

La néguentropie de cyclicité

Quand « être cyclique » ne coûte rien : un pont vers l'arithmétique

Hugues Genzrin — Programme du grain

September 9, 2026

Résumé

Prolongeant la quantification informationnelle des axiomes, on mesure le coût de la contrainte « être cyclique » parmi les groupes d'ordre n : $\mathcal{N}_{\text{cyc}}(n) = \log_2 \text{gnu}(n)$, où $\text{gnu}(n)$ est le nombre de groupes d'ordre n à isomorphisme près. Résultat central : $\mathcal{N}_{\text{cyc}}(n) = 0$ si et seulement si $\gcd(n, \varphi(n)) = 1$ — les « nombres cycliques ». Cette condition inclut tous les nombres premiers (par Lagrange) mais aussi certains composés (15, 33, 35, ...). La néguentropie de cyclicité est donc un détecteur non pas de primalité, mais d'unicité de structure de groupe — un pont exact entre la quantification des axiomes et l'indicatrice d'Euler. On signale au passage l'erreur de comptage (« $n!$ tables ») que ce résultat corrige.

1 Le comptage

Proposition 1 (Tables étiquetées de $\mathbb{Z}/n\mathbb{Z}$). *Le nombre de tables de groupe cyclique d'ordre n , sur un ensemble d'éléments étiquetés, est*

$$\frac{n!}{|\text{Aut}(\mathbb{Z}/n\mathbb{Z})|} = \frac{n!}{\varphi(n)},$$

où φ est l'indicatrice d'Euler.

Proof. $\mathbb{Z}/n\mathbb{Z}$ possède $\varphi(n)$ générateurs (les éléments d'ordre n). Choisir l'un ou l'autre comme générateur privilégié produit la même table à réétiquetage près : le groupe $\text{Aut}(\mathbb{Z}/n\mathbb{Z})$, de cardinal $\varphi(n)$, agit librement sur les étiquetages en préservant la structure. On divise donc $n!$ par $\varphi(n)$. $\square$

Remarque 2 (L'oscillation du coût). Le coût de spécifier une table de $\mathbb{Z}/n\mathbb{Z}$ est $\log_2(n!/\varphi(n))$. Il croît globalement comme $\log_2 n! \approx n \log_2 n$, mais la correction $-\log_2 \varphi(n)$ le fait osciller avec l'arithmétique de n : les sauts sont grands quand $\varphi(n)$ est petit (n très composé) et petits quand $\varphi(n)$ est grand (n premier). Le coût zigzague selon la structure des diviseurs.

2 La néguentropie de cyclicité

Définition 3 (Néguentropie de cyclicité). Soit $\text{gnu}(n)$ le nombre de groupes d'ordre n à isomorphisme près (group number, OEIS A000001). Comme le groupe cyclique $\mathbb{Z}/n\mathbb{Z}$ est unique pour chaque n , la contrainte « être cyclique » parmi les groupes d'ordre n a pour coût

$$\mathcal{N}_{\text{cyc}}(n) = \log_2 \frac{\text{gnu}(n)}{1} = \log_2 \text{gnu}(n) \geq 0.$$

Remarque 4. $\mathcal{N}_{\text{cyc}}(n)$ mesure combien d'information il faut ajouter pour sélectionner la structure cyclique parmi toutes les structures de groupe d'ordre n . Elle est nulle exactement quand il n'y a rien à sélectionner — quand le groupe cyclique est le seul groupe d'ordre n .

3 Le résultat : nullité $\Leftrightarrow$ nombre cyclique

Théorème 5 (Annulation de la néguentropie de cyclicité). *Pour tout $n \geq 1$,*

$$\mathcal{N}_{cyc}(n) = 0 \iff \text{gnu}(n) = 1 \iff \gcd(n, \varphi(n)) = 1.$$

Les entiers vérifiant $\gcd(n, \varphi(n)) = 1$ sont les nombres cycliques (OEIS A003277).

Proof. $\mathcal{N}_{cyc}(n) = 0 \iff \log_2 \text{gnu}(n) = 0 \iff \text{gnu}(n) = 1$: le groupe cyclique est le seul groupe d'ordre n . L'équivalence $\text{gnu}(n) = 1 \iff \gcd(n, \varphi(n)) = 1$ est un théorème classique (T. Szele) : un ordre n n'admet qu'un seul groupe (nécessairement $\mathbb{Z}/n\mathbb{Z}$) si et seulement si n et $\varphi(n)$ sont premiers entre eux. $\square$

Corollaire 6 (Tous les premiers, et davantage). *Tout nombre premier p vérifie $\mathcal{N}_{cyc}(p) = 0$ (par Lagrange, tout groupe d'ordre premier est cyclique). Mais la réciproque est fautive : certains composés annulent aussi $\mathcal{N}_{cyc}$ — les premiers sont 15, 33, 35, 51, 65, 69, ... Ainsi $\mathcal{N}_{cyc}$ détecte l'unicité de structure, non la primalité.*

n	premier ?	$\text{gnu}(n)$	$\mathcal{N}_{cyc}(n)$	
5	oui	1	0	premier $\Rightarrow$ nul
7	oui	1	0	premier $\Rightarrow$ nul
8	non	5	2,322	très composé : coût élevé
12	non	5	2,322	
15	non	1	0	composé mais cyclique ($\gcd(15, 8) = 1$)
16	non	14	3,807	
24	non	15	3,907	
35	non	1	0	composé mais cyclique ($\gcd(35, 24) = 1$)

```
import math
from math import gcd
gnu = {1:1,2:1,3:1,4:2,5:1,6:2,7:1,8:5,9:2,10:2,11:1,12:5,13:1,14:2,
       15:1,16:14,17:1,18:5,19:1,20:5,21:2,22:2,23:1,24:15}
phi = lambda n: sum(1 for k in range(1,n+1) if gcd(k,n)==1)
for n in range(2,25):
    Ncyc = math.log2(gnu[n])
    cyclic = (gcd(n, phi(n)) == 1) # nombre cyclique ?
    assert (Ncyc == 0) == cyclic # le theoreme, verifie
    print(n, gnu[n], round(Ncyc,3), "cyclique" if cyclic else "")
# N_cyc(n)=0 <=> gcd(n,phi(n))=1 : verifie pour tout n teste
```

4 Le vrai « rebond », et un faux à éviter

Remarque 7 (Le rebond authentique). La non-monotonie que l'on observe est réelle mais porte sur le *coût de table* $\log_2(n!/\varphi(n))$, qui oscille avec $\varphi(n)$: un n premier « rebondit » vers un coût relatif moindre (beaucoup de générateurs, forte symétrie d'étiquetage), un n très composé vers un coût plus élevé. La néguentropie de cyclicité $\mathcal{N}_{cyc}(n) = \log_2 \text{gnu}(n)$, elle, retombe à *zéro* précisément aux nombres cycliques : c'est un « rebond » vers le sol, aux premiers et à leurs cousins sans-facteur-commun.

Un faux rebond à écarter. Comparer les *tables étiquetées* de $\mathbb{Z}/n\mathbb{Z}$ ($n!/\varphi(n)$) au nombre de groupes à *isomorphisme près* ($\text{gnu}(n)$) mélange deux conventions de comptage et produit des néguentropies faussement négatives (p.ex. $\mathbb{Z}/n\mathbb{Z}$ « aurait plus de tables que tous les groupes d'ordre n » dès $n = 6$). Il n'y a là aucun rebond : seulement deux bases de

comptage incompatibles. On compare toujours à *isomorphisme près* avec à *isomorphisme près*, ou *étiqueté* avec *étiqueté* — jamais l'un avec l'autre.

5 Portée

Remarque 8 (Acquis). La néguentropie de cyclicité $\mathcal{N}_{\text{cyc}}(n) = \log_2 \text{gnu}(n)$ s'annule exactement aux nombres cycliques $\gcd(n, \varphi(n)) = 1$ (théorème 5), qui incluent tous les premiers sans s'y réduire (corollaire 6). La quantification des axiomes touche ainsi l'arithmétique : la contrainte « être cyclique » est gratuite précisément quand l'ordre n force l'unicité de la structure de groupe. Le coût de table, lui, oscille avec l'indicatrice d'Euler $\varphi(n)$.

Limites. (i) $\text{gnu}(n)$ (le *group number*) n'a pas de formule close ; il se lit dans les tables (OEIS A000001). L'équivalence avec $\gcd(n, \varphi(n)) = 1$ ne vaut que pour $\text{gnu}(n) = 1$, pas pour les valeurs supérieures. (ii) On compte à *isomorphisme près* ; le comptage étiqueté donne une autre échelle (et sert seulement au coût de table, proposition 1). (iii) Le résultat est un pont *descriptif* entre néguentropie de contrainte et arithmétique — il n'ajoute rien à la théorie des groupes finis, il la relit en bits.