Chapitre 3

Anneau des classes de congruence

3.1 Anneau $\mathbb{Z}/n\mathbb{Z}$

Théorème 3.1.1. *La multiplication est bien définie dans $\mathbb{Z}/n\mathbb{Z}$, et $\mathbb{Z}/n\mathbb{Z}$ avec addition et multiplication est un anneau commutatif.*

Théorème 3.1.2. *La classe $\overline{k}$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$ si et seulement si k et n sont premiers entre eux.*

Exercice 3.1.3. Montrer qu'un élément de $\mathbb{Z}/n\mathbb{Z}$ est inversible si et seulement s'il est générateur du groupe $(\mathbb{Z}/n\mathbb{Z}, +)$.

Corollaire 3.1.4. *$\mathbb{Z}/p\mathbb{Z}$ est un corps si et seulement si p est un nombre premier.*

Proposition 3.1.5. *L'ensemble des éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$ muni de la multiplication forme un groupe.*

Notation : $\mathcal{U}(\mathbb{Z}/n\mathbb{Z})$.

3.2 Petit théorème de Fermat

Théorème 3.2.1. *Si p est un nombre premier, alors pour tout k qui n'est pas multiple de p, on a : $k^{p-1} \equiv 1 \pmod{p}$*

La réciproque de ce théorème est fausse, par exemple : $561 = 3 \times 11 \times 17$ n'est pas premier et pourtant pour tout entier a premier avec 561, on a $a^{560} \equiv 1 \pmod{561}$.

Le théorème de Fermat donne un test de primalité : si pour un entier $a < n$, on a $a^{n-1} \not\equiv 1 \pmod{n}$, alors n n'est pas premier ; si pour plusieurs valeurs de a, on a $a^{n-1} \equiv 1 \pmod{n}$, alors n est probablement premier.

Calcul rapide des puissances modulo n.

```
Fonction puissance(a,m,n) // entier, exposant, module
R ← 1 ;
Tant que (m > 0) faire
    Si (m est impair) Alors
        R ← (R × a)mod n ;
    Fin Si
    a ← (a × a)mod n ;
    m ← m/2 ; // la division par 2 est un décalage binaire (shift)
Fait
Retouner R ;
```

Algorithme 6: Calcul rapide des puissances modulo n

Théorème 3.2.2. *L'algorithme précédent calcul a^m modulo n, avec au plus $2(\log_2(m)+1)$ multiplications modulo n.*

Remarque 3.2.3. On montre que le coût d'une multipliation modulo n est $O(\log(n)^2)$. La complexité de l'algorithme est donc $O(\log(m)\log(n)^2)$.

3.3 Théorème chinois

Théorème 3.3.1. *Si a et b sont premiers entre eux, alors l'application qui à $\overline{k} \in \mathbb{Z}/ab\mathbb{Z}$ associe $(\dot{k}, \hat{k}) \in \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$ est bijective.*
Si (u, v) est un couple de Bezout : $au + vb = 1$, alors l'application réciproque associe à $(\dot{\alpha}, \hat{\beta}) \in \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$ la classe de $\overline{k} = \overline{vb\alpha + ua\beta} \in \mathbb{Z}/ab\mathbb{Z}$.

La reformulation en termes de congruence est :

Théorème 3.3.2 (Théorème chinois)**.** *Si a et b sont premiers entre eux, et $au+vb = 1$, alors le système de congruence :*

$$\begin{cases} x & \equiv & \alpha & (\text{mod } a) \\ x & \equiv & \beta & (\text{mod } b) \end{cases}$$

est équivalent à :

$$x \equiv vb\alpha + ua\beta \quad (mod\ ab)\ .$$

3.4 Indicateur d'Euler

Définition 3.4.1. 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 $\mathcal{U}(\mathbb{Z}/nZ)$.

Théorème 3.4.2 (Théorème de Fermat généralisé)**.** *Pour tout entier k premier avec n, on a :*

$$k^{\phi(n)} \equiv 1 \pmod{n} .$$

Théorème 3.4.3. *a) Pour p premier et $\alpha > 0$, $\phi(p^\alpha) = p^\alpha - p^{\alpha-1}$.*
b) Pour a et b premiers entre eux, $\phi(ab) = \phi(a)\phi(b)$.
c) Si $n = \prod_i p_i^{\alpha_i}$ est la décomposition en facteurs premiers, alors :

$$\phi(n) = \prod_i p_i^{\alpha_i} - p_i^{\alpha_i - 1} = n \prod_i (1 - \frac{1}{p_i}) .$$