La structure de $\mathbb{Z}_n^\times$

Marc Lorenzi

21 décembre 2025

1 Le théorème des restes chinois

Pour tout entier non nul n, nous noterons $\mathbb{Z}_n$ l'anneau des *entiers modulo* n et $\mathbb{Z}_n^\times$ le groupe multiplicatif des éléments inversibles de $\mathbb{Z}_n$. Pour tout $x \in \mathbb{Z}$, nous noterons $x + n\mathbb{Z}$ la classe de x modulo n.

Soit $r \in \mathbb{N}^*$. Soient $a_1, \ldots, a_r \in \mathbb{N}^*$. Soient $x, y \in \mathbb{Z}$. Supposons que $x+a_1 \ldots a_r\mathbb{Z} = y+a_1 \ldots a_r\mathbb{Z}$. On a alors pour tout $i \in [\![1, r]\!]$, $x+a_i\mathbb{Z} = y+a_i\mathbb{Z}$. On définit donc une application $f : \mathbb{Z}_{a_1 \ldots a_r} \longrightarrow \mathbb{Z}_{a_1} \times \ldots \times \mathbb{Z}_{a_r}$ en posant pour tout $x \in \mathbb{Z}$,

$$f(x + a_1 \ldots a_r\mathbb{Z}) = (x + a_1\mathbb{Z}, \ldots, x + a_r\mathbb{Z})$$

Proposition 1. *L'application f est un morphisme d'anneaux.*

Démonstration. Ce sont de simples vérifications. □

Proposition 2. *Si les entiers $a_1, \ldots, a_r$ sont premiers entre eux deux à deux, alors f est un isomorphisme d'anneaux.*

Démonstration. Supposons les a_i premiers entre eux deux à deux. Soit $\alpha = x + a_1 \ldots a_r\mathbb{Z}$ où $x \in \mathbb{Z}$. Supposons $f(\alpha) = (0, \ldots, 0)$. Pour tout $i \in [\![1, r]\!]$, $x \equiv 0 \bmod a_i$, c'est à dire a_i divise x. Comme les a_i sont premiers entre eux deux à deux, leur produit divise x et donc $\alpha == 0$. Le noyau de f est donc $\{0\}$. Le morphisme f est ainsi injectif. Remarquons maintenant que

$$|\mathbb{Z}_{a_1} \times \ldots \times \mathbb{Z}_{a_r}| = |\mathbb{Z}_{a_1}| \times \ldots \times |\mathbb{Z}_{a_r}| = a_1 \ldots a_r = |\mathbb{Z}_{a_1 \ldots a_r}|$$

Les anneaux de départ et d'arrivée de f sont finis, de même cardinal, donc f est bijective. □

Proposition 3. *Soit $x \in \mathbb{Z}$. On a $x+a_1 \ldots a_r \in \mathbb{Z}_{a_1 \ldots a_r}^\times$ si et seulement si $(x+a_1\mathbb{Z}, \ldots, x+a_r\mathbb{Z}) \in \mathbb{Z}_{a_1}^\times \times \ldots \times \mathbb{Z}_{a_r}^\times$.*

Démonstration. En effet, x est premier avec $a_1 \ldots a_r$ si et seulement si il est premier avec chacun des a_i. □

Corollaire 4. *Si les entiers $a_1, \ldots, a_r$ sont premiers entre eux deux à deux, alors f est un isomorphisme de $\mathbb{Z}_{a_1 \ldots a_r}^\times$ sur $\mathbb{Z}_{a_1}^\times \times \ldots \times \mathbb{Z}_{a_r}^\times$.*

Corollaire 5. *Pour tout $n \in \mathbb{N}^*$,*

$$\mathbb{Z}_n^\times \simeq \prod_{p \in \mathcal{P}} \mathbb{Z}_{p^{\nu_p(n)}}^\times$$

2 La structure de $\mathbb{Z}_p^\times$

Donnons-nous un nombre premier p. L'anneau $\mathbb{Z}_p$ est un corps, on a donc $\mathbb{Z}_p^\times = \mathbb{Z}_p \setminus \{0\}$. Par le théorème de Lagrange, pour tout $a \in \mathbb{Z}_p^\times$, l'ordre de a divise $|\mathbb{Z}_p^\times| = p - 1$.

Lemme 6. *Soit d un diviseur de $p-1$. Si le groupe $\mathbb{Z}_p^\times$ possède un élément d'ordre d, alors il en possède exactement $\varphi(d)$.*

Démonstration. Supposons qu'il existe $x \in \mathbb{Z}_p^\times$ d'ordre d. Soit G le groupe engendré par x. Le groupe cyclique G possède $\varphi(d)$ générateurs, c'est à dire $\varphi(d)$ éléments d'ordre d. Par ailleurs, le polynôme $P = X^d - 1$ a au plus d racines. Or, pour tout $a \in G$, $a^d = 1$ donc a est racine de P. Donc, le polynôme P a exactement d racines, qui sont les éléments de G. En conséquence, tous les éléments de $\mathbb{Z}_p^\times$ d'ordre d sont dans G. Il y a donc dans $\mathbb{Z}_p^\times$ $\varphi(d)$ éléments d'ordre d. □

Proposition 7. *Pour tout $n \in \mathbb{N}^*$,*

$$\sum_{d|n} \varphi(d) = n$$

Démonstration. Soit $n \in \mathbb{N}^*$. Pour tout diviseur d de n, notons

$$E_d = \{a \in [\![1, n]\!] : a \wedge n = d\}$$

Les ensembles E_d forment clairement une partition de $[\![1, n]\!]$. Notons également

$$F_d = \{k\frac{n}{d} : k \in [\![1, d]\!], k \wedge d = 1\}$$

Remarquons que $|F_d| = \varphi(d)$.

Soit d un diviseur de n. Soit $a \in F_d$. Soit $k \in [\![1, d]\!]$ premier avec d tel que $a = k(n/d)$. On a $a \in [\![1, n]\!]$ et

$$a \wedge n = k\frac{n}{d} \wedge n = k\frac{n}{d} \wedge d\frac{n}{d} = \frac{n}{d}(k \wedge d) = \frac{n}{d}$$

Ainsi, $a \in E_{n/d}$ et donc $F_d \subseteq E_{n/d}$. Inversement, soit $a \in E_{n/d}$. On a

$$\frac{n}{d} = a \wedge n = \left(\frac{a}{n/d}\frac{n}{d}\right) \wedge \left(d\frac{n}{d}\right) = \frac{n}{d}\left(\frac{a}{n/d} \wedge d\right)$$

On en déduit que

$$\frac{a}{n/d} \wedge d = 1$$

et donc

$$a = \frac{a}{n/d}\frac{n}{d} \in F_d$$

Ainsi, $E_{n/d} \subseteq F_d$ et finalement $E_{n/d} = F_d$.

On a l'union disjointe

$$[\![1, n]\!] = \bigcup_{d|n} E_d = \bigcup_{d|n} E_{n/d} = \bigcup_{d|n} F_d$$

On en déduit

$$n = |\,[\![1, n]\!]\,| = \sum_{d|n} |F_d| = \sum_{d|n} \varphi(d)$$

□

Proposition 8. *Pour tout diviseur d de $p-1$, $\mathbb{Z}_p^\times$ possède $\varphi(d)$ éléments d'ordre d.*

Démonstration. Pour tout diviseur d de $p-1$, le nombre d'éléments de $\mathbb{Z}_p^\times$ d'ordre d est $\lambda_d\varphi(d)$ où $\lambda_d = 0$ ou 1. Comme l'ordre des éléments de $\mathbb{Z}_p^\times$ est un diviseur de $p-1$,

$$\sum_{d|p-1} \lambda_d\varphi(d) = p-1$$

De plus, par la proposition précédente,

$$\sum_{d|p-1} \varphi(d) = p-1$$

En supposant l'un des λ_d nul, on obtient une contradiction. □

Proposition 9. *Le groupe $\mathbb{Z}_p^\times$ est cyclique.*

Démonstration. Il suffit de prendre $d = p-1$ dans la proposition précédente. □

3 La structure de $\mathbb{Z}_{p^2}^\times$

On suppose ici encore que p est un nombre premier. Le groupe $\mathbb{Z}_{p^2}^\times$ est un groupe d'ordre $\varphi(p^2) = p(p-1)$.

Proposition 10. *$\mathbb{Z}_{p^2}^\times$ est un groupe cyclique.*

p	générateurs de $\mathbb{Z}_p^\times$
2	1
3	1
5	2, 3
7	3, 5
11	2, 6, 7, 8
13	2, 6, 7, 11
17	3, 5, 6, 7, 10, 11, 12, 14
19	2, 3, 10, 13, 14, 15
23	5, 7, 10, 11, 14, 15, 17, 19, 20, 21
29	2, 3, 8, 10, 11, 14, 15, 18, 19, 21, 26, 27

FIGURE 1 – Les générateurs de $\mathbb{Z}_p^\times$

Démonstration. Considérons l'application de réduction $\rho : \mathbb{Z}_{p^2}^\times \to \mathbb{Z}_p^\times$ définie par

$$\rho(x + p^2\mathbb{Z}) = x + p\mathbb{Z}$$

Cette application est bien définie, car si $x \equiv y \bmod p^2$, alors $x \equiv y \bmod p$. L'application ρ est clairement un morphisme de groupes. Remarquons que si $a \in \mathbb{Z}_{p^2}^\times$ est d'ordre d, alors

$$\rho(a)^d = \rho(a^d) = \rho(1) = 1$$

et donc, l'ordre de $\rho(a)$ divise d.

Soit $x \in \mathbb{Z}$ tel que $a = x + p\mathbb{Z}$ engendre $\mathbb{Z}_p^\times$. On a $\rho(x + p^2\mathbb{Z}) = x + p\mathbb{Z}$, donc $p - 1$ divise l'ordre de $x + p^2\mathbb{Z}$. On a aussi $\rho(x + p + p^2\mathbb{Z} = x + p\mathbb{Z}$, donc $p - 1$ divise l'ordre de $x + p + p^2\mathbb{Z}$.

Par ailleurs, l'ordre de $x + p^2\mathbb{Z}$ et celui de $x + p + p^2\mathbb{Z}$ divisent $p(p - 1)$, ces deux ordres sont donc égaux à $p - 1$ ou à $p(p - 1)$.

Supposons que $x + p^2\mathbb{Z}$ n'est pas d'ordre $p(p - 1)$ (et donc est d'ordre $p - 1$). Par la formule du binôme,

$$(x + p)^{p-1} = x^{p-1} + (p - 1)x^{p-2}p + kp^2$$

où $k \in \mathbb{N}$. Comme $[x]_{p^2}$ est d'ordre $p - 1$, on a donc

$$(x + p)^{p-1} \equiv 1 + (p - 1)x^{p-2}p \bmod p^2$$

Supposons, par l'absurde, que $x + p + p^2\mathbb{Z}$ est d'ordre $p - 1$. On a alors

$$(p - 1)x^{p-2}p \equiv 0 \bmod p^2$$

d'où

$$(p - 1)x^{p-2} \equiv 0 \bmod p$$

Dans $\mathbb{Z}_p$, cette congruence devient

$$-a^{p-2} = 0$$

Contradiction, puisque $a \in \mathbb{Z}_p^\times$. Ainsi, $x + p + p^2\mathbb{Z}$ est d'ordre $p(p - 1)$, c'est donc un générateur de $\mathbb{Z}_{p^2}^\times$. □

4 La structure de $\mathbb{Z}_{p^n}^\times$ pour p impair

Proposition 11. *Soient p un nombre premier impair, $n \in \mathbb{N}^*$ et $x \in \mathbb{Z}$. On suppose $\text{pgcd}(x,p) = 1$. Alors, $x^p \equiv 1 \bmod p^{n+1}$ si et seulement si $x \equiv 1 \bmod p^n$.*

Démonstration. Supposons $x \equiv 1 \bmod p^n$. On a donc $p^n \mid x-1$. On a donc aussi $p \mid x-1$, donc $x \equiv 1 \bmod p$. De là,

$$\sum_{k=0}^{p-1} x^k \equiv \sum_{k=0}^{p-1} 1 = p \equiv 0 \bmod p$$

Or,

$$x^p - 1 = (x-1)\sum_{k=0}^{p-1} x^k$$

Le facteur $x-1$ est divisible par p^n et la somme est divisible par p, donc

$$x^p - 1 \equiv 0 \bmod p^{n+1}$$

Prouvons la réciproque par récurrence sur n. Pour $n = 1$, supposons $x^p \equiv 1 \bmod p^2$. Par le petit théorème de Fermat, il existe $k \in \mathbb{Z}$ tel que

$$x^p = x \times x^{p-1} = x(1+kp)$$

De là,

$$x + xkp \equiv 1 \bmod p^2$$

et donc

$$x \equiv x + xkp \equiv 1 \bmod p$$

Soit maintenant $n \in \mathbb{N}^*$. Supposons la propriété vérifiée par n. Supposons que $x^p \equiv 1 \bmod p^{n+2}$. On a donc aussi $x^p \equiv 1 \bmod p^{n+1}$ donc, par l'hypothèse de récurrence, $x \equiv 1 \bmod p^n$. Écrivons $x = 1 + kp^n$ où $k \in \mathbb{Z}$. On a, par le binôme de Newton,

$$x^p = (1+kp^n)^p = \sum_{j=0}^{p} \binom{p}{j} k^j p^{nj} = 1 + pkp^n + \sum_{j=2}^{p-1} \binom{p}{j} k^j p^{nj} + k^p p^{np}$$

Pour tout $j \in [\![2, p-1]\!]$, p divise $\binom{p}{j}$. De là, la somme ci-dessus est divisible par p^{2n+1}. Or, $2n+1 \geq n+2$ et, comme $p \geq 3$, $np \geq n+2$. On a donc

$$1 \equiv x^p \equiv 1 + kp^{n+1} \bmod p^{n+2}$$

d'où

$$kp^{n+1} \equiv 0 \bmod p^{n+2}$$

Ainsi, p divise k et donc

$$x = 1 + kp^n \equiv 0 \bmod p^{n+1}$$

□

Proposition 12. *Soit p un nombre premier impair. Pour tout $n \geq 2$, $Z_{p^n}^{\times}$ est cyclique.*

Démonstration. Nous avons déjà montré le résultat pour $n = 1$ et $n = 2$. Montrons le cas général par récurrence sur n. Soit $n \geq 2$. Supposons que $Z_{p^n}^{\times}$ est cyclique. Soit $x \in \mathbb{Z}$ tel que $x + p^n\mathbb{Z}$ engendre $Z_{p^n}^{\times}$. Nous allons montrer que $g = x + p^{n+1}\mathbb{Z}$ engendre $Z_{p^{n+1}}^{\times}$.

Soit $\rho : \mathbb{Z}_{p^{n+1}}^{\times} \longrightarrow \mathbb{Z}_{p^n}^{\times}$ le morphisme de réduction défini pour tout $a \in \mathbb{Z}$ par

$$\rho(a + p^{n+1}\mathbb{Z}) = a + p^n\mathbb{Z}$$

L'ordre de $\rho(g) = x + p^n\mathbb{Z}$ est $\varphi(p^n) = p^{n-1}(p-1)$. On en déduit que l'ordre de g est un multiple de $p^{n-1}(p-1)$. Le cardinal de $\mathbb{Z}_{p^{n+1}}^{\times}$ est $\varphi(p^{n+1}) = p^n(p-1)$. L'ordre de g divise ce cardinal. On en déduit que l'ordre de g est $p^{n-1}(p-1)$ ou $p^n(p-1)$.

Supposons, par l'absurde, que g est d'ordre $p^{n-1}(p-1)$. On a donc

$$x^{p^{n-1}(p-1)} \equiv 1 \bmod p^{n+1}$$

Par le lemme ? ? ?

$$x^{p^{n-2}(p-1)} \equiv 1 \bmod p^n$$

ou encore, dans $\mathbb{Z}_{p^n}$,

$$(x + p^n\mathbb{Z})^{p^{n-2}(p-1)} = 1$$

Contradiction, puisque $x + p^n\mathbb{Z}$ est d'ordre $p^{n-1}(p-1)$. Ainsi, g est d'ordre $p^n(p-1)$, donc g engendre $\mathbb{Z}_{p^{n+1}}^{\times}$. □

Bilan. Supposons trouvé $x \in \mathbb{Z}$ tel que $x + p\mathbb{Z}$ engendre $\mathbb{Z}_p^{\times}$. Alors, pour tout $n \geq 2$, $x + p + p^n\mathbb{Z}$ engendre $\mathbb{Z}_{p^n}^{\times}$.

5 La strcture de $\mathbb{Z}_{2^n}^{\times}$

Proposition 13. *Soit $n \geq 3$. Soit $x \in \mathbb{Z}$ impair. On a $x^{2^{n-2}} \equiv 1 \bmod 2^n$.*

Démonstration. Faisons une récurrence sur n. Si $n = 3$, un entier impair x est congru à 1, 3, 5 ou 7 modulo 8. Les carrés de ces entiers sont tous congrus à 1 modulo 8.

Soit $n \geq 3$. Supposons la propriété vraie pour n. Soit $x \in \mathbb{Z}$ impair. Par l'hypothèse de récurrence, il existe $k \in \mathbb{Z}$ tel que $x^{2^{n-2}} = 1 + k2^n$. De là,

$$x^{2^{n-1}} = (1 + k2^n)^2 = 1 + k2^{n+1} + k2^{2n} \equiv 1 \bmod 2^{n+1}$$

□

Ceci montre que pour tout $n \geq 3$, les éléments de $\mathbb{Z}_{2^n}^{\times}$ ont un ordre qui divise 2^{n-2}. Or, le cardinal de ce groupe est $\varphi(2^n) = 2^{n-1}$. Ce groupe n'est donc pas cyclique.

Proposition 14. *Pour tout $n \in \mathbb{N}$, $\nu_2(5^{2^n} - 1) = n + 2$.*

Démonstration. On a $5^{2^0} - 1 = 4 = 2^2$. Soit $n \in \mathbb{N}$. Supposons que $\nu_2(5^{2^n} - 1) = n + 2$. On a

$$5^{2^{n+1}} - 1 = (5^{2^n})^2 - 1 = (5^{2^n} - 1)(5^{2^n} + 1)$$

d'où

$$\nu_2(5^{2^{n+1}} - 1) = \nu_2(5^{2^n} - 1) + \nu_2(5^{2^n} + 1) = n + 2 + \nu_2(5^{2^n} + 1)$$

Par l'hypothèse de récurrence, on a en particulier

$$5^{2^n} + 1 \equiv 1 + 1 = 2 \bmod 4$$

donc 4 ne divise pas $5^{2^n} + 1$. De plus, cet entier est pair, donc $\nu_2(5^{2^n} + 1) = 1$. Ainsi,

$$\nu_2(5^{2^{n+1}} - 1) = n + 2 + \nu_2(5^{2^n} + 1) = n + 3$$

□

Proposition 15. *Soit $n \geq 3$. L'ordre de $5 + 2^n\mathbb{Z}$ dans $\mathbb{Z}_{2^n}^\times$ est 2^{n-2}.*

Démonstration. Par la proposition 13, l'ordre de $5 + 2^n\mathbb{Z}$ divise 2^{n-2}. Par la proposition 14, $\nu_2(5^{2^{n-3}} - 1) = n - 1$ donc $5^{2^{n-3}} \not\equiv 1 \bmod 2^n$, d'où le résultat. □

Proposition 16. *Pour tout $n \geq 2$ et tout $m \in \mathbb{N}$, $5^m \not\equiv -1 \bmod 2^n$.*

Démonstration. Soit $n \geq 2$. Soit $m \in \mathbb{N}$. Supposons $5^m \equiv -1 \bmod 2^n$. A fortiori, $5^m \equiv -1 \bmod 4$. Or, $5^m \equiv 1^m = 1 \bmod 4$, contradiction. □

Proposition 17. *Soit $n \geq 3$. Le groupe $\mathbb{Z}_{2^n}^\times$ est isomorphe au groupe $\mathbb{Z}_2 \times \mathbb{Z}_{2^{n-2}}$.*

Démonstration. Soit G' le sous-groupe de $\mathbb{Z}_{2^n}^\times$ engendré par -1. Le groupe G' est cyclique d'ordre 2, donc isomorphe à $\mathbb{Z}_2$. Soit G'' le sous-groupe de $\mathbb{Z}_{2^n}^\times$ engendré par 5. Par la proposition 15, le groupe G'' est cyclique d'ordre 2^{n-2}, donc isomorphe à $\mathbb{Z}_{2^{n-2}}$.

Soit $f : G' \times G'' \longrightarrow \mathbb{Z}_{2^n}^\times$ définie par

$$f(\varepsilon + 2^n\mathbb{Z}, 5^k + 2^n\mathbb{Z}) = \varepsilon 5^k + 2^n\mathbb{Z}$$

On vérifie facilement que f est un morphisme de groupes. Les groupes $G' \times G''$ et $\mathbb{Z}_{2^n}^\times$ sont tous les deux de cardinal 2^{n-1}. Pour montrer que f est un isomorphisme, il suffit donc de prouver que $\ker f = \{1 + 2^n\mathbb{Z}\}$. Soient $\varepsilon \in \{-1, 1\}$ et $k \in [\![0, 2^{n-2} - 1]\!]$. Supposons que

$$f(\varepsilon + 2^n\mathbb{Z}, 5^k + 2^n\mathbb{Z}) = 1 + 2^n\mathbb{Z}$$

c'est à dire

$$\varepsilon 5^k + 2^n\mathbb{Z} = 1 + 2^n\mathbb{Z}$$

En multipliant par $\varepsilon^{-1} = \varepsilon$, il vient

$$5^k + 2^n\mathbb{Z} = \varepsilon + 2^n\mathbb{Z}$$

Par la proposition 16, $\varepsilon \neq -1$, donc $\varepsilon = 1$. On a donc

$$5^k + 2^n\mathbb{Z} = 1 + 2^n\mathbb{Z}$$

Maintenant, par la proposition 15, $k = 0$, d'où le résultat. □

6 Quand $\mathbb{Z}_n^\times$ est-il cyclique ?

Pour tout groupe abélien fini $(G, \times)$ de neutre e, posons $G(2) = \{x \in G : x^2 = e\}$. On vérifie facilement que $G(2)$ est un sous-groupe de G. Le sous-groupe $G(2)$ est le *sous-groupe de 2-torsion de G*.

Proposition 18. *Soit G un groupe cyclique d'ordre pair. On a $|G(2)| = 2$.*

Démonstration. Posons $|G| = 2n$ où $n \in \mathbb{N}^*$. Soit g un générateur de G. Soit $k \in [\![0, 2n-1]\!]$. On a $g^k \in G(2)$ si et seulement si

$$e = (g^k)^2 = g^{2k}$$

ou encore $2k \in 2n\mathbb{Z}$, c'est à dire $k \in n\mathbb{Z}$. Comme $0 \leq k < 2n - 1$, il vient $G(2) = \{g^0, g^n\}$. □

Proposition 19. *Soient $G_1, \ldots, G_n$ des groupes abéliens. Soit $G = G_1 \times \ldots \times G_n$. On a*

$$G(2) = G_1(2) \times \ldots \times G_n(2)$$

Démonstration. Vérification immédiate. □

Soit $n \in \mathbb{N}^*$. Écrivons

$$n = 2^m \prod_{k=1}^{r} p_i^{k_i}$$

où $r \in \mathbb{N}$, les p_i sont des nombres premiers impairs distincts, et $m \in \mathbb{N}$, $k_1, \ldots, k_r \in \mathbb{N}^*$.

Proposition 20. *Soit $n \in \mathbb{N}^*$. On suppose $r \geq 2$. Alors, $\mathbb{Z}_n^\times$ n'est pas cyclique.*

Démonstration. Les groupes $G_i = \mathbb{Z}_{p_i^{k_i}}^\times$, $i = 1, 2$ sont cycliques d'ordre pair. On a donc $|G_i(2)| = 2$. Par la proposition 19, $|\mathbb{Z}_n^\times(2)| \geq 4$ donc, par la proposition 18, $\mathbb{Z}_n^\times$ n'est pas cyclique. □

Nous supposons désormais que

$$n = 2^m p^k$$

où $m \in \mathbb{N}^*$ et $k \in \mathbb{N}$.

Proposition 21. *On suppose que $m \geq 2$ et $k \geq 1$. Alors, $\mathbb{Z}_n^\times$ n'est pas cyclique.*

Démonstration. Si $m = 2$, alors

$$\mathbb{Z}_n^\times \simeq Z_2 \times G$$

où G est un groupe cyclique d'ordre pair. L'argument de la démonstration de la proposition précédente montre que $\mathbb{Z}_n^\times$ n'est pas cyclique. Si $m \geq 3$, alors

$$\mathbb{Z}_n^\times \simeq Z_2 \times \mathbb{Z}_{2^{m-2}} \times G$$

Les deux premiers facteurs montrent que $|\mathbb{Z}_n^\times(2)| \geq 4$, donc $\mathbb{Z}_n^\times$ n'est pas cyclique. □

Proposition 22. *Soit $n \in \mathbb{N}^*$. Le groupe $\mathbb{Z}_n^\times$ est cyclique dans un et un seul des cas suivants.*

1. *$n = 2$ ou $n = 4$.*
2. *$n = p^k$ où p est premier impair et $k \geq 1$.*
3. *$n = 2p^k$ où p est premier impair et $k \geq 1$.*

Démonstration. Les deux propositions précédentes montrent que si $\mathbb{Z}_n^\times$ est cyclique, alors on est dans l'un des trois cas. Inversement, le cas 1 est immédiat. Le cas 2 a déjà été traité. Il reste à voir le cas 3. Considérons le morphisme de réduction

$$\rho : \mathbb{Z}_{2p^k}^\times \longrightarrow \rho : \mathbb{Z}_{p^k}^\times$$

défini par $\rho(x + 2p^k\mathbb{Z}) = x + p^k\mathbb{Z}$. Ce morphisme est surjectif. De plus,

$$|\mathbb{Z}_{2p^k}^\times| = \varphi(2p^k) = \varphi(2)\varphi(p^k) = \varphi(p^k) = |\mathbb{Z}_{p^k}^\times|$$

Ainsi, ρ est un isomorphisme. Comme $\mathbb{Z}_{p^k}^\times$ est cyclique, il en est donc de même de $\mathbb{Z}_{2p^k}^\times$. □

7 Une amélioration du théorème de Wilson

Le théorème de Wilson affirme qu'un entier $p \in \mathbb{N}^*$ est premier si et seulement si $(p-1)! \equiv -1 \bmod p$. La preuve classique consiste à regrouper dans le produit $(p-1)!$ chaque élément de $\mathbb{Z}_p^\times$ avec son inverse. Nous allons généraliser ce résultat.

Soit $n \geq 3$. Notons $G = \mathbb{Z}_n^\times$. En regroupant chaque élément de G avec son inverse, on obtient

$$\prod_{g \in G} g = \prod_{g \in G(2)} g$$

Proposition 23.

$$\prod_{g \in G(2)} g = (-1)^{|G(2)|/2} + n\mathbb{Z}$$

Démonstration. Soit $a \in \mathbb{Z}$. Supposons que $a + n\mathbb{Z} \in G(2)$. On a alors

$$(-a + n\mathbb{Z})^2 = (-a)^2 + n\mathbb{Z} = a^2 + n\mathbb{Z} = 1 + n\mathbb{Z}$$

Ainsi, $-a + n\mathbb{Z} \in G(2)$. De plus, $-a + n\mathbb{Z} \neq a + n\mathbb{Z}$. En effet, dans le cas contraire, on aurait $n \mid 2a$. Mais $n \wedge a = 1$ (car $a + n\mathbb{Z} \in G$) donc, par le lemme de Gauss, n divise 2, contradiction.

Remarquons également que

$$(a + n\mathbb{Z})(-a + n\mathbb{Z}) = -a^2 + n\mathbb{Z} = -1 + n\mathbb{Z}$$

En regroupant dans le produit des éléments de $G(2)$ chaque élément avec son *opposé*, on obtient le résultat. □

Pour tout $n \in \mathbb{N}^*$, posons

$$F(n) = \prod_{a \in [\![1,n]\!], a \wedge n = 1} a$$

Proposition 24. *Soit $n \geq 3$. Si $\mathbb{Z}_n^\times$ est cyclique, alors $F(n) \equiv -1 \bmod n$. Sinon, $F(n) \equiv 1 \bmod n$.*

Démonstration. Supposons $G = \mathbb{Z}_n^\times$ cyclique. Par la proposition 18, $|G(2)| = 2$, donc $(-1)^{|G(2)|/2} = -1$.

Supposons maintenant G non cyclique. Le groupe $\mathbb{Z}_n^\times$ est isomorphe à un produit de $N \geq 2$ groupes cycliques, tous d'ordre pair. L'entier 2^N divise $|G(2)|$, donc $|G(2)|/2$ est pair. □