2 Calculs dans Z/nZ

Exercice 2.1. — Nombre de Carmichael. Soit $n = 561$.

1. Montrer que pour tout a premier avec n, on a $a^n = a \pmod n$.
2. Montrer que pour tout a, on a $a^n = a \pmod n$.

Exercice 2.2. — Soit $n = p_1 \cdots p_k$ un entier sans facteur carré et $k \geq 3$.

1. Que vaut $\varphi(n)$?
2. Montrer que tout $x \in (\mathbf{Z}/n\mathbf{Z})^*$ vérifie $x^{1/2\varphi(n)} = 1$. En déduire que $(\mathbf{Z}/n\mathbf{Z})^*$ n'est pas cyclique.
3. Montrer que pour tout x premier avec n, on a $x^{\varphi(n)} \equiv 1 \pmod n$.
4. Montrer que pour tout $\lambda \equiv 1 \pmod{\varphi(n)}$, et tout x premier avec n, on a $x^\lambda \equiv x \pmod n$.
5. Montrer que pour tout $x \in \mathbf{Z}$, on a $x^\lambda \equiv x \pmod n$.

Exercice 2.3. — Ordres
Pour chacun de ces groupes, écrire l'inverse et l'ordre des éléments : $(\mathbf{Z}/18\mathbf{Z}, +)$, $\mathbf{Z}/26\mathbf{Z}^*$, $\mathbf{Z}/31\mathbf{Z}^*$.

Exercice 2.4. — Soit G un groupe commutatif. Montrer que si a est d'ordre n et b est d'ordre m avec $(n,m) = 1$, alors ab est d'ordre nm. Montrer que si G n'est plus commutatif ce résultat ne subsiste pas.

Exercice 2.5. —

1. Soit G un groupe d'ordre N. Montrer que g est d'ordre N si et seulement si pour tout diviseur premier p de N, on a $g^{N/p} \neq 1$.
2. Calculer la complexité du test : g est un générateur de $(\mathbf{Z}/p\mathbf{Z})^*$, supposant que l'on sait factoriser $p-1$.
3. Quel est la probabilité que g soit un générateur ? Trouver une estimation du temps moyen nécessaire à trouver un générateur de $(\mathbf{Z}/p\mathbf{Z})^*$.
4. Trouver un générateur des groupes $(\mathbf{Z}/p\mathbf{Z})^*$, pour p premier de 11 à 41. On pourra commencer par 2, puis 3 et utiliser également l'exercice 2.5.

Exercice 2.6. — Soit $p = 31$ et $q = 37$ et $n = p \cdot q$.

1. Calculer $\varphi(n)$.
2. Bob choisit l'algorithme RSA pour recevoir des messages (modulo n) et publie la clé publique $(n, e = 11)$.
   (a) Montrer que $x^{ed} = x$ pour tout $x \in \mathbf{Z}/n\mathbf{Z}$ si et seulement si $ed \equiv 1 \pmod{180}$.
   (b) Trouver d tel que $ed \equiv 1 \pmod{180}$.

Exercice 2.7. — Afin de communiquer en utilisant le protocole RSA, Alice choisit (et publie) la clé publique $(e,n) = (37, 65)$.

1. Déterminer la clé secrète.
2. Déterminer toutes les clés de déchiffrement $(r, \varphi(n))$ avec $0 < r < \varphi(n)$.
3. Alice réalise avoir fait un très mauvais choix. Pourquoi ?