Devoir surveillé n°5

Sujet donné le samedi 16 décembre 2023, 4h.

L'usage de la calculatrice n'est pas autorisé.

La notation tiendra particulièrement compte de **la qualité de la rédaction, la précision des raisonnements et l'énoncé des formules utilisées. Les réponses aux questions seront numérotées et séparées par un trait horizontal. Les résultats essentiels devront être encadrés ou soulignés.**

BON TRAVAIL

Problème - Racines de congruence

Dans tout le problème, on considère des polynômes à coefficients entiers. On étudie leurs propriétés en calculant les racines entières de ces polynômes modulo certains entiers fixés. Réciproquement, le choix de certains polynômes permet de démontrer certaines propriétés.

Notations :

- On note $\mathbb{Z}[x]$, l'ensemble des fonctions polynomiales dont les coefficients sont pris dans $\mathbb{Z}$.
- On note, pour tout $p \in \mathbb{N}$, X^p la fonction polynomiale entière $X^p : x \mapsto x^p$. Par exemple, on notera : $X - a : x \mapsto x - a$
- On note, dans ce problème, $[[f]]_k$, le coefficient devant x^k dans l'écriture de f.
  Ainsi si $f : x \mapsto 1 + 2x^2 - 5x^3$, alors $[[f]]_1 = 0$, $[[f]]_3 = -5$ et $[[f]]_5 = 0$.
- Pour $m \in \mathbb{Z}$ et $f \in \mathbb{Z}[x]$, on appelle racine de congruence de f modulo $[m]$ les entiers $a \in [\![0, m-1]\!]$ tels que $f(a) \equiv 0\,[m]$

Objectifs des prochaines parties :

- En partie I, par quelques calculs, nous essayons de comprendre ce qui peut se passer en terme de nombres de racines de congruence pour un polynôme de degré d fixé.
- En partie II, nous définissons deux adaptations de l'égalité et de la divisibilité, afin d'étudier les factorisations dans le cas de racines de congruence modulo m. Nous verrons que les choses ne se passent pas bien si m n'est pas premier. Tout n"est pas perdu dans le cas où m est un nombre premier.
- En partie III, nous exploitons les racines de congruence pour démontrer de nouveau le petit théorème de Fermat, selon la méthode de Lagrange. Ensuite, nous démontrerons aisément le théorème de Wilson et celui de Wolstenholme
- En partie IV, nous étudierons l'indicatrice d'Euler (grâce à une structure de groupe) afin d'essayer de généraliser la méthode de la partie III pour des nombres non premier.
- En partie V, nous énoncerons une forme de généralisation du résultat de Lagrange obtenu en partie III. Ce sont les théorèmes de Bauer. *A aborder que si on n'a plus rien à faire.*

Bien que le problème forme un tout unifié, les différentes parties peuvent être abordées séparément. Tous les résultats de l'énoncé peuvent être admis pour les questions suivantes. Lorsqu'un résultat d'une partie est exploitée dans une autre, cela est indiqué dans l'énoncé.

I Calculs arithmétiques

I.1. Quelles sont les racines entières de congruence de $X^4 - 1$, modulo 5 ?

I.2. Quelles sont les racines entières de congruence de $X^6 + 1$, modulo 7 ?

I.3. Quelles sont les racines entières de congruence de $X^4 - 1$, modulo 16 ?
Notons qu'il y a, pour cette dernière situation, un nombre de racines strictement supérieur au degré du polynôme.

II Polynômes entiers et congruence modulo un nombre premier

On fixe $m \in \mathbb{N}$. Sur cet ensemble, on définit les deux relations :

$$\begin{array}{rcl} f \overset{\cdots}{=} g\,[m] & \iff & \forall\, k \in \mathbb{N}, \quad [[f]]_k \equiv [[g]]_k\ [m] \\ g|f\,[m] & \iff & \exists\, h \in \mathbb{Z}[X] \text{ tel que } g \times h \overset{\cdots}{=} f[m] \end{array}$$

II.1. Relation $\overset{\cdots}{=}\ [m]$.

(a) Montrer que $\overset{\cdots}{=}\ [m]$ est une relation d'équivalence sur $\mathbb{Z}[x]$.

(b) Montrer que $(x-1)(x-2)(x-3)(x-4) \overset{\cdots}{=} x^4 - 1[5]$.

On rappelle que pour tout polynôme f et h et tout $k \in \mathbb{N}$: $[[f \times h]]_k = \sum_{i=0}^{k} [[f]]_i \times [[h]]_{k-i}$.

(c) Soit $f, g \in \mathbb{Z}[x]$. Montrer que si $f \overset{\cdots}{=} g\,[m]$, alors pour tout $h \in \mathbb{Z}[x]$, $f \times h \overset{\cdots}{=} g \times h\,[m]$.

On cherche à étudier l'implication réciproque (pour un h donné).

(d) Dans le cas où m est un nombre premier que l'on note p, montrer que si $f \times h \overset{\cdots}{=} 0\,[p]$ alors $f \overset{\cdots}{=} 0\,[p]$ ou $h \overset{\cdots}{=} 0\,[p]$.
On pourra faire un raisonnement par contraposée

(e) Soit $h \in \mathbb{Z}[x]$ tel que $f \times h \overset{\cdots}{=} g \times h\,[p]$. Montrer que $f \overset{\cdots}{=} g\,[p]$ ou $h \overset{\cdots}{=} 0\,[p]$

(f) Pour $m = 6$, donner trois polynômes f, g, h tels que $f \times h \overset{\cdots}{=} g \times h\,[m]$ et $f \overset{\cdots}{\neq} g\,[m]$ et $h \overset{\cdots}{\neq} 0\,[m]$

II.2. Relation $|\,[m]$

(a) Montrer que $|\,[m]$ est une relation réflexive et transitive sur $\mathbb{Z}[x]$ (on dit relation de pré-ordre).

(b) En prenant des polynômes constants, modulo 8, montrer que cette relation n'est pas une relation d'ordre, même associée à la relation d'équivalence $\cdot \overset{\cdots}{=} \cdot\,[8]$.

II.3. Lien avec les racines de congruence.

(a) Montrer que si $f \overset{\cdots}{=} g[m]$ alors pour tout $a \in \mathbb{Z}$, $f(a) \equiv g(a)[m]$.

(b) Soit $f \in \mathbb{Z}[x]$ et $a \in \mathbb{Z}$.
Factoriser $f(x) - f(a)$ dans $\mathbb{Z}[x]$

(c) Montrer l'équivalence (rappel : $X^k : x \mapsto x^k$, application polynomiale) :

$$X - a \,|f \quad [m] \qquad \Longleftrightarrow f(a) \equiv 0[m]$$

On notera que si $f \overset{\cdots}{=} (X-a)h$, on peut prendre dans l'équivalence h avec $\deg h = \deg f - 1$.

II.4. Factorisation lorsque m est premier.
On suppose que m est un nombre premier. On le note d'ailleurs p.

(a) Soient $f, g, h \in \mathbb{Z}[x]$. On suppose que $f \overset{\cdots}{=} g \times h[p]$.
Montrer que : $f(a) \equiv 0[p]$ si et seulement si $g(a) \equiv 0[p]$ ou $h(a) \equiv 0[p]$

(b) Conclure que si $f \in \mathbb{Z}[x]$ est de degré d, admettant d racines de congruence modulo p distinctes : a_1, a_2,…a_d (distinctes modulo p), alors il existe $c \in \mathbb{Z}$ tel que $f \overset{\cdots}{=} c(X-a_1)(X-a_2)\cdots(X-a_d)$.
Que dire de f, si f est de degré d avec $d+1$ racines distinctes de congruence modulo p ?

(c) En prenant $f = x^2$, trouver g et h tels que $f \overset{\cdots}{=} g \times h\,[4]$ et pourtant 0 n'est racine de congruence ni de g ni de h.
Conclure sur le caractère nécessaire que m soit premier.

III Diverses applications

On démontre quelques théorèmes connus avec les résultats précédents

III.1. Démonstration de Lagrange du petit théorème de Fermat. On ne peut l'utiliser pour les questions de 1.(a) à 1.(e).
On fixe un nombre premier p, impair (ie. $p \neq 2$). On considère le polynôme $L : x \mapsto (x-1)(x-2)\cdots(x-p+1)$.

(a) Quel est le degré de L ? Que vaut $[[L]]_{p-1}$?
On notera par la suite : $[[L]]_{-1} = [[L]]_p = 0$.

(b) Montrer que pour tout $x \in \mathbb{Z}$, $(x-p) \times L(x) = (x-1) \times L(x-1)$ (lire L en x, puis L en $x-1$).
En réalité il vaut mieux lire cette relation comme une relation polynomiale : $(X-p) \times L = (X-1) \times L \circ (X-1)$.

(c) En déduire : $\forall\, h \in [\![0, p]\!]$, $\quad [[L]]_{h-1} - p[[L]]_h = \displaystyle\sum_{i=h}^{p} \binom{i}{h} (-1)^{i-h} [[L]]_{i-1}$.

Puis que $\forall\, i \in [\![0, p-2]\!]$, $(p-i-1)\,[[L]]_i = \displaystyle\sum_{j=i+1}^{p-1} (-1)^{j-i} \binom{j+1}{i} [[L]]_j$.

(d) Puis montrer que pour tout $h \in \mathbb{N}_{p-2}$, $[[L]]_h \equiv 0[p]$

(e) Donner un polynôme simple F tel que $F \overset{\cdots}{=} L\,[p]$.
En déduire une nouvelle démonstration du petit théorème de Fermat.

(f) En déduire également le théorème de Wilson :

$$\text{Si } p \text{ est premier impair, } (p-1)! \equiv -1 \qquad [p]$$

(g) Avons-nous les mêmes résultats pour $p = 2$?

III.2. Théorème de Wolstenholme.
On fixe de nouveau p un nombre premier impair.
On rappelle que nous avons démontré en 1.(d), *en particulier pour* $h = 1$: $[[L]]_1 \equiv 0[p]$.

On note $H_p = 1 + \dfrac{1}{2} + \cdots \dfrac{1}{p-1} = \displaystyle\sum_{h=1}^{p-1} \frac{1}{h}$

(a) Montrer que $H_p = \dfrac{[[L]]_1}{(p-1)!}$.

(b) Montrer qu'après simplification, le numérateur de H_p est divisible par p.

(c) Montrer que le numérateur de H_5 (simplifié) est en fait divisible par $5^2 = 25$.
Est-ce le cas de H_3 (le numérateur est-il divisible par 9) ?

Par la suite on supposera que $p \geqslant 5$.

(d) Montrer que pour tout $k \in [\![1, p-1]\!]$, il existe $\overline{k} \in \mathbb{Z}$ tel que $k \times \overline{k} \equiv 1[p^2]$.

(e) On note, pour tout $k \in [\![1, p-1]\!]$, $b_k = \dfrac{(p-1)!}{k} \in \mathbb{Z}$ car $k|(p-1)!$
Montrer que $\overline{k} \times (p-1)! \equiv b_k[p^2]$

(f) En déduire que $(p-1)! \times H_p \equiv (p-1)! \times (\overline{1} + \overline{2} + \cdots + \overline{p-1})\ [p^2]$.

(g) En évaluant $L(p)$, et en simplifiant par $(p-1)!$, montrer que

$$\sum_{k=0}^{p-2} [[L]]_{k+1} p^k = 0$$

(h) En déduire, en exploitant 1.(d) que $[[L]]_1$ est divisible par p^2.

(i) Conclure en démontrant le théorème de Wolstenholme :

Si p est impair $\geqslant 5$, alors le numérateur simplifié de de H_p est divisible par p^2

(j) Montrer que, pour $p \geqslant 5$, le numérateur de $C_p = \displaystyle\sum_{k=1}^{p-1} \frac{1}{k^2}$ est divisible par p.

IV Ensemble premier à un entier m. Indicatrice d'Euler

On considère encore un entier m fixé pour toute cette partie.
On note $A_m = \{k \in [\![1, m]\!] \mid k \wedge m = 1\}$ et on note $\varphi(m) = \text{card}(A_m)$
On définit pour tout entier de $[\![1, m]\!]$, $\overline{\times}$ la règle opératoire (loi interne) :

$$\forall\ a, b \in [\![1, m]\!], \qquad a \overline{\times} b = (a \times b)\%m \textbf{ reste de la division euclidienne de } a \times b \textbf{ par } m.$$

IV.1. Donner A_3, A_4, A_5 et A_6.
Donner la valeur de $\varphi(3)$, $\varphi(4)$, $\varphi(5)$ et $\varphi(6)$.

IV.2. Structure de $(A_m, \overline{\times})$.

(a) Soit $k \in [\![1, m]\!]$. Montrer l'équivalence : $k \in A_m$ si et seulement si $\exists!\ h_k \in A_m$ tel que $h_k \overline{\times} k = 1$.

On note $\psi : A_m \to A_m$, $k \mapsto h_k$.

(b) Montrer que $(A_m, \overline{\times})$ est un groupe commutatif.

(c) Montrer que ψ est un morphisme de groupe.

(d) Que vaut $\ker \psi$? ψ est-elle injective ?

IV.3. Calcul de $\varphi(m)$.

(a) Décrire explicitement A_p et A_{p^a} si p est un nombre premier et $a \in \mathbb{N}$. En déduire la valeur de $\varphi(p)$ puis que $\varphi(p^a) = (p-1)p^{a-1}$, si p est un nombre premier et $a \in \mathbb{N}$.

(b) Soient p, q deux nombres premiers distincts. Décrire, de même A_{pq}, en déduire $\varphi(pq) = (p-1)(q-1) = \varphi(p)\varphi(q)$.

(c) On fixe $n \in \mathbb{N}$ et p un nombre premier avec n. Soit $a \in \mathbb{N}^*$.

i. Montrer que $\{k \in [\![1, p^a n]\!] \text{ tq. } k \wedge n = 1\} = \{m + qn; m \in A_n, q \in [\![0, p^a - 1]\!]\}$.

ii. Soit $m \in A_n$. Montrer qu'il existe $(q_0, r_0) \in \mathbb{Z}^2$ tel que $m + q_0 n = r_0 p$.
Montrer ensuite l'équivalence : $m + qn = rp \iff \exists\ k \in \mathbb{Z}$ tel que $q = q_0 + kp$ et $r = r_0 + kn$.

iii. En déduire que dans l'ensemble $\{m + qn; m \in A_n, q \in [\![0, p^a - 1]\!]\}$, exactement $(p-1)p^{a-1}$ termes sont premiers avec p.

iv. Conclure que $\varphi(p^a n) = \varphi(p^a) \times \varphi(n)$.

(d) En déduire que pour tout $m \in \mathbb{N}^*$:

$$\varphi(m) = \prod_{p \in \mathcal{P},\ p|m} (p-1)p^{v_p(m)-1}$$

V (*) Congruence composée

Le but de cette partie est généraliser l'idée de Lagrange pour démontrer le petit théorème de Fermat. Cela conduit aux théorèmes de Bauer.
On fixe $m \in \mathbb{N}$. On considère, par prolongement de la partie III, $L'_m = \displaystyle\prod_{t \in A_m} (x - t)$ (il ne s'agit pas du polynôme dérivé).
Dans cette partie, on exploitera la décomposition de A_{np^α} vu en IV.3.(c).

V.1. Montrer que pour $m = 9$, $L'_9 \overset{\cdots}{=} X^6 - 3X^4 + 3X^2 - 1\ [9]$

V.2. Montrer que si $m = p^a$ (avec $p > 2$), alors $L'_{p^a} \overset{\cdots}{=} (x^{p-1} - 1)^{p^{a-1}}\ [p^a]$.

V.3. Montrer que si $m = 2^a$, alors $L'_{2^a} \overset{\cdots}{=} (x^2 - 1)^{2^{a-2}}\ [2^a]$.

V.4. Montrer que si $p|m$ et $p > 2$: $L'_m \overset{\cdots}{=} (x^{p-1} - 1)^{\varphi(m)/(p-1)}\ [p^{v_p(m)}]$
et si $2|m$, : $L'_m \overset{\cdots}{=} (x^2 - 1)^{\varphi(m)/2}\ [2^{v_2(m)}]$

Correction

Problème - Racines de congruence

I Calculs arithmétiques

I.1. Quelles sont les racines entières de congruence de $X^4 - 1$, modulo 5 ?

D'après le théorème de Fermat, $a^4 \equiv 1[5]$, pour tout $a \wedge 5 = 1$.
Donc 1, 2, 3 et 4 étant premiers à 5, ce sont des solutions de l'équation.
En revanche, $0^4 \not\equiv 1[5]$.

$$\boxed{\mathcal{S} = \{1, 2, 3, 4\}}$$

I.2. Quelles sont les racines entières de congruence de $X^6 + 1$, modulo 7 ?

Pour les mêmes raisons que précédemment, 7 étant un nombre premier : $a^6 \equiv 1[7]$, pour tout nombre $a \in \mathbb{N}_6$.
Puis $0^6 \equiv 0[7]$.

$$\boxed{\mathcal{S} = \emptyset}$$

I.3. Quelles sont les racines entières de congruence de $X^4 - 1$, modulo 16 ?

On peut faire la liste des puissances :

k	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
k^2 [16]	0	1	4	9	0	9	4	1	0	1	4	9	0	9	4	1
k^4 [16]	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1

$$\boxed{\text{Donc } \mathcal{S} = \{1\ ,\ 3\ ,\ 5\ ,\ 7\ ,\ 9\ ,\ 11\ ,\ 13\ ,\ 15\}.}$$

(Nous verrons plus loin que tous les nombres premiers à 16, donc les nombres impairs vérifient $x^{\varphi(16)} = x^4 \equiv 1[16]$.)

Notons qu'il y a pour cette dernière situation, un nombre de racine strictement supérieur au degré du polynôme.

II Polynômes entiers et congruence modulo un nombre premier

On fixe $m \in \mathbb{N}$. Sur cet ensemble, on définit les deux relations :

$$\begin{array}{rcl} f \overset{\cdots}{=} g\ [m] & \iff & \forall\ k \in \mathbb{N}, \quad [[f]]_k \equiv [[g]]_k\ \ [m] \\ g|f\ [m] & \iff & \exists\ h \in \mathbb{Z}[X] \text{ tel que } g \times h \overset{\cdots}{=} f[m] \end{array}$$

II.1. Relation $\overset{\cdots}{=}\ [m]$.

(a) Montrer que $\overset{\cdots}{=}\ [m]$ est une relation d'équivalence sur $\mathbb{Z}[x]$.

La relation est :
— Réflexive : pour tout $f \in \mathbb{Z}[x] : \forall\ k \in \mathbb{N}$, $[[f]]_k = [[f]]_k[p]$, donc $f \overset{\cdots}{=} f\ [m]$.
— Symétrique : pour tout $f, g \in \mathbb{Z}[x]$, si $f \overset{\cdots}{=} g\ [m]$, alors $\forall\ k \in \mathbb{N}, [[f]]_k \equiv [[g]]_k\ \ [m]$,
donc $\forall\ k \in \mathbb{N}, [[g]]_k \equiv [[f]]_k\ \ [m]$ et ainsi $g \overset{\cdots}{=} f\ [m]$
— Transitive : pour tout $f, g, h \in \mathbb{Z}[x]$, si $f \overset{\cdots}{=} g\ [m]$ et $g \overset{\cdots}{=} h\ [m]$, alors $\forall\ k \in \mathbb{N}, [[f]]_k \equiv [[g]]_k \equiv [[h]]_k\ \ [m]$,
et ainsi $f \overset{\cdots}{=} h\ [m]$

$$\boxed{\overset{\cdots}{=}\ [m] \text{ est une relation d'équivalence sur } \mathbb{Z}[x].}$$

(b) Montrer que $(x-1)(x-2)(x-3)(x-4) \overset{\cdots}{=} x^4 - 1[5]$.

On fait le calcul (on pourrait aussi exploiter proprement le théorème de Fermat).

$$\boxed{(x-1)(x-2)(x-3)(x-4) = (x^2 - 3x + 2)(x^2 - 7x + 12) = x^4 - 10x^3 + 35x^2 - 50x + 24 \overset{\cdots}{=} x^4 - 1[5]}$$

car 5 divise -10, 35, -50 et que $24 \equiv -1[4]$.

On rappelle que pour tout polynôme f et h et tout $k \in \mathbb{N}$: $[[f \times h]]_k = \sum_{i=0}^{k} [[f]]_i \times [[h]]_{k-i}$.

(c) Soit $f, g \in \mathbb{Z}[x]$. Montrer que si $f \overset{\cdots}{=} g\,[m]$, alors pour tout $h \in \mathbb{Z}[x]$, $f \times h \overset{\cdots}{=} g \times h\,[m]$.

Soient $f, g \in \mathbb{Z}[x]$. Supposons que $f \overset{\cdots}{=} g\,[m]$. On a donc pour tout $i \in \mathbb{N}$, $[[f]]_i \equiv [[g]]_i\,[m]$.
Soit $h \in \mathbb{Z}[x]$. Soit $k \in \mathbb{N}$,

$$[[f \times h]]_k = \sum_{i=0}^{k} [[f]]_i \times [[h]]_{k-i} \equiv \sum_{i=0}^{k} [[g]]_i \times [[h]]_{k-i} \equiv [[g \times h]]_k \qquad [m]$$

On a donc, pour tout $k \in \mathbb{N}$, $[[f \times h]]_k \equiv [[g \times h]]_k\,[m]$, donc :

$$\boxed{\text{pour tout } h \in \mathbb{Z}[x],\ f \times h \overset{\cdots}{=} g \times h\,[m].}$$

On cherche à étudier l'implication réciproque (pour un h donné).

(d) Dans le cas où m est un nombre premier que l'on note p, montrer que si $f \times h \overset{\cdots}{=} 0\,[p]$ alors $f \overset{\cdots}{=} 0\,[p]$ ou $h \overset{\cdots}{=} 0\,[p]$.
On pourra faire un raisonnement par contraposée

Soient f et $h \in \mathbb{Z}[x]$ tel que $f \overset{\cdots}{\neq} 0[p]$ et $h \overset{\cdots}{\neq} 0[p]$.
L'ensemble $\{k \in \mathbb{N} \mid [[f]]_k \not\equiv 0[p]\}$ est donc non vide, il en est de même de $\{k \in \mathbb{N} \mid [[h]]_k \not\equiv 0[p]\}$.
Ce sont des ensembles d'entiers naturels, ils admettent donc un plus petit élément chacun.
Notons $k_1 = \min\{k \in \mathbb{N} \mid [[f]]_k \not\equiv 0[p]\}$ et $k_2 = \min\{k \in \mathbb{N} \mid [[h]]_k \not\equiv 0[p]\}$.
On a donc, pour tout $i < k_1$, $[[f]]_{k_1} \equiv 0[p]$ et pour tout $i < k_2$, $[[h]]_{k_1} \equiv 0[p]$ Alors

$$\begin{aligned}
[[f \times h]]_{k_1+k_2} &= \sum_{i=0}^{k_1-1} [[f]]_i [[h]]_{k_1+k_2-i} + [[f]]_{k_1}[[h]]_{k_2} + \sum_{i=k_1+1}^{k_1+k_2} [[f]]_i [[h]]_{k_1+k_2-i} \\
&= \sum_{i=0}^{k_1-1} [[f]]_i [[h]]_{k_1+k_2-i} + [[f]]_{k_1}[[h]]_{k_2} + \sum_{i=0}^{k_2-1} [[f]]_{k_1+k_2-j} [[h]]_j \\
&\equiv \sum_{i=0}^{k_1-1} 0 \times [[h]]_{k_1+k_2-i} + [[f]]_{k_1}[[h]]_{k_2} + \sum_{i=0}^{k_2-1} [[f]]_{k_1+k_2-j} \times 0 \equiv [[f]]_{k_1}[[h]]_{k_2} \qquad [p]
\end{aligned}$$

Or p ne divise pas $[[f]]_{k_1}$, donc $p \wedge [[f]]_{k_1} = 1$ (car p est premier), de même $p \wedge [[h]]_{k_2} = 1$.
Et donc d'après un corollaire du lemme de Gauss : $p \wedge [[f]]_{k_1}[[h]]_{k_2} = 1$. Donc $[[f]]_{k_1}[[h]]_{k_2} \not\equiv 0[p]$.
Et finalement : $f \times h \overset{\cdots}{\neq} 0[p]$.
On a donc montré : $f \overset{\cdots}{\neq} 0[p]$ et $h \overset{\cdots}{\neq} 0[p] \Longrightarrow f \times h \overset{\cdots}{\neq} 0[p]$.
Par contraposée :

$$\boxed{\text{Si } f \times h \overset{\cdots}{=} 0\,[p] \text{ alors } f \overset{\cdots}{=} 0\,[p] \text{ ou } h \overset{\cdots}{=} 0\,[p].}$$

(e) Soit $h \in \mathbb{Z}[x]$ tel que $f \times h \overset{\cdots}{=} g \times h\,[p]$. Montrer que $f \overset{\cdots}{=} g\,[p]$ ou $h \overset{\cdots}{=} 0\,[p]$

Supposons que $f \times h \overset{\cdots}{=} g \times h\,[p]$, on a donc

$$\forall\, k \in \mathbb{N}, \qquad \sum_{i=0}^{k} [[f]]_i [[h]]_{k-i} \equiv \sum_{i=0}^{k} [[g]]_i [[h]]_{k-i} \qquad [p] \Rightarrow \sum_{i=0}^{k} \left([[f]]_i - [[g]]_i\right) [[h]]_{k-i} \equiv 0 \qquad [p]$$

Et par conséquent : $(f-g) \times h \overset{\cdots}{=} 0\,[p]$ (car $[[f]]_i - [[g]]_i = [[f-g]]_i$).
Et d'après la proposition précédente : $f - g \overset{\cdots}{=} 0\,[p]$ ou $h \overset{\cdots}{=} 0\,[p]$.
Enfin, toujours en utilisant $[[f]]_i - [[g]]_i = [[f-g]]_i$, on trouve alors que $f - g \overset{\cdots}{=} 0\,[p]$ est équivalent à $f \overset{\cdots}{=} g\,[p]$.

$$\boxed{\text{Si } h \in \mathbb{Z}[x] \text{ est tel que } f \times h \overset{\cdots}{=} g \times h\,[p], \text{ alors } f \overset{\cdots}{=} g\,[p] \text{ ou } h \overset{\cdots}{=} 0\,[p].}$$

(f) Pour $m = 6$, donner trois polynômes f, g, h tels que $f \times h \overset{\cdots}{=} g \times h\,[m]$ et $f \overset{\cdots}{\neq} g\,[m]$ ou $h \overset{\cdots}{\neq} 0\,[m]$

$$\boxed{\text{Prenons les polynômes constants } f = 2,\ g = 4 \text{ et } h = 3.}$$

On a alors $f \times h = 6 \equiv 0[6]$ et $g \times h = 12 \equiv 0[12]$, donc $f \times h \overset{\cdots}{=} g \times h\,[6]$.
Alors que $f \overset{\cdots}{\neq} g\,[6]$ et $h \overset{\cdots}{\neq} 0\,[6]$.

II.2. Relation $|\,[m]$

(a) Montrer que $|\,[m]$ est une relation réflexive et transitive sur $\mathbb{Z}[X]$ (on dit relation de pré-ordre).

La relation est
— réflexive ; puisque pour tout $f \in \mathbb{Z}[x]$, avec $h = 1 \in \mathbb{Z}[x]$, on a $f \times h = f$. Donc $f|f\,[m]$.
— transitive ; puisque pour tout $f, g, h \in \mathbb{Z}[x]$ tels que $f|g\,[m]$ et $g|h\,[m]$, il existe φ_1, $\varphi_2 \in \mathbb{Z}[x]$ tels que
$g \overset{\cdots}{=} \varphi_1 \times f[m]$ et $h \overset{\cdots}{=} \varphi_2 \times g[m]$. Alors $h \overset{\cdots}{=} \varphi_1 \times \varphi_2 \times f[m]$.
Et comme $\varphi_1 \times \varphi_2 \in \mathbb{Z}[x]$, on a bien $f|h\,[m]$.

$\boxed{|\,[m] \text{ est une relation de préordre sur } \mathbb{Z}[x].}$

(b) En prenant des polynômes constants, modulo 8, montrer que cette relation n'est pas une relation d'ordre, même associée à la relation d'équivalence $\cdot \overset{\cdots}{=} \cdot\,[8]$.

$\boxed{\text{Prenons } f = 2 \text{ et } g = 6.}$

Alors avec $h = 3$, on a $f \times h = g$, donc $f|g[8]$.
Et toujours avec $h = 3$, on trouve $g \times h = 18 \equiv 2[8]$, donc $g|f[8]$.
Et pourtant on n'a pas $f \overset{\cdots}{=} g[8]$ car $2 \not\equiv 6\,[8]$.

II.3. Lien avec les racines de congruence.

(a) Montrer que si $f \overset{\cdots}{=} g[m]$ alors pour tout $a \in \mathbb{Z}$, $f(a) \equiv g(a)[m]$.

Soient $f, g \in \mathbb{Z}[x]$. On suppose que $f \overset{\cdots}{=} g[m]$. Soit $a \in \mathbb{Z}$.
Donc $\forall\, k \in \mathbb{N}$, $m \mid [[f]]_k - [[g]]_k$.

Et par conséquent : $m \mid ([[f]]_k - [[g]]_k)a^k = [[f]]_k a^k - [[g]]_k a^k$. Et donc $m \mid \left(\sum_{k\in\mathbb{N}} [[f]]_k a^k - \sum_{k\in\mathbb{N}} [[g]]_k x^k\right)$.

Donc mł : $|\, f(a) - g(a)$, c'est-à-dire : $f(a) \equiv g(a)[m]$.

$\boxed{\text{Si } f \overset{\cdots}{=} g[m] \text{ alors pour tout } a \in \mathbb{Z},\ f(a) \equiv g(a)[m].}$

(b) Soit $f \in \mathbb{Z}[x]$ et $a \in \mathbb{Z}$.
Factoriser $f(x) - f(a)$ dans $\mathbb{Z}[x]$

On applique la formule des « petits Bernoullis ». Supposons $f(x) = \sum_{k=0}^{n} c_k x^k$, donc

$$f(x) - f(a) = \sum_{k=0}^{n} c_k x^k - \sum_{k=0}^{n} x_k a^k = \sum_{k=1}^{n} c_k (x^k - a^k) = (x-a) \underbrace{\sum_{k=1}^{n} c_k \sum_{h=0}^{k-1} a^{k-1-h} x^h}_{=h(x)\in\mathbb{Z}[x]}$$

$$\boxed{f(x) - f(a) = (x-a) \times \sum_{k=1}^{n} c_k \left(\sum_{h=0}^{k-1} a^{k-1-h} x^h\right)}$$

(c) Montrer l'équivalence (rappel : $X^k : x \mapsto x^k$, application polynomiale) :

$$X - a \,|f \ \ [m] \qquad \Longleftrightarrow f(a) \equiv 0[m]$$

On notera que si $f \overset{\cdots}{=} (X-a)h$, on peut prendre dans l'équivalence h avec $\deg h = \deg f - 1$.

Si $f(a) \equiv 0[m]$, alors $f \overset{\cdots}{=} (X-a) \times h\,[m]$ (en reprenant h de la question 3.(a) - il est de degré $n-1$, si $\deg f = n$).
On a donc $X - a \mid f\ [m]$.
Réciproquement, supposons que $X - a \mid f\ [m]$.
Il existe $g \in \mathbb{Z}[x]$ tel que $(X-a) \times g \overset{\cdots}{=} f\,[m]$.
Donc, d'après 3.(b), pour tout $b \in \mathbb{Z}$ $\big((X-a) \times g\big)(b) \equiv f(b)\,[m]$.
Et ainsi, comme a est une racine de $\big(X-a) \times g$, on a $0 \equiv f(a)\,[m]$.

$$\boxed{X - a \,|f \ \ [m] \qquad \Longleftrightarrow f(a) \equiv 0\,[m]}$$

II.4. Factorisation lorsque m est premier.
On suppose que m est un nombre premier. On le note d'ailleurs p.

(a) Soient $f, g, h \in \mathbb{Z}[x]$. On suppose que $f \overset{\cdots}{=} g \times h[p]$.
Montrer que : $f(a) \equiv 0[p]$ si et seulement si $g(a) \equiv 0[p]$ ou $h(a) \equiv 0[p]$

On a vu que pour tout $b \in \mathbb{Z}$, $f(b) \equiv g(b)h(b)\ [p]$.
Donc si $a \in \mathbb{Z}$ est tel que $g(a) \equiv 0[p]$ ou $h(a) \equiv 0[p]$, alors on a bien $f(a) \equiv 0[p]$.
Réciproquement, supposons que $f(a) \equiv 0[p]$.
On a donc $g(a)h(a) \equiv 0[p]$, donc $p | g(a) \times h(a)$.
Mais p est un nombre premier, donc il divise $g(a)$ (en entier) ou $h(a)$.
Ainsi $g(a) \equiv 0[p]$ ou $h(a) \equiv 0[p]$.

$$\boxed{f(a) \equiv 0[p] \text{ si et seulement si } g(a) \equiv 0[p] \text{ ou } h(a) \equiv 0[p].}$$

(b) Conclure que si $f \in \mathbb{Z}[x]$ est de degré d, admettant d racines de congruence modulo p distinctes : a_1, a_2,...a_d (distinctes modulo p), alors il existe $c \in \mathbb{Z}$ tel que $f \overset{\cdots}{=} c(X - a_1)(X - a_2) \cdots (X - a_d)$.
Que dire de f, si f est de degré d avec $d + 1$ racines distinctes de congruence modulo p ?

Considérons $f \in \mathbb{Z}[x]$, de degré d, et admettant d racines de congruence modulo p distinctes : a_1, a_2,...a_d .
Posons pour tout $n \in [\![1, d]\!]$, $\mathcal{P}_n$: « $\exists\ g \in \mathbb{Z}[x]$ tel que $f \overset{\cdots}{=} g \times (X - a_1) \cdots (X - a_n)$ avec $\deg g = d - n$ ».

— $f(a_1) \equiv 0[p]$, donc d'après 3.(c), $X - a_1 | f[m]$, donc il existe $g \in \mathbb{Z}[x]$ tel que $f \overset{\cdots}{=} (X - a)g\ [p]$ Notons que la fonction g trouvée, grâce au petit Bernoulli est de degré au plus $n - 1$.
Donc $\mathcal{P}_1$ est vraie.

— Soit $n \in \mathbb{N}_{d-1}$ tel que $\mathcal{P}_n$ est vraie.
Donc il existe $g \in \mathbb{Z}[x]$ tel que $f \overset{\cdots}{=} g \times (X - a_1) \cdots (X - a_n)$ avec $\deg g = d - n$.
Puis $f(a_{n+1}) \equiv 0[p]$, donc d'après la question précédente : ou bien $g(a_{n+1}) \equiv 0[p]$, ou bien $\exists\ k \in \mathbb{N}_n$ tel que $(a_{n+1} - a_k \equiv 0[p]$.
Or par hypothèse, tous les a_i sont distincts modulo p.
Donc nécessairement $g(a_{n+1} \equiv 0[p]$. On applique ensuite 3.(c).
Il existe g_1 de degré $\deg g - 1 = d - n - 1$ tel que $g \overset{\cdots}{=} g_1 \times (X - a_{n+1})$.
Et donc $f \overset{\cdots}{=} g_1 \times (X - a_1) \cdots (X - a_n)(X - a_{n+1})$ avec $\deg g = d - n - 1$.
Donc $\mathcal{P}_{n+1}$ est vraie.

La récurrence est démontrée.
Par conséquent $\mathcal{P}_d$ est également vraie. Comme $\deg g = d - d = 0$, signifie que g est constant, elle dit exactement :

$$\boxed{\text{il existe } c \in \mathbb{Z} \text{ tel que } f \overset{\cdots}{=} c(X - a_1)(X - a_2) \cdots (X - a_d).}$$

Si f est de degré d avec $d + 1$ racines distinctes de congruence modulo p, on trouve $f \overset{\cdots}{=} c(X - a_1)(X - a_2) \cdots (X - a_d)$, avec $f(a_{d+1}) \equiv 0[p]$. Impossible sauf si $c \equiv 0[p]$, et donc

$$\boxed{\text{Si } f \text{ est de degré } d \text{ avec } d + 1 \text{ racines distinctes de congruence modulo } p, \text{ alors } f \overset{\cdots}{=} 0[p].}$$

(c) En prenant $f : x \mapsto x^2$, trouver g et h tels que $f \overset{\cdots}{=} g \times h\ [4]$ et pourtant 0 n'est racine de congruence ni de g ni de h.
Conclure sur le caractère nécessaire que m soit premier.

$$\boxed{\text{En prenons } g : x \mapsto x - 2 \text{ et } h : x \mapsto x + 2,}$$

alors $g(x)h(x) = x^2 - 4$. Donc $f \overset{\cdots}{=} g \times h$.
Et pourtant $g(0) \equiv h(0 \equiv 2[4]$, Donc 0 n'est racine de congruence ni de g, ni de h. Dans le cas où m n'est pas premier, le théorème précédent est donc mis en défaut.

III Diverses applications

III.1. Démonstration de Lagrange. On fixe un nombre premier p, impair (ie. $p \neq 2$).
On considère le polynôme $L : x \mapsto (x - 1)(x - 2) \cdots (x - p + 1)$.

(a) Quel est le degré de L ? Que vaut $[[L]]_{p-1}$?

$$\boxed{\text{Le degré de } L \text{ est } p - 1, \text{ son coefficient dominant est } [[L]]_{p-1} = 1.}$$

On notera par la suite : $[[L]]_{-1} = [[L]]_p = 0$.

(b) Montrer que pour tout $x \in \mathbb{Z}$, $(x-p) \times L(x) = (x-1) \times L(x-1)$ (lire L en x, puis L en $x-1$).
En réalité il vaut mieux lire cette relation comme une relation polynomiale : $(X-p) \times L = (X-1) \times L \circ (X-1)$.

Puisque $L(x) = \prod_{k=1}^{p-1}(x-k)$, on a directement, pour tout $x \in \mathbb{Z}$,

$$\begin{aligned}(x-p) \times L(x) &= (x-p)\prod_{k=1}^{p-1}(x-k) = \prod_{k=1}^{p}(x-k) = (x-1)\prod_{k=2}^{p}(x-k) \\ &= (x-1)\underbrace{\prod_{h=1}^{p-1}(x-(h+1))}_{h=k-1} = (x-1)\prod_{h=1}^{p-1}((x-1)-h) = (x-1) \times L(x-1)\end{aligned}$$

$$\boxed{\forall\, x \in \mathbb{Z}, (x-p) \times L(x) = (x-1) \times L(x-1)}$$

(c) En déduire : $\forall\, h \in [\![0,p]\!]$, $\quad [[L]]_{h-1} - p[[L]]_h = \sum_{i=h}^{p} \binom{i}{h}(-1)^{i-h}[[L]]_{i-1}$.

Puis que $\forall\, i \in [\![0,p-2]\!]$, $(p-i-1)\,[[L]]_i = \sum_{j=i+1}^{p-1}(-1)^{j-i}\binom{j+1}{i}[[L]]_j$.

Remplaçons L par son expression développée, puis identification par unicité d'écriture polynomiale.
D'abord, en exploitant $[[L]]_{-1} = 0$ et $[[L]]_p = 0$:

$$\begin{aligned}(x-p)L(x) &= \sum_{k=0}^{p-1}[[L]]_k x^{k+1} - \sum_{k=0}^{p-1} p[[L]]_k x^k = \underbrace{\sum_{h=0}^{p}[[L]]_{h-1}x^h}_{h=k+1} + \underbrace{\sum_{h=0}^{p}[[L]]_h x^h}_{h=k} \\ &= \sum_{i=0}^{p}\left([[L]]_{i-1} - p[[L]]_i\right)x^i\end{aligned}$$

Puis, toujours avec $[[L]]_{-1} = 0$ et le binôme de Newton :

$$\begin{aligned}(x-1)L(x-1) &= \sum_{k=0}^{p-1}[[L]]_k(x-1)^{k+1} = \sum_{h=0}^{p}[[L]]_{h-1}(x-1)^h = \sum_{h=0}^{p}\sum_{i=0}^{h}\binom{h}{i}[[L]]_{h-1}(-1)^{h-i}x^i \\ &= \sum_{i=0}^{p}\left(\sum_{h=i}^{p}\binom{h}{i}[[L]]_{h-1}(-1)^{h-i}\right)x^i\end{aligned}$$

On peut alors identifier :

$$\boxed{\forall\, i \in [\![0,p]\!], \quad [[L]]_{i-1} - p[[L]]_i = \sum_{h=i}^{p}\binom{h}{i}[[L]]_{h-1}(-1)^{h-i}}$$

Continuons le calcul précédent, on trouve : $[[L]]_{i-1} - p[[L]]_i = \sum_{h=i+1}^{p}\binom{h}{i}(-1)^{h-i}[[L]]_{h-1} + \binom{i}{i}[[L]]_{i-1}(-1)^{i-i}$.

Donc en faisant le changement d'indice $j = h-1$ et en simplifiant par $[[L]]_{i-1}$:

$-p[[L]]_i = \sum_{j=i}^{p-1}(-1)^{j+1-i}\binom{j+1}{i}[[L]]_j$. Ainsi (la dernière somme étant vide, donc nulle si $i = p-1$) :

$$\boxed{\left(p - \binom{i+1}{i}\right)[[L]]_i = (p-i-1)\,[[L]]_i = \sum_{j=i+1}^{p-1}(-1)^{j-i}\binom{j+1}{i}[[L]]_j}$$

(d) Puis montrer que pour tout $h \in \mathbb{N}_{p-2}$, $[[L]]_h \equiv 0[p]$

Posons, pour tout $h \in [\![2,p-1]\!]$, $\mathcal{P}_h$: « p divise $[[L]]_{p-h}$ »
— Pour $i = p-2$, le calcul précédent donne :

$$(p-(p-2)-1)[[L]]_{p-2} = (-1)^{(p-1)-(p-2)}\binom{p}{p-2}[[L]]_{p-1}$$

Donc $[[L]]_{p-2} = -\binom{p}{p-2}[[L]]_{p-1} = -p\dfrac{p-1}{2}$ car $[[L]]_{p-1} = 1$. p est impair par hypothèse (soulignée), donc $p|[[L]]_{p-2}$.
Par conséquent $\mathcal{P}_2$ est vraie.

— Soit $h \in [\![2, p-2]\!]$. Supposons que $\mathcal{P}_2$,...$\mathcal{P}_h$ sont vraies.
Pour $i = p-(h+1) = p-h-1$, on trouve :

$$(p-(p-h-1)-1)[[L]]_{p-h-1} = h[[L]]_{p-h-1} = \sum_{j=p-h}^{p-1} (-1)^{j-p+h+1}\binom{j+1}{p-h-1}[[L]]_j$$

. Or comme $\mathcal{P}_2$, $\mathcal{P}_3 \cdots \mathcal{P}_h$ sont vraies : $[[L]]_j \equiv 0[p]$, pour $j \in \{p-2, p-3, \dots p-h\}$.

Donc $h[[L]]_{p-h-1} \equiv (-1)^h\binom{p}{p-h+1}[[L]]_{p-1} + 0 + \cdots + 0[p]$.

Or $(p-h+1) \times \binom{p}{p-h+1} = p \times \binom{p-1}{p-h}$. Donc p divise $(p-h+1) \times \binom{p}{p-h+1}$.

Mais comme $h \in [\![2, p-2]\!]$, $p-h+1 \in [\![3, p-1]\!]$, donc $(p-h+1) \wedge p = 1$, et donc $p | \binom{p}{p-h+1}$.

Ainsi $h[[L]]_{p-h-1} \equiv 0[p]$, et comme $h \wedge p = 1$, on a donc $[[L]]_{p-h-1} \equiv 0[p]$.
Donc $\mathcal{P}_{h+1}$ est vraie.

Ainsi, pour tout $h \in \mathbb{N}_{p-2}$, $[[L]]_h \equiv 0[p]$.

(e) Donner un polynôme simple F tel que $F \overset{\cdots}{=} L\,[p]$.
En déduire une nouvelle démonstration du petit théorème de Fermat.

D'après les questions précédentes : $\forall\ h \in N_{p-2}$, $[[L]]_h \equiv 0[p]$.
Par ailleurs, on a vu que $[[L]]_{p-1} = 1 \equiv 1[p]$ Il reste à calculer $[[L]]_0$, modulo p. Toujours avec la même relation en $i = 0$:

$$(p-1)[[L]]_0 = \sum_{j=1}^{p-1}(-1)^j\binom{j+1}{0}[[L]]_j \equiv 0 + \cdots 0 + (-1)^{p-1}\binom{p}{0}[[L]_{p-1} = -[[L]]_{p-1} = 1[p]$$

Or $p-1 \equiv -1[p]$, donc en multipliant par -1 : $[[L]]_0 \equiv -1[p]$

Avec $F = X^{p-1} - 1$, on a $F \overset{\cdots}{=} L\,[p]$.

Comme $1, 2, \dots p-1$ sont des racines de L, elles sont également des racines de congruence de F.

Et donc pour tout $k \in \mathbb{N}_{p-1}$, $F(k) = k^{p-1} - 1 \equiv L(k) \equiv 0\,[p]$.

(f) En déduire également le théorème de Wilson :

Si p est premier impair, $(p-1)! \equiv -1 \quad [p]$

$L(0) = (-1) \times (-2) \dots (-(p-1)) = (-1)^{p-1}(p-1)! = (p-1)!$, car p est impair.
On sait également que $[[L]]_0 = L(0)$, donc $[[L]]_0 = (p-1)!$.
D'après un calcul précédent (p est un premier impair car $\geqslant 3$) : $[[L]]_0 \equiv -1[p]$, donc

Si p est premier impair, $(p-1)! \equiv -1 \quad [p]$.

(g) Avons-nous les mêmes résultats pour $p = 2$?

Si $p = 2$, $(p-1)! = 1! = 1 \equiv -1\ [2]$

Le théorème de Wilson est doc vrai également pour $p = 2$.

Remarquons que l'on a aussi

$$L(x) = (x-1) = x^{2-1} - 1 = F(x)$$

III.2. Théorème de Wolstenholme.

On note $H_p = 1 + \frac{1}{2} + \cdots \frac{1}{p-1} = \sum_{h=1}^{p-1}\frac{1}{h}$

(a) Montrer que $H_p = \frac{[[L]]_1}{(p-1)!}$.

Pour faire le calcul de H_p, on élève au même dénominateur : $(p-1)!$, le k-ième terme de la somme qui est $\frac{1}{k}$ est alors multiplié par

$$b_k := \frac{(p-1)!}{k} = \prod_{i \in \mathbb{N}_{p-1}\setminus\{k\}} i = 1 \times 2 \times \cdots (k-1) \times (k+1) \times \cdots (p-1) \in \mathbb{Z}$$

On trouve donc $H_p = \frac{\sum_{k=1}^{p-1} b_k}{(p-1)!}$.

Par ailleurs, lorsque l'on développe le produit $L(x) = \prod_{k=1}^{p-1}(x-k)$, le coefficient $[[L]]_1$ que l'on trouve devant x est celui obtenu en prenant tous les termes du produit égal à k, excepté un seul, le i-ième qui vaut x et cela pour i allant de 1 à $p-1$.

Ainsi $[[L]]_1 = \sum_{i=1}^{p-1}(\prod_{k\neq i} k)$. C'est exactement le nombre $\sum_{k=1}^{p-1} b_k$.

$$\boxed{H_p = \frac{[[L]]_1}{(p-1)!}}$$

(b) Montrer qu'après simplification, le numérateur de H_p est divisible par p.

On sait que $[[L]]_1 \equiv 0[p]$, donc p divise $\sum_{k=1}^{p-1} b_k$.

Ce n'est pas encore suffisant, car H_p peut a priori se simplifier. Notons donc $\delta = \sum_{k=1}^{p-1} b_k \wedge (p-1)!$.

Alors δ divise $(p-1)!$, nécessairement comme $(p-1)! \wedge p = 1$ (p est premier), on a $\delta \wedge p = 1$.

Donc, il n'y a pas de simplification par p de $\sum_{k=1}^{p-1} b_k$ en simplifiant par δ.

Autrement écrit $\frac{\sum_{k=1}^{p-1} b_k}{\delta} (\in \mathbb{N})$ reste divisible par p.

$$\boxed{\text{Le numérateur de } H_p \text{ est divisible par } p.}$$

(c) Montrer que le numérateur de H_5 (simplifié) est en fait divisible par $5^2 = 25$.
Est-ce le cas de H_3 (le numérateur est-il divisible par 9) ?

$H_5 = 1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} = \frac{24+12+8+6}{24} = \frac{50}{24} = \frac{25}{12}$.
Le numérateur « minimal »est $25 = 5^2$, donc tous les autres en sont un multiple.

$$\boxed{\text{Le numérateur simplifié de } H_5 \text{ (et tous les autres) est divisible par } 5^2 = 25.}$$

Et $H_3 = 1 + \frac{1}{2} = \frac{3}{2}$.

$$\boxed{\text{Le numérateur simplifié de } H_3 \text{ n'est pas divisible par 9.}}$$

Par la suite on supposera que $p \geqslant 5$.

(d) Montrer que pour tout $k \in [\![1, p-1]\!]$, il existe $\overline{k} \in \mathbb{Z}$ tel que $k \times \overline{k} \equiv 1[p^2]$.

Soit $\delta = k \wedge p^2$, donc $\delta | p^2$, donc $\delta | p$, car p est un nombre premier. Ainsi $\delta = p$ ou $\delta = 1$
Mais on ne peut avoir $\delta = p$, car $k \wedge p = 1$ (k n'est pas divisible par p).
Donc $k \wedge p^2 = 1$. D'après le théorème de Bézout, il existe $u, v \in \mathbb{Z}$ tel que $uk + vp^2 = 1$.

$$\boxed{\text{On a alors, en notant } \overline{k} := u,\ \overline{k} \times k = 1\ [p^2].}$$

(e) On note, pour tout $k \in [\![1, p-1]\!]$, $b_k = \frac{(p-1)!}{k} \in \mathbb{Z}$ car $k | (p-1)!$
Montrer que $\overline{k} \times (p-1)! \equiv b_k[p^2]$

Par définition de b_k, $kb_k = (p-1)!$, et donc $\overline{k} \times k \times b_k = (p-1)!$.
Plongeons cette relation, modulo p^2, comme $\overline{k} \times k \equiv 1[p^2]$, on trouve

$$\boxed{1 \times b_k \equiv \overline{k} \times (p-1)![p^2]}$$

(f) En déduire que $(p-1)! \times H_p \equiv (p-1)! \times (\overline{1} + \overline{2} + \cdots + \overline{p-1})\ [p^2]$.

On se souvient que $H_p = \dfrac{[[L]]_1}{(p-1)!} = \dfrac{\sum_{k=1}^{p-1} b_k}{(p-1)!}$. Donc

$$(p-1)! \times H_p = \sum_{k=1}^{p-1} b_k \equiv \sum_{k=1}^{p-1} \overline{k} \times (p-1)! \equiv (p-1)! \sum_{k=1}^{p-1} \overline{k} \qquad [p^2]$$

$$\boxed{(p-1)! \times H_p \equiv (p-1)! \times (\overline{1} + \overline{2} + \cdots + \overline{p-1}) \quad [p^2]}$$

(g) En évaluant $L(p)$, et en simplifiant par $(p-1)!$, montrer que

$$\sum_{k=0}^{p-2} [[L]]_{k+1} p^k = 0$$

$L(p) = \prod_{k=1}^{p-1} (p-k) = \prod_{h=1}^{p-1} h = (p-1)!$. Et par ailleurs, $L(p) = \sum_{k=0}^{p-1} [[L]]_k p^k = [[L]]_0 + \sum_{k=1}^{p-1} [[L]]_k p^k$.
Or, on a vu que $[[L]]_0 = L(0) = (p-1)!$, donc, en additionnant $-(p-1)!$, on trouve (avec $h = k-1$) :

$$0 = \sum_{h=0}^{p-2} [[L]]_{h+1} p^{h+1} = p \sum_{h=0}^{p-1} [[L]]_{h+1} p^h$$

En simplifiant par $p \neq 0$:

$$\boxed{\sum_{k=0}^{p-2} [[L]]_{k+1} p^k = 0}$$

(h) En déduire, en exploitant 1.(d) que $[[L]]_1$ est divisible par p^2

On a donc $[[L_1]] = -\sum_{k=1}^{p-2} [[L]]_{k+1} p^k$.
Or d'après 1.(d) : pour tout $h \in \mathbb{N}_{p-2}$, $[[L]]_h \equiv 0[p]$, donc p divise $[[L]]_2$, $[[L]]_3, \cdots [[L]]_{p-2}$ Donc pour tout $k \in [\![2, p-2]\!]$, il existe u_k tel que $[[L]]_h = u_k \times p$.
Ainsi :

$$[[L]]_1 = -\sum_{k=1}^{p-2} u_k p \times p^k = p^2 \times \left(\underbrace{-\sum_{k=1}^{p-2} u_k p^{k-1}}_{\in \mathbb{Z}} \right)$$

$$\boxed{\text{Donc } [[L]]_1 \text{ est divisible par } p^2.}$$

Cette somme a bien un sens car $p > 3$.

(i) Conclure en démontrant le théorème de Wolstenholme :

Si p est impair $\geqslant 5$, alors le numérateur simplifié de de H_p est divisible par p^2

On a vu que le numérateur simplifiée de H_p est égal à $N := \dfrac{[[L]]_1}{\delta}$ où $\delta = [[L]]_1 \wedge (p-1)!$.
On vient de démontrer que p^2 divise $[[L]]_1 = N \times \delta$,
et par ailleurs, $p^2 \wedge (p-1)! = 1$ car p est premier, donc $p^2 \wedge \delta = 1$.
Donc nécessairement, d'après le lemme de Gauss :

$$\boxed{p^2 \text{ divise } N, \text{ le numérateur simplifié de } H_p \text{ (et donc tous les numérateurs possibles).}}$$

(j) Montrer que, pour $p \geqslant 5$, le numérateur de $C_p = \sum_{k=1}^{p-1} \dfrac{1}{k^2}$ est divisible par p.

C'est toujours la même stratégie.
On met au même dénominateur : $C_p = \dfrac{N_2}{((p-1)!)^2}$, où $N_2 = \sum_{k=1}^{p-1} b_k^2 = \sum_{k=1}^{p-1} \left(\dfrac{(p-1)!}{k} \right)^2$.

Par ailleurs : $L(x) \times L(x) = \prod_{k=1}^{p-1}(x-k)^2$. On a alors $[[L^2]]_2 = \sum_{k=1}^{p-1} b_k^2 + 4\sum_{i<j} b_i b_j$

(Ce 4 s'explique par les couples (i,j) possible à prendre :
ou bien i et j dans le 1er, - ou bien i dans le 1er, j dans le 2nd, - ou bien i dans le 2nd, j dans le 1er,
- ou bien i et j dans le 2nd,)

Et par ailleurs, avec la formule de Cauchy :

$$[[L^2]]_2 = [[L]]_0[[L]]2 + [[L]]_1[[L]]_1 + [[L]]_2[[L]]_0 = -2(p-1)![[L]]_2 + (\sum_{k=1}^{p-1} b_k)^2 = -2(p-1)![[L]]_2 + \sum_{k=1}^{p-1} b_k^2 + 2\sum_{i<j} b_i b_j$$

Donc, on a

$$\begin{cases} 4\sum_{i<j} b_i b_j = [[L^2]]_2 - \sum_{k=1}^{p-1} b_k^2 \\ 2\sum_{i<j} b_i b_j = -2(p-1)![[L]]_2 - \sum_{k=1}^{p-1} b_k^2 \end{cases}$$

Donc en faisant : $L_1 - 2L_2$: $[[L^2]]_2 - \sum_{k=1}^{p-1} b_k^2 = -4(p-1)![[L]]_2 - 2\sum_{k=1}^{p-1} b_k^2$.

Ainsi $\sum_{k=1}^{p-1} b_k^2 = -4(p-1)![[L]]_2 - [[L^2]]_2 = -4(p-1)![[L]]_2 + 2(p-1)![[L]]_2 - [[L]]_1^2 = -2(p-1)![[L]]_2 - [[L]]_1^2$.

Or p divise $[[L]]_2$ et $[[L]]_1$, donc divise $\sum_{k=1}^{p-1} b_k^2$. Il est premier avec $(p-1)^2$, donc

Pour $p \geqslant 5$, le numérateur de $C_p = \sum_{k=1}^{p-1} \frac{1}{k^2}$ est divisible par p.

IV Ensemble premier à un entier m. Indicatrice d'Euler

IV.1. Donner A_3, A_4, A_5 et A_6.
Donner la valeur de $\varphi(3)$, $\varphi(4)$, $\varphi(5)$ et $\varphi(6)$.

$A_3 = \{1,2\}$ $\quad A_4 = \{1,3\}$, $\quad A_5 = \{1,2,3,4\}$ $\quad A_6 = \{1,5\}$

$\varphi(3) = 2$ $\quad \varphi(4) = 2$ $\quad \varphi(5) = 4$ $\quad \varphi(6) = 2$

IV.2. Structure de $(A_m, \overline{\times})$.

(a) Soit $k \in [\![1,m]\!]$. Montrer l'équivalence : $k \in A_m$ si et seulement si $\exists!\, h_k \in A_m$ tel que $h_k \overline{\times} k = 1$.

Si il existe un unique $h_k \in A_m$ tel que $h_k \overline{\times} k = 1$.
alors $h_k \times k \% m = 1$. Donc il existe q tel que $h_k \times k = mq + 1$ (division euclidienne).
On a donc la relation de Bézout : $h_k k - qm = 1$ donc $k \wedge m = 1$. Ainsi $k \in A_m$ (car par hypothèse, $k \in [\![1,m]\!]$ également).
Réciproquement, si $k \in A_m$.
Alors $k \wedge m = 1$. D'après le théorème de Bézout, il existe $u, v \in \mathbb{Z}$ tel que $uk + vm = 1$.
Considérons $u_k = u\%m[m]$, alors $u_k \in [\![1,m]\!]$. Il existe q' tel que $u = mq' + u_k$.
On a donc $1 = uk + vm = (mq' + u_k)k + vm = u_k \times k + m(q'k + v)$. Donc (Bézout) $u_k \wedge m = 1$ ainsi $u_k \in A_m$,
et $1 \equiv u_k \times k[m]$, donc $u_k \overline{\times} k = 1$.
On a trouvé l'existence de u_k. Reste à démontrer l'unicité
Si u_k' vérifie les mêmes conditions : $(u_k - u_k')k \equiv u_k k - u_k' k \equiv 1 - 1 \equiv 0[m]$.
Donc $m|(u_k - u_k')k$. Or $m \wedge k = 1$, donc $m|(u_k - u_k')$.
Mais $u_k, u_k\prime \in A_m \subset [\![1, m-1]\!]$, donc $u_k - u_k' \in [\![1-m, m-1]\!] \cap m\mathbb{Z} = \{0\}$.

Pour $k \in [\![1,m]\!]$, on a : $k \in A_m$ si et seulement si $\exists!\, h_k \in A_m$ tel que $h_k \overline{\times} k = 1$.

On note $\psi : A_m \to A_m$, $k \mapsto h_k$.

(b) Montrer que $(A_m, \overline{\times})$ est un groupe commutatif.

— Soit $k_1, k_2 \in A_m$. Soit $k_3 = k_1 \overline{\times} k_2$. Par définition de la division euclidienne $k_3 \in [\![0, m-1]\!]$
Mais aussi $m \wedge k_1 = 1$, $m \wedge k_2 = 1$, donc $m \wedge k_1 k_2 = 1$ (corollaire du lemme de Gaus).
Donc $1 = (k_1 k_2) \wedge m = m \wedge (k_1 k_2 \% m) = m \wedge k_3$. Donc $k_3 \in A_m$.
$\overline{\times}$ est bien un loi de composition interne.

— Si $k_1, k_2 \in A_m$, alors $k_1 \times k_2 = k_2 \times k_1$, donc $k_1 \overline{\times} k_2 = k_2 \overline{\times} k_1$..
Ainsi la loi est bien commutative.
— $1 \wedge m = 1$, donc $1 \in A_m$ et pour tout $k \in A_m$, $1 \overline{\times} k = k \% m = k$ car $k \in [\![0, m-1]\!]$.
Et comme la loi est commutative : $k \overline{\times} 1 = k$.
Ainsi $\overline{\times}$ est bien unifère. Son élément neutre 1

— Enfin, d'après la question précédente, tout élément k de A_m admet un inverse ($\psi(k)$) dans A_m

$$\boxed{(A_m, \overline{\times}) \text{ est un groupe commutatif.}}$$

(c) Montrer que ψ est un morphisme de groupes.

Soient $k_1, k_2 \in A_m$.
$h_{k_1} h_{k_2} \times k_1 k_2 = h_{k_1} k_1 h_{k_2} k_2 \equiv 1 \times 1 \equiv 1[m]$.
Donc $h_{k_1} \overline{\times} h_{k_2}$ est l'inverse $k_1 k_2$ (on utilise la commutativité et la congruence modulo m).
Ainsi

$$\psi(k_1 \overline{\times} k_2) = h_{k_1} \overline{\times} h_{k_2} = \psi(k_1) \overline{\times} \psi(k_2)$$

$$\boxed{\psi \text{ est un morphisme de groupe } A_m \text{ dans } A_m.}$$

(d) Que vaut $\ker \psi$? ψ est-elle injective ?

Soit $k \in A_m$. $k \in \ker \psi \iff \psi(k) = 1$.
Or si $k \overline{\times} \psi(k) = 1$, on a par unicité de l'inverse (question 3) : $\psi(\psi(k)) = k$. Donc : $k \in \ker \psi \iff k = \psi(\psi(k)) = \psi(1) = 1$

$$\boxed{\ker \psi = \{1\} \text{ et } \psi \text{ est injective.}}$$

IV.3. Calcul de $\varphi(m)$.

(a) Décrire explicitement A_p et A_{p^a} si p est un nombre premier et $a \in \mathbb{N}$. En déduire la valeur de $\varphi(p)$ puis que $\varphi(p^a) = (p-1)p^{a-1}$, si p est un nombre premier et $a \in \mathbb{N}$.

$$\boxed{\text{On a } A_p = \{1, 2, \cdots, p-1\}, \text{ donc } \varphi(p) = p - 1.}$$

Soit $m \in [\![1, p^a]\!]$. $m \notin A_{p^a} \iff m \wedge p^a \neq 1$.
Supposons $m \notin A_{p^a}$. Le PGCD de m et de p^a divise de p^a. Et comme p est premier, alors $m \wedge p^a \in \{1, p, p^2, \dots p^a\}$.
Et comme par hypothèse, $m \wedge p^a \neq 1$, on a $p | (m \wedge p^a)$. Et par transitivité : $p | m$.
Réciproquement, si $p | m$, alors $m \notin A_{p^a}$.

$$\boxed{\text{Donc } A_{p^a} = [\![1, p^a]\!] \setminus \underbrace{\{p, 2p, 3p, \dots p^a\}}_{p^{a-1} \text{ éléments}} \text{ et } \varphi(p^m) = p^a - p^{a-1} = p^{a-1}(p-1).}$$

(b) Soient p, q deux nombres premiers distincts. Décrire, de même A_{pq}, en déduire $\varphi(pq) = (p-1)(q-1) = \varphi(p)\varphi(q)$.

Soit $m \in [\![1, pq]\!]$. $m \notin A_{pq} \iff m \wedge pq \neq 1$.
Supposons $m \notin A_{pq}$. Le PGCD de m et de pq, noté δ divise de pq.
Et comme p et q sont premiers, alors $m \wedge pq \in \{1, p, 2p, \dots qp, q, 2q, \cdots q(p-1)\}$.
Et comme par hypothèse, $\delta \neq 1$, soit p, soit q, soit les deux divise δ.
Et par transitivité, soit p, soit q, soit les deux divise δ divise m.
Réciproquement, si $p | m$, ou $q | m$, alors $m \wedge pq \neq 1$.

$$\boxed{\text{Donc } A_{pq} = [\![1, pq]\!] \setminus \underbrace{\{p, 2p, 3p, \dots qp, q, 2q, \dots (p-1)q\}}_{q+p-1 \text{ éléments}} \text{ et } \varphi(pq) = pq - p - q + 1 = (p-1)(q-1) = \varphi(p) \times \varphi(q).}$$

(c) On fixe $n \in \mathbb{N}$ et p un nombre premier avec n. Soit $a \in \mathbb{N}^*$.

i. Montrer que $\{k \in [\![1, p^a n]\!] \text{ tq. } k \wedge n = 1\} = \{m + qn; m \in A_n, q \in [\![0, p^a - 1]\!]\}$.

Soit $m \in A_n$. Clairement, $m + qn \equiv m[n]$, alors $m + qn \wedge n = m \wedge n = 1$.
Ainsi si $q \in [\![0, p^a - 1]\!]$, comme $m \in [\![1, n]\!]$, $m + qn \in [\![1, (p^a - 1)n + n]\!] = [\![1, p^a n]\!]$.
Donc $\{m + qn; m \in A_n, q \in [\![0, p^a - 1]\!]\} \subset \{k \in [\![1, p^a n]\!] \text{ tq. } k \wedge n = 1\}$.

Réciproquement, si $k \in [\![1, p^a n]\!]$ tq. $k \wedge n = 1\}$, alors $k = (k\%n) + qn$ (division euclidienne),
et nécessairement $(k\%n) \wedge n = k \wedge n = 1$ et $qn \leqslant p^a n - 1$, donc $q < p^a$.
Comme q est entier positif, $q \leqslant p^a - 1$.
$\{k \in [\![1, p^a n]\!]$ tq. $k \wedge n = 1\} \subset \{m + qn; m \in A_n, q \in [\![0, p^a - 1]\!]\}$

$$\boxed{\{k \in [\![1, p^a n]\!] \text{ tq. } k \wedge n = 1\} = \{m + qn; m \in A_n, q \in [\![0, p^a - 1]\!]\}}$$

---

ii. Soit $m \in A_n$. Montrer qu'il existe $(q_0, r_0) \in \mathbb{Z}^2$ tel que $m + q_0 n = r_0 p$.
Montrer ensuite l'équivalence : $m + qn = rp \iff \exists\, k \in \mathbb{Z}$ tel que $q = q_0 + kp$ et $r = r_0 + kn$.

Puisque $n \wedge p = 1$, alors $n\mathbb{Z} + p\mathbb{Z} = (n \wedge p)\mathbb{Z} = 1\mathbb{Z} = \mathbb{Z}$.
Donc tout élément de $\mathbb{Z}$ est une combinaison linéaire entière de n et de p.
En particulier $m \in \mathbb{Z}$, il existe donc $(\alpha, \beta) \in \mathbb{Z}^2$ tel que $m = \alpha n + \beta p$.

$$\boxed{\text{En prenant } r_0 = \beta \text{ et } q_0 = -\alpha : m + q_0 n = r_0 p.}$$

Mais ce couple n'est pas unique. Soit $(q, r) \in \mathbb{Z}^2$ tel que $m + qn = rp$.
alors $m = rp - qn = r_0 p - q_0 n$, donc $(r_0 - r)p = (q_0 - q)n$.
Par conséquent, $n|(r - r_0)p$. Mais $n \wedge p = 1$, donc d'après le lemme de Gauss : $n|r - r_0$.
il existe donc $k \in \mathbb{Z}$ tel que $r - r_0 = nk$, i.e. $r = r_0 + nk$.
On a alors : $(r_0 - r)p = -nkp = (q_0 - q)n$, donc $q - q_0 = kp$.
La réciproque étant simple à démontrer (un simple calcul) :

$$\boxed{m + qn = rp \iff \exists\, k \in \mathbb{Z} \text{ tel que } q = q_0 + kp \text{ et } r = r_0 + kn.}$$

---

iii. En déduire que dans l'ensemble $\{m + qn; m \in A_n, q \in [\![0, p^a - 1]\!]\}$, exactement $(p-1)p^{a-1}$ termes sont premiers avec p.

$m + qn$ n'est pas premier avec p, qui est un nombre premier, si et seulement si p divise ce nombre.
Ce qui signifie exactement que $m + qn = rp$.
Or d'après la question précédente, si tel est le cas de $m + q_0 n$, il en sera de même uniquement pour les nombres $m + (q_0 + p)n$, $m + (q_0 + 2p)n \ldots$.
Donc, si q varie dans $[\![0, p^a - 1]\!]$, alors exactement, chaque p fois, le nombre $m + qn$ n'est pas premier avec p.
Il y a donc $\dfrac{p^a - 1 + 1}{p} = p^{a-1}$ termes qui ne sont pas premiers avec p,

$$\boxed{\text{les } (p^a - 1 + 1) - p^{a-1} = p^{a-1}(p-1) \text{ autres termes de } \{m + qn; m \in A_n, q \in [\![0, p^a - 1]\!]\} \text{ sont premiers avec } p.}$$

---

iv. Conclure que $\varphi(p^a n) = \varphi(p^a) \times \varphi(n)$.

Il s'agit de calculer le cardinal de A_{np^a}.
Comme $n \wedge p$ sont premiers entre eux, si k n'est pas premiers avec np^α,
c'est qu'il n'est pas premiers avec n ou qu'il n'est pas premier avec p^a ;
c'est donc qu'il n'est pas premiers avec n ou qu'il n'est pas premier avec p.
Or d'après les questions précédentes, on a :

$$A_{np^a} = \{k \in [\![1, p^a n]\!] \text{ tq. } k \wedge n = 1 \& k \wedge p = 1\} = \{m + qn; m \in A_n, q \in [\![0, p^a - 1]\!] \& (m + qn) \wedge p = 1\}$$

Pour ce dernier ensemble, il faut choisir :
— m dans A_n : $\varphi(n)$ possibilités
— PUIS (pour chaque m ainsi choisi), choisir q dans $[\![0, p^a - 1]\!]$ tel que $(m + qn) \wedge p = 1$: $p^{a-1}(p-1)$ possibilités
Le principe de dénombrement par décomposition (ou principe multiplicatif ou principe des bergers), permet d'affirmer

$$\boxed{\varphi(np^a) = \text{card}(A_{np^a}) = \varphi(n) \times p^{a-1}(p-1) = \varphi(n)\varphi(p^a)}$$

(d) En déduire que pour tout $m \in \mathbb{N}^*$: $\varphi(m) = \displaystyle\prod_{p \in \mathcal{P},\, p|m} (p-1)p^{v_p(m)-1}$

Montrons, pour tout $s \in \mathbb{N}^*$, $\mathcal{P}_s$:
« si $m = \displaystyle\prod_{i=1}^{s} p_i^{\alpha_i}$, avec $p_i \in \mathcal{P}$, alors $\varphi(m) = \prod_{i=1}^{s}(p_i - 1)p_i^{\alpha_i - 1}$ ».
— D'après la question 3.(a), $\mathcal{P}_1$ est vraie.
— Soit $s \in \mathbb{N}^*$. Supposons que $\mathcal{P}_s$ est vraie.
Soit $m \in \mathbb{N}$ tel que $\displaystyle\prod_{i=1}^{s+1} p_i^{\alpha_i}$ avec pour tout $i \in \mathbb{N}_{s+1}$, $p_i \in \mathcal{P}$ (et $p_i \neq p_j$).

Alors d'après la question précédente, en notant $n = \prod_{i=1}^{s} p_i^{\alpha_i}$,

$\varphi(m) = \varphi(np_{s+1}^{\alpha_{s+1}}) = \varphi(n)\varphi(p_{s+1}^{\alpha_{s+1}}) = (p_{s+1}-1)p_{s+1}^{\alpha_{s+1}-1}\varphi(n)$.

Or d'après $\mathcal{P}_n$, $\varphi(n) = \prod_{i=1}^{s}(p_i-1)p_i^{\alpha_i-1}$. On a donc $\varphi(m) = \prod_{i=1}^{s+1}(p_i-1)p_i^{\alpha_i-1}$ et donc $\mathcal{P}_{s+1}$ est vraie.

On a donc $\mathcal{P}_s$ qui est vraie pour tout $s \in \mathbb{N}$.

Donc pour tout $m \in \mathbb{N}$ et $m \geqslant 2$, $\varphi(m) = \prod_{p\in\mathcal{P}, p|m} (p-1)p^{v_p(m)-1}$.

Enfin, si $m = 1$, alors $\varphi(1) = 1$ et $\prod_{p\in\mathcal{P}, p|m} (p-1)p^{v_p(m)-1} = 1$, comme produit vide.

$$\boxed{\forall\, m \in \mathbb{N}^*, \quad \varphi(m) = \prod_{p\in\mathcal{P},\, p|m} (p-1)p^{v_p(m)-1}}$$

V (*) Congruence composée

V.1. Montrer que pour $m = 9$, $L'_9 \overset{\cdots}{=} X^6 - 3X^4 + 3X^2 - 1\ [9]$

Pour $m = 9 = 3^2$, on a $\varphi(m) = (3-1)\times 3^1 = 6$ et $A_9 = \{1,2,4,5,7,8\}$.
Pour tout $x \in \mathbb{Z}$,

$$L'(x) \equiv (x-1)(x-8)(x-2)(x-7)(x-4)(x-5) \equiv (x-1)(x+1)(x-2)(x+2)(x-4)(x+4) \equiv (x^2-1)(x^2-4)(x^2+2)\ [9]$$

$$L'(x) \equiv (x^2-1)(x^4-2x^2+1) \equiv x^6 - 3x^4 + 3x^2 - 1\ [9]$$

$$\boxed{L' \equiv X^6 - 3X^4 + 3X^2 - 1\ [9]}$$

Cela est différent de $X^6 - 1$, comme on aurait pu s'y attendre...

V.2. Montrer que si $m = p^a$ (avec $p > 2$), alors $L'_{p^a} \overset{\cdots}{=} (x^{p-1}-1)^{p^{a-1}}\ [p^a]$.

Nous démontrons ce résultat par récurrence sur a. $A_{p^a} = \{t + kp^{a-1}, t \in A_{p^{a-1}}, k \in [\![0, p-1]\!]\}$.

Donc, pour tout $x \in \mathbb{Z}$: $L'_{p^a}(x) = \prod_{k=0}^{p-1} L'_{p^{a-1}}(x + kp^{a-1})$ Or, en utilisant le binôme de Newton

$$(x+kp^{a-1})^s = x^s + skp^{a-1}x^{s-1} + \underbrace{\frac{s(s-1)}{2}k^2p^{2a-2}x^2 + \cdots + k^sp^{s(a-1)}}_{\text{factorisable par } p^a} = x^s + skp^{a-1}x^{s-1} + p^aK \equiv x^s + skp^{a-1}x^{s-1}[p^a]$$

Et en exploitant la linéarité :

$$L'_{p^{a-1}}(x + kp^{a-1}) \equiv L'_{p^{a-1}}(x^s) + kp^{a-1}\partial L'_{p^{a-1}}(x)\ [p^a]$$

Et par multiplication :

$$L'_{p^a}(x) \equiv (L'_{p^{a-1}}(x))^p - \sum_{k=0}^{p-1} kp^{a-1}(L'_{p^{a-1}}(x))^{p-1}\partial L'_{p^{a-1}}(x)\ [p^a]$$

On peut factoriser la dernière somme, on trouve $\sum_{k=0}^{p-1} k = \frac{p(p-1)}{2}$, donc $\sum_{k=0}^{p-1} kp^{a-1}$ est divisible par p^a.

Finalement :

$$L'_{p^a}(x) \equiv (L'_{p^{a-1}}(x))^p\ [p^a]$$

Et enfin par récurrence (puisque $L'_{p^1}(x) = x^{p-1} - 1$) :

$$\boxed{L'_{p^a} \overset{\cdots}{=} (x^{p-1}-1)^{p^{a-1}}\ [p^a]}$$

V.3. Montrer que si $m = 2^a$, alors $L'_{2^a} \overset{\cdots}{=} (x^2-1)^{2^{a-2}}\ [2^a]$.

Dans le cas où $a = 1$, on a $L'_2(x) = (x-1) = (x^2-1)^{\frac{1}{2}}\ [4]$,
car $(x-1)^2 = x^2 - 2x + 1 \equiv x^2 - 1\ [2]$.

Dans le cas où $a = 2$, on a $L'_{2^2} = (x-1)(x-3) = x^2 - 4x + 3 \equiv x^2 - 1 = (x^2-1)^{2^{2-2}}\ [4]$ Donc la formule est vraie pour $a = 2$.

On va démontrer le résultat par récurrence sur a. Supposons que $L'_{2^{a-1}}(x) \equiv (x^2-1)^{2^{a-3}}\ [2^{a-1}]$

Alors $\partial L'_{2^{a-1}}(x) = 2^{a-3} \times 2 \times x(x^2-1)^{2^{a-3}-1} \equiv 0[2]$ Comme à la question précédente, notons que $A_{2^a} = \left\{t + k2^{a-1}, t \in A_{2^{a-1}}, k \in \{0,1\}\right\}$. Donc

$$\begin{aligned} L'_{2^a}(x) &= L'_{2^{a-1}}(x) \times L'_{2^{a-1}}(x - 2^{a-1}) = L'_{2^{a-1}}(x) \times \left(L'_{2^{a-1}}(x) - 2^{a-1}\partial L'_{2^{a-1}}(x)\right) \\ &= [L'_{2^{a-1}}(x)]^2 - 2^{a-1}L'_{2^{a-1}}(x)\partial L'_{2^{a-1}}(x) \equiv [L'_{2^{a-1}}(x)]^2 \equiv (x^2-1)^{2^{a-3}\times 2} \quad [2^a] \end{aligned}$$

Le résultat est donc vraie en a également.

$$\boxed{\text{Si } m = 2^a, \text{ alors } {L'_{2^a}}' \overset{\cdots}{=} (x^2-1)^{2^{a-2}} \, [2^a].}$$

V.4. Montrer que si $p|m$ et $p > 2$: $L'_m \overset{\cdots}{=} (x^{p-1}-1)^{\varphi(m)/(p-1)} \, [p^{v_p(m)}]$
et si $2|m$, : $L'_m \overset{\cdots}{=} (x^2-1)^{\varphi(m)/2} \, [2^{v_2(m)}]$

Dans le premier cas, on va écrire $m = p^\alpha n$ avec $\alpha = v_p(m)$, donc $p \wedge m = 1$.
Comme en question IV. 3 (c),

$$A_m = A_{np^\alpha} = \{sn + vp^a \% [m]; v \in A_n, s \in A_{p^a}\}$$

Donc par indépendance :

$$L'_m(x) \equiv \prod_{v \in A_n} \prod_{s \in A_{p^a}} (x - sn - vp^a) \, [m]$$

Concentrons nous sur le produit intérieur. Pour $v \in A_n$ fixé :

$$\prod_{s \in A_{p^a}} (x - sn - vp^a) \equiv \prod_{s \in A_{p^a}} (x - sn) \equiv \prod_{s' \in A_{p^a}} (x - s')[p^a]$$

Cette dernière congruence est du au fait que $s \mapsto sn$ est bijective dans A_{p^a} car $p \wedge n = 1$.
Donc

$$\begin{aligned} L'_m(x) &\equiv \prod_{v \in A_n} \prod_{s' \in A_{p^a}} (x - s') \prod_{v \in A_n} L_{p^a}(x) \, [p^a] \\ &\equiv \left(L_{p^a}(x)\right)^{\text{card}(A_n)} \equiv \left(L'_{p^a}(x)\right)^{\varphi(n)} \, [p^a] \end{aligned}$$

Et donc en appliquant le résultat de V.2. :

$$\boxed{L'_m(x) \equiv \left((x^{p-1}-1)^{p^{a-1}}\right)^{\varphi(n)} \, [p^a] = L'_m \overset{\cdots}{=} (x^{p-1}-1)^{\varphi(m)/(p-1)} \, [p^{v_p(m)}]}$$

puisque $\varphi(m) = \varphi(np^a) = \varphi(n)p^{a-1}(1-p)$.
Pour le cas $p = 2$. La démonstration est la même.
