UFR-SFA 2019-2020   L2 MI G2

FICHE de TD N°1 ARITHMETIQUE

Lundi, 20 *juillet* 2020

<u>Exercice n°1</u>:

$a)$ Montrons que $(n!)_q = \dfrac{(q-1)(q^2-1)\dots(q^n-1)}{(q-1)^n}$, $q \neq 1$.

Par définition

$(n!)_q = \prod\limits_{k=1}^{n} (k)_q = \prod\limits_{k=1}^{n} \left(\sum\limits_{i=0}^{k-1} q^i\right) = \prod\limits_{k=1}^{n} \left(\dfrac{1-q^k}{1-q}\right) = \left(\dfrac{1}{1-q}\right)^n \prod\limits_{k=1}^{n} \left(1-q^k\right) = \dfrac{1}{(1-q)^n} \prod\limits_{k=1}^{n} \left(1-q^k\right).$

Soit

$$(n!)_q = \frac{1}{(q-1)^n} \prod_{k=1}^{n} \left(q^k - 1\right) = \frac{(q-1)(q^2-1)\dots(q^n-1)}{(q-1)^n}, q \neq 1.$$

$b)$ Montrons que $\begin{pmatrix} n \\ k \end{pmatrix}_q = \begin{pmatrix} n \\ n-k \end{pmatrix}_q$

Par définition

$\begin{pmatrix} n \\ k \end{pmatrix}_q = \dfrac{(n!)_q}{(k!)_q \left((n-k)_q\right)} = \dfrac{(n!)_q}{(n-(n-k!))_q \left((n-k)_q\right)} = \dfrac{(n!)_q}{\left((n-k)_q\right)(n-(n-k!))_q},$

Soit

$$\begin{pmatrix} n \\ k \end{pmatrix}_q = \begin{pmatrix} n \\ n-k \end{pmatrix}_q.$$

$c)$ Montrons que $\begin{pmatrix} n \\ k \end{pmatrix}_q = \begin{pmatrix} n-1 \\ k-1 \end{pmatrix}_q + q^k \begin{pmatrix} n-1 \\ k \end{pmatrix}_q = \begin{pmatrix} n-1 \\ k \end{pmatrix}_q + q^{n-k} \begin{pmatrix} n-1 \\ k-1 \end{pmatrix}_q$

On a

$\begin{pmatrix} n-1 \\ k-1 \end{pmatrix}_q + q^k \begin{pmatrix} n-1 \\ k \end{pmatrix}_q = \dfrac{((n-1)!)_q}{\left[((k-1)!)_q\,((n-1)-(k-1))!\right]_q} + q^k \dfrac{((n-1)!)_q}{\left[(k!)_q\,((n-1)-k)!\right]_q}$

$$= \frac{(k!)_q}{(k!)_q} \times \frac{((n-1)!)_q}{\left[((k-1)!)_q (n-k)!\right]_q} + q^k \frac{(n-k)_q}{(n-k)_q} \times$$
$$\frac{((n-1)!)_q}{\left[(k!)_q ((n-1)-k)!\right]_q}$$
$$= \frac{(k)_q ((n-1)!)_q}{\left[(k)_q ((k-1)!)_q\right] (n-k)!_q} +$$
$$q^k \frac{(n-k)_q ((n-1)!)_q}{(k!)_q \left[(n-k)_q ((n-1)-k)!_q\right]}$$
$$= \frac{(k)_q ((n-1)!)_q}{(k!)_q (n-k)!_q} + q^k \frac{(n-k)_q ((n-1)!)_q}{(k!)_q ((n-k)!)_q},$$
en factorisant, on a
$$\begin{aligned}
\left(\begin{array}{c} n-1 \\ k-1 \end{array}\right)_q + q^k \left(\begin{array}{c} n-1 \\ k \end{array}\right)_q &= \frac{((n-1)!)_q}{(k!)_q} \left[\frac{(k)_q}{(n-k)!_q} + q^k \frac{(n-k)_q}{((n-k)!)_q}\right] \\
&= \frac{((n-1)!)_q}{(k!)_q} \left[\frac{(k)_q + q^k (n-k)_q}{(n-k)!_q}\right] \\
&= \frac{((n-1)!)_q}{(k!)_q} \left[\frac{1+q+q^2 ... + q^{k-1} + q^k \left(1+q+q^2+...+q^{n-k-1}\right)}{(n-k)!_q}\right] \\
&= \frac{((n-1)!)_q}{(k!)_q} \left[\frac{1+q+q^2 ... + q^{k-1} + q^k + q^{k+1} + ... + q^{n-1}}{(n-k)!_q}\right] \\
&= \frac{((n-1)!)_q}{(k!)_q} \left[\frac{(n)_q}{(n-k)!_q}\right] = \frac{((n-1)!)_q (n)_q}{(k!)_q (n-k)!_q} =
\end{aligned}$$
$$\frac{(n!)_q}{(k!)_q (n-k)!_q} = \left(\begin{array}{c} n \\ k \end{array}\right)_q.$$

Conclusion 1

$$\left(\begin{array}{c} n-1 \\ k-1 \end{array}\right)_q + q^k \left(\begin{array}{c} n-1 \\ k \end{array}\right)_q = \left(\begin{array}{c} n \\ k \end{array}\right)_q.$$

De façon analogue, on montre que

$$\left(\begin{array}{c} n-1 \\ k \end{array}\right)_q + q^{n-k} \left(\begin{array}{c} n-1 \\ k \end{array}\right)_q = \left(\begin{array}{c} n \\ k \end{array}\right)_q.$$

Exercice n°5: $f : G \longrightarrow H$ est un morphisme de groupes finis.
G' est un sous groupe de G d'ordre premier avec l'ordre de H.
Montrons que $G' \subset \ker f$
On a montré dans l'exercice n°4 que f étant un morphisme de groupes finis et G' un sous groupe de G,

$$|f(G')| \text{ divise } |G'|.$$

On sait en outre que G' est un sous groupe de G donc $f(G')$ est un sous groupe H qui est fini, par conséquent le théorème de Lagrange nous permet de dire que

$$|f(G')| \text{ divise } |H|.$$

$\left\{ \begin{array}{l} |f(G')| \text{ divise } |G'| \\ |f(G')| \text{ divise } |H| \end{array} \right. \Longrightarrow |f(G')| \text{ divise}\, pgcd\,(|G'|\,, |H|) = 1 \Longrightarrow |f(G')| = 1 \Longleftrightarrow f(G')$ est un sous groupe d' ordre 1 $\Longleftrightarrow f(G') = \{1_H\} \Longleftrightarrow \forall x \in G', f(x) = 1_H \Longleftrightarrow \forall x \in G', x \in f^{-1}(1_H) = \ker f$.

Conclusion 2 $\forall x \in G', x \in \ker f \Longrightarrow G' \subset \ker f$.

Exercice n°6: Soit $n \in \mathbb{N}$.
Démontrons que:
1. $n^3 - n$ est divisible par 6.
On sait que:
$i)$ 3 étant un nombre premier on a
$n^3 - n \underset{\text{petit théo.de Fermat}}{\equiv} 0 \pmod 3 \Longleftrightarrow (n^3 - n) \in 3\mathbb{Z}$.
$ii)$ $n^3 - n = n(n-1)(n+1)$ est produit de trois entiers naturels consécutifs, donc $n^3 - n = n(n-1)(n+1) \equiv 0 (\text{mod}\, 2) \Longleftrightarrow (n^3 - n) \in 2\mathbb{Z}$.
Donc

$$\left(n^3 - n\right) \in 3\mathbb{Z} \cap 2\mathbb{Z} = 6\mathbb{Z}.$$

Conclusion 3 $\forall n \in \mathbb{N}, (n^3 - n)$ *est un multiple de* 6.

Application: On donne

$$\begin{array}{rccc} \varphi : & \mathbb{Z}/6\mathbb{Z} & \longrightarrow & \mathbb{Z}/6\mathbb{Z} \\ & n & \longmapsto & n^3 \end{array}$$

Que peut-on dire de φ?

On a $\forall n \in \mathbb{Z}/6\mathbb{Z}, \varphi(n) = n^3$ avec $n^3 - n \underset{n^3-n \,\in\, 6\mathbb{Z}}{=} \overline{0} \Longrightarrow n^3 = n = \varphi(n)$.
Donc $\forall n \in \mathbb{Z}/6\mathbb{Z}, \varphi(n) = n$, d'où

$$\varphi = id_{\mathbb{Z}/6\mathbb{Z}}.$$

2. $n^5 - n$ est divisible par 30.
On sait que:
$i)$ 5 étant un nombre premier, on a
$n^5 - n \underset{\text{petit théo.de Fermat}}{\equiv} 0 \pmod 5 \Longleftrightarrow (n^5 - n) \in 5\mathbb{Z}$.
$ii)$ $n^5 - n = n(n^4 - 1) = n(n^2 - 1)(n^2 + 1) = (n^3 - n)(n^2 + 1)$.
Or $n^3 - n \equiv 0 \pmod 6 \Longrightarrow (n^3 - n)(n^2 + 1) = n^5 - n \equiv 0 \pmod 6 \Longleftrightarrow (n^5 - n) \in 6\mathbb{Z}$.
Donc

$$\left(n^5 - n\right) \in 5\mathbb{Z} \cap 6\mathbb{Z} = 30\mathbb{Z}.$$

Conclusion 4 $\forall n \in \mathbb{N}, (n^5 - n)$ *est un multiple de* 30.

3. $n^7 - n$ est divisible par 42.
On sait que:
$i)$ 7 étant un nombre premier, on a
$n^7 - n \underset{\text{petit théo.de Fermat}}{\equiv} 0 \pmod 7 \Longleftrightarrow (n^7 - n) \in 7\mathbb{Z}$.
$ii)$ $n^7 - n = n(n^6 - 1) = n(n^2 - 1)(n^4 + n^2 + 1) = (n^3 - n)(n^4 + n^2 + 1) \equiv 0 \pmod 6$ car $n^3 - n \equiv 0 \pmod 6 \Longleftrightarrow (n^7 - n) \in 6\mathbb{Z}$.
Donc

$$\left(n^7 - n\right) \in 7\mathbb{Z} \cap 6\mathbb{Z} = 42\mathbb{Z}.$$

Conclusion 5 $\forall n \in \mathbb{N}, (n^7 - n)$ *est un multiple de* 42.

Exercice n°7: Soit $n \in \mathbb{N}$.
P_n : "3 divise $4^n - 1$", et Q_n : "3 divise $4^n + 1$".
1. **Montrons que P_n est vraie pour tout** $n \in \mathbb{N}$.
On a
$4 \equiv 1 \pmod 3 \Longrightarrow 4^n \equiv 1 \pmod 3 \Longrightarrow 4^n - 1 \equiv 0 \pmod 3$.
2. **Que pensez-vous de** "$\exists n_0 \in \mathbb{N} \mid \forall n \geq n_0, Q_n$ **est vraie?**"
On sait que
$4 \equiv 1 \pmod 3 \Longrightarrow 4^n \equiv 1 \pmod 3 \Longrightarrow 4^n + 1 \equiv 2 \pmod 3$.
Donc la proposition est fausse pour tout $n \in \mathbb{N}$.

Conclusion 6 *La proposition* Q_n : "3 *divise* 4^n+1" *est fausse pour tout* $n \in \mathbb{N}$.

3. **Montrons que** $\forall n \in \mathbb{N}$, **l'entier** $3^{n+3}-4^{4n+2}$ **est un multiple de** 11.

On a

$4^2 \equiv 5 (\bmod 11) \Longrightarrow 4^4 \equiv 5^2 \equiv 3 (\bmod 11) \Longrightarrow 4^{4n} = (4^4)^n \equiv 3^n (\bmod 11)$
$\Longrightarrow 4^{4n+2} = 4^{4n} \times 4^2 \equiv 3^n \times 5 (\bmod 11)$.

Ainsi

$3^{n+3}-4^{4n+2} = 3^n \times 3^3 - 4^{4n+2} \equiv 3^n \times 3^3 - 3^n \times 5 (\bmod 11)$
$\Longrightarrow 3^{n+3}-4^{4n+2} \equiv 3^n\left(3^3-5\right) (\bmod 11)$
$\Longrightarrow 3^{n+3}-4^{4n+2} \equiv 3^n \times 22 = 3^n \times 2 \times 11 (\bmod 11)$
$\Longrightarrow 3^{n+3}-4^{4n+2} \equiv 0 (\bmod 11)$.

Conclusion 7 $\forall n \in \mathbb{N}$, *l'entier* $3^{n+3}-4^{4n+2}$ *est un multiple de* 11.

Jeudi, 30 *juillet* 2020

Exercice n°8:

a) **Démontrons que l'entier** $2^{2\times 3^n}-1$ **est divisible par** $3^{n+1}, \forall n \in \mathbb{N}$.

Posons P_n : "$\forall n \in \mathbb{N}, 2^{2\times 3^n}-1$ est divisible par 3^{n+1}".

Initialisation : $n=0$, on a $2^{2\times 3^0}-1 = 2^2-1 = 3 \equiv 0 (\bmod 3^{0+1})$.

Donc P_0 est vraie.

Hérédité : (Hypothèse de recurrence).

Supposons que P_n vraie i.e $\forall n \in \mathbb{N}, 2^{2\times 3^n}-1$ est divisible par 3^{n+1} c-à-dire

$$2^{2\times 3^n}-1 = 3^{n+1}q, q \in \mathbb{N}^*$$
$$\Updownarrow$$
$$2^{2\times 3^n} = 3^{n+1}q+1, q \in \mathbb{N}^*.$$

Au rang $n+1$, on a

$2^{2\times 3^{n+1}}-1 = 2^{2\times 3^n \times 3}-1 = \left(2^{2\times 3^n}\right)^3-1 = \left(3^{n+1}q+1\right)^3-1$.

Soit

$$2^{2\times 3^{n+1}}-1 = \left(3^{n+1}q+1\right)^3-1, q \in \mathbb{N}^*.$$

Mais

$\left(3^{n+1}q+1\right)^3 = \left(3^{n+1}q\right)^3 + 3\left(3^{n+1}q\right)^2 + 3\left(3^{n+1}q\right)+1$,

donc

$$
\begin{aligned}
2^{2\times 3^{n+1}}-1 &= \left[\left(3^{n+1}q\right)^{3}+3\left(3^{n+1}q\right)^{2}+3\left(3^{n+1}q\right)+1\right]-1\\
&= \left(3^{n+1}q\right)^{3}+3\left(3^{n+1}q\right)^{2}+3\left(3^{n+1}q\right)\\
&= 3^{3n+3}q^{3}+3\times 3^{2n+2}q^{2}+3\times 3^{n+1}q\\
&= 3^{n+2}\times\left[3^{2n+1}q^{3}+3^{n+1}q^{2}+q\right]\\
&= 3^{(n+1)+1}\times\left[3^{2n+1}q^{3}+3^{n+1}q^{2}+q\right].
\end{aligned}
$$

En définitive

$2^{2\times 3^{n+1}}-1=3^{(n+1)+1}\times k, k=\left[3^{2n+1}q^{3}+3\times 3^{n}q^{2}+q\right]\in\mathbb{N}^{*}$, et donc

P_n vraie $\Longrightarrow P_{n+1}$ est vraie.

Conclusion 8 $\forall n\in\mathbb{N}, 2^{2\times 3^{n}}-1$ *est divisible par* 3^{n+1}.

$b)$ **Démontrons que l'entier** $5^{3^{n}}+1$ **est divisible par** $3^{n+1}, \forall n\in\mathbb{N}$.

Posons P_n : "$\forall n\in\mathbb{N}, 5^{3^{n}}+1$ est divisible par 3^{n+1}".

Initialisation : $n=0$, on a $5^{3^{0}}+1=5+1=3^{1}\times 2\equiv 0 \pmod{3^{0+1}}$.

Donc P_0 est vraie.

Hérédité : Hypothèse de recurrence.

Supposons que P_n vraie i.e $\forall n\in\mathbb{N}, 5^{3^{n}}+1$ est divisible par 3^{n+1} c-à-dire

$$
\begin{gathered}
5^{3^{n}}+1=3^{n+1}q, q\in\mathbb{N}^{*}\\
\Updownarrow\\
5^{3^{n}}=3^{n+1}q-1, q\in\mathbb{N}^{*}.
\end{gathered}
$$

Au rang $n+1$, on a

$5^{3^{n+1}}+1=5^{3^{n}\times 3}+1=\left(5^{3^{n}}\right)^{3}+1=\left(3^{n+1}q-1\right)^{3}+1.$

Soit

$$5^{3^{n+1}}+1=\left(3^{n+1}q-1\right)^{3}+1.$$

Mais

$\left(3^{n+1}q-1\right)^{3}=\left(3^{n+1}q\right)^{3}-3\left(3^{n+1}q\right)^{2}+3\left(3^{n+1}q\right)-1,$

donc

$$
\begin{aligned}
5^{3^{n+1}}+1 &= \left[\left(3^{n+1}q\right)^{3}-3\left(3^{n+1}q\right)^{2}+3\left(3^{n+1}q\right)-1\right]+1\\
&= \left(3^{n+1}q\right)^{3}-3\left(3^{n+1}q\right)^{2}+3\left(3^{n+1}q\right)\\
&= 3^{3n+3}q^{3}-3\times 3^{2n+2}q^{2}+3\times 3^{n+1}q\\
&= 3^{n+2}\times\left[3^{2n+1}q^{3}-3\times 3^{n}q^{2}+q\right]\\
&= 3^{(n+1)+1}\times\left[3^{2n+1}q^{3}-3\times 3^{n}q^{2}+q\right].
\end{aligned}
$$

En définitive

$5^{3^{n+1}}+1=3^{(n+1)+1}\times k, k=\left[3^{2n+1}q^{3}-3\times 3^{n}q^{2}+q\right]\in\mathbb{N}^{*}$, et donc

P_n est vraie $\Longrightarrow P_{n+1}$ est vraie.

Conclusion 9 *$\forall n \in \mathbb{N}, 5^{3^{n+1}} + 1$ est divisible par 3^{n+1}.*

Exercice n°9: $n \in \mathbb{N}$ et $p \in \mathbb{Z}$

Rappel: $C_n^p = \binom{n}{p}$

1. **Montrons que** $p\binom{n}{p} = n\binom{n-1}{p-1}$

En remarquant que $n - p = (n-1) - (p-1)$, on a

$$p\binom{n}{p} \underset{\text{déf.}}{=} p \times \frac{n!}{p!\,(n-p)!} = p \times \left(n \times \frac{(n-1)!}{p\,(p-1)!\,((n-1)-(p-1))!}\right)$$
$$= p \times \frac{1}{p} \times n \times \left(\frac{(n-1)!}{(p-1)!\,((n-1)-(p-1))!}\right)$$
$$= n \times \left(\frac{(n-1)!}{(p-1)!\,((n-1)-(p-1))!}\right).$$

Or $\dfrac{(n-1)!}{(p-1)!\,((n-1)-(p-1))!} = \binom{n-1}{p-1}$.

Donc

$$p\binom{n}{p} = n\binom{n-1}{p-1}.$$

Conclusion 10 *$\forall n \in \mathbb{N}$ et $\forall p \in \mathbb{Z}$, on a*

$$p\binom{n}{p} = n\binom{n-1}{p-1}.$$

2. On donne $a)$ $S_0 = \sum_{p=0}^{n} \binom{n}{p} = \binom{n}{0} + \binom{n}{1} + ... + \binom{n}{n}$

$b)$ $S_1 = \sum_{p=0}^{n} p\binom{n}{p} = 0\binom{n}{0} + 1\binom{n}{1} + ... + n\binom{n}{n}$

$b)$ $S_2 = \sum_{p=0}^{n} p^2\binom{n}{p} = 0^2\binom{n}{0} + 1^2\binom{n}{1} + ... + n^2\binom{n}{n}$

$b)$ $S_3 = \sum_{p=1}^{n} \binom{n}{p} \times 3^{p-1} = 3^0\binom{n}{1} + 3^1\binom{n}{2} + ... + 3^{n-1}\binom{n}{n}$

Définition 11 *Posons $f(x) = (1+x)^n, n \in \mathbb{N}$.*

On sait alors que

$f(x) = (1+x)^n = \sum_{p=0}^{n} \binom{n}{p} 1^{n-p} x^p,$

donc

$$f(x) = (1+x)^n = \sum_{p=0}^{n} \binom{n}{p} x^p. \tag{1}$$

Mais alors

$$f'(x) = n\,(1+x)^{n-1} = \sum_{p=1}^{n} p \binom{n}{p} x^{p-1} = \sum_{p=0}^{n} p \binom{n}{p} x^p. \tag{2}$$

Et

$f''(x) = n\,(n-1)\,(1+x)^{n-1} = \sum_{p=2}^{n} p\,(p-1)\,\binom{n}{p} x^{p-2} \overset{en\ d\acute{e}velopp.}{=}$
$\sum_{p=2}^{n} p^2 \binom{n}{p} x^{p-2} - \sum_{p=2}^{n} p \binom{n}{p} x^{p-2}$

$$\begin{aligned} f''(x) = n\,(n-1)\,(1+x)^{n-2} = & \left[\sum_{p=0}^{n} p^2 \binom{n}{p} x^p - \left[0^2 \binom{n}{0} x^0 + 1^2 \binom{n}{1} x^1\right]\right] \\ & - \left[\sum_{p=0}^{n} p \binom{n}{p} x^p - \left[0^0 \binom{n}{0} x^0 + 1^1 \binom{n}{1} x^1\right]\right] \end{aligned}$$

$$f''(x) = n\,(n-1)\,(1+x)^{n-2} = \sum_{p=0}^{n} p^2 \binom{n}{p} x^p - \sum_{p=0}^{n} p \binom{n}{p} x^p$$
$$- \underbrace{\left[0^2 \binom{n}{0} x^0 + 1^2 \binom{n}{1} x^1\right] + \left[0^0 \binom{n}{0} x^0 + 1^1 \binom{n}{1} x^1\right]}_{\overset{\shortparallel}{0}}$$

Soit

$$f''(x) = n\,(n-1)\,(1+x)^{n-2} = \sum_{p=0}^{n} p^2 \binom{n}{p} x^p - \sum_{p=0}^{n} p \binom{n}{p} x^p = S_2 - S_1 \tag{3}$$

$a)$ Calcul de S_0

Dans (1), on a

$f\,(1) = 2^n = \sum_{p=0}^{n} \binom{n}{p}$, donc

$$S_0 = \sum_{p=0}^{n} \binom{n}{p} = 2^n.$$

$b)$ Calcul de S_1

Dans (2), on a

$f'(1) = n \times 2^{n-1} = \sum_{p=0}^{n} p \binom{n}{p}$, donc

$$S_1 = \sum_{p=0}^{n} p \binom{n}{p} = n \times 2^{n-1}.$$

$b)$ Calcul de S_2

Dans (3), on a

$f''(1) = n(n-1) \times 2^{n-2} = S_2 - S_1$, donc $S_2 = n(n-1) \times 2^{n-2} + S_1 = n(n-1) \times 2^{n-2} + n \times 2^{n-1} = n \times 2^{n-2}[(n-1)+2]$.

Ce qui nous donne

$$S_2 = \sum_{p=0}^{n} p^2 \binom{n}{p} = n(n+1) \times 2^{n-2}.$$

3. **Montrons que** $\sum_{k=n}^{p} \binom{k}{n} = \binom{p+1}{n+1}$

Raisonnons par recurrence sur k, pour un n fixé (quelconque).

Soit $p \geq n$, considérons $P(p)$: " $\sum_{k=n}^{p} \binom{k}{n} = \binom{p+1}{n+1}$ ".

Initialisation : Pour $p = n$, on a:

$\sum_{k=n}^{n} \binom{n}{n} = \binom{n}{n} = 1 = \binom{n+1}{n+1} \Longrightarrow P(n)$ est vraie.

Hérédité : Supposons que $P(p)$: " $\sum_{k=n}^{p} \binom{k}{n} = \binom{p+1}{n+1}$ " soit vraie.

Au rang $p+1$, on a

$\sum_{k=n}^{p+1} \binom{k}{n} = \sum_{k=n}^{p} \binom{k}{n} + \binom{p+1}{n} \underset{\text{hypo.de recurr}}{=} \binom{p+1}{n+1} + \binom{p+1}{n} = \binom{(p+1)+1}{n+1}$.

$P(p)$ vraie $\Longrightarrow P(p+1)$ est vraie.

Conclusion 12 *$\forall p \geq n$, on a* $\sum_{k=n}^{p} \binom{k}{n} = \binom{p+1}{n+1}$.

Interprètation: Dans le triangle de Pascal, quand on descend le long de la colonne n du coefficient $\binom{n}{n} = 1$ (ligne n) au coefficient $\binom{p}{n}$ (ligne

p), en additionnant ces deux coefficients, on trouve $\binom{p+1}{n+1}$ = au coefficient qui se trouve une ligne plus bas et une colonne plus loin.

$p \diagdown n$	1	2	3	4	5	6	7	8	9	10
0	1									
1	1	1								
2	1	2	1							
3	1	3	3	1						
4	1	4	6	4	1					
5	1	5	10	10	5	1				
6	1	6	15	20	15	6	1			
7	1	7	21	35	35	21	7	1		
8	1	8	28	56	70	56	28	8	1	
9	1	9	36	84	126	126	84	36	9	1
10	1									

Exercice n°10: On pose $div(n)$ = l'ensemble des diviseurs positifs de $n \in \mathbb{Z}$, et on donne l'application

$$\begin{array}{cccc} \sigma: & \mathbb{Z} & \longrightarrow & \mathbb{N} \\ & n & \longmapsto & |div(n)| \end{array}.$$

a) p est un nombre premier

Calculons $\sigma(p)$

$div(p) = \{1, p\} \Longrightarrow \sigma(p) = 2$

Calculons $\sigma(p^\alpha)$

$div(p^\alpha) = \{1 = p^0, p^1, p^2, ..., p^\alpha\} \Longrightarrow \sigma(p^\alpha) = \alpha + 1$

Exemple $5^3 = 125 \Longrightarrow \sigma(5^3) = 4$

b) $\forall a, b \in \mathbb{Z}$, on définit l'application

$$\begin{array}{cccc} \varphi: & div(a) \times div(b) & \longrightarrow & div(ab) \\ & (k, l) & \longmapsto & kl \end{array}.$$

Préliminaire

- Notons que

$\left.\begin{array}{r} \forall m \in div(a), \text{ on a } a = mk \\ \forall n \in div(b), \text{ on a } b = nk' \end{array}\right\} \Longrightarrow ab = mknk' = mn(kk') \Longrightarrow mn \in div(ab) \Longrightarrow \varphi$ est bien définie.

- Supposons que

$$\left.\begin{array}{c} a = p_1^{\alpha_1} p_2^{\alpha_2} ... p_r^{\alpha_r} \\ b = q_1^{\beta_1} q_2^{\beta_2} ... q_s^{\beta_s} \\ pgcd(a,b) = 1 \end{array}\right\} \Longrightarrow \forall i,j, \text{ on a } p_i \neq q_j.$$

Montrons que φ est une bijection

• Injectivité de φ

Soient (m,n) et $(m',n') \in div(a) \times div(b)$.

Alors

$$m \mid a \Longrightarrow m = p_1^{\mu_1} p_2^{\mu_2} ... p_r^{\mu_r} : 0 \leq \mu_i \leq \alpha_i \qquad n \mid b \Longrightarrow n = q_1^{v_1} q_2^{v_2} ... q_s^{v_s} : 0 \leq v_j \leq \beta_j$$
$$m' \mid a \Longrightarrow m' = p_1^{\mu_1'} p_2^{\mu_2'} ... p_r^{\mu_r'} : 0 \leq \mu_i' \leq \alpha_i \qquad n' \mid b \Longrightarrow n' = q_1^{v_1'} q_2^{v_2'} ... q_s^{v_s'} : 0 \leq v_j' \leq \beta_j$$

Donc

$\varphi(m,n) = mn = (p_1^{\mu_1} p_2^{\mu_2} ... p_r^{\mu_r}) \times (q_1^{v_1} q_2^{v_2} ... q_s^{v_s})$ et

$\varphi(m',n') = m'n' = \left(p_1^{\mu_1'} p_2^{\mu_2'} ... p_r^{\mu_r'}\right) \times \left(q_1^{v_1'} q_2^{v_2'} ... q_s^{v_s'}\right).$

Ainsi

$$\varphi(m,n) = \varphi(m',n') \Longrightarrow mn = m'n'$$
$$\Longrightarrow p_1^{\mu_1} p_2^{\mu_2} ... p_r^{\mu_r} q_1^{v_1} q_2^{v_2} ... q_s^{v_s} = p_1^{\mu_1'} p_2^{\mu_2'} ... p_r^{\mu_r'} q_1^{v_1'} q_2^{v_2'} ... q_s^{v_s'}.$$

Et l'unicité de la décomposition d'un entier implique que

$\forall i,j$, on a $\mu_i = \mu_i'$ et $v_j = v_j' \Longrightarrow (m = m' \text{ et } n = n') \Longrightarrow (m,n) = (m',n')$.

Conclusion 13 $\forall (m,n),(m',n') \in div(a) \times div(b), \varphi(m,n) = \varphi(m',n') \Longrightarrow (m,n) = (m',n')$.

Donc φ est une application injective.

• Surjectivité de φ

Soit $d \in div(ab)$, alors on a $d = p_1^{t_1} p_2^{t_2} ... p_r^{t_r} q_1^{w_1} q_2^{w_2} ... q_s^{w_s} : 0 \leq t_i \leq \alpha_i$ et $0 \leq w_j \leq \beta_j$.

En posant $k = p_1^{t_1} p_2^{t_2} ... p_r^{t_r}$ et $l = q_1^{w_1} q_2^{w_2} ... q_s^{w_s}$, on a bien

$k = p_1^{t_1} p_2^{t_2} ... p_r^{t_r} \in div(a)$ et $l = q_1^{w_1} q_2^{w_2} ... q_s^{w_s} \in div(b)$ tels que $\varphi(k,l) = kl = d$.

Conclusion 14 *$\forall d \in div(ab)$, on peut trouver au moins un couple $(k,l) \in div(a) \times div(b)$ tel que $\varphi(k,l) = d$. Donc φ est surjective.*

En définitive

$$\left\{\begin{array}{l} \varphi \text{ est une application injective} \\ \varphi \text{ est une application surjective} \end{array}\right. \Longrightarrow \varphi \text{ est une application bijective.}$$

$c)$ On suppose que a et b sont premiers entre eux.

Relation entre $\sigma(ab), \sigma(a)$ et $\sigma(b)$.

Puisque φ est une application bijective, on a bien

$$\sigma(ab) = \sigma(a) \times \sigma(b), \ \forall a \text{ et } b \text{ premiers eux.}$$

$d)$ Soit $n = p_1^{\alpha_1} p_2^{\alpha_2} ... p_r^{\alpha_r}$, la décomposition en nombres premiers de n.

Expression de $\sigma(n) = f(\alpha_i)$

$n = p_1^{\alpha_1} p_2^{\alpha_2} ... p_r^{\alpha_r}$ avec $\forall i, j, pgcd(p_i^{\alpha_i}, p_j^{\alpha_j}) = 1 \underset{\text{d'après c)}}{\Longrightarrow} \sigma(p_i^{\alpha_i} p_j^{\alpha_j}) = \sigma(p_i^{\alpha_i}) \times \sigma(p_j^{\alpha_j}) \underset{\text{d'après a)}}{=} (\alpha_i + 1)(\alpha_j + 1)$.

Donc

$$\sigma(n) = \prod_{i=1}^{r} (\alpha_i + 1)$$

Exemple 15 $12 = 2^2 \times 3 \Longrightarrow \sigma(12) = (2+1)(1+1) = 6.$

$10 = 2 \times 5 \Longrightarrow \sigma(10) = (1+1)(1+1) = 4.$

$120 = 2^3 \times 3 \times 5 \Longrightarrow \sigma(120) = (3+1)(1+1)(1+1) = 16.$

Attention *Ici c) n'est pas vérifiée car* $pgcd(12, 10) = 2 \neq 1$.