Feuille d'exercices 3

Groupe symétrique

1. (Structure des groupes cycliques) On rappelle qu'un groupe est *cyclique* s'il est engendré par un unique élément.
   (a) Dans un groupe G, montrer que pour tout élément $x \in G$, l'application $f\colon \mathbb{Z} \to G$, $n \mapsto f(n) = x^n$ est un morphisme de groupes.
   (b) Montrer que, si G est cyclique et fini d'ordre n, alors G est isomorphe à $\mathbb{Z}/n\mathbb{Z}$. Si G est cyclique et infini, il est isomorphe à $\mathbb{Z}$.
   (c) En utilisant le théorème de Lagrange, en déduire que tout groupe fini d'ordre p premier est isomorphe à $\mathbb{Z}/p\mathbb{Z}$. Donner un exemple de groupe d'ordre n non premier, tel que G n'est pas isomorphe à $\mathbb{Z}/n\mathbb{Z}$.
   (d) Montrer indépendamment des résultats précédents que tout groupe cyclique est commutatif.
2. (Ordre de permutations) Soit $\sigma = \sigma_1 \cdots \sigma_p$ la décomposition en cycles disjoints d'un élément $\sigma \in S_n$. Montrer que l'ordre de σ est le *ppcm* des ordres de $\sigma_1, \ldots, \sigma_p$.
3. On rappelle que la *signature* ε d'une permutation $\sigma \in S_n$ est définie par :

$$\varepsilon(\sigma) = (-1)^{\#\{(i,j)\,:\,i<j \text{ et } \sigma(i)>\sigma(j)\}}.$$

   (a) Montrer que la signature d'un cycle de longueur p dans S_n vaut $(-1)^{p-1}$.
   (b) Montrer que l'ensemble A_n des éléments $\sigma \in S_n$ tels que $\varepsilon(\sigma) = 1$ est un sous-groupe de S_n. On l'appelle *groupe alterné*.
   (c) Montrer que le groupe alterné A_6 contient un élément d'ordre 4, mais que le groupe alterné A_5 n'en contient pas.

Indicatrice d'Euler et le théorème chinois

4. (a) On rappelle que $\phi(n)$ dénote le nombre d'entiers positifs plus petits que n premiers avec n. Calculer $\phi(n)$ pour $n \in \{5, 8, 13, 18, 19, 21, 25, 27, 33, 36\}$.
   (b) Pour quelles valeurs de n, parmi celles de la question (4a), le groupe $(\mathbb{Z}/n\mathbb{Z})^*$ est-il cyclique ?
5. Pour quels entiers n a-t-on $\phi(n) = \frac{n}{3}$?
6. (a) Existe-t-il un entier $n > 1$ tel que $x^n \equiv 1 \pmod{15}$ pour tout $x \in \mathbb{Z}$?
   (b) Trouver un entier $n > 1$ tel que $x^n \equiv 1 \pmod{15}$ pour tout entier $x \in \mathbb{Z}$ premier avec 15.
7. (a) Soit $n = p_1 \cdots p_r$ un produit de nombres premiers distincts deux à deux, et soit :

$$a = 1 + (p_1 - 1) \times \cdots \times (p_r - 1).$$

   Montrer qu'on a $x^a \equiv x \pmod{n}$ pour tout $x \in \mathbb{Z}$.

(b) Soit $n = p^k q$ où p est premier, $k \geq 2$, et p ne divise pas q. Montrer qu'il existe $x \in \mathbb{Z}$ tel que $x \equiv p^{k-1} \pmod{p^k}$ et $x \equiv 0 \pmod{q}$. Montrer que pour tout $a > 1$, $x^a \not\equiv x \pmod{n}$.

8. Soit p un nombre premier. Pour $k \in \mathbb{Z}/p\mathbb{Z}$, $k \neq 0$, on définit une application $f_k \colon \mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ par $f_k(x) = kx$.

   (a) En observant que f_k est bijective, vérifier l'égalité suivante dans $\mathbb{Z}/p\mathbb{Z}$:

$$\prod_{x=1}^{p-1} f_k(x) = (p-1)!$$

   (b) En déduire une démonstration du petit théorème de Fermat, $a^{p-1} \equiv 1 \pmod{p}$ pour tout entier a premier avec p.

9. Déterminer les entiers $x \in \mathbb{N}$ tels que $3^x \equiv 11 \pmod{14}$.

10. Déterminer les entiers $n \geq 1$ tels que le morphisme $x \mapsto x^n$ de $(\mathbb{Z}/35\mathbb{Z})^*$ dans lui-même soit bijectif.

11. Soit p un nombre premier différent de 2.

   (a) Montrer que p est de la forme $4k+1$ ou $4k+3$.

   (b) Vérifier que l'équation

$$x^2 + 1 \equiv 0 \pmod{p} \tag{1}$$

   n'a pas de solution si p est de la forme $4k+3$. [*Indication :* déterminer l'ordre de x.]

   (c) Si $p = 4k+1$, vérifier que $x = (2k)!$ est solution de l'équation (1). [*Indication :* utiliser le théorème de Wilson, $(p-1)! \equiv -1 \pmod{p}$.]

   (d) Exemple : donner les solutions de l'équation $x^2 + 1 \equiv 0 \pmod{13}$.

12. Soit $f(x,y) = x^3 - y^3 + 2xy + x - 2$; notons $G(m)$ le nombre de solutions modulo m de la congruence $f(x,y) \equiv 0 \pmod{m}$. C'est-à-dire

$$G(m) = \#\left\{(x,y) \in \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} : f(x,y) \equiv 0 \pmod{m}\right\}.$$

   Montrer que si m et n sont premiers entre eux alors $G(mn) = G(m)G(n)$. [*Indication* : utiliser le théorème des restes chinois, l'énoncé vaut pour tout polynôme à coefficients dans $\mathbb{Z}$.]

Nombres pseudo-premiers

Dans la suite, on appelle base *d'un entier $n > 1$ tout entier $b \geq 1$ premier avec n. On dit qu'un nombre $n > 1$ est* pseudo-premier *pour une de ses bases b si n n'est pas premier et si $b^{n-1} \equiv 1 \pmod{n}$.*

13. (a) Montrer que $2^{10} \equiv 1 \pmod{341}$. En déduire que $n = 341$ est pseudo-premier pour la base 2.

   (b) Montrer que 3^{10} n'est pas congru à 1 modulo 341. Montrer que 3 est inversible modulo 341, et calculer l'ordre du groupe $(\mathbb{Z}/341\mathbb{Z})^*$. Déterminer l'ordre de 3 dans $(\mathbb{Z}/341\mathbb{Z})^*$, et en déduire que 341 n'est pas pseudo-premier pour la base 3.

   (c) Soit n un nombre pseudo-premier pour la base 2 et soit $n' = 2^n - 1$. Montrer que $n | n' - 1$. Montrer que n' est pseudo-premier pour la base 2 (utiliser $a \mid b \Rightarrow 2^a - 1 \mid 2^b - 1$). En déduire qu'il existe une infinité de nombres pseudo-premiers pour la base 2.

14. Trouver toutes les bases pour lesquelles 15 est pseudo-premier.

15. Soit p un nombre premier. Montrer que p^2 est pseudo-premier pour la base b si et seulement si $b^{p-1} \equiv 1 \pmod{p^2}$.

16. Soit $n = pq$ avec p et q deux nombres premiers distincts. On pose $d = \text{pgcd}(p-1, q-1)$. Montrer que n est pseudo-premier pour la base b si et seulement si $b^d \equiv 1 \pmod{n}$. [*Indication :* utiliser le théorème chinois. Calculer en fonction de d le nombre de bases pour lesquelles le nombre n est pseudo-premier.]

17. (Nombres de Mersenne et de Fermat pseudo-premiers pour la base 2.)
    (a) Montrer qu'un nombre de Mersenne $M_p = 2^p - 1$ non premier est pseudo-premier pour la base 2.
    (b) Même question pour les nombres de Fermat non premiers $F_n = 2^{2^n} + 1$.