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 générareurs du groupe additif $\mathbb{Z}/nZ$.

Exemples.

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.*

Corollaire 4.2.3. *Le PPCM des ordres des éléments du groupe $(\mathbb{Z}/p\mathbb{Z})^*$ est égal à $p-1$.*

Proposition 4.2.4. *Si un groupe commutatif contient un élément x d'ordre a, et un élément y d'ordre b, alors il contient un élément z d'ordre $PPCM(a,b)$.*

On obtient la preuve du théorème comme corollaire : $(\mathbb{Z}/p\mathbb{Z})^*$ contient un élément d'ordre $p-1$ qui est le PPCM des ordres de tous les éléments.

4.3 Structure de $\mathcal{U}(\mathbb{Z}/p^2Z)$ pour p premier

Théorème 4.3.1. *Le groupe* $\mathcal{U}(\mathbb{Z}/pZ) = (\mathbb{Z}/p^2\mathbb{Z})^*$ *est cyclique.*

Cela revient à dire qu'il existe un élément d'ordre $\phi(p) = p(p-1)$.

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 et d ≠ n − 1) Alors
    |     | k ← 0 ;
    |     | Tant que (k < b) faire
    |     |     | d ← (d^2 mod n) ;k ← k + 1 ;
    |     |     | Si (d = 1) Alors
    |     |     |     | Sortie("non premier") ;
    |     |     | Fin Si
    |     | Fait
    | Fin Si
    | Si (d ≠ b − 1) Alors
    |     | Sortie("non premier") ;
    | Fin Si
    | Sortie("très probablement premier") ;
Fin Pour
```

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 : $a^{r2^k} \equiv -1 \pmod{n}$.

Chapitre 5

Résidus quadratiques

5.1 Résidus quadratiques modulo un premier

Définition 5.1.1. Soit p un nombre premier. Un élément $\overline{a} \in (\mathbb{Z}/p\mathbb{Z})^*$ est un résidu quadratique si et seulement si c'est un carré. On dit aussi que l'entier a est un résidu quadratique modulo p.

Théorème 5.1.2. *Soit $p = 2l + 1$ un nombre premier impair.*
a) Les résidus quadratiques modulo p forme un sous-groupe de cardinal l de $(\mathbb{Z}/p\mathbb{Z})^*$.
b) $\overline{a} \in \mathbb{Z}/p\mathbb{Z}$ est un résidu quadratique si et seulement si : $\overline{a}^l = \overline{1}$ dans $\mathbb{Z}/p\mathbb{Z}$.
c) -1 est un résidu quadratique modulo p si et seulement si $p \equiv 1$ (mod 4).

5.2 Symbole de Legendre

Définition 5.2.1. Soit p est nombre premier, et a un entier. Le symbole de Legendre noté $\left(\frac{a}{p}\right)$ vaut :

0 si p divise a,
1 si $\overline{a} \in (\mathbb{Z}/p\mathbb{Z})^*$ est un carré (résidu quadratique),
-1 si $\overline{a} \in (\mathbb{Z}/p\mathbb{Z})^*$ n'est pas un carré (non-résidu quadratique).

Remarque 5.2.2. Si $a \equiv b \pmod p$, alors $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

Proposition 5.2.3. *a) Pour p premier impair, $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$.*
b) Pour p premier impair et a premier avec p, $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}}$ (mod p).
c) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.

Théorème 5.2.4 (Réciprocité quadratique)**.** *Pour p et q premiers impairs, on a :*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{4}\frac{q-1}{4}} = \begin{cases} -1 & \text{si } p \text{ et } q \text{ sont congrus à } 3 \text{ modulo } 4, \\ 1 & \text{si } p \text{ ou } q \text{ est congru à } 1 \text{ modulo } 4. \end{cases}$$

On pourra trouver une démonstration (d'après Zolotarev) à l'adresse : http ://math.unice.fr/∼serman/recip.pdf.

5.3 Symbole de Jacobi

On étend le symbole de Legendre au cas de nombres qui ne sont plus nécessairement premiers.

Définition 5.3.1. Si b est le produit des nombres premiers $p_1,\ldots,p_m$, alors :

$$\left(\frac{a}{b}\right) = \prod_{j=1}^{m} \left(\frac{a}{p_j}\right) .$$

Proposition 5.3.2. *a)* $\left(\frac{a}{b}\right) = 0$ *si et seulement si* $PGCD(a,b) > 1$.
b) $\left(\frac{1}{p}\right) = 1$, *et* $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.
c) Si $a \equiv a'$ *(mod b), alors* $\left(\frac{a}{b}\right) = \left(\frac{a'}{b}\right)$.
d) Si a et b sont premiers entre eux et impairs, alors :

$$\left(\frac{a}{b}\right)\left(\frac{b}{a}\right) = (-1)^{\frac{a-1}{2}\frac{b-1}{2}} = \begin{cases} -1 & \textit{si } a \textit{ et } b \textit{ sont congrus à } 3 \textit{ modulo } 4, \\ 1 & \textit{si } a \textit{ ou } b \textit{ est congru à } 1 \textit{ modulo } 4. \end{cases}$$

e) $\left(\frac{2}{b}\right) = (-1)^{\frac{b^2-1}{4}} = \begin{cases} 1 & \textit{si } a \textit{ est congru à } \pm 1 \textit{ modulo } 8, \\ -1 & \textit{si } b \textit{ est congru à } \pm 3 \textit{ modulo } 8. \end{cases}$

5.4 Application aux tests de primalité

5.4.1 Nombres de Fermat

Le n-ième nombre de Fermat est : $F_n = 2^{2^n} + 1$.

Proposition 5.4.1. *Si un nombre premier p divise* F_n, $n \geq 2$, *alors il est de la forme*

$$p = k2^{n+2} + 1 .$$

Exercice 5.4.2. Soit a un élément d'un groupe G noté multiplicativement, de neutre e. Montrer que s'il existe un nombre premier p et un entier k tels que :

$$a^{p^k} = e \text{ , et } a^{p^{k-1}} \neq e ,$$

alors a est d'ordre p^k.

Théorème 5.4.3 (Critère de Pépin)**.** *Le nombre de Fermat* F_n, $n \geq 1$, *est premier si et seulement si*

$$3^{\frac{F_n-1}{2}} \equiv -1 \mod F_n .$$

5.4.2 Test de Solovay et Strassen

Théorème 5.4.4. *Soit $n > 2$ un entier impair.*
a) $G_n = \{\overline{a} \in \mathbb{Z}/n\mathbb{Z},\ 0 \neq \left(\frac{a}{n}\right) \equiv a^{\frac{n-1}{2}} \bmod n\}$ est un sous groupe de $(\mathcal{U}(\mathbb{Z}/n\mathbb{Z}), \times)$.
b) Si n est premier, alors : $G_n = (\mathcal{U}(\mathbb{Z}/n\mathbb{Z}), \times)$ est de cardinal $n-1$.
c) Si n n'est pas premier, alors G_n est de cardinal inférieur ou égal à $\frac{n-1}{2}$.

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

Pour i **de** 1 **à** t **faire**
  choisir au hasard a entre 2 et $n-2$;
  $p \leftarrow (a^{\frac{n-1}{2}} \bmod n)$;
  Si ($p \neq 1$ et $p \neq n-1$) **Alors**
    Sortie("non premier") ;
  Fin Si
  $j \leftarrow \left(\frac{a}{n}\right)$;
  Si ($p \neq (j \bmod n)$) **Alors**
    Sortie("non premier") ;
  Fin Si
Fin Pour
Sortie("très probablement premier") ;

Algorithme 8: Test de Solovay et Strassen

Remarque 5.4.5. En utilisant un algorithme de calcul rapide de puissances, on obtient une complexité $O(t\log(n)^3)$. La probabilité pour qu'un nombre non premier ne soit pas détecté est inférieure à 2^{-t}.