Université Paris 7 - Denis Diderot 2018-2019

UFR de Mathématiques M1 - Arithmétique

Feuille d'exercices 2

Exercice 1 Soient $a > 0, n > 1$, montrer que l'ordre de a dans $(\mathbb{Z}/(a^n - 1)\mathbb{Z})^*$ est n. En déduire que n divise $\phi(a^n - 1)$.

Exercice 2 Montrer qu'il existe une infinité de nombres premiers congrus à 3 modulo 4 (respectivement congrus à 1 modulo 4). Astuce : dans le 2e cas construire un nouveau premier p tel que -1 est un carré modulo p.

Exercice 3 Un nombre entier N est dit de Carmichael si N n'est pas premier, mais pour tout a premier avec N on a $a^{N-1} \equiv 1 \bmod N$. Monter que N est de Carmichael si et seulement si il est sans facteurs carrés et, pour chaque facteur premier p de N, on a que $p - 1$ divise $N - 1$.

Exercice 4 Soit $L = 11396 = 2^2 \cdot 7 \cdot 11 \cdot 37$, $M = 16200 = 2^3 \cdot 3^4 \cdot 5^2$ et $N = 13176 = 2^3 \cdot 3^3 \cdot 61$ et $G_1 = (\mathbb{Z}/L\mathbb{Z})^*$, $G_2 = (\mathbb{Z}/M\mathbb{Z})^*$ et $G_3 = (\mathbb{Z}/N\mathbb{Z})^*$.

1. Les groupes G_i ont-ils même cardinal et sont-ils isomorphes ?
2. Calculer l'exposant du chacun des G_i, c'est-à-dire le plus petit entier $m \geq 1$ tel que $a^m = 1$ pour tout $a \in G_i$.
3. Combien de solutions l'équation $x^2 = 1$ a-t-elle dans G_1, G_2, G_3 ?
4. Combien de solutions l'équation $x^{L-1} = 1$ a-t-elle dans G_1 ? Même question avec $x^{N-1} = 1$ dans G_3. (On notera que $L - 1 = 11395 = 5 \cdot 43 \cdot 53$ et $N - 1 = 13175 = 5^2 \cdot 17 \cdot 31$.)

Exercice 5 Soit $M = 21560 = 2^3 \cdot 5 \cdot 7^2 \cdot 11$, $N = 21576 = 2^3 \cdot 3 \cdot 29 \cdot 31$ et $G_1 = (\mathbb{Z}/M\mathbb{Z})^*$, $G_2 = (\mathbb{Z}/N\mathbb{Z})^*$.

1. Les groupes G_1 et G_2 ont-ils même cardinal et sont-ils isomorphes ?
2. Calculer l'exposant du groupe G_1.
3. Combien de solutions l'équation $x^2 = 1$ a-t-elle dans G_1 ?
4. Combien de solutions l'équation $x^2 = -1$ a-t-elle dans G_1 ?
5. Combien de solutions l'équation $x^2 = 9$ a-t-elle dans G_1 ?

Exercice 6 Soit $K = \mathbb{F}_{q^m}$ et soit $k = \mathbb{F}_q$. Montrer que les applications $\mathrm{N} = \mathrm{N}_k^K : K^* \to k^*$ et $\mathrm{Tr} = \mathrm{Tr}_k^K : K \to k$ sont surjective. Montrer que $\ker(\mathrm{N}) = \mathbb{F}_{q^m}^{*q-1}$ et que $\ker(\mathrm{Tr}) = \{x^q - x \mid x \in \mathbb{F}_{q^m}\}$.