Corrigé de la Série 2

1.2. & 1.3. Récurrence et nombres entiers

1. Soit l'affirmation $A(n)$: "le nombre $10^n + 1$ est un multiple de 3".

(a) Montrer que pour tout $n \in \mathbb{N}$, si $A(n)$ est vraie, alors $A(n+1)$ est vraie aussi.

(b) Pourquoi ne peut-on pas conclure par récurrence que $\forall n \in \mathbb{N}$, $A(n)$ est vraie?

(a) Supposons que $10^n + 1$ soit un multiple de 3 pour un certain $n \in \mathbb{N}$. On peut donc écrire $10^n + 1 = 3m$ pour un $m \in \mathbb{N}$. Mais alors,

$$10^{n+1} + 1 = 10 \times 10^n + 1 = 10^n + 1 + 9 \times 10^n = 3(m + 3 \times 10^n)$$

et $10^{n+1} + 1$ est un multiple de 3 aussi.

(b) Pour $n = 0$ on a $10^n + 1 = 10^0 + 1 = 2$, qui n'est pas un multiple de 3. On ne peut donc pas initialiser le raisonnement par récurrence en prenant $n_0 = 0$.
Pour $n = 1$ on a $10^n + 1 = 10^1 + 1 = 11$, qui n'est pas un multiple de 3. On ne peut donc pas initialiser le raisonnement par récurrence en prenant $n_0 = 1$.
En fait, on peut même montrer par récurrence, qu'aucun nombre naturel qui s'écrit comme 10^n+1 n'est multiple de 3. En effet, on montre d'abord facilement que

$$10^n + 1 = 2 + 10^n - 1 = 2 + 9\sum_{k=0}^{n-1} 10^k.$$

La somme $9\sum_{k=0}^{n-1} 10^k$ est clairement un multiple de 3 alors que 2 ne l'est pas. Ainsi, c'est l'affirmation contraîre qui est vraie: $\forall n \in \mathbb{N}$, $10^n + 1$ n'est pas un multiple de 3.

2. On définit sur $\mathbb{N}^2$ la relation

$$(n, m) \sim (n', m') \Leftrightarrow n + m' = m + n'.$$

(a) Déterminer parmi les couples suivants, ceux qui sont en relation:

$$(1, 3),\ (2, 5),\ (7, 2),\ (4, 6),\ (5, 0).$$

(b) Montrer que $\sim$ est une relation d'équivalence sur $\mathbb{N}$, i.e.

i. $\forall (n, m) \in \mathbb{N}^2$, $(n, m) \sim (n, m)$,

ii. $\forall (n, m), (n', m') \in \mathbb{N}^2$, $(n, m) \sim (n', m')$ implique $(n', m') \sim (n, m)$,

iii. $\forall (n, m), (n', m'), (n'', m'') \in \mathbb{N}^2$, $(n, m) \sim (n', m')$ et $(n', m') \sim (n'', m'')$ impliquent $(n, m) \sim (n'', m'')$.

(a) $(1, 3) \sim (4, 6)$, car $1 + 6 = 3 + 4$.
$(7, 2) \sim (5, 0)$, car $7 + 0 = 2 + 5$.
$(2, 5)$ n'est en relation avec aucun des quatre autres couples de nombres naurels.

(b) i. Clairement, $\forall (n,m) \in \mathbb{N}^2$, $m+n = m+n$, d'où $(n,m) \sim (n,m)$.

ii. Si $(n,m) \sim (n',m')$, on a par définition $n+m' = n'+m = n+m'$, d'où $(n',m') \sim (n,m)$.

iii. Si $n+m' = n'+m$ et $n'+m'' = n''+m'$, alors $n+m''+(n'+m') = n+m'+n'+m'' = n'+m+n''+m' = n''+m+(n'+m')$, et puisque $\mathbb{N}$ possède la propriété de simplification, on a $n+m'' = m+n''$. Ainsi, $(n,m) \sim (n',m')$ et $(n',m') \sim (n'',m'')$ impliquent $(n,m) \sim (n'',m'')$:

3. Pour tout $(m,n) \in \mathbb{N}^2$ on définit la classe d'équivalence

$$[(m,n)] := \{(m',n') \in \mathbb{N}^2 \,:\, (m',n') \sim (m,n)\}.$$

On pose alors l'opération

$$[(m,n)] + [(m',n')] := [(m+m', n+n')].$$

(a) Décrire l'ensemble qui correspond à la classe d'équivalence $[(1,3)]$.

(b) Décrire l'ensemble qui correspond à la classe d'équivalence $[(1,3)] + [(3,1)]$.

(c) Montrer que l'ensemble des classes d'équivalences $\{[(n,m)] \,:\, (n,m) \in \mathbb{N}^2\}$ muni de $+$ est un groupe commutatif.

(a) On a par définition

$$\begin{gathered}[(1,3)] := \{(m',n') \in \mathbb{N}^2 \,:\, (m',n') \sim (1,3)\} \\ = \{(m',n') \in \mathbb{N}^2 \,:\, m'+3 = n'+1\} = \{(m',n') \in \mathbb{N}^2 \,:\, n' = m'+2\}\end{gathered}$$

(b) On a par définition

$$\begin{gathered}[(1,3)] + [(3,1)] := [(1+3, 3+1)] = [(4,4)] \\ = \{(m',n') \in \mathbb{N}^2 \,:\, (m',n') \sim (4,4)\} = \{(m',n') \in \mathbb{N}^2 \,:\, m'+4 = n'+4\} \\ = \{(m',n') \in \mathbb{N}^2 \,:\, n' = m'\} = [(0,0)].\end{gathered}$$

(c) i. $+$ est commutative: en effet,
$[(a,b)] + [(n,m)] = [(a+n, b+m)] = [(n+a, m+b)] = [(n,m)] + [(a,b)]$.

ii. $+$ est associative: en effet,

$$\begin{gathered}[(a,b)] + \big([(k,l)] + [(n,m)]\big) = [(a,b)] + [(k+n, l+m)] \\ = [(a+k+n, b+l+m)] = \\ = [(a+k, b+l)] + [(n,m)] = \big([(a,b)] + [(k,l)]\big) + [(n,m)].\end{gathered}$$

iii. $+$ possède un élément neutre: en effet, pour tout $(a,b) \in \mathbb{N}^2$, on a

$$[(a,b)] + [(0,0)] = [(a,b)] = [(0,0)] + [(a,b)].$$

iv. Chaque classe $[(a,b)]$ possède une réciproque pour l'opération $+$: en effet, on remarque déjà que puisque $\forall (n,n) \in \mathbb{N}^2$, $(n,n) \sim (0,0)$ on a $[(0,0)] = [(n,n)]$. Puis,

$$[(b,a)] + [(a,b)] = [(a,b)] + [(b,a)] = [(a+b, a+b)] = [(0,0)].$$

4. Vrai ou faux (donner un contre-exemple si c'est faux)?

(a) l'opération $n \star m := n^m$ est commutative sur $\mathbb{N}$.

(b) l'opération $n \star m := n^m$ est associative sur $\mathbb{N}$.

(c) l'opération $n \star m := n^m$ sur $\mathbb{N}$ possède un élément neutre.

(a) Faux. Par exemple $8 = 2^3 \neq 3^2 = 9$. Donc, $2 \star 3 \neq 3 \star 2$.

(b) Faux. Par exemple $256 = 2^{2^3} \neq (2^2)^3 = 64$. Donc, $2 \star (2 \star 3) \neq (2 \star 2) \star 3$.

(c) L'opération $\star$ possède un élément neutre à droite, qui est 1. En effet $(n \star 1) = n^1 = n$ pour tout $n \in \mathbb{N}$. Par contre, $(1 \star n) = 1^n = 1$ pour tout $n \in \mathbb{N}$ et dès que $n \neq 1$, $1 \star n \neq n$.

5. En utilisant le théorème fondamental de l'arithmétique, montrer que si $m, n \in \mathbb{N}^*$ et si m est un multiple de n, alors tous les facteurs premiers de n sont aussi des facteurs premiers de m.

Si $n = 1$ et $m = 1 \times m$, alors n ne possède aucun facteurs premiers. Donc, trivialement, tous les facteurs premiers de n sont aussi facteurs premiers de m.
Si $n > 1$ on sait d'après le TFA, que $n = p_1 p_2 \dots p_s$, où $p_1, p_2, \dots, p_s$ sont les facteurs premiers de n, énumérés par ordre croissant. Si m est un multiple de n, il existe $k \in \mathbb{N}$ tel que $m = kn$. Si $q_1 q_2 \dots q_t = k$ est une factorisation de k, on a que

$$m = kn = q_1 q_2 \dots q_t p_1, p_2, \dots, p_s$$

et ceci est donc l'unique factorisation en premier de m (à l'ordre des facteurs près). Ainsi, tous facteur premier de n est aussi facteur premier de m.

6. En utilisant l'exercice précédent, montrer que si $m, n \in \mathbb{N}^*$, le plus petit commun multiple (PPCM(n, m)) et le plus grand commun diviseur (PGCD(n, m)) de n et m existent. Comment les calcule-t-on? Donner le résultat pour $n = 117$ et $m = 66$.

Si $n = 1$ ou $m = 1$ on a clairement que PPCM$(n, m) = \max(n, m)$ et PGCD$(n, m) = 1$.
Si $n, m \geq 2$, alors le TFA nous garantit l'existence (et l'unicité) de décompositions en facteurs premiers de n et m

$$n = p_1^{n_1} p_2^{n_2} \dots p_r^{n_r} \quad \text{et} \quad m = p_1^{m_1} \dots p_r^{m_r},$$

où $p_1, p_2, \dots$ est la liste des nombres premiers en ordre croissant et $n_1, \dots, n_s, m_1, \dots, m_t \in \mathbb{N}$. Si $k \in \mathbb{N}$ est un diviseur commun de n et m, et d'après l'exercice précédent, chaque facteur premier de k doit être un facteur permier de n et de m simultanément. On a donc que

$$\text{PGCD}(n, m) = p_1^{n_1 \wedge m_1} \dots p_r^{n_r \wedge m_r},$$

où $n_j \wedge m_j := \min(n_j, m_j)$. Si $k \in \mathbb{N}$ est un multiple commun de n et m, et d'après l'exercice précédent, chaque facteur premier de n et m doit être un facteur permier de k. On a donc que

$$\text{PPCM}(n, m) = p_1^{n_1 \vee m_1} \dots p_r^{n_r \vee m_r},$$

où $n_j \vee m_j := \max(n_j, m_j)$.
Comme exemple on prend $n = 117$ et $m = 66$, on a

$$117 = 3 \times 3 \times 13 = 2^0 3^2 5^0 7^0 11^0 13^1,$$
$$66 = 2 \times 3 \times 11 = 2^1 3^1 5^0 7^0 11^1 13^0,$$
$$\mathrm{PGCD}(117, 66) = 2^0 3^1 5^0 7^0 11^0 13^0 = 3,$$
$$\mathrm{PPCM}(117, 66) = 2^1 3^2 5^0 7^0 11^1 13^1 = 2'574.$$

7. On pose
$$2\mathbb{Z} := \{2n \, : \, n \in \mathbb{Z}\} \text{ et } 3\mathbb{Z} := \{3n \, : \, n \in \mathbb{Z}\}.$$
Montrer que
$$2\mathbb{Z} \cap 3\mathbb{Z} = 6\mathbb{Z}.$$
Montrer qu'en général, si $a, b \in \mathbb{N}^*$,
$$a\mathbb{Z} \cap b\mathbb{Z} = \mathrm{PPCM}(a, b)\mathbb{Z}.$$

Soient $a, b \in \mathbb{N}^*$. On a

$$a\mathbb{Z} = \{[(an, am)] \, : n, m \in \mathbb{N}\}, \quad b\mathbb{Z} = \{[(bn, bm)] \, : n, m \in \mathbb{N}\},$$
$$a\mathbb{Z} \cap b\mathbb{Z} = \{[(n, m)] \in \mathbb{Z} \, : \exists k, k', l, l' \in \mathbb{N} \text{ t.q.} n = ak = bk', m = al = bl'\}.$$

Par l'exercice 5., si $n = ak = bk'$, tous les facteurs de a ou de b sont facteurs de n et reciproquement. Ainsi, n, ainsi que m, doit être un multiple de $\mathrm{PPCM}(a, b)$ Ainsi

$$a\mathbb{Z} \cap b\mathbb{Z} = \mathrm{PPMC}(a, b)\mathbb{Z}.$$

Clairement, on a alors
$$2\mathbb{Z} \cap 3\mathbb{Z} = 6\mathbb{Z}.$$

Problèmes supplémentaires

(PS1) Vérifier les propriétés suivantes pour la multiplication dans $\mathbb{Z}$: $\forall n, m, p \in \mathbb{Z}$, on a

(a) $m \times n = n \times m$ (commutativité),

(b) $m \times (n \times p) = (m \times n) \times p$ (associativité),

(c) $m \times (n + m) = m \times n + m \times p$ (distributivité),

(d) $m \times [(1, 0)] = m$ (existence d'un élément neutre pour $\times$),

(e) $m \times [(0, 0)] = [(0, 0)]$ (existence d'un élément annulateur pour $\times$),

(f) $(-m) \times n = -(m \times n)$ (compatibilité de $\times$ avec $>$).

Representons n m et p par leur classes d'equivalences $[(a_n, b_n)]$, $[(a_m, b_m)]$ et $[(a_p, b_p)]$ respectivement.

(a)

$$\begin{aligned} m \times n &= [(a_m, b_m)] \times [(a_n, b_n)] = [(a_m a_n + b_m b_n, a_m b_n + b_m a_n)] \\ &= [(a_n a_m + b_n b_m, a_n b_m + b_n a_m)] = [(a_n, b_n)] \times [(a_m, b_m)] = n \times m. \end{aligned}$$

(b)

$$\begin{aligned} m \times (n \times p) &= [(a_m, b_m)] \times \big([(a_n, b_n)] \times [a_p, b_p)]\big) \\ &= [(a_m, b_m)] \times [(a_n a_p + b_n b_p, a_n b_p + b_n a_p)] \\ &= [\big(a_m(a_n a_p + b_n b_p) + b_m(a_n b_p + b_n a_p), a_m(a_n b_p + b_n a_p) + b_m(a_n a_p + b_n b_p)\big)] \\ &= [\big((a_m a_n + b_m b_n)a_p + (a_m b_n + b_m a_n)b_p, (a_m a_n + b_m b_n)b_p + (a_m b_n + b_m a_n)a_p\big)] \\ &= [(a_m a_n + b_m b_n, a_m b_n + b_m a_n)] \times [(a_p, b_p)] \\ &= \big([(a_m, b_m)] \times [(a_n, b_n)]\big) \times [a_p, b_p)] = (m \times n) \times p. \end{aligned}$$

(c)

$$\begin{aligned} m \times (n + p) &= [(a_m, b_m)] \times \big([(a_n, b_n)] + [(a_p, b_p)]\big) \\ &= [(a_m, b_m)] \times [(a_n + a_p, b_n + b_p)] \\ &= [\big(a_m(a_n + a_p) + b_m(b_n + b_p), b_m(a_n + a_p) + a_m(b_n + b_p)\big)] \\ &= [(a_m a_n + a_m a_p + b_m b_n + b_m b_p, b_m a_n + b_m a_p + a_m b_n + a_m b_p)] \\ &= [(a_m a_n + b_m b_n, a_m b_n + b_m a_n)] + [(a_m a_p + b_m b_p, a_m b_p + b_m a_p)] \\ &= [(a_m, b_m)] \times [(a_n, b_n)] + [(a_m, b_m)] \times [(a_p, b_p)] = m \times n + m \times p. \end{aligned}$$

(d)

$$m \times [(1, 0)] = [(a_m, b_m)] \times [(1, 0)] = [(a_m, b_m)] = m.$$

(e)

$$m \times [(0,0)] = [(a_m, b_m)] \times [(0,0)] = [(0,0)].$$

Notons que sans tenir compte des classes d'équivalences, mais en utilisant que les règles de calcul sur les groupes, la neutralité de 1 et la distributivité du produit, on peut aussi montrer que $\forall n \in \mathbb{Z}$, $0 \times n = 0$ (où on a identifié 0 à $[(0,0)]$ et 1 à $[(1,0)]$). En effet,

$$\begin{aligned} 0 = n + (-n) = 1 \times n + (-n) = (0+1) \times n + (-n) = (0 \times n + 1 \times n) + (-n) \\ = 0 \times n + (n + (-n)) = 0 \times n + 0 = 0 \times n. \end{aligned}$$

(f) Par associativite du produit et puisque $[(0,0)]$ est annulateur, on a

$$[(0,0)] = [(0,0)] \times n = (m + (-m)) \times n = m \times n + (-m) \times n.$$

Ainsi, $-(m \times n) = (-m) \times n$.