



## Corrigé RMS 2024

Alex6oko L. Mai 2025

---

### Note sur les intitulés des exercices :

Les lettres qui précèdent les énoncés indiquent la provenance de l'exercice :

- **X** : École polytechnique
- **U** : ENS Ulm
- **L** : ENS Lyon
- **S** : ENS Paris-Saclay
- **R** : ENS Rennes

*Corrigé personnel qui retrace l'évolution de la pensée du narrateur au cours de sa résolution, le narrateur le juge "solide" (sans laisser de définition de solidité). S'il te semble friable à certains endroits [ou partout ? Impossible frère...], fais-le moi savoir, mais sache que... : alexislcrd@gmail.com. Le narrateur a délibérément enlevé les étoiles de difficulté. Clique ici pour avoir tout les énoncés RMS*

### Exercice – ULSR

On étend de façon naturelle la valuation 2-adique  $v_2$  à  $\mathbb{Q}$ . Pour un entier  $N$ , soit :

$$H_N = \sum_{k=1}^N \frac{1}{k}$$

Calculer  $v_2(H_N)$ .

### Proposition de corrigé :

Premièrement, pour tout  $N \in \mathbb{N}^*$ , on a :

$$H_N = \sum_{k=1}^{N-1} \frac{1}{k} + \frac{1}{N} = H_{N-1} + \frac{1}{N}$$

Notons  $H_{N-1} = \frac{p}{q}$  écrit en fraction irréductible, ainsi on peut réécrire  $H_{N-1}$  sous la forme  $\frac{a}{2^b d}$ , avec :

$$\gcd(a, 2) = 1, \quad \gcd(2, d) = 1, \quad b = -v_2(H_{N-1}) \in \mathbb{Z} \text{ à priori.}$$

Toutefois si l'on avait  $b$  entier naturel, alors  $H_N = \frac{aN + 2^b d}{2^b d N}$ . Ainsi en supposant ensuite  $N$  impair, on aurait  $2 \nmid aN + 2^b d$ , car

$\gcd(a, 2) = 1$ , ainsi dans ce cas  $v_2(H_N) = v_2(H_{N-1})$ , car  $\gcd(2, d) = 1$ . En calculant pour quelques valeurs  $v_2(H_N)$ , on "sent" que  $b$  est un entier naturel.

Montrons alors par récurrence sur l'entier  $N$  que  $v_2(H_N) \leq 0$  (**Lemme 1**).

Initialisation en  $N=1$  : jugée triviale

Hérédité : Soit  $N \geq 2$ , supposons le résultat vrai au rang  $N-1$ , montrons le au rang  $N$ .

En gardant l'écriture qu'on avait précédemment,  $H_N = \frac{aN+2^bd}{2^bdN}$  (avec N impair ou pair ici parcontre). Par "extension" de  $v_2$  de  $\mathbb{Z}$  à  $\mathbb{Q}$ ,  $v_2(H_N) = v_2(\frac{aN+2^bd}{2^bdN}) = v_2(aN+2^bd) - v_2(2^bdN)$ , si N est impair alors le résultat est trivial. Si N est pair, le calcul donne  $v_2(H_N) = v_2(aN+2^bd) - v_2(2^bdN) = \min(v_2(N), b) - (v_2(N) + b)$ .

Si  $\min(v_2(N), b) = b$  alors  $v_2(H_N) = -v_2(N) \leq 0$ , car  $N \in \mathbb{N}$ .

Sinon si  $\min(v_2(N), b) = v_2(N)$  alors  $v_2(H_N) = -b \leq 0$ , par hypothèse de récurrence.

Conclusion : Ok !

Donc on a établi par le **Lemme 1** que si N est impair,  $v_2(H_N) = v_2(H_{N-1})$ . On sait alors que  $(v_2(H_N))$  est une suite par paliers (de taille au moins 2 quand n est plus grand que 2). En calculant les valuations 2-adiques pour plusieurs valeurs, on conjecture le résultat suivant :

$$v_2(H_n) = -k \quad \text{pour } n = \sum_{i=0}^{k-1} 2^i + 1 = 2^{k-1} + 1 \text{ à } \sum_{i=0}^k 2^i = 2^k \text{ occurrences consécutives.}$$

C'est-à-dire  $v_2(H_n) = -\lfloor \log_2(n) \rfloor$ , pour tout entier naturel n.

Montrons le résultat par récurrence (on ne fait que l'hérédité mes frères). Soit n un entier naturel non nul, On a  $H_{n+1} = H_n + \frac{1}{n+1}$  donc  $v_2(H_{n+1}) = \min(v_2(H_n), v_2(\frac{1}{n+1})) = \min(-\lfloor \log_2(n) \rfloor, v_2(\frac{1}{n+1}))$  (par hypothèse de récurrence).

Or  $v_2(\frac{1}{n+1}) = -v_2(n+1) \geq -\lfloor \log_2(n+1) \rfloor$ .

Et si n+1 n'est pas une puissance de 2, alors  $\lfloor \log_2(n+1) \rfloor = \lfloor \log_2(n) \rfloor$ .

Sinon si  $n+1 = 2^k$ , alors  $v_2(n+1) = k = \log_2(n+1)$ , donc :  $v_2(\frac{1}{n+1}) = -k = -\lfloor \log_2(n+1) \rfloor \leq -\lfloor \log_2(n) \rfloor$

Donc dans tout les cas,  $v_2(\frac{1}{n+1}) \leq -\lfloor \log_2(n) \rfloor$ . Donc  $v_2(H_{n+1}) = -\lfloor \log_2(n+1) \rfloor$

CQFD

## Exercice – ULSR

Soit  $(m, n, p) \in \mathbb{N}^3$ , avec  $p$  un nombre premier supérieur ou égal à 5, et  $m$  premier avec  $p$ .

a) Montrer que :

$$\binom{np}{m} \equiv 0 \pmod{p}$$

b) Montrer que :

$$\binom{np}{mp} = \sum_{k=0}^p \binom{p(n-1)}{mp-k} \binom{p}{k}$$

c) Montrer que :

$$\binom{np}{mp} \equiv \binom{n}{m} \pmod{p^2}$$

L'objectif de la suite est de montrer que :

$$\binom{2p}{p} \equiv 2 \pmod{p^3}$$

d) Montrer que :

$$\forall k \in \llbracket 1, p \rrbracket, \quad \binom{p-1}{k-1} \equiv \pm 1 \pmod{p}.$$

e) Montrer que :

$$\sum_{k=1}^{p-1} \left( \frac{(p-1)!}{k} \right)^2 \equiv 0 \pmod{p}$$

f) Conclure.

### Proposition de corrigé :

a) Premièrement, on élague tout les cas pathologiques (qui sont triviaux car  $p|0$ ) en prenant  $m$  dans  $\llbracket 1, np \rrbracket$ . Ensuite, un exo classique, que l'on nommera **Lemme uno**, consiste à montrer que si  $\gcd(m, p) = 1$ , alors  $p \mid \binom{p}{m}$ . Le narrateur le laisse en guise d'exercice, il suffit d'appliquer la Formule du pion + le lemme de Gauss. Avec le **Lemme uno**, on a gratuitement (si vous savez le montrer) le cas  $n=1$ .

Pour  $n \geq 2$ . Il suffit d'observer que  $\binom{p}{m} \mid \binom{np}{m}$  (développer les coefficients binomiaux pour s'en convaincre). Donc  $p$  divise  $\binom{np}{m}$ .

b) Par un raisonnement combinatoire :

On veut prendre  $mp$  éléments d'un ensemble  $E$  à  $np$  éléments, soit. Considérons  $F$  un sous-ensemble de  $E$  à  $p$  éléments. Prendre  $mp$  éléments de  $E$ , revient à prendre  $k$  éléments de  $F$  (pour  $k \in \llbracket 0, p \rrbracket$ ), puis à compléter indépendamment avec  $mp-k$  éléments dans  $E \setminus F$  de cardinal  $pn-p$ .

D'où :

$$\binom{np}{mp} = \sum_{k=0}^p \binom{p(n-1)}{mp-k} \binom{p}{k} \quad (\text{"Analogue" à l'identité de Vandermonde})$$

c) 6oko a trimé... En utilisant b), puisque on montre aisément (lecteur [...])

que  $p$  divise  $\binom{p}{k}$  et  $p$  divise  $\binom{p(n-1)}{mp-k}$ , pour  $k \in \llbracket 1, p-1 \rrbracket$ . Alors  $\binom{np}{mp} \equiv \binom{p(n-1)}{p(m-1)} + \binom{p(n-1)}{mp} \pmod{p^2}$ .

Maintenant, si l'on suppose par récurrence (l'initialisation uniquement pour le lecteur) que la formule qu'on veut montrer est vraie au rang  $n-1$  et  $m$  premier avec  $p$ , on a :

$$\binom{p(n-1)}{p(m-1)} \equiv \binom{n-1}{m-1} \pmod{p^2} \text{ et } \binom{p(n-1)}{mp} \equiv \binom{n-1}{m} \pmod{p^2}.$$

Donc  $\binom{np}{mp} \equiv \binom{n-1}{m-1} + \binom{n-1}{m} \pmod{p^2}$ , i.e (Formule de Pascal)  $\binom{np}{mp} \equiv \binom{n}{m} \pmod{p^2}$ .

d) Montrons le résultat par récurrence.

Initialisation : Triviale.

Hérédité : Supposons le résultat vrai jusqu'au rang  $k \in \llbracket 2, p-1 \rrbracket$ .

Alors d'après la formule de Pascal  $\binom{p-1}{k-1} + \binom{p-1}{k} = \binom{p}{k} \equiv 0 \pmod{p}$ , d'après le **Lemme uno**.

Donc  $\binom{p-1}{k} \equiv -\binom{p-1}{k-1} \equiv \pm 1 \pmod{p}$  (par hypothèse de récurrence).

Conclusion : Ok !

e) Le " $(p-1)! \pmod{p}$ " fait évidemment penser au **Théorème de Wilson** :

$\forall p \in \mathbb{P}, (p-1)! \equiv -1 \pmod{p}$ . (Le narrateur a le coeur sur la main et va vous donner une preuve de ce classique). Rapidement, on se place dans  $\mathbb{Z}/p\mathbb{Z}$ ,  $(p-1)!$  est le produit de tout les éléments (non nuls) de  $\mathbb{Z}/p\mathbb{Z}$ . Or  $\mathbb{Z}/p\mathbb{Z}$  est un corps ( $p$  est premier), donc tout ses éléments non nuls sont inversibles. Donc vu que  $\mathbb{Z}/p\mathbb{Z}$  est commutatif, les éléments se simplifie avec leur inverses dans le produit, si  $p-1$  avait son inverse  $k$  représenté dans  $\llbracket 2, p-2 \rrbracket$ , alors  $(p-1)k=1$  alors  $1=k$ , ce qui est absurde ! Donc  $p-1$  est son propre inverse ainsi que 1 et aucun autre (sinon si  $k^2 = 1$  alors  $(k-1)(k+1) = 0$  alors  $k-1=0$  ou  $k+1=0$  i.e  $k=1$  ou  $k=p-1$ ). Il restera alors  $1.(p-1) = -1 \pmod{p}$ .

Ainsi, on réécrit la somme  $\sum_{k=1}^{p-1} \left( \frac{(p-1)!}{k} \right)^2 \equiv \sum_{k=1}^{p-1} (k^{-1})^2 \pmod{p}$ . Sauf que  $\mathbb{Z}/p\mathbb{Z}$  est un corps, sommer sur les inverses au lieu des éléments en soi ne change rien. Cette somme vaut alors (modulo  $p$ )  $\sum_{k=1}^{p-1} k^2 = \frac{p(p-1)(2p-1)}{6}$ . Or  $6 \mid (p-1)(2p-1)$  (6oko invite le lecteur a montrer cela, c'est vite fait technique (penser à  $6=2 \times 3$ )). On a alors montré que  $\sum_{k=1}^{p-1} \left( \frac{(p-1)!}{k} \right)^2$  était divisible par  $p$ . CQFD

f) On a d'après b),

$$\binom{2p}{p} = \sum_{k=0}^p \binom{p}{k}^2 = \sum_{k=1}^{p-1} \binom{p}{k}^2 + 2 = 2 + \sum_{k=1}^{p-1} \frac{p^2}{k^2} \binom{p-1}{k-1}^2 \text{ (Form. du pion)}$$

Or d'après d),  $\forall k \in \llbracket 1, p \rrbracket, \binom{p-1}{k-1} \equiv \pm 1 \pmod{p}$ . Alors ce coefficient binomial  $\pm 1$  est un multiple de  $p$ . Il restera alors modulo  $p^3$  :  $2 \pm p^2 \sum_{k=1}^{p-1} \frac{1}{k^2} = 2 \pm \frac{p^2}{((p-1)!)^2} \sum_{k=1}^{p-1} \frac{((p-1)!)^2}{k^2}$ . Or d'après e),  $\sum_{k=1}^{p-1} \frac{((p-1)!)^2}{k^2}$  est un multiple de  $p$ . Ainsi il ne restera que le 2 modulo  $p^3$ .

### Exercice – L

On considère l'équation :

$$2^a + 3^b = 5^c \quad \text{où } (a, b, c) \in \mathbb{N}^3.$$

- (a) Résoudre l'équation dans le cas où  $a = b = c$ .
- (b) Traiter le cas où  $b$  est impair.
- (c) Traiter le cas où  $c$  est impair.
- (d) Traiter le cas général.

### Proposition de corrigé :

a) 6oko a d'abord essayé de mettre des coups de valuation p-adique, mais ça n'aboutit jamais ici. Car, par exemple on aura :  $v_5(2^a + 3^a) = a$ , on a ensuite envie de dire, comme dans l'exercice 1, que  $v_5(2^a + 3^a) = \min(v_5(2^a), v_5(3^a)) = 0 = a$  ; or la formule du min n'a plus de sens, si les éléments ne sont pas divisibles par 5 (car ça découle d'une factorisation).

Mais, par chance, il a pensé à un **exo classique tout droit sorti du Alain Pommelet** :

Etant donné  $n$  entier, trouver tous les couples  $(x, y) \in \mathbb{R}^{+*}$ , tels que  $(x + y)^n = x^n + y^n$

Pour le résoudre, on divise tout par  $y^n$ , et on pose  $t = \frac{x}{y}$ , on a alors  $(1 + t)^n = 1 + t^n$ . Or en binômiant de Newton, comme  $t > 0$ , on a  $(1 + t)^n > 1 + t^n$  sauf si  $n=1$  (le vrai exo : c'est pas puissance  $n$ , mais puissance  $r$  réel positif, et on dérive une fonction auxiliaire pour résoudre). Donc on a aucune solution, sauf si  $n=1$ .

Donc  $a=1$  obligatoirement si on a une solution, or ça marche, donc  $a=1$  est la seule solution.

b) En supposant  $b$  impair ( $b > 1$ ), on a  $3^b \equiv 1 \pmod{4}$ . Or  $2^a \equiv 0 \pmod{4}$  et  $5^c \equiv 1 \pmod{4}$ . Donc on a aucune solution si  $b$  est impair.

c) A tâtons, modulo 8 on a une contradiction, en calculant toutes les combinaisons possibles.

d) Si on a une solution, alors  $c$  et  $b$  sont pairs (d'après b) et c)). De plus en raisonnant modulo 3, on a nécessairement  $c$  et  $a$  qui ont même parité. Donc  $a, b$  et  $c$  sont pairs. L'équation se réécrit ainsi :  $2^{2l} + 3^{2m} = 5^{2n}$ , où  $(l, m, n) \in \mathbb{N}$ . En faisant passer  $2^{2l}$  de l'autre côté, on a  $25 - 4 = 21$  qui divise  $3^{2m}$ , ce qui est impossible. Donc la seule solution c'est quand  $a=b=c=1$  (d'après a)).

### Exercice – ULSR

- (a) Montrer que les sous-groupes de  $\mathbb{Z}/n\mathbb{Z}$  sont cycliques.
- (b) Alice et Barbara jouent à un jeu. Elles choisissent à tour de rôle un élément de  $\mathbb{Z}/n\mathbb{Z}$  sans remise qu'elles ajoutent à un ensemble  $S$ . Le jeu s'arrête quand  $S$  engendre  $\mathbb{Z}/n\mathbb{Z}$  et la joueuse ayant tiré le dernier numéro perd. Selon  $n$ , y a-t-il une stratégie gagnante pour la première joueuse ?
- (c) Même question avec le groupe  $S_n$ .

**Proposition de corrigé :**

a) Il est classique de savoir montrer que tout les sous groupes d'un groupe cyclique sont cycliques. C'est exactement ce qu'on nous demande, car tout groupe cyclique est isomorphe à  $\mathbb{Z}/n\mathbb{Z}$ .

Une preuve ? Allez !

Soit  $H$  un sous-groupe de  $G = \mathbb{Z}/n\mathbb{Z}$ ,  $H$  est fini car  $G$  est fini.

Montrons maintenant que  $H$  est monogène (partie délicate) :

Puisque  $G$  est monogène,  $G$  s'écrit en extension  $\{1, p, p^2, \dots, p^{n-1}\}$ , avec  $p$  premier avec  $n$ . Si  $p \in H$  alors  $H = G$  et  $H$  est monogène, sinon il existe un plus petit élément  $j \in \llbracket 2, n-1 \rrbracket$  tel que  $p^j \in H$ . Montrons que  $H = \langle p^j \rangle$ .

L'inclusion réciproque est évidente. L'inclusion directe moins. Soit  $h \in H$ ,  $h = p^a$ , où  $a \in \llbracket 2, n-1 \rrbracket$  (à priori). Par division euclidienne, il existe  $v \in \mathbb{N}$  et  $r \in \llbracket 0, j-1 \rrbracket$ , tels que  $a = jv + r$ . Alors  $h = p^{jv+r} = p^r (p^j)^v$  (car  $H$  est commutatif car  $G$  l'est). En multipliant à droite par l'inverse de  $(p^j)^v$ , on a  $p^r \in H$  donc  $r=0$  (car  $j$  est le plus petit exposant, n'oublions pas). Donc  $h \in \langle p^j \rangle$

b) Deux mains.