27/02/2007

Rappels

① R et S relations d'équivalence sur X et Y et $f : X \to Y$

alors f passe au quotient

$$\begin{tikzcd} X \arrow[r, "f"] \arrow[d, "\pi_R"] & Y \arrow[d, "\pi_S"] \\ X/_R \arrow[r, "\bar f"] & Y/_S \end{tikzcd}$$

$\exists\ \bar f : X/_R \to Y/_S$ t.q. $\bar f \circ \pi_R = \pi_S \circ f$

② Si $g, h : X \to X$ passent au quotient en $\bar g, \bar h : X/_R \to X/_R$

alors $g \circ h : X \to X$ passe au quotient et $\overline{g\circ h} = \bar g \circ \bar h$:

$$\begin{tikzcd} X/_R \arrow[r, "\bar h"] \arrow[rr, bend right, "\overline{g\circ h}"'] & X/_R \arrow[r, "\bar g"] & X/_R \end{tikzcd}$$

<u>Proposition</u> Soit N et n des entiers naturels ($N, n \in \mathbb{N}$) alors

(1) $n+ : \mathbb{N} \to \mathbb{N},\ m \mapsto n+m$ et $n* : \mathbb{N} \to \mathbb{N},\ m \mapsto nm$

passent au quotient en $\overline{n+} = n+ : \mathbb{N}/_{\mathrm{mod}\,N} \to \mathbb{N}/_{\mathrm{mod}\,N}$ et $\overline{n*} = n* : \mathbb{N}/_{\mathrm{mod}\,N} \to \mathbb{N}/_{\mathrm{mod}\,N}$

(2) Si $0 \neq N = N' + 1$ alors

(i) $\overline{n+}$ est bijective d'inverse $\overline{nN'+} : \mathbb{N}/_{\mathrm{mod}\,N} \to \mathbb{N}/_{\mathrm{mod}\,N}$

(ii) $\overline{n*}$ est injective ssi $\forall m \in \mathbb{N}\ \ nm \equiv 0 \bmod N \Rightarrow m \equiv 0 \bmod N$

(N divise nm $[N|nm]$) $\Rightarrow$ (N divise m $[N|m]$)

pr (1) : $\forall m, m' \in \mathbb{N}$ $m \equiv m' \bmod N$, cad $\exists k, l \in \mathbb{N}$ tq $m + kN = m' + lN$

donc
$$\left.\begin{aligned} (n+m) + kN &= n + (m+kN) = n + (m' + lN) = (n+m') + lN \\ nm + nkN &= n(m+kN) = n(m'+lN) = nm' + nlN \end{aligned}\right\} \text{c.a.d.} \quad \begin{aligned} n+m &\equiv n+m' \bmod N \\ nm &\equiv nm' \bmod N \end{aligned}$$
□

(2)(i) $\overline{nN'+} \circ \overline{n+}(\bar m) = \overline{nN'+}(\overline{n+m}) = \overline{nN'+(n+m)} = \overline{(nN'+n)+m} = \overline{n(N'+1)+m} = \overline{nN+m} = \bar m$

$\overline{n+} \circ (\overline{nN'+})(\bar m) = \overline{n+}(\overline{nN'+m}) = \overline{n+(nN'+m)} = \overline{(n+nN')+m} = \overline{n(1+N')+m} = \overline{nN+m} = \bar m$

donc $\overline{nN+} \circ \overline{n+} = Id_{\mathbb{N}/_{\mathrm{mod}\,N}}$ et $\overline{n+} \circ (\overline{nN+}) = Id_{\mathbb{N}/_{\mathrm{mod}\,N}}$ et $\overline{n+}$ est bijective d'inverse $\overline{nN'+}$ □

(ii) Rappel $f : X \to Y$ injective ssi $\forall x, x' \in X \left(f(x) = f(x')\right) \Rightarrow (x = x')$

donc $\Rightarrow$ clair en prenant $m' = 0$

$\Leftarrow$ $(nm \equiv nm' \bmod N) \Rightarrow 0 \equiv \overline{nmN'_+}(nm) = \overline{nmN' + nm} \equiv \overline{nmN' + nm'}$

$\equiv n\,(mN' + m') \bmod N \Rightarrow mN' + m' \equiv 0 \bmod N$

$\Rightarrow \overline{m'} = \overline{m_+}\left(\overline{mN' + m'}\right) = \overline{m_+}\,(0) = \overline{m}$ c.à.d $m' \equiv m \bmod N$ $\square$

4 Applications au dénombrement des ensembles finis

<u>Notation</u> Si $n \in \mathbb{N}$ $\{1, \dots, n\} = \{m \in \mathbb{N} \mid 1 \leq m \leq n\}$ (donc $\{1, \dots, 0\} = \emptyset$)

<u>Corollaire</u> Soit $m, n \in \mathbb{N}$ et $f : \{1, \dots, m\} \to \{1, \dots, n\}$ injective alors $m \leq n$ et si il y a égalité f est aussi surjective, donc bijective.

pr récurrence sur n. Si $n = 0$ alors $\{1, \dots, n\} = \emptyset$ donc $\underbrace{\{1, \dots, m\} = \emptyset \text{ et } m = 0}_{[\exists f : X \to \emptyset \Rightarrow X = \emptyset]}$

Si $0 \neq n = N = n' + 1$ soit $m = 0$ et $m \lneq n$

si $0 \neq m = m' + 1$ alors $f(m) \in \{1, \dots, n\}$ et il y a $k \in \mathbb{N}$ tq $n = k + f(m)$

En considérant $\{1, \dots, n\}$ comme le système des plus petits représentants positifs mod N

alors $g = \overline{k_+} \circ f : \{1, \dots, m\} \to \{1, \dots, n\}$ est injective avec $g(m) = k + f(m) = n$

donc $\forall \ell \in \{1, \dots, m\} \setminus \{m\} = \{1, \dots, m'\}$ on a $g(\ell) \neq g(m) = n$ donc $g(\ell) \in \{1, \dots, n'\}$

et g induit $g_1 : \{1, \dots, m'\} \to \{1, \dots, n'\}$ injective donc $m = m' + 1 \underset{\text{réc}}{\leq} n' + 1 = n$

et si il y a égalité $g_1(\{1,\dots,m'\}) = \{1,\dots,n'\}$, comme $g(m) = n$

on a $g(\{1,\dots,m\}) = \{1,\dots,n\}$ donc $g = \overline{k+} \circ f$ est surjective et,

comme $\overline{k+}$ est bijective, f est aussi surjective. □

Lemme Si $f : \{1,\dots,m\} \to \{1,\dots,n\}$ est surjective

elle a une section $s : \{1,\dots,n\} \to \{1,\dots,m\}$ [c.a.d $f \circ s = Id_{\{1,\dots,n\}}$]

En particulier il y a $g (= s) : \{1,\dots,n\} \to \{1,\dots,m\}$ injective.

pv : • f surjective $\overset{def}{\iff} \forall \ell \in \{1,\dots,n\}\ f^{-1}(\ell) \neq \emptyset$, il suffit de poser

$s(\ell) = m(f^{-1}(\ell))$ et $f \circ s(\ell) = f(m(f^{-1}(\ell))) \in \{\ell\}$ donc $f \circ s(\ell) = \ell$ □

• Rappel $\left.\begin{array}{l} Id \text{ injective} \\ f \circ g \text{ injective} \Rightarrow g \text{ injective} \end{array}\right\} \Rightarrow g = s$ injective

□

définition un ensemble X est fini s'il y a $n \in \mathbb{N}$ et

une bijection $f : X \to \{1,\dots,n\}$

Si $g : X \to \{1,\dots,m\}$ est une autre bijection alors le cas

pour $f \circ g^{-1} : \{1,\dots,m\} \to \{1,\dots,n\}$ et $g \circ f^{-1} : \{1,\dots,n\} \to \{1,\dots,m\}$

donne $m \leq n$ et $n \leq m$, c.a.d $m = n$

Le nombre d'éléments ou cardinal de l'ensemble fini X est

$\text{Card}(X) = n$ tq. il y a $f : X \to \{1,\dots,n\}$ bijective

<u>Thm 1</u> Soit X, Y deux ensembles finis et $f : X \to Y$ alors

(1) Si f est injective $\operatorname{card} X \leq \operatorname{card} Y$ et si $\operatorname{card} X = \operatorname{card} Y$ f est aussi surjective

(2) Si f est surjective $\operatorname{card} X \geq \operatorname{card} Y$ ———————— injective.

pv Exercice : Prop $\Rightarrow (1)$; Lemme $\Rightarrow \big((1) \Rightarrow (2)\big)$

<u>Corollaire</u> Si X, Y sont finis avec $\operatorname{card} X = \operatorname{card} Y$ et $f : X \to Y$ alors f est bijective dès qu'elle est injective ou surjective.

<u>Thm 2</u> Soit R une relation d'équivalence sur un ensemble X tq $X/_R$ est fini et $\forall x \in X$ $\bar{x}$ est fini alors X est fini et

$$\operatorname{card} X = \sum_{\bar{x} \in X/_R} \operatorname{card} \bar{x} \qquad \text{(formule des classes)}$$

<u>Thm 2'</u> Soit $f : X \to Y$ avec Y fini et $\forall y \in Y$ $f^{-1}(y)$ fini alors X est fini et

$$\operatorname{card} X = \sum_{y \in Y} \operatorname{card} f^{-1}(y)$$

<u>def</u> Si Y est fini et $\varphi : Y \to \{1, \dots, n\}$ bijective et $a : Y \to \mathbb{N}$ [resp. $\mathbb{Z}, \mathbb{Q}, \mathbb{C}$]

$$\sum_{y \in Y} a_y = \sum_{k=1}^{n} a_{\varphi^{-1}(k)} \quad \left(\underset{\text{def}}{=} 0 \text{ si } n = 0\right).$$

· pv Thm 2 est Thm 2' pour $f = \pi_R : X \to X/_R$

· par def de $\sum_{y \in Y}$ il suffit de prouver thm 2' pour $Y = \{1, \dots, n\}$

pv de Thm 2 : récurrence sur $n = \text{card}\, Y \in \mathbb{N}$ $(Y = \{1, \dots, n\})$

Si $n = 0$ $Y = \{1, \dots, n\} = \emptyset$ donc $X = \emptyset$ et $\text{card}\, X = 0 = \sum_{y \in Y} \text{card}\, f^{-1}(y)$

Si $0 < n = n'+1$ $X' = f^{-1}(\{1, \dots, n'\})$

par récurrence il y a $h' : X' \to \{1, \dots, \sum_{k=1}^{n'} \text{card}\, f^{-1}(k)\}$ bijective

$m_n = \text{card}\, f^{-1}(n)$ par hypothèse — $h_n : f^{-1}(n) \to \{1, \dots, m_n\}$ bijective

d'où $h : X \to \{1, \dots, \sum_{k=1}^{n'} \text{card}\, f^{-1}(k) + m_n = \sum_{\ell=1}^{n} \text{card}\, f^{-1}(\ell)\}$

Si $x \in X'$ $h(x) = h'(x)$

si $x \in X \setminus X' = f^{-1}(n)$ $h(x) = \sum_{k=1}^{n'} \text{card}\, f^{-1}(k) + h_n(x)$

est bijective d'inverse $k : \{1, \dots, \sum_{\ell=1}^{n} \text{card}\, f^{-1}(\ell)\} \to X$

si $\ell \leq \sum_{\ell=1}^{n'} \text{card}\, f^{-1}(\ell)$ $k(\ell) = 1_{X'}^{X} \circ (h')^{-1}(\ell)$

si $\sum_{\ell=1}^{n'} \text{card}\, f^{-1}(\ell) < \ell = \sum_{\ell=1}^{n'} \text{card}\, f^{-1}(\ell) + \ell'$ $k(\ell) = 1_{f^{-1}(n)}^{X} \circ h_n^{-1}(\ell')$ $\square$

<u>Corollaire</u> Si X et Y sont finis alors $X \times Y$ est fini et

$$\text{card}\, X \times Y = \text{card}\, X \times \text{card}\, Y$$

pv $f = pr_2 : X \times Y \to Y$ $\forall y \in Y$ $pr_1 : f^{-1}(y) = X \times \{y\} \to Y$ bijective

donc $f^{-1}(y)$ fini et $\text{card}\, f^{-1}(y) = \text{card}\, X$ le thm 2' donne

$X \times Y$ fini et

$$\text{card}(X \times Y) = \sum_{y \in Y} \text{card}\, f^{-1}(y) = \sum_{y \in Y} \text{card}\, X = \text{card}\, X \sum_{y \in Y} 1 = \text{card}\, X \times \text{card}\, Y. \ \square$$

5. Applications à l'arithmétique de $\mathbb{N}$

def Soit $m, n \in \mathbb{N}$, m *divise* n, noté $m|n$, s'il y a $k \in \mathbb{N}$ tq $n = mk$

Remarques a) si $n, m, k \in \mathbb{N}$ tq $n = mk$ alors $m|n$ et $k|n$

b) $\forall m \in \mathbb{N}$ $m|0$ $(0 = m \cdot 0)$ et si $n \neq 0$ et $m|n$ alors $m \neq 0$ et

$$1 \leq m \leq n$$

pv $0 \neq n = mk \Rightarrow 0 \neq k = k'+1$ et $n = (k'+1)m = k'm + m \geq m$ $\square$

c) Exercice (voir TD4) $|$ est une relation d'ordre sur $\mathbb{N}$.

Corollaire Si $n \neq 0$ $\mathrm{Div}(n) \overset{\text{def}}{=} \{m \in \mathbb{N} \mid m|n\}$ est fini et $1, n \in \mathrm{Div}(n)$

donc soit $n = 1$ soit $\mathrm{card}(\mathrm{Div}(n)) \geq 2$ $\square$

def un entier naturel n est $\left\{\begin{array}{l} \text{un } \textit{nombre premier} \\ \textit{premier} \end{array}\right\}$ si $\mathrm{card}\,\mathrm{Div}(n) = 2$ $(\mathrm{Div}(n) = \{1, n\})$

ainsi un entier $n > 1$ est premier ssi il y a $m', m'' \in \mathbb{N}$

avec $n = n' n''$ et $1 < n', n'' < n$

Corollaire Soit $n \in \mathbb{N}$, $n > 1$ alors il y a $k > 0$ et $p_1, \dots, p_k$ premiers t.q.

$$n = p_1 \cdots p_k = \prod_{i=1}^{k} p_i$$

pv si n est premier $k = 1$ et $p_1 = n$, sinon $n = n'n''$ avec $1 < n', n'' < n$, $k = k' + k''$

récurrence sur n donne $p_1, \dots, p_{k'}, p_{k'+1}, \dots, p_{k'+k''}$ premiers tq $n' = \prod_{i=1}^{k'} p_i$, $n'' = \prod_{j=1}^{k''} p_{k'+j}$, $n = \prod_{i=1}^{k} p_i$ ∎

<u>Théorème</u> Soit p un nombre premier et $n \in \mathbb{N}$ tq $p \nmid n$ alors

$$\overline{n*} : \mathbb{N}/_{\mathrm{mod}\, p} \to \mathbb{N}/_{\mathrm{mod}\, p} \text{ est injective}$$

(donc bijective puisque $\mathbb{N}/_{\mathrm{mod}\, p}$ est fini puisque $p \neq 0$)

pr: Soit $n = r + pq$ avec $0 \leq r < p$, $q \in \mathbb{N}$

$\forall m \in \mathbb{N}$ $nm = (r + pq)m = rm + pqm \equiv rm \mod p$

il suffit (i.s.p.) de prouver dans le cas $p > r = n$ (≥ 1 car $p \nmid n$)

Si $n = 1$ $\overline{n*} = Id_{\mathbb{N}/_{\mathrm{mod}\, p}}$ est injective

Sinon $n = q_1 \cdots q_k$ avec pour $1 \leq i \leq k$, q_i premier

Comme $\overline{q_1 \cdots q_k *} = (\overline{q_1 *}) \circ \cdots \circ (\overline{q_k *})$

et le composé d'applications injectives est injective,

i.s.p. quand $n = q$ est premier et $q < p$

Par (2)(ii) de la prop. $\overline{*q}$ est injective si $\forall m \in \mathbb{N}$

$$qm \equiv 0 \mod p \Rightarrow m \equiv 0 \mod p$$

mais $qm \equiv 0 \mod p \Rightarrow \exists k \in \mathbb{N}$ $qm = kp \Rightarrow pk \equiv 0 \mod q$

comme p est premier et $1 < q < p$ on a $q \nmid p$

comme q est premier et $q < p$ récurrence sur le thm donne $k \equiv 0 \mod q$

$\exists \ell \in \mathbb{N}$ $k = q\ell$ donc $qm = q\ell p$ et $m = \ell p \equiv 0 \mod p$ ∎

<u>Corollaire</u> (unicité de la décomposition en facteurs premiers)

Soit $n \in \mathbb{N}\ (n>1)$ et $p_1 \leq \cdots \leq p_k$, $q_1 \leq \cdots \leq q_\ell$ premiers t.q. $p_1 \cdots p_k = n = q_1 \cdots q_\ell$

Alors $k = \ell$ et pour $1 \leq i \leq \ell$ on a $q_i = p_i$

pr Comme $p_k | n$ $\forall m \in \mathbb{N}$ $p_k | nm$ et $\overline{n*} : \mathbb{N}/_{\mathrm{mod}\, p_k} \to \mathbb{N}/_{\mathrm{mod}\, p_k}$
est l'application constante $\overline{m} \mapsto \overline{p_k}$ non injective puisque
$\mathrm{card}(\mathbb{N}/_{\mathrm{mod}\, p_k}) = p_k > 1$ (car p_k premier : une raison de ne pas considérer 1 comme premier !)
comme $\overline{n*} = \overline{q_1*} \circ \cdots \circ \overline{q_\ell *}$ un des $\overline{q_j *}$ est non injectif
et donc (thm) $p_k | q_j$ d'où (q_j premier) $p_k = q_j \leq q_\ell$
Les hypothèses étant symétriques en les p_* et q_* on a aussi $q_\ell \leq p_k$ $\Big\} \Rightarrow p_k = q_\ell$
Si $k=1$ alors $n = p_1$ est premier d'où $\ell = 1$ et $q_1 = p_1$
Sinon $k = k'+1$ avec $k'>0$, $n = (p_1 \cdots p_{k'})\, p_k$ n'est pas premier
d'où $1 < \ell = \ell' + 1$ avec $\ell' > 0$ et $q_1 \cdots q_{\ell'} = p_1 \cdots p_{k'} < n = p_1 \cdots p_k$
par récurrence sur n, $\ell' = k'$ et si $1 \leq i' \leq \ell'$, $q_{i'} = p_{i'}$. $\square$

⚠ <u>Remarque</u> la def des premiers et l'existence de la factorisation en premiers ne fait intervenir que $\times$ dans $\mathbb{N}$ et si $n = km$ avec $k \neq 1$ alors $m < n$.
Ici en raisonnant dans $\mathbb{N}/_{\mathrm{mod}\, p_k}$ on a aussi utilisé $+$

<u>Exemple</u> $\{n \in \mathbb{N} \mid n \equiv 1 \bmod 4\}$ est stable par $\times$

$$\left((4k+1)(4l+1) = 4(4kl+k+l)+1 \right)$$

on peut définir $4k+1$ "pseudo premier" si

$$4k+1 = (4k'+1)(4k''+1) \Rightarrow k'=0 \text{ ou } k''=0$$

le début de la suite de ces pseudo premiers est

$$5, 9, 13, 17, 21, 29, 33, 37, 41, 49$$

il y a toujours existence de la décomposition $25 = 5\times 5$, $45 = 5\times 9$

mais $21 \times 21 = 481 = 9 \times 49$ il n'y a pas unicité.

<u>def</u> Soit $n \in \mathbb{N}$, $n > 1$ Sa {décomposition réduite / factorisation réduite} en premiers est

$$n = \prod_{i=1}^{k} p_i^{v_i} \text{ où } p_1 < \dots < p_k \text{ sont premiers et}$$

pour $1 \leq i \leq k$ on a $v_i \geq 1$

<u>Co-corollaire 1</u> Soit $n \in \mathbb{N}$ $n > 1$ de factorisation réduite $n = \prod_{i=1}^{k} p_i^{v_i}$

alors $\mathrm{Div}(n) = \left\{ \prod_{i=1}^{k} p_i^{\nu_i} \;\middle|\; 0 \leq \nu_i \leq v_i \right\}$

En particulier $\mathrm{card}\, \mathrm{Div}(n) = \prod_{i=1}^{k} (v_i + 1)$

<u>def</u> $n, m \in \mathbb{N}$ sont premiers entre eux si 1 est le seul diviseur commun

à n et m : $\mathrm{Div}(n) \cap \mathrm{Div}(m) = \{1\}$

Co-corollaire 2 Soit m, n entiers positifs premiers entre eux alors

$$\overline{n*} : \mathbb{N}/_{\mathrm{mod}\, m} \to \mathbb{N}/_{\mathrm{mod}\, m}$$ est injective (donc bijective)

En particulier $n \mid mk$ ~~et~~ n première à $m \Rightarrow n \mid k$.

pv Exercice reprendre la pv du théorème.

Application (Identité de Bezout) Si $m \leq n \in \mathbb{N}$ sont premiers entre eux alors il y a $k, l \in \mathbb{N}$ t.q. $nk = 1 + ml$

pv Si $m = 0$ alors $n = 1$ et $k = 1$ $l \in \mathbb{N}$ convient

sinon $\mathbb{N}/_{\mathrm{mod}\, m}$ est fini et par co-cor 2 $\overline{n*} : \mathbb{N}/_{\mathrm{mod}\, m} \to \mathbb{N}/_{\mathrm{mod}\, m}$ surjective

il y a donc $k \in \mathbb{N}$ t_q $nk \equiv 1 \mod m$ c.a.d. $\exists l \in \mathbb{N}$ t_q $nk = 1 + ml$. $\square$

fin 27/02/2007

6 Opérations dans $\mathbb{N}/_{\mathrm{mod}\, N}$.

Proposition Soit R, S, T des relations d'équivalence sur des ensembles X, Y, Z et $f : X \times Y \to Z$ alors f passe au quotient en $\overline{f} : X/_R \times Y/_S \to Z/_T$ (t.q. $\overline{f} \circ (\pi_R \times \pi_S) = \pi_T \circ f : X \times Y \to Z/_T$ ssi $\forall x, x' \in X, y, y' \in Y$ on a

(1) $x \equiv x' \mod R \Rightarrow f(x, y) \equiv f(x', y) \mod T$

et (2) $y \equiv y' \mod S \Rightarrow f(x', y) \equiv f(x', y') \mod T$

[donc $(x \equiv x' \mod R)$ et $(y \equiv y' \mod S) \Rightarrow f(x, y) \equiv f(x', y') \mod T$]

pv $\Rightarrow$ (1) $\pi_T(f(x, y)) = \overline{f}(\overline{x}_R, \overline{y}_S) \underset{\text{car } \overline{x}_R = \overline{x'}_R}{=} \overline{f}(\overline{x'}_R, \overline{y}_S) = \pi_T(f(x', y))$ donc $f(x, y) \equiv f(x', y) \mod T$

(2) $\pi_T(f(x', y)) = \overline{f}(\overline{x'}_R, \overline{y}_S) \underset{\text{car } \overline{y}_S = \overline{y'}_S}{=} \overline{f}(\overline{x'}_R, \overline{y'}_S) = \pi_T(f(x', y'))$ donc $f(x', y) \equiv f(x', y') \mod T$

$\Leftarrow$ $\forall\, x', y' \in \overline{x}_R \times \overline{y}_S$ on a [le donc de la prop] $f(x',y') \equiv f(x,y) \bmod T$

donc $\overline{f(x',y')}_T = \overline{f(x,y)}_T$ et on peut définir $\overline{f} : X/_R \times Y/_S \to Z/_T$

par $\overline{f}(\overline{x}_R, \overline{y}_T) = \overline{f(x,y)}_T$ (ça ne dépend pas du choix $x \in \overline{x}_R$ et $y \in \overline{y}_S$)

<u>Corollaire</u> Soit $N \in \mathbb{N}$ alors $+, \times : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ passent au quotient en

$$\overline{+}, \overline{\times} : \mathbb{N}/_{\text{mod} N} \times \mathbb{N}/_{\text{mod} N} \to \mathbb{N}/_{\text{mod} N}$$

pv Les vérifications (1) et (2) de la prop. ont déjà été faites

<u>Lemme</u> Si $N = p$ est premier alors $\Phi : \mathbb{N}/_{\text{mod} p} \to \mathbb{N}/_{\text{mod} p}$ $\Phi(x) = x^p = \underbrace{x \times \cdots \times x}_{p \text{ fois}}$

vérifie $\forall\, x, y \in \mathbb{N}/_{\text{mod} p}$ (1) $\Phi(x+y) = \Phi(x) + \Phi(y)$

[(2) $\Phi(xy) = \Phi(x) \times \Phi(y)$]

pv (1) comme $\forall\, x, y, z \in \mathbb{N}/_{\text{mod} p}$ on a $xy = yx$ et $(x+y)z = xy + yz$

on a $(x+y)^p = \sum_{k=0}^{p} \binom{p}{k} x^{p-k} y^k = x^p + \sum_{k=1}^{p-1} \binom{p}{k} x^{p-k} y^k + y^p$

où $\binom{p}{k} \in \mathbb{N}$: $\binom{p}{0} = 1 = \binom{p}{p}$ et si $0 < k < p$ $\binom{p}{k} = \frac{p!}{k!(p-k)!}$

on a $k!(p-k)! \binom{p}{k} = p! = p \times (p-1)!$

Si $0 < k < p-k$ comme p est premier et $p > k$, $p-k$

p est premier à $k!(p-k)!$ et divise $p! = k!(p-k)! \binom{p}{k}$

donc $p \mid \binom{p}{k}$ d'où $\binom{p}{k} x^{p-k} y^k \equiv 0 \bmod p$ c.a.d $\Phi(x+y) = \Phi(x) + \Phi(y)$

(2) Exercice

Corollaire $\forall x \in \mathbb{N}/_{\text{mod } p}$ on a $x^p = x$

pv On a $\Phi(1) = 1^p = 1$

pour tout $n \in \mathbb{N}$, $n > 0$ on a $n = \underbrace{1 + \cdots + 1}_{n \text{ fois}}$ donc

$$\Phi(\bar{n}) = \Phi(\underbrace{\bar{1} + \cdots + \bar{1}}_{n \text{ fois}}) \underset{\substack{\uparrow \\ \text{recurrence} \\ \text{utilisant}(1)}}{=} \underbrace{\Phi(\bar{1}) + \cdots + \Phi(\bar{1})}_{n \text{ fois}} = \underbrace{\bar{1} + \cdots + \bar{1}}_{n \text{ fois}} = \bar{n} \quad \square$$

Co-corollaire $\forall x \in \mathbb{N}/_{\text{mod } p} \setminus \{p\}$ on a $x^{p-1} = 1$

pv soit $n \in \mathbb{N}$ tq $x = \bar{n}$ on a $p \nmid n$ et

$$0 = x^p - x = x(x^{p-1} - 1) = \bar{n}\,(x^{p-1} - 1) = \overline{n*}(x^{p-1} - 1)$$

donc (théorème) $x^{p-1} - 1 = 0$, c.a.d. $x^{p-1} = 0$. $\square$