Chapitre 3

Groupe des inversibles de $\mathbb{Z}/nZ$ et recherche de nombres premiers

Introduction

Rappel : $(\mathbb{Z}/nZ)^* = \{\overline{k},\ PGCD(k,n) = 1\}$ est le groupe des éléments inversibles de $\mathbb{Z}/nZ$.
Exemples, détermination de l'ordre des éléments, problème d'existence d'un générateur.

3.1 Structure de $(\mathbb{Z}/pZ)^*$ pour p premier

Théorème 3.1.1. *Pour tout entier premier p, le groupe $(\mathbb{Z}/p\mathbb{Z})^*$ 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 le corps $\mathbb{Z}/p\mathbb{Z}$.

Théorème 3.1.2. *Un polynôme de degré m à coefficients dans un corps (par exemple $\mathbb{Z}/p\mathbb{Z}$, avec p premier) a au plus m racines.*

Corollaire 3.1.3. *Le PPCM des ordres des éléments du groupe $(\mathbb{Z}/p\mathbb{Z})^*$ est égal à $p-1$.*

Exercice 3.1.4. Montrer que dans un groupe multiplicatif, si x est d'ordre $a = bc$, b et c étant des entiers positifs, alors $y = x^b$ est d'ordre c.

Exercice 3.1.5. Montrer que dans un groupe multiplicatif commutatif, si x est d'ordre a et y d'ordre b avec a et b premiers entre eux, alors xy est d'ordre ab.

Proposition 3.1.6. *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.

3.2 Test de Fermat et nombres de Carmichael

Rappel : Le test de Fermat s'appuie sur le théorème de Fermat : Pour p premier, on a : $a^{p-1} \equiv 1 \pmod{p}$ pour tout a premier avec p.

Si pour un nombre n impair on trouve $2 \leq a < n$ tel que a^{n-1} n'est pas congru à 1 modulo n, alors on dit que a est témoin de la non primalité de n. Il existe des nombres impairs non premiers (composés) qui sont difficilement détectables avec le test de Fermat, dans le sens qu'en choisissant a au hasard on a peu de chance d'obtenir un témoin de non primalité.

Définition 3.2.1. Un nombre impair non premier n est de Carmichael si et seulement si pour tout a premier avec n on a : $a^{n-1} \equiv 1 \pmod{n}$

Théorème 3.2.2. *Un nombre impair 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.

Le plus petit nombre de Carmichael est $561 = 3 \times 11 \times 17$.

Fin du cours 20/02

Exercice 3.2.3. 1. Combien y a-t-il de nombre premiers avec 561 entre 2 et 560 ?
2. Quelle est la probabilité que le test de Fermat détecte que 561 est non premier,
a) avec un témoin ? b) avec deux témoins ? c) avec k témoins ?

Exercice 3.2.4. Démontrer qu'un nombre de 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 ;
While (r est pair) do
    | b ← b + 1 ; r ← r/2 ; // n − 1 = 2^b r r impair
done
For j from 1 to t do
    | choisir au hasard d entre 2 et n − 2 ;
    | d ← (d^r mod n) ; // positif si d vaut 1 ou n − 1
    | If (d ≠ 1 et d ≠ n − 1) then
    |     | k ← 1 ;
    |     | While (k < b et d ≠ n − 1 ) do
    |     |     | d ← (d^2 mod n) ; k ← k + 1 ; // calcul des carrés successifs
    |     |     | If (d = 1) then
    |     |     |     | Sortie("non premier") ; // plus d'espoir de trouver −1 : négatif
    |     |     | end If
    |     | done
    | end If
    | If (d ≠ n − 1) then
    |     | Sortie("non premier") ;
    | end If
end For
Sortie("très probablement premier") ;
```

Algorithm 6: Test de Miller-Rabin

Exercice 3.2.5. 1. En s'appuyant sur le théorème suivant, justifier le test de Miller-Rabin. 2. On admet que dans le test de Miller-Rabin le nombre de faux témoins pour un entier n non premier est au plus $n/4$. Combien de témoins suffisent pour que la réponse positive soit exacte avec une probabilité supérieure à $1 - \epsilon$ (A.N. $\epsilon = 10^{-6}$).

La validité du test de Miller-Rabin pour la réponse *non premier* :

Théorème 3.2.6. *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 : $a^{r2^k} \equiv -1 \pmod{n}$.

Remarque 3.2.7. On démontre que pour un nombre non premier la proportion de témoins qui détectent la non primalité dépasse $\frac{3}{4}$.

Exercice 3.2.8. Ecrire une fonction python **MRtemoin(n)** qui compte le nombre de témoin de la non primalité de n avec le test de Miller-Rabin. On utilisera **MillerRabin(n,d)** qui retourne **True** ou **False**.

3.3 Structure de $(\mathbb{Z}/p^mZ)^*$ pour p premier

Théorème 3.3.1. *Pour p premier impair et pour $m > 0$, le groupe $= (\mathbb{Z}/p^m\mathbb{Z})^*$ est cyclique.*

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

Théorème 3.3.2. *Pour $m \geq 3$, le groupe $= (\mathbb{Z}/2^m\mathbb{Z})^*$ n'est pas cyclique. L'élément $\overline{5}$ est d'ordre 2^{m-2}, et tout élément s'écrit sous la forme $\pm\overline{5}^k$.*