Le groupe multiplicatif $(\mathbb{Z}/n\mathbb{Z})^\times$

Solutions

Exercice 1.

1. $\varphi(n)$ est l'ordre du groupe multiplicatif $(\mathbb{Z}/n\mathbb{Z})^\times$.
2. Pour p premier, tous les entiers de 1 à $p-1$ sont premiers avec p, donc on a que $\varphi(p) = |\{a | 1 \leq a \leq p \text{ et } pgcd(a,p) = 1\}| = |\{1, 2, 3 \ldots, p-1\}| = p-1$.
3. Être premier avec p^α équivaut à ne pas être divisible par p. Il y a $p^{\alpha-1}$ multiples de p compris entre 1 et p^α, donc $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$. (**Lemme 2.4**, cours)
4. Comme p et q premiers entre eux, on a que $\varphi(pq) = \varphi(p)\varphi(q) = (p-1)(q-1)$.
5. $\varphi(64) = 32, \quad \varphi(100) = 40, \quad \varphi(108) = 36, \quad \varphi(125) = 100.$
6. Si n impaire, alors n et 2 sont premiers entre eux et $\varphi(2n) = \varphi(2)\varphi(n) = \varphi(n)$.
7. Si n paire, alors on a que

$$\begin{aligned} |\{a | 1 \leq a \leq n \text{ et } pgcd(a,n) = 1\}| &= |\{a | \quad 1 \leq a \leq n \text{ et } pgcd(a,2n) = 1\}| \\ &= |\{a | \ n+1 \leq a \leq 2n \text{ et } pgcd(a,2n) = 1\}| \end{aligned}$$

   d'où $\varphi(2n) = 2\varphi(n)$.
8. Analogue à la question précédente.
9. $\varphi(2^k) = 2^k - 2^{k-1} = 2^{k-1}$.
10. Résultat du cours.
11. Si on compare les valuations p-adiques des $\varphi(n)$ et $n!$ on obtient la division.
12. En utilisant la question précédente et le **Théoréeme 2.6** (Euler) du cours.
13. D'après le résultat du cours **Lemme 2.5**.

Exercice 2.

1. D'après le cours, le groupe G est d'ordre $\varphi(12) = 4$, où φ désigne la fonction indicatrice d'Euler.
2. Les éléments de G sont (représentés par les entiers) :
   1 (d'ordre 1), 5, 7 et 11 (d'ordre 2).
3. Le groupe G n'est pas cyclique, car tous ses éléments sont d'ordre divisant 2.

Exercice 3.

1. $\overline{17}$ inversible dans $\mathbb{Z}/20\mathbb{Z}$) car 17 est premier avec 20 ($pgcd(17, 20) = 1$) et $\overline{17}^{-1} = \overline{13}$.
2. $\overline{18}$ inversible dans $\mathbb{Z}/49\mathbb{Z}$ car il est premier avec 49 et $\overline{18}^{-1} = \overline{30}$.
3. $\overline{38}$ inversible dans $\mathbb{Z}/77\mathbb{Z}$ car il est premier avec 77 et $\overline{38}^{-1} = \overline{75}$.
4. $\overline{42}$ n'est pas inversible dans $\mathbb{Z}/135\mathbb{Z}$ car $pgcd(42, 135) = 3$.

Exercice 4.

1. $\mathsf{ordre}(\mathbb{Z}/15\mathbb{Z})^\times = \varphi(15) = 8$
2. $\mathsf{ordre}(\mathbb{Z}/401\mathbb{Z})^\times = \varphi(401) = 400$