper les diviseurs de n par couples dont la somme est un multiple de 24.

Indication 3.2.6

(1) On trouve $\frac{3}{8}=\frac{2}{3!}+\frac{1}{4!}$, $\frac{5}{7}=\frac{1}{2!}+\frac{1}{3!}+\frac{1}{4!}+\frac{0}{5!}+\frac{4}{6!}+\frac{2}{7!}$, $\frac{13}{21}=\frac{1}{2!}+\frac{0}{3!}+\frac{2}{4!}+\frac{4}{5!}+\frac{1}{6!}+\frac{5}{7!}$.
(2) Montrer par récurrence que $\frac{p}{q}=\frac{a_2}{2}+\cdots+\frac{a_m}{m!}+\frac{r_m}{qm!}$ avec $a_i\leqslant i-1$ et $r_m<q$ puis prouver qu'il existe $n\in\mathbb{N}$ tel que $r_n=0$. Avec $q=84=2^2.3.7$ on aura $n=7$.
Montrer ensuite l'unicité de la décomposition.

Indication 3.2.7 Prendre $[\![N!+2, N!+N]\!]$.

Indication 3.2.8

(1) On a l'équivalence $E\left(\frac{a+x}{b}\right)=E\left(\frac{a}{b}\right)+1\Leftrightarrow 1\leqslant\frac{r+x}{b}<2\Leftrightarrow b-r\leqslant x\leqslant 2b-r-1$.
(2) On a alors $E\left(\frac{a}{b}\right)+\cdots+E\left(\frac{a+b-1}{b}\right)=(b-r)q+r(q+1)=a$.

Indication 3.2.9 On trouve $q=3$, $p=6$.

Indication 3.2.10

(1) Raisonner par l'absurde.
(2) Tout diviseur de n s'écrit $2^k(2^p-1)$.
(3) Écrire $n=2^ab$ où $a\geqslant 1$ et b est impair puis montrer que $2^{a+1}-1$ divise b, que b est premier.

Indication 3.2.11

(1) Raisonner par l'absurde et faire le produit des $4k+3$ premiers.
(2) On procède de même avec $6k+5$.

Indication 3.2.12

(1) Le nombre $P=p_1p_2\dots p_n+1$ n'est divisible par aucun des nombres premiers p_i.
(2) Montrer par récurrence que $p_n\leqslant 2^{2^n}$ en utilisant le (1).
(3) Si $x>1$ alors il existe $n\in\mathbb{N}^*$ tel que $e^{e^{n-1}}<x\leqslant e^{e^n}$, utiliser alors que pour $n\geqslant 3$ $e^{e^{n-1}}\geqslant 2^{2^n}$.

Indication 3.2.13

(1) Montrer par récurrence sur n que d est bien définie de manière unique.
(2) Montrer par récurrence que si p est premier alors $d(p^n)=np^{n-1}$ puis que si $n=p_1^{\alpha_1}\dots p_r^{\alpha_r}$ alors $d(n)=n\sum_{i=1}^r\frac{\alpha_i}{p_i}$.
La résolution de l'équation $d(n)=n$ donne $n=p^p$.

1. Solutions

Solution 1.1.1

$(i) \Rightarrow (ii)$: $\forall y \in F, \exists x \in E : y = f(x)$ donc $f(f^{-1}(\{y\})) \supset \{y\}$ ($f(f^{-1}(B)) \subset B$ cf remarque 7.1.9 page 114) on peut conclure

$$\forall y \in F, f(f^{-1}(\{y\})) = \{y\}.$$

$(ii) \Rightarrow (iii)$: évident car c'est vrai pour chaque élément de Y : l'image d'une réunion est la réunion des images, cf proposition 7.1.2 page 114.
$(iii) \Rightarrow (iv)$: $f^{-1}(Y) = \emptyset$ donc

$$Y = f(f^{-1}(Y)) = \emptyset.$$

$(iv) \Rightarrow (i)$: $\forall y \in F, f^{-1}(\{y\}) \neq \emptyset$ donc tout élément y de F a un antécédent, f est surjective.

La version f injective sera
(i) f injective. (ii) $\forall x \in E$, $f^{-1}(\{f(x)\}) = \{x\}$. (iii) $\forall X \subset E$, $f^{-1}(f(X)) = X$. (iv) Le seul X de $\mathcal{P}(E)$ tel que $f(X) = f(E)$ est E.

Solution 1.1.2 Il suffit de définir g sur $f(E)$. Pour $z \in f(E)$, $\exists x \in E : z = f(x)$. Si $x' \in E$ est tel que $f(x) = f(x')$ alors $h(x) = h(x')$ donc on peut poser : $g(z) = h(x)$ (bien défini car indépendant du choix de x)).
Réciproque immédiate.
On remarque que g n'est définie ainsi que sur l'image de f.
g est déterminé de façon unique ssi (f est surjective ou $\operatorname{Card} G = 1$).
En effet, supposons que g soit uniquement déterminé. Si on écarte le cas où $\operatorname{Card} G = 1$ (et dans ce cas il n'existe qu'une seule application de F dans G) alors cela signifie que pour tout x de F, il n'y a qu'un seul choix pour $g(x)$. Vu la remarque faite ci-dessus cela entraîne que $x \in \operatorname{Im} f$ pour tout x de F i.e. f surjective.
Là aussi la réciproque est immédiate.
Ce genre de résultat permet de *factoriser un morphisme*.

Solution 1.1.3 On utilise ici le résultat de la question (i) page 115.
$g \circ f$ bijective $\Rightarrow$ g surjective ;
$h \circ g$ bijective $\Rightarrow$ g injective,
donc g est bijective, d'où f et h sont aussi bijectives.

Solution 1.1.4 Soit $A \subset E$: $A \neq \emptyset$; on pose $\alpha = \sup\{x \mid (x, y) \in A\}$.

- S'il existe $y \in [0, 1]$ tel que : $(\alpha, y) \in A$, alors on pose $\beta = \sup\{y, (\alpha, y) \in A\}$ et dans ce cas : $(\alpha, \beta) = \sup A$.
  - (α, β) est bien un majorant de A. Si $(x, y) \in A$ alors $x \leqslant \alpha$.
    - Si $x = \alpha$ alors $y \leqslant \beta$ donc $(x, y) \leqslant (\alpha, \beta)$.
    - Si $x < \alpha$ alors $(x, y) < (\alpha, \beta)$.
  - (α, β) est le plus petit des majorants. Soit (x', y') un majorant de A alors $\forall (x, y) \in A$, $x' \geqslant x$ donc $x' \geqslant \alpha$ (par définition de α).
    - Si $x' > \alpha$ alors $(x', y') > (\alpha, \beta)$.
    - Si $x' = \alpha$ alors $\forall y \in [0, 1]$ tel que $(\alpha, y) \in A$ on a $y \leqslant y'$ d'où $\beta \leqslant y'$.

  Conclusion : on a bien a propriété annoncée.
- Si $\forall y \in [0, 1], (\alpha, y) \notin A$ alors : $(\alpha, 0) = \sup A$. La démonstration se fait de la même manière que dans l'autre cas.

On voit bien que, en regardant le $2^{iéme}$ cas ci-dessus, si $E = [0,1]\times]0,1]$, la propriété ne subsiste pas.

Solution 1.1.5

- f n'est pas injective (on a par exemple $f(1,0) = f(1,1)$.
- f est surjective. Soit $(a,b) \in \mathbb{R}^2$ alors on prend $x = a$ et une étude de la fonction $y \mapsto xy - y^3 - b$ prouve qu'il existe au moins une solution en y.

Solution 1.1.6

- h est injective, en fait il suffit que f ou g soit injective.
- h n'est pas surjective en général, si on prend $f = g$ où f est l'application identité de $\mathbb{R}$ alors $h(\mathbb{R}) = \{(x,x),\ x \in \mathbb{R}\} \neq \mathbb{R}^2$.

Solution 2.1.1 Soit $x \in E$ et $\mathcal{A}$ une partition de E, on peut raisonner sur le nombre d'éléments de A_x où A_x est le seul ensemble de la partition $\mathcal{A}$ qui contient x :
si $\mathrm{Card}(A_x) = n - k + 1$ le nombre de partitions correspondantes sera :

$$\binom{n}{n-k} P_k = \binom{n}{k} P_k$$

car on a $\binom{n}{n-k}$ possibilités pour choisir $n-k$ éléments de E complétant A_x et P_k partitions des k éléments restant (les cardinaux se multiplient).
D'où la relation en additionnant les cas rencontrés.

Solution 2.1.2 Il suffit d'écrire l'égalité des coefficients de x^k.

Solution 2.1.3

(1) On écrit que $\mathfrak{S}_n = \mathfrak{S}_{n,0} \cup \mathfrak{S}_{n,1} \cup \ldots \cup \mathfrak{S}_{n,n}$ où $\mathfrak{S}_{n,h}$ désigne l'ensemble des permutations laissant exactement h éléments invariants : $\mathrm{Card}(\mathfrak{S}_{n,h}) = \binom{n}{h} p_{n-h}$. On utilise alors la proposition 7.2.6 page 119 pour additionner les cardinaux de cette partition.

(2) On a : $\binom{n}{k}\binom{n-k}{p-k} = \binom{n}{p}\binom{p}{k}$, les deux relations s'obtiennent alors en écrivant que $2^p = (1+1)^p$ et $0^p = (1-1)^p$.

(3) On raisonne (par exemple) par récurrence sur n en utilisant la relation (2) ;

De façon plus précise, on veut prouver que $p_n = n! \sum_{k=0}^{n} \dfrac{(-1)^k}{k!} = q_n$. Comme les p_k sont déterminés de manière unique par la relation du 1, il suffit de prouver que la suite (q_n) vérifie la même relation :

$$\sum_{k=0}^{n} \binom{n}{k} q_k = \sum_{k=0}^{n} \frac{n!}{k!(n-k)!} \times k! \sum_{p=0}^{k} \frac{(-1)^p}{p!} = n! \underbrace{\sum_{k=0}^{n} \frac{1}{(n-k)!} \sum_{p=0}^{k} \frac{(-1)^p}{p!}}_{\sum_{p=0}^{n} \left(\sum_{k=p}^{n} \frac{(-1)^p}{p!(n-k)!} \right)}$$

$$= n! \sum_{p=0}^{n} \left(\sum_{k=0}^{n-p} \frac{(-1)^p}{p!k!} \right) = n! \sum_{p+k \leqslant n} \frac{(-1)^p}{p!k!}$$

et, en regroupant les termes de cette somme avec $q = p + k$, on obtient

$$\sum_{k=0}^{n} \binom{n}{k} q_k = n! \sum_{q=0}^{n} \left(\frac{1}{q!} \sum_{p=0}^{q} (-1)^p \binom{q}{p} \right) = n!$$

car toutes les sommes sur p sont nulles sauf celle qui correspond à $q = 0$. on trouve ensuite que $p_n \sim n!/e$.

Solution 2.1.4 Le nombre cherché vaut $\binom{n}{p}$ car on établit facilement une bijection de l'ensemble des applications strictement croissantes de $[\![1, p]\!]$ dans $[\![1, n]\!]$ sur l'ensemble des parties à p éléments de $[\![1, n]\!]$.

Solution 2.1.5 On remplace z par $n - x - y$ et l'ensemble des solutions s'écrit

$$S = \{(x, y, n - x - y) \mid x \leqslant n/2,\ n/2 - x \leqslant y \leqslant n/2\}.$$

- Si n est pair on a $\operatorname{Card} S = \dfrac{(n+2)(n+4)}{8}$.
- Si n est impair on a $\operatorname{Card} S = \dfrac{(n-1)(n+1)}{8}$.

Solution 2.1.6

(1) $A \mapsto (A, A^c)$ établit une bijection de $\mathcal{P}(E)$ sur F donc $\operatorname{Card} F = 2^n$.
(2) $X \in \mathcal{P}(A) \mapsto A^c \cup X$ est une bijection de $\mathcal{P}(A)$ sur G_A donc $\operatorname{Card} G_A = 2^p$.
(3) $H = \bigcup_{A \subset E} \{(A, B) \mid B \in G_A\}$ donc

$$\operatorname{Card}(H) = \sum_{A \subset E} \operatorname{Card}(G_A) = \sum_{p=0}^{n} \binom{n}{p} = (1+2)^n = 3^n.$$

Solution 2.1.7

(1) $S_{n+1,n} = n\binom{n+1}{2}(n-1)! = \dfrac{n(n+1)!}{2}$ car on choisit un élément parmi n de l'ensemble d'arrivée qui a 2 antécédents, on choisit les 2 antécédents parmi $n+1$ de l'ensemble de départ et enfin on a $(n-1)!$ façons de construire les images des autres éléments.
$S_{p,2} = 2^p - 2$ car il n'y a que 2 applications non surjectives de E dans F qui sont les deux applications constantes.
(2) On a la réunion disjointe suivante

$$\mathcal{F}(E, F) = \bigcup_{i \in [\![1,n]\!]} \{f \in \mathcal{F}(E, F) \mid \operatorname{Card} f(E) = i\}$$

Puis $\{f \in \mathcal{F}(E, F) \mid \operatorname{Card} f(E) = i\} = \bigcup_{\operatorname{Card} A = i} \{f \in \mathcal{F}(E, F) \mid f(E) = A\}$ où la réunion est aussi disjointe. Mais comme $\operatorname{Card}\{f \in \mathcal{F}(E, F) \mid f(E) = A\} = S_{p,i}$ pour $\operatorname{Card} A = i$ on a $\operatorname{Card}\{f \in \mathcal{F}(E, F) \mid \operatorname{Card} f(E) = i\} = \binom{n}{i} S_{p,i}$ d'où la relation demandée.

Solution 2.1.8 Le nombre cherché vaut

$$\binom{n}{a_1}\binom{n-a_1}{a_2}\binom{n-a_1-a_2}{a_3}\cdots\binom{n-a_1-\cdots-a_p}{a_p}=\frac{n!}{a_1!\ldots a_p!}.$$

Solution 2.1.9 Il y a en tout $P_{n-1,p}$ partitions de E qui contiennent une partie X à p éléments. Comme on a $\binom{np}{p}$ choix pour X, cela fait $\binom{np}{p}P_{n-1,p}$ qui sont constitués de n partie à p éléments mais dans ce décompte, on retrouve n fois chaque partition d'où la réponse.
Il est immédiat ensuite de déduire que $P_{n,p}=\dfrac{(np)!}{n!(p!)^n}$.

Solution 3.1.1

(1) A^* est non vide par définition et si xy^{-1} et zt^{-1} sont deux éléments de A^* alors

$$(xy^{-1})(zt^{-1})^{-1}=xy^{-1}tz^{-1}=xt(yz)^{-1}$$

car G est abélien.

(2) Si G est fini alors, si x est un élément de G, il vérifie $(x)\subset G$ donc $\exists N\in\mathbb{N}^*$ tel que $x^N=e$.
Conclusion : A est stable contient e et l'inverse de tous ses éléments, A est donc un groupe.
On trouve ensuite $A=A^*$.

Solution 3.1.2 On a :

$$AB=BA\Leftrightarrow\forall(a,b)\in A\times B,\begin{cases}(\exists(a',b')\in A\times B\ :ab=b'a')\\ \text{ et}\\ (\exists(a",b")\in A\times B\ :ba=a"b")\end{cases}$$

on garde cette notation pour la suite i.e. si $AB=BA$ et si $(x,y)\in A\times B$ alors $xy=y'x'$ et $yx=x''y''$.

($\Leftarrow$) Montrons que P est un sous-groupe : $e=ee\in P$ puis $a_1b_1a_2b_2=a_1(b_1a_2)b_2=a_1a"_2b"_1b_2\in P$.
Enfin $(ab)^{-1}=b^{-1}a^{-1}=(a^{-1})"(b^{-1})"\in P$ donc P est un sous-groupe.

($\Rightarrow$) $(ba)^{-1}=a^{-1}b^{-1}\in BA$, donc $\exists(a",b")\in A\times B:\ a^{-1}b^{-1}=b"a"$, d'où : $ba=a"^{-1}b"^{-1}$.

On démontre de même l'autre propriété d'où l'équivalence.

Solution 3.1.3 Supposons $A\not\subset B$: i.e. $\exists x\in A\ :x\notin B$.
Or $\forall y\in B$, $xy\in A\cup B$, comme : $xy\in B$ est impossible (sinon $x=xy.y^{-1}\in B$), on a : $xy\in A$ donc

$$y=x^{-1}xy\in A$$

i.e. $B\subset A$ c.q.f.d.
La solution est relativement simple mais l'exercice n'est pas évident de prime abord.

Solution 3.1.4 La clé de cet exercice est de considérer l'application $N\ :\mathbb{Z}[\sqrt{13}]\to\mathbb{Z}$ définie par $N(x+y\sqrt{13})=x^2-13y^2$;

(1) Les éléments inversibles de $\mathbb{Z}[\sqrt{13}]$ vérifient nécessairement $x^2 - 13y^2 = \pm 1$ (car si $z = x + \sqrt{13}y$ est inversible dans $\mathbb{Z}[\sqrt{13}]$ alors $N(z)$ est inversible dans $\mathbb{Z}$).
On a de plus $18^2 - 5.13 = -1$ donc $18 + 5\sqrt{13}$ est inversible dans $\mathbb{Z}[\sqrt{13}]$.
Montrons maintenant que si $\alpha = x + y\sqrt{13}$ est inversible et supérieur à 1, alors $x > 0$ et $y > 0$: en effet,
$\alpha^{-1} = x' + y'\sqrt{13} \in]0, 1[$ donc x' et y' ne peuvent être de même signe (sinon α^{-1} serait négatif ou supérieur à 1).
Comme xy et $x'y'$ sont de signe contraire ($\alpha^{-1} = \dfrac{x - y\sqrt{13}}{N(\alpha)}$) on en déduit que $x > 0$ et $y > 0$.
Pour finir, il suffira de prouver (en examinant les cas $y = 1, 2, 3, 4, 5$) que $y = 5$.
Maintenant, soit $\alpha \in U \cap \mathbb{R}$, $\alpha > 1$, on pose $E_\alpha = \{p \in \mathbb{N} \mid \alpha\alpha_0^{-p} \geqslant 1\}$ où $\alpha_0 = 18 + 5\sqrt{13}$. Comme E_α est un ensemble majoré de $\mathbb{N}$, on pose $n = \max E_\alpha$. On obtient : $\alpha\alpha_0^{-n} \geqslant 1$ et $\alpha\alpha_0^{-(n+1)} < 1$ donc $1 \leqslant \alpha\alpha_0^{-n} < \alpha_0$ ce qui entraîne $\alpha = \alpha_0^n$.
Si $0 < \alpha < 1$, on s'intéresse à $1/\alpha$ et si $\alpha < 0$, on prend $-\alpha$.

(2) Si $2 = rs$ alors $N(2) = 4 = N(r)N(s)$. Or, en raisonnant sur la parité, on montre que $N(r)$ ne peut être congru à 2 modulo 4, donc $N(r)$ ou $N(s)$ vaut 1, i.e. 2 est irréductible. Il en est de même pour $3 - \sqrt{13}$ et $-3 - \sqrt{13}$.
On remarque enfin que $4 = 2.2 = (3 - \sqrt{13}).(-3 - \sqrt{13})$.
Ceci montre que la décomposition en éléments irréductibles dans un anneau intègre quelconque n'est pas immédiate dans le cas général.

Solution 3.1.5
$\boxed{\Rightarrow}$ Si A est un corps alors pour tout x de B on sait que $x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0$. On peut supposer a_0 non nul car B est intègre. Dans ce cas là, $x[x^{n-1} + \cdots + a_1] = -a_0$ donc x est inversible et B est un corps.
$\boxed{\Leftarrow}$ On reprend le polynôme écrit ci-dessus en prenant pour x, l'inverse d'un élément a de A non nul. Alors, en multipliant l'égalité par a^{n-1} on aura : $x = -a_{n-1} - \cdots - a_0 a^{n-1}$, i.e. $x \in A$ c.q.f.d.

Solution 3.2.1 On a $(x - y)(x + y) = a^2b^2$ d'où les 4 cas :

$$x - y = 1, x + y = a^2b^2 \; ; x - y = b, x + y = a^2b \; ; x - y = a, x + y = ab^2 \; ; x - y = b^2, x + y = a^2.$$

- Si $(a, b) = (7, 2)$ alors le seul cas non trivial est : $x = 50$, $y = 48$.
- Si $(a, b) = (11, 5)$ alors on trouve :

$$x = 1512, y = 1511 \; ; x = 305, y = 300 \; ; x = 143, y = 132 \; ; x = 73, y = 48.$$

Solution 3.2.2 On a : $(a + b) \wedge a = 1$ et $(a + b) \wedge b = 1$ d'où $(a + b) \wedge ab = 1$ en utilisant la propriété 7.3.7 page 125.
$a^2 - ab + b^2 = (a + b)^2 - 3ab \Rightarrow (a + b) \wedge ((a + b)^2 - 3ab) = (a + b) \wedge 3ab$. Donc

- $(a + b) \wedge (a^2 - ab + b^2) = 3$ si $3|(a + b)$ et
- $(a + b) \wedge (a^2 - ab + b^2) = 1$ sinon.

On remarque que $a^2 + b^2 = (a + b)^2 - 2ab$ et on fait de même.
Enfin, on pose $a' = 2a + b, b' = 5a + 2b \Rightarrow a = b' - 2a', b = 5a' - 2b'$ et on remplace dans Bézout.

Solution 3.2.3

- Si $8m = 105d + 30$ alors $15|m$ et $2|d$ et comme $d|m$ on en déduit que $30|m$. En posant $m = 30m'$ et $d = 2d'$, on a $8m' - 7d' = 1$ soit, en utilisant le résultat de la question (iv) page 125 on obtient $m' = 1+7k$, $d' = 1+8k$ ce qui donne $m = 30(1+7k)$, $d = 2(1+8k)$.

  On a ensuite, comme $m|d$, $1+8k|15(1+7k)$ et comme $1+8k$ et $1+7k$ sont premiers entre eux, $1+8k|15$ (cf le théorème de Gauss 7.6 page 124) ce qui entraîne $k = 0$ (car $k \geqslant 0$, le p.p.c.m. et le p.g.c.d. sont positifs). On a donc $m = 30$, $d = 2$, si on pose $a = 2a'$, $b = 2b'$ alors $a' \wedge b' = 1$ et $a'b' = 15$ donc $a' = 3$, $b' = 5$ est solution et l'ensemble des solutions est donné par $\{(6, 10), (10, 6), (2, 30), (30, 2)\}$.
- On trouve : $(a, b) \in \{(10, 15), (15, 10)\}$, en effet, si $d = 1$ alors $ab = m$ (cf proposition 7.3.6 page 124) donc 5 divise l'un des deux nombres a ou b mais comme 5 divise $a^2 + b^2$, il divise l'autre, ce qui est impossible. Conclusion : $d \neq 1$.

  On a alors $d^2(a'^2 + b'^2) = 325$ (en posant $a = da'$, $b = db'$). Or le seul carré divisant 325 est 25 donc $d = 5$, la conclusion est alors immédiate.
- Enfin, pour $m = d^2$, $m + d = 156$, on écrit $a = a'd$, $b = b'd$, puis, comme $ab = md$ (cf proposition 7.3.6 page 124) on a

$$ab = a'b'd^2 = d^3$$

  donc $d = a'b'$. On a ensuite $d(d + 1) = 156$ qui admet la seule solution positive $d = 12$ d'où les couples (a, b) solutions : $(36, 48)$ et $(48, 36)$.

Solution 3.2.4

(1) $a = 3, b = 13, c = 23$ seule solution car nécessairement l'un des trois est divisible par 3.
(2) (i) Dans $\mathbb{Z}/3\mathbb{Z}$: $\dot{v} - \dot{w} = 0$ c.q.f.d.
$(ii)\dot{v} = \dot{w} = r$, le reste est immédiat.

Solution 3.2.5 Soit $n = 24k - 1 = pq$. $p \neq q$ car $p^2 \equiv -1[4]$ est impossible (cf. remarque ci-dessous) alors posons $p = 24k - 1 - h$ et $q = \dfrac{24k-1}{24k-1-h}$. On peut choisir h pair car n est impair et p ou q est impair (ici, on a pris p impair) ; d'autre part p et 24 sont premiers entre-eux.

$$\begin{aligned}(p+q)p^2 &\equiv [(-1-h)(24k-1-h)-1](24k-1-h)\ [24]\\ &\equiv -[(1+h)^2-1](h+1)\ [24]\\ &\equiv -h(h+1)(h+2) \equiv 0\ [24]\end{aligned}$$

car $h(h + 1)(h + 2)$ est un multiple de 3 et que, comme h est pair, c'est aussi un multiple de 8. Comme $24k - pq = 1$ alors $p \wedge 24 = 1$ (Bézout) donc $24|p + q$. On peut alors regrouper les diviseurs de n par couples dont la somme est un multiple de 24.
Remarque : en utilisant les anneaux $\mathbb{Z}/n\mathbb{Z}$ (cf. page 175) on peut proposer la solution plus élégante qui suit :
Si $kk' = n$, prouvons que $24|k + k'$:
dans $\mathbb{Z}/24\mathbb{Z}$, les éléments inversibles sont de la forme $6c\pm1$ et comme $(6c\pm1)^2 = 1$, ils sont égaux à leur propre inverse.
Or $kk' \equiv -1$ est équivalent à $ab = -1$ où a et b désignent les classes respectives de k et k' donc $a + b = 0$ c.q.f.d.
Donc, si n n'est pas un carré parfait, on pourra regrouper les diviseurs de n 2 par 2 et avoir ainsi $\sum_{d|n} d \equiv 0\ [24]$.
Si $n = p^2$, alors p est impair et $n \equiv 1\ [4]$ ce qui n'est pas possible car on doit avoir $n \equiv -1\ [24]$.

Solution 3.2.6

(1) On trouve $\frac{3}{8}=\frac{2}{3!}+\frac{1}{4!}$, $\frac{5}{7}=\frac{1}{2!}+\frac{1}{3!}+\frac{1}{4!}+\frac{0}{5!}+\frac{4}{6!}+\frac{2}{7!}$, $\frac{13}{21}=\frac{1}{2!}+\frac{0}{3!}+\frac{2}{4!}+\frac{4}{5!}+\frac{1}{6!}+\frac{5}{7!}$.

(2) On montre par récurrence que

$$(H_m)\qquad \frac{p}{q}=\frac{a_2}{2}+\cdots+\frac{a_m}{m!}+\frac{r_m}{qm!}\quad \text{avec } a_i\leqslant i-1 \text{ et } r_m<q$$

Pour (H_2) c'est OK.

$H_m\Rightarrow H_{m+1}$: On a $r_m(m+1)=a_{m+1}q+r_{m+1}$ par division euclidienne donc $a_{m+1}\leqslant m$ et $r_{m+1}<q$ et

$$\frac{r_m}{qm!}=\frac{a_{m+1}}{(m+1)!}+\frac{r_{m+1}}{q(m+1)!}$$

ce qui achève la récurrence.

Cet algorithme se poursuit tant que $r_m\neq 0$. Soit n le plus petit entier tel que $q|n!$ alors, compte tenu de la récurrence précédente, on a

$$\frac{p}{q}=\frac{a_2}{2}+\cdots+\frac{a_n}{n!}+\frac{r_n}{qn!}.$$

On multiplie alors par $n!$ et on obtient $\frac{r_n}{q}\in\mathbb{Z}$ donc $r_n=0$.

En fait, on trouve $a_2=\left[\frac{2p}{q}\right]$, $a_m=\left[\left(\frac{(m-1)!p}{q}-\frac{(m-1)!a_2}{2}-\cdots-a_{m-1}\right)m\right]$.

Avec $q=84=2^2.3.7$ on aura $n=7$.

Il reste à prouver l'unicité de la décomposition. En effet, on a bien entendu unicité par construction mais rien ne nous dit qu'il y a unicité de la solution.

Supposons donc que l'on ait

$$\frac{p}{q}=\frac{a_2}{2!}+\frac{a_3}{3!}+\cdots+\frac{a_n}{n!}=\frac{a'_2}{2!}+\frac{a'_3}{3!}+\cdots+\frac{a'_n}{n!}$$

(on a pris le même entier n quitte à compléter par des 0).

On raisonne alors par l'absurde : soit $i\in[2,n]$ le plus petit entier tel que $a_i\neq a'_i$, on peut supposer que $a_i>a'_i$. On a alors

$$\underbrace{a_i-a'_i}_{\geqslant 1}=\underbrace{\frac{a'_{i+1}-a_{i+1}}{i+1}}_{\leqslant \frac{i}{i+1}=1-\frac{1}{i+1}}+\cdots+\underbrace{\frac{a'_n-a_n}{n(n-1)(\ldots)(i+1)}}_{\leqslant \frac{1}{(n-1)(\ldots)(i+1)-\frac{1}{n(\ldots)(i+1)}}}$$

On arrive alors à la contradiction

$$1\geqslant a_i-a'_i\geqslant 1-\frac{1}{n(\ldots)(i+1)}$$

ce qui permet de conclure.

(3) On a l'algorithme suivant qui permet de faire la décomposition :

```
> u:=proc(p,q)
> local n,a,b;
> b:=p;n:=1;
> while b<>0 do
>   n:=n+1;a:=floor(b*n/q); print (a,n);
>   b:=b*n-a*q
> od;
> end;
```

Solution 3.2.7 Soit $N \geqslant 2$ alors l'intervalle $[\![N!+2, N!+N]\!]$ est de longueur $N-1$ et ne contient aucun nombre premier.

Solution 3.2.8

(1) Soit $a = bq + r$, $0 \leqslant r < b$ la division euclidienne de a par b.

$$E\left(\frac{a+x}{b}\right) = E\left(\frac{a}{b}\right) \Leftrightarrow 0 \leqslant \frac{r+x}{b} < 1 \Leftrightarrow -r \leqslant x \leqslant b-r-1$$

$$E\left(\frac{a+x}{b}\right) = E\left(\frac{a}{b}\right) + 1 \Leftrightarrow 1 \leqslant \frac{r+x}{b} < 2 \Leftrightarrow b-r \leqslant x \leqslant 2b-r-1$$

(2) On a alors

$$\begin{aligned} E\left(\frac{a}{b}\right) + \cdots + E\left(\frac{a+b-1}{b}\right) &= \sum_{0 \leqslant x \leqslant b-r-1} E\left(\frac{a+x}{b}\right) + \sum_{b-r \leqslant x \leqslant b-1} E\left(\frac{a+x}{b}\right) \\ &= (b-r)q + r(q+1) = a. \end{aligned}$$

Solution 3.2.9 Si $m|n$ alors $m = 3^i 5^j$ et le produit des diviseurs de m vaut

$$\prod_{(i,j) \in [\![0,p]\!] \times [\![0,q]\!]} 3^i 5^j = \left(3^{\frac{p(p+1)}{2}}\right)^{q+1} \left(5^{q(q+1)}\right)^{p+1}.$$

donc on a à résoudre les équations $p(p+1)(q+1) = 168$ et $q(q+1)(p+1) = 84$ d'où $p = 2q$ et $q = 3$, $p = 6$.

Solution 3.2.10

(1) Si p n'est pas premier alors $p = hk$ et $2^{hk} - 1 = (2^h - 1)a$ n'est pas premier.

(2) Comme $2^p - 1$ est premier on a la décomposition de n en produit de facteurs premiers. Tout diviseur de n s'écrit $2^k(2^p - 1)$, $k \leqslant p-2$ où 2^k et le résultat est immédiat.

(3) Soit n un nombre parfait pair, $n = 2^a b$ où $a \geqslant 1$ et b est impair. Si on note $\Sigma(n)$ la somme des diviseurs de n (n y compris) alors on a

$$\Sigma(n) = (2^{a+1} - 1)\Sigma(b) = 2n = 2^{a+1} b$$

et comme $2^{a+1}-1$ et 2^{a+1} sont premiers entre eux, $2^{a+1}-1$ divise b. $\Sigma(b) = b + \dfrac{b}{2^{a+1}-1}$. b est nécessairement premier car la somme des diviseurs de b est $b + \dfrac{b}{2^{a+1}-1}$, b et $\dfrac{b}{2^{a+1}-1}$ sont les seuls diviseurs de b.
Conclusion : b est premier et $b = 2^{a+1} - 1$.

Solution 3.2.11

(1) Supposons qu'il n'existe qu'un nombre fini de nombres premiers de la forme $4k+3$. On note $n = 3 \times 7 \times \ldots \times 4p + 3$ leur produit. Soit $m = 4n - 1$, m n'est divisible par aucun nombre premier de la forme $4k+3$. Tous les facteurs premiers de m sont donc de la forme $4k+1$, le reste de la division de m par 4 est donc 1 ce qui est impossible.

(2) On procède de même en faisant le produit des nombres premiers de la forme $6k+5$ et en prenant cette fois-ci le nombre $6n-1$.

Solution 3.2.12

(1) Le nombre $P = p_1 p_2 \dots p_n + 1$ n'est divisible par aucun des nombres premiers p_i, $i \in [\![1, n]\!]$ donc soit il est premier soit il est divisible par un nombre premier $> p_n$. On a bien $p_{n+1} \leqslant P$.

(2) Montrons par récurrence que $p_n \leqslant 2^{2^n}$.
C'est évidemment vrai pour $n = 1$.
On suppose la propriété vraie jusqu'à l'ordre n alors

$$\begin{aligned} p_{n+1} &\leqslant p_1 \dots p_n + 1 \leqslant 2^{2^1} \dots 2^{2^n} + 1 \\ &\leqslant 2^{2^{n+1}-2} + 1 < 2^{2^{n+1}} + 1. \end{aligned}$$

(3) Si $x > 1$ alors il existe $n \in \mathbb{N}^*$ tel que $e^{e^{n-1}} < x \leqslant e^{e^n}$ et comme pour $n \geqslant 3$ $e^{e^{n-1}} \geqslant 2^{2^n}$ alors, pour $x > e^{e^2}$ on a

$$\pi(x) \geqslant \pi\left(e^{e^{n-1}}\right) \geqslant \pi\left(2^{2^n}\right) \geqslant n \geqslant \ln(\ln x).$$

Comme il est évident que $x \geqslant \pi(x)$ on a bien l'encadrement demandé.
Remarque : le théorème des nombres premiers nous dit plus précisément que $\pi(x) \sim \dfrac{x}{\ln x}$.

Solution 3.2.13

(1) On montre par récurrence sur n que d est bien définie de manière unique.
$n = 1$ OK.
Si d est définie pour $k \leqslant n$ alors, si $n+1$ est premier c'est OK, si $n+1 = uv$ avec $u \leqslant n$, $v \leqslant n$ on utilise la propriété.
Si d' est une autre application qui vérifie les mêmes propriétés alors $(d - d')(n) = 0$ pour tout n par récurrence.

(2) On montre par récurrence sur n que, si p est premier alors $d(p^n) = np^{n-1}$.
Par récurrence sur r, on montre que, si $n = p_1^{\alpha_1} \dots p_r^{\alpha_r}$ alors $d(n) = n \sum_{i=1}^{r} \dfrac{\alpha_i}{p_i}$.
La résolution de l'équation $d(n) = n$ donne $\sum_{i=1}^{r} \dfrac{\alpha_i}{p_i} = 1$. Supposons $\alpha_1 \neq 0$ alors $\alpha_1 p_2 \dots p_r = p_1 k$ en multipliant par $p_1 \dots p_r$ donc, par le théorème de Gauss, $p_1 | \alpha_1$ d'où $\alpha_i = 0$ pour $i \geqslant 2$. Nécessairement $n = p^p$ (en posant $p_1 = p$).
Réciproquement, $d(p^p) = p^p$ donc les seules solutions de cette équation sont les entiers de la forme $n = p^p$ où p est un nombre premier.
