Retour TP 4 – Corps finis I

► **Prérequis** : *Chapitre 4 du poly, jusqu'aux corps de rupture (§4.2.2 inclus).*

1 Inversion modulo n

Le type renvoyé est un entier modulo n.

2 Calculs dans les corps finis

1. Non, la commande `factor` n'a aucun effet car la factorisation dépend du corps de base qui ici n'est pas spécifié.

Une façon de manipuler des polynômes à coefficients dans un anneau R avec `Sage` consiste à définir l'anneau $A = R[X]$ de la façon suivante :

```
A.<X>=PolynomialRing(R)
```

3. On commence par obtenir une factorisation du polynôme $X^{p^d} - X$ avec la commande `factor` et on utilise le fait que tout polynôme irréductible de degré d sur $\mathbf{F}_p$ le divise. On parcourt alors la liste des diviseurs irréductibles de $X^{p^d} - X$ jusqu'à en trouver un de degré d.

4. Pour définir le domaine *corps de rupture de P sur $\mathbf{F}_2$*, on utilise la commande `K.<z>=GF(2**5,modulus = P)` comme étant le corps fini $\mathbf{F}_{2^5}$ défini comme corps de rupture de P :

$$\mathbf{F}_{2^5} \cong \mathbf{F}_2[X]/(P).$$

6. La méthode utilisée ci-dessus pour déterminer un polynôme irréductible pour $p = 2$ et $d = 42$ fonctionne en théorie mais $2^{42} = 4398046511104$ est beaucoup trop grand pour permettre d'obtenir un résultat en un temps raisonnable [1].

7. Tirer un polynôme unitaire de degré d au hasard est en réalité beaucoup plus efficace ! En effet, soit p un nombre premier. On a alors p^d polynômes unitaires de degré d dans $\mathbf{F}_p[X]$. Par ailleurs, le nombre de polynômes irréductibles unitaires de degré d est donné par

$$N_d = \frac{1}{d} \sum_{\ell | d} \mu(\ell) p^{\frac{d}{\ell}}$$

où $\mu : \mathbf{N}^* \to \{-1, 0, 1\}$ est la fonction de Möbius définie par $\mu(1) = 1$ et

$$\mu(n) = \begin{cases} \mu(n) = 0 \text{ s'il existe un nombre premier } p \text{ tel que } p^2 \mid n \\ \mu(n) = (-1)^n \text{ si } n = \prod_{i=1}^{r} p_i \text{ avec } r \in \mathbf{N}^* \text{ et } p_1, \ldots, p_r \text{ premiers distincts.} \end{cases}$$

On a en particulier [2]

$$N_d = \frac{p^d}{d} + O\left(p^{\frac{d}{2}}\right)$$

de sorte que la probabilité $\mathbb{P}_d$ qu'un polynôme unitaire tiré uniformément au hasard de degré d soit irréductible vérifie à p fixé

$$\mathbb{P}_d \underset{d \to +\infty}{\sim} \frac{1}{d}.$$

Ici, il faudra donc en moyenne une quarantaine d'essais avant de trouver un polynôme irréductible de degré 42 dans $\mathbf{F}_2[X]$.

1. Et d'ailleurs faire le test permet de déclencher un message d'erreur *"The kernel has died."*.
2. On peut montrer de façon plus précise que

$$\frac{p^d - p^{\lfloor \frac{d}{2} \rfloor + 1}}{d} \leqslant N_d \leqslant \frac{p^d}{d}.$$

3 Générateurs de $\mathbf{F}_q^\times$

8. On a que le groupe $\mathbf{F}_{32}^\times$ est d'ordre 31 qui est premier. Ainsi, tout élément différent de 1 de $\mathbf{F}_{32}^\times$ est générateur (car son ordre est différent de 1 et doit diviser 31), d'où le résultat.

9. Le polynôme $P = X^3 - X + 1$ de degré 3 et sans racine dans $\mathbf{F}_3$ donc irréductible sur $\mathbf{F}_3[X]$. En effet, en notant $\overline{n}$ la classe de n dans $\mathbf{Z}/3\mathbf{Z}$, on a

$$P(\overline{0}) = P(\overline{1}) = P(\overline{2}) = 1 \neq 0.$$

Pour vérifier que x est un générateur du groupe $\mathbf{F}_{27}^\times$, il suffit de vérifier que x est d'ordre 26. Puisque $26 = 2 \times 13$ et que tous les ordres possibles sont 1, 2, 13 ou 26, pour cela il suffit de vérifier que $x^2 \neq 1$ et $x^{13} \neq 1$.

10. Puisque $5^3 - 1 = 2^2 \times 31$, un élément de $\mathbf{F}_{5^3}^\times$ qui n'est pas générateur est d'ordre qui divise 4 ou $2 \times 31 = 62$. Il s'agit donc de déterminer un élément tel que $x^4 \neq 1$ et $x^{62} \neq 1$. Un candidat naturel à tenter est l'élément x engendrant $F_{5^3} = \mathbf{F}_5(x)$, à savoir la racine privilégiée du polynôme irréductible de degré 3 sur $\mathbf{F}_5$ dont on a construit F_{5^3} comme le corps de rupture sur $\mathbf{F}_5[X]$. Ici, cela fonctionne mais noter que cela dépend du choix du polynôme irréductible choisi au hasard! Cette méthode ne fonctionne pas dans tous les cas! Une meilleure méthode (décrite dans le cours avec description de la probabilité de succès) est alors de tirer un élément de F_{5^3} au hasard et de tester si $x^4 \neq 1$ et $x^{62} \neq 1$.

11. Ici, on peut remarquer que pour que y engendre $\mathbf{F}_{5^{10}}^\times$, il faut et il suffit que $y^{\frac{5^{10}-1}{p}} \neq 1$ pour tout nombre premier p divisant $5^{10} - 1$.

4 Comptage

Soit q une puissance d'un nombre premier. Si $\mathbf{F}_q$ est un corps fini à q éléments et N_d est le nombre de polynômes unitaires irréductibles de degré d dans $\mathbf{F}_q[X]$, alors on sait que

$$q^n = \sum_{d|n} dN_d.$$

12. Il suffit en degré inférieur à 3 de tester que le polynôme n'admet pas de racine et en degré 4 que polynôme n'admet pas de racine et n'est pas produit de deux irréductibles de degré 2 (dont on peut faire la liste). Évidemment cette méthode n'est pas efficace, elle nécessite de tester les divisibilités par toutes les partitions du degré et pour cela de garder la liste des polynômes irréductibles de degré inférieur, ce qui devient vite impraticable! On verra comment faire mieux dans la suite du cours!

13. On utilise le fait que

$$N_n = \frac{1}{n}\left(q^n - \sum_{\substack{d|n \\ d\neq n}} dN_d\right)$$

qui exprime N_n en fonction de quantités N_d avec $d < n$.