

## Corrigé du 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

*Solution* : L'ordre de l'élément inversible  $a$  est le plus petit entier  $d > 0$  tel que  $a^d = 1$ .

On pose  $d = \text{ordre}(a)$  et on fait la division euclidienne de  $k$  par  $d$ , toujours possible puisque  $d \neq 0$ ,  $k = dq + r$  donc  $a^k = (a^d)^q a^r = a^r$  avec  $0 \leq r < \text{ordre}(a)$ . On a donc  $\{a^k, k \in \mathbb{N}\} = \{a^r, 0 \leq r < \text{ordre}(a)\}$ .

Pour montrer que  $\{a^r, 0 \leq r < \text{ordre}(a)\}$  a  $\text{ordre}(a)$  éléments il faut montrer que les  $a^r, 0 \leq r < \text{ordre}(a)$  sont tous distincts. Si  $a^i = a^j$  avec  $0 \leq i \leq j < \text{ordre}(a)$  alors  $a^{j-i} = 1$  avec  $0 \leq j - i < \text{ordre}(a)$  donc  $j - i = 0$  d'après la définition de  $\text{ordre}(a)$  et  $i = j$ .

Toujours avec les notations précédentes on a  $k = dq + r$  donc  $a^k = a^r = 1$  avec  $0 \leq r < \text{ordre}(a)$ , d'après la définition de  $\text{ordre}(a)$  on a  $r = 0$  et  $k = dq$ .

Comme  $a$  est inversible on a  $a^{\varphi(n)} = 1$  (théorème d'Euler) donc  $\text{ordre}(a)$  divise  $\varphi(n)$ .

### Exercice 2 (4,5 pts)

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

0,5 pt

Montrer que  $b$  est inversible modulo  $n$ .

Montrer que

2+2 pts

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

*Solution* :  $a$  est inversible, soit  $a'$  son inverse alors  $b(a')^d = (aa')^d = 1$ .

On a  $b^{\frac{\text{ordre}(a)}{\text{pgcd}(d, \text{ordre}(a))}} = (a^d)^{\frac{\text{ordre}(a)}{\text{pgcd}(d, \text{ordre}(a))}} = (a^{\text{ordre}(a)})^{\frac{d}{\text{pgcd}(d, \text{ordre}(a))}} = 1$  donc  $\text{ordre}(b)$  divise  $\frac{\text{ordre}(a)}{\text{pgcd}(d, \text{ordre}(a))}$ .

On a  $b^{\text{ordre}(b)} = 1 = a^{d \cdot \text{ordre}(b)}$  donc  $\text{ordre}(a)$  divise  $d \cdot \text{ordre}(b)$

donc  $\frac{\text{ordre}(a)}{\text{pgcd}(d, \text{ordre}(a))}$  divise  $\frac{d}{\text{pgcd}(d, \text{ordre}(a))} \cdot \text{ordre}(b)$

or  $\frac{\text{ordre}(a)}{\text{pgcd}(d, \text{ordre}(a))}$  et  $\frac{d}{\text{pgcd}(d, \text{ordre}(a))}$  sont premiers entre eux donc  $\frac{\text{ordre}(a)}{\text{pgcd}(d, \text{ordre}(a))}$  divise  $\text{ordre}(b)$

et finalement

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

### 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 `Generateur:=proc(n) ... end` qui rend un générateur de  $(\mathbb{Z}/n\mathbb{Z})^*$  s'il existe, `FAIL` sinon.  
 Écrire une fonction Maple `Generateurs:=proc(n) ... end` qui rende l'ensemble, éventuellement vide, des générateurs de  $(\mathbb{Z}/n\mathbb{Z})^*$ . 5 pts

*Solution :*

- $a$  est un générateur de  $(\mathbb{Z}/n\mathbb{Z})^*$  si  $\{a^k, k \in \mathbb{N}\} = (\mathbb{Z}/n\mathbb{Z})^*$ .  
 L'ensemble  $\{a^k, k \in \mathbb{N}\}$  a  $\text{ordre}(a)$  éléments (cf. exercice 1) et est inclus dans  $(\mathbb{Z}/n\mathbb{Z})^*$  qui a  $\varphi(n)$  éléments par définition de  $\varphi(n)$ . Ces deux ensembles sont donc égaux si et seulement si  $\text{ordre}(a) = \varphi(n)$ .
- $b = a^k$  (puisque  $a$  est un générateur) est lui-même un générateur si et seulement si  $\text{ordre}(b) = \varphi(n)$ . Mais  $\text{ordre}(b) = \frac{\text{ordre}(a)}{\text{pgcd}(k, \text{ordre}(a))}$  (cf. exercice 2) et  $\text{ordre}(a) = \varphi(n)$  d'après 1. donc  $b = a^k$  est un générateur si et seulement si  $\text{pgcd}(k, \varphi(n)) = 1$ . On calcule donc les  $a^k$  pour  $2 \leq k \leq \varphi(n) - 1$  et  $k$  premier avec  $\varphi(n)$ .  
 Les générateurs sont les  $a^k$  avec  $k$  premier avec  $\varphi(n)$ , il y en a donc  $\varphi(\varphi(n))$ .
- On sait que  $2^{10} = 1 \pmod{11}$ , donc l'ordre de 2 est un diviseur de 10.  
 Or  $2^2 = 4 \neq 1 \pmod{11}$  et  $2^5 = 32 = 10 = -1 \pmod{11}$  donc 2 est d'ordre  $10 = \varphi(11)$ , 2 est un générateur de  $(\mathbb{Z}/11\mathbb{Z})^*$ .  
 Les autres générateurs sont les  $2^k$  avec  $k$  premier avec  $\varphi(11)$ . Les générateurs de  $(\mathbb{Z}/11\mathbb{Z})^*$  sont  $\{2, 2^3, 2^7, 2^9\} = \{2, 6, 7, 8\}$ . On remarque qu'il y en a  $4 = \varphi(\varphi(11))$ .
- C'est l'application de la question 2.

```

Generateurs:=proc(n)
local a,s,k,phin;
a:=Generateur(n);
if a=FAIL then {}
else s:=a;phin:=phi(n);
  for k from 2 to phin-1 do
    if igcd(k,phin)=1 then s:=s,a&^k mod n fi
  od;
{s} fi
end
  
```

#### 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),

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

*Solution rapide :* On remarque que  $(\mathbb{Z}/2\mathbb{Z})^* = \{1\}$  donc si  $a$  est un générateur de  $(\mathbb{Z}/11\mathbb{Z})^*$   $(1, a)$  est un générateur de  $(\mathbb{Z}/2\mathbb{Z})^* \times (\mathbb{Z}/11\mathbb{Z})^*$  et son antécédent un générateur de  $(\mathbb{Z}/22\mathbb{Z})^*$ .

- 2 est un générateur de  $(\mathbb{Z}/11\mathbb{Z})^*$  donc  $x$  tel que  $(x = 1 \pmod{2}, x = 2 \pmod{11})$  est un générateur de  $(\mathbb{Z}/22\mathbb{Z})^*$ , donc  $x = 2 + 11 = 13$  est un générateur de  $(\mathbb{Z}/22\mathbb{Z})^*$ .
- Les autres générateurs correspondent à  $(x = 1 \pmod{2}, x = 6 \pmod{11})$ ,  $(x = 1 \pmod{2}, x = 7 \pmod{11})$  et  $(x = 1 \pmod{2}, x = 8 \pmod{11})$  soit  $x = 6 + 11 = 17$ ,  $x = 7$  et  $x = 8 + 11 = 19$ .

Généralisation : dans la remarque du début remplacer 11 par  $n$ .