Chapitre 4

Groupe des inversibles de $\mathbb{Z}/nZ$ et applications

4.1 Rappels et exemples

$$\mathcal{U}(\mathbb{Z}/nZ) = \{\overline{k},\ PGCD(k,n) = 1\}$$

est le groupe des éléments inversibles de $\mathbb{Z}/nZ$; c'est aussi l'ensemble des générateurs (éléments d'ordre n) dans le groupe additif $\mathbb{Z}/nZ$.

Exercice 4.1.1. Démontrer que l'ordre de $\overline{k}$ dans $(\mathbb{Z}/nZ, +)$ est $\frac{n}{PGCD(k,n)}$.

Définition 4.1.2. Pour un entier $n \geq 2$), l'indicateur d'Euler $\phi(b)$ est le nombre d'éléments inversibles dans $\mathbb{Z}/n\mathbb{Z}$, c'est à dire le nombre d'éléments du groupe $\mathcal{U}(\mathbb{Z}/nZ)$.

Exemples.

Théorème 4.1.3. *Pour a et b premiers entre eux, on a un isomorphisme :*

$$\mathbb{Z}/ab\mathbb{Z} \simeq \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}\ .$$

Corollaire 4.1.4. *Pour a et b premiers entre eux, on a : $\phi(ab) = \phi(a)\phi(b)$.*

Théorème 4.1.5. *Pour p premier et $\alpha > 0$, on a : $\phi(p^\alpha) = (p-1)p^{\alpha-1}$.*

4.2 Structure de $\mathcal{U}(\mathbb{Z}/pZ)$ pour p premier

Théorème 4.2.1. *Le groupe $\mathcal{U}(\mathbb{Z}/pZ) = (\mathbb{Z}/p\mathbb{Z})^*$ est engendré par un seul élément ; on dit qu'il est cyclique.*

Cela revient à dire qu'il existe un élément d'ordre $p-1$. Pour la preuve, on va considérer les polynômes à coefficient dans $\mathbb{Z}/p\mathbb{Z}$.

Théorème 4.2.2. *Un polynôme de degré m à coefficients dans un corps (par exemple $\mathbb{Z}/p\mathbb{Z}$, avec p premier) a au plus n racines.*

La dérivation est définie pour les polynômes à coefficients dans $\mathbb{Z}/p\mathbb{Z}$, et la formule habituelle de dérivation d'un produit est valide.

Proposition 4.2.3. *Soit P est un polynôme à coefficients dans $\mathbb{Z}/p\mathbb{Z}$. Si $a \in \mathbb{Z}/p\mathbb{Z}$ est tel que :*

$$P(a) = 0 \quad et \quad P'(a) \neq 0 \ ,$$

alors a est racine simple, i.e. $P = (X-a)Q$ avec $Q(a) \neq 0$.

Corollaire 4.2.4. *Le PPCM des ordres des éléments du groupe $(\mathbb{Z}/p\mathbb{Z})^*$ est égal à $p-1$.*

On obtient la preuve du théorème en démontrant qu'il existe un élément d'ordre $p-1$. Cela résulte du résultat général suivant.

Proposition 4.2.5. *Soit G un groupe abélien fini, m le PPCM des ordres de ses éléments. Alors G contient un élément d'ordre m.*

4.3 Structure de $\mathcal{U}(\mathbb{Z}/p^\alpha Z)$

4.3.1 Cas p premier impair

Théorème 4.3.1. *Le groupe $(\mathcal{U}(\mathbb{Z}/p^\alpha Z), \times)$ est cyclique.*

Cela revient à dire qu'il existe un élément d'ordre $\phi(p) = (p-1)p^{\alpha-1}$. Le lemme suivant montre que $a = 1+p$ est d'ordre $p^{\alpha-1}$.

Lemme 4.3.2. *Pour p premier, $k \geq 0$:*

$$(1+p)^{p^k} \equiv 1 + p^{k+1} \pmod{p^{k+2}} \ .$$

Lemme 4.3.3. *$\mathcal{U}(\mathbb{Z}/p^\alpha Z)$ contient un élément b d'ordre $p-1$.*

L'élément ab est d'ordre $(p-1)p^{\alpha-1}$.

4.3.2 Cas $p = 2$, $\alpha \geq 3$

Le groupe $\mathcal{U}(\mathbb{Z}/2^\alpha Z)$ est de cardinal $2^{\alpha-1}$.

Théorème 4.3.4. *Pour $\alpha \geq 3$*
a) Le groupe $(\mathcal{U}(\mathbb{Z}/2^\alpha\mathbb{Z}), \times)$ n'est pas cyclique.
b) Dans $\mathcal{U}(\mathbb{Z}/2^\alpha Z)$ la classe $\overline{5}$ est d'ordre $p^{\alpha-2}$.
c) Tout élément de $\mathcal{U}(\mathbb{Z}/2^\alpha Z)$ s'écrit sous la forme $\pm\overline{5}^k$.
d) Les éléments de $\mathcal{U}(\mathbb{Z}/2^\alpha Z)$ sont d'ordre 2^k, avec $k \leq \alpha - 2$.

Lemme 4.3.5. *Pour $k \geq 0$:*

$$(1+4)^{2^k} \equiv 1 + 2^{k+2} \pmod{2^{k+3}} .$$

4.4 Application à l'étude de la primalité

Définition 4.4.1. a) Un nombre non premier (composé) est pseudo-premier pour la base a si et seulement si : $a^{n-1} \equiv 1 \pmod{n}$.
b) Un nombre non premier n est de Carmichael si et seulement s'il est pseudo-premier pour toute base première avec n.

Théorème 4.4.2. *Un nombre non premier n est de Carmichael si et seulement si pour tout diviseur premier de n :*
a) $p - 1$ divise $n - 1$,
b) p^2 ne divise pas n.

Exercice 4.4.3. Démontrer qu'un nombre Carmichael a au moins 3 diviseurs premiers.

Test de Miller-Rabin.
Entrée : entier impair n à tester, entier t donnant le nombre de *témoins*.

```
[recherche de la plus grande puissance de 2 qui divise n − 1]
b ← 0 ;r ← n − 1 ;
Tant que (r est pair) faire
    | b ← b + 1 ;r ← r/2 ;
Fait
Pour j de 1 à t faire
    | choisir au hasard d entre 2 et n − 2 ;
    | d ← (d^r mod n) ;
    | Si (d ≠ 1) Alors
    |     | k ← 0 ;
    |     | Tant que (k < b et d ≠ n − 1) faire
    |     |     | d ← (d^2 mod n) ;k ← k + 1 ;
    |     | Fait
    |     | Si (d ≠ n − 1) Alors
    |     |     | Sortie("non premier") ;
    |     | Fin Si
    | Fin Si
Fin Pour
Sortie("très probablement premier") ;
```

Algorithme 7: Test de Miller-Rabin

Le théorème suivant démontre que le test de Miller-Rabin est correct :

Théorème 4.4.4. *Si p est premier impair, et si $n - 1 = 2^b r$, avec r impair, alors pour tout a premier avec n :*
soit $a^r \equiv 1 \pmod{n}$,
soit il existe k , $0 \leq k < b$, tel que : $a^{r2^k} \equiv -1 \pmod{n}$.