Autour de $\mathbb{Z}/n\mathbb{Z}$

Soit $n \geq 2$ un entier. On note $\mathbb{Z}/n\mathbb{Z}$ l'ensemble des classes d'entiers modulo n. Étant donné un entier a, on notera $[a]_n$ sa classe d'équivalence dans $\mathbb{Z}/n\mathbb{Z}$. Si $[a]_n = [b]_n$, on pourra écrire $a \equiv b \mod n$.

On rappelle que $(\mathbb{Z}/n\mathbb{Z}, +, .)$ est un anneau commutatif. On rappelle que si A_1 et A_2 sont des groupes (resp. des anneaux), alors le produit cartésien $A_1 \times A_2$ a naturellement une structure de groupe (resp. d'anneau).

Remarque : ce sujet ne nécessite pas de connaissances spéciale sur les anneaux (mis à part leur définition). Par contre, les résultats de cours sur les groupes doivent être connus.

1 Un théorème d'isomorphisme

1.1. Soient n_1, n_2 deux entiers supérieurs ou égaux à 2, et $n = n_1 n_2$. Soit

$$\begin{array}{rccc} f: & \mathbb{Z}/n\mathbb{Z} & \to & \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \\ & [a]_n & \mapsto & ([a]_{n_1}, [a]_{n_2}) \end{array}$$

Justifier que f est bien définie. Montrer que c'est un morphisme du groupe $(\mathbb{Z}/n\mathbb{Z}, +)$ vers le groupe produit $(\mathbb{Z}/n_1\mathbb{Z}, +) \times (\mathbb{Z}/n_2\mathbb{Z}, +)$.

1.2. On suppose que $pgcd(n_1, n_2) = 1$. Justifier que f est un isomorphisme de groupe. On pourra commencer par déterminer son noyau.

2 Le groupe $(\mathbb{Z}/n\mathbb{Z})^*$

On définit $(\mathbb{Z}/n\mathbb{Z})^* = \{[a] \in \mathbb{Z}/n\mathbb{Z}, pgcd(a, n) = 1\}$

2.1. Donner la liste des éléments de $(\mathbb{Z}/12\mathbb{Z})^*$ et $(\mathbb{Z}/11\mathbb{Z})^*$.

2.2. Soit $x \in \mathbb{Z}/n\mathbb{Z}$. Montrer qu'il existe $y \in \mathbb{Z}/n\mathbb{Z}$ tel que $x.y = [1]$ si et seulement si $x \in (\mathbb{Z}/n\mathbb{Z})^*$. Montrer que $((\mathbb{Z}/n\mathbb{Z})^*, .)$ est un groupe.

2.3. Déterminer la table de $((\mathbb{Z}/12\mathbb{Z})^*, .)$.

2.4. Montrer que $((\mathbb{Z}/n\mathbb{Z})^*, +)$ *n'est pas* un groupe. Même question avec $(\mathbb{Z}/n\mathbb{Z}, .)$. Ainsi, par la suite, on pourra parler du groupe $\mathbb{Z}/n\mathbb{Z}$, ou du groupe $(\mathbb{Z}/n\mathbb{Z})^*$ sans avoir a préciser la loi considérée (qui est donc nécéssairement l'addition dans le premier cas et la multiplication dans le second cas)

2.5. On suppose que n_1, n_2 sont premiers entre eux. Montrer que

$$f((\mathbb{Z}/n\mathbb{Z})^*) = (\mathbb{Z}/n_1\mathbb{Z})^* \times (\mathbb{Z}/n_2\mathbb{Z})^*$$

Indication : ou pourra utiliser la question 1.2.

On rappelle qu'un groupe fini G est cyclique si il existe $x \in G$ tel que $G = \{x^k,\ k \in \{0, \ldots, card(G)-1\}$. On dit que x est un générateur de G.

2.6. Justifier que $(\mathbb{Z}/11\mathbb{Z})^*$ est cyclique en donnant un générateur.

2.7. Démontrer que $(\mathbb{Z}/12\mathbb{Z})^*$ n'est pas cyclique.

Dans toute la suite, on admettra que, si p est premier $(\mathbb{Z}/p\mathbb{Z})^*$ est cyclique.

3 Indicatrice d'Euler

Soit n un entier positif. On pose $\varphi(n) = card((\mathbb{Z}/n\mathbb{Z})^*)$

3.1. Soit p un nombre premier. Déterminer $\varphi(p)$.

3.2. Soit p un nombre premier, et $\alpha \in \mathbb{N}^*$. Déterminer $\varphi(p^\alpha)$. On pourra commencer par décrire l'ensemble des entiers $a \in \{0, \ldots, n-1\}$ tels que a et p^α ne sont *pas* premiers entre eux.

3.3. Soit n_1, n_2 des entiers premiers entre eux. Justifier que $\varphi(n_1 n_2) = \varphi(n_1)\varphi(n_2)$. *Indication :* ou pourra utiliser un résultat de la partie 2.

3.4. Soient $p_1, \ldots, p_r$ des nombres premiers distincts. Soient $\alpha_1, \ldots \alpha_n$ des entiers non nuls. Déduire des questions précédentes que pour $n = p_1^{\alpha_1} \ldots p_r^{\alpha_r}$, on a

$$\varphi(n) = n \prod_{i=1}^{r} (1 - \frac{1}{p_i})$$

4 Nombres pseudo-premiers

4.1. Soit $(G, .)$ un groupe fini et n son cardinal. Soit $x \in G$. Démontrer que $x^n = e$, où e designe l'élément neutre de G.

4.2. En déduire que $\forall a \in \mathbb{Z}$, $pgcd(a, n) = 1 \Rightarrow a^{\varphi(n)} \equiv 1 \mod n$.

4.3. On suppose que n est premier. Déduire de la question précédente que $\forall a \in \mathbb{Z}$, si a, n sont premiers entre eux alors $a^{n-1} \equiv 1 \mod n$, puis que $\forall a \in \mathbb{Z}$, $a^n \equiv a \mod n$.

4.4. Soit n un nombre composé. On dit qu'il est *pseudo-premier* en base a si $a^n \equiv a \mod n$.
On suppose que $n = n_1 n_2$, avec n_1, n_2 premiers entre eux. Démontrer que n est pseudo premier en base a si et seulement si $a^n \equiv a \mod n_1$ et $a^n \equiv a \mod n_2$.

4.5. Soit $n = 341 = 11 \times 31$. Montrer que n est pseudo-premier en base 2, mais pas en base 3 (*remarque :* contrairement aux apparences, on n'a pas besoin de faire de lourd calculs pour répondre à cette question.).

4.6. Soit $n = 561 = 3 \times 11 \times 17$. Montrer que n est pseudo-premier pour toute base (même remarque que précédement).

5 Une caractérisation

Le but de cette section est de démontrer qu'un nombre $n \geq 2$ est pseudo-premier pour toute base si et seulement si

$$\forall p \in \mathbb{N}, p \text{ premier}, \qquad p \mid n \Rightarrow p - 1 \mid n - 1 \text{ et } p^2 \nmid n. \tag{1}$$

5.1. On suppose que (1) est réalisé. Démontrer que n est pseudo-premier pour toute base. *Indication :* $n = p_1 p_2 \ldots p_r$.

5.2. On suppose maintenant que n est pseudo-premier pour toute base.

1. On suppose que n est de la forme $n = p^2 k$. Posons $a = 1 + kp$.
   a) Démontrer que a est premier avec n. En déduire que $a^{n-1} \equiv 1 \mod n$.
   b) Montrer que $a^p \equiv 1 \mod n$ (on pourra développer a^p avec le binome de Newton).
   c) En déduire que $p \mid n - 1$. Conclure.

2. On suppose que n est de la forme $n = p_1 \dots p_r$ avec $p_1, \dots, p_r$ des nombres premiers distincts. Pour tout $i \in \{1, \dots, r\}$ on considère un générateur α_i de $(\mathbb{Z}/p_i\mathbb{Z})^*$ (un tel α_i existe d'après la propriété admise dans la fin de la partie 2).
   a) Justifier qu'il existe $a \in \mathbb{Z}$, tel que, pour tout i, $[a]_{p_i} = \alpha_i$.
   b) Justifier que, pour tout i $\alpha_i^{(n-1)} = [1]_{p_i}$ dans $(\mathbb{Z}/p_i\mathbb{Z})^*$.
   c) En déduire que pour tout i, $p_i - 1$ divise $n - 1$.

Remarque : on peut montrer qu'il existe une infinité de nombres pseudo-premiers en toute base (c'est un résultat de 1994).

6 Un test de primalité

6.1. Soit n un nombre premier impair. Déterminer toutes les solutions dans $\mathbb{Z}/nZ$ de l'équation

$$x^2 = [1]$$

On pose $n - 1 = 2^k q$, avec q impair. Déduire de la question précédente que, quelquesoit $a \in \{1, \dots, n\}$, on a l'alternative suivante :

— ou bien $a^q \equiv 1 \mod n$

— ou bien il existe $r < k$, tel que $a^{q2^r} \equiv -1 \mod n$.

On pourra commencer par s'interroger sur les valeurs possibles de $a^{\frac{n-1}{2}} \mod n$.

6.2. Montrer que pour $n = 561$. L'alternative précédente n'est pas vérifiée pour $a = 2$.

Remarque : Le théorème de Miller–Rabin affirme que si n n'est pas premier, au moins $3n/4$ entiers $a \in \{1, \dots, n\}$ ne vont pas réaliser cette alternative précédente. Ce qui permet en pratique d'obtenir des grand nombres "probablement premiers".