

Contrôle du 9 novembre 2011

Sans documents. La rédaction sera notée : soyez précis et rigoureux.

Exercice 1 (4,5 pts)

Soit $a \in (\mathbb{Z}/n\mathbb{Z})^*$. Rappeler la définition de l'ordre de a .

0,5 pt

Montrer que l'ensemble $\{a^k, k \in \mathbb{N}\} = \{a^r, 0 \leq r < \text{ordre}(a)\}$ et qu'il a $\text{ordre}(a)$ éléments.

1+1 pt

Soit un entier $k > 0$. Montrer que si $a^k = 1$ alors l'ordre de a divise k .

1 pt

Montrer que l'ordre de a divise $\varphi(n)$.

1 pt

Exercice 2 (4,5 pts)

Soit $a \in (\mathbb{Z}/n\mathbb{Z})^*$ et un entier $d > 0$. On pose $b = a^d [n]$.

Montrer que b est inversible modulo n .

0,5 pt

Montrer que

2+2 pts

$$\text{ordre}(b) = \frac{\text{ordre}(a)}{\text{pgcd}(d, \text{ordre}(a))}$$

Exercice 3 (11 pts)

1. Rappeler la définition de générateur de $(\mathbb{Z}/n\mathbb{Z})^*$.

0,5 pt

Montrer que a est un générateur de $(\mathbb{Z}/n\mathbb{Z})^*$ si et seulement si $\text{ordre}(a) = \varphi(n)$.

1,5 pt

2. On suppose a générateur de $(\mathbb{Z}/n\mathbb{Z})^*$.

Comment calculer les autres générateurs en utilisant l'exercice 2 ?

1 pt

Combien y a-t-il de générateurs ?

1 pt

3. Montrer que 2 est un générateur de $(\mathbb{Z}/11\mathbb{Z})^*$.

1 pt

Calculer les autres générateurs de $(\mathbb{Z}/11\mathbb{Z})^*$.

1 pt

4. On suppose disposer d'une fonction Maple `Générateur:=proc(n) ... end` qui rend un générateur de $(\mathbb{Z}/n\mathbb{Z})^*$ s'il existe, FAIL sinon.

Écrire une fonction Maple `Générateurs:=proc(n) ... end` qui rende l'ensemble, éventuellement vide, des générateurs de $(\mathbb{Z}/n\mathbb{Z})^*$.

5 pts

Exercice 4 (? pts)

En utilisant l'isomorphisme $(\mathbb{Z}/22\mathbb{Z})^* \xrightarrow{\sim} (\mathbb{Z}/2\mathbb{Z})^* \times (\mathbb{Z}/11\mathbb{Z})^*$ qu'on ne demande pas de démontrer (c'est la version abstraite du théorème chinois),

1. Montrez que $(\mathbb{Z}/22\mathbb{Z})^*$ a un générateur et calculez le.

2. Calculez tous les générateurs de $(\mathbb{Z}/22\mathbb{Z})^*$.

Généralisation : Si $(\mathbb{Z}/n\mathbb{Z})^*$, n impair, a un générateur alors $(\mathbb{Z}/2n\mathbb{Z})^*$ a un générateur.