FEUILLE D'EXERCICES n° 12
Travail sur machine

On va programmer les algorithmes de factorisation sur un corps fini vus en cours afin de mieux comprendre leur fonctionnement. Pour simplifier, on va travailler sur $\mathbb{F}_p$, où p est premier.

On rappelle que pour définir $\mathbb{F}_p$ sur sage, on peut écrire

```
k=GF(p)
```

(où p est bien sûr préalablement défini). Ensuite, on définit l'anneau $k[x]$ par

```
pr.<x>=PolynomialRing(k)
```

Dans ces algorithmes, on doit faire des calculs modulo f (où f est le polynôme à factoriser). Pour cela, on définit l'anneau quotient $k[x]/(f)$:

```
AnneauQuotient.<z>=pr.quotient(f)
```

Alors z est l'image de x dans le quotient $k[x]/(f)$. Par exemple, si on veut calculer $h = x^p$ modulo f, on peut faire :

```
h=z**p
```

Si ensuite on veut considérer h comme un polynôme en x, on écrit

```
h.lift()
```

Plus généralement, si g est un polynôme en x et si on veut calculer g^i modulo f, on peut faire

```
(g(z)**i).lift()
```

Exercice 1 – [Factorisation en degrés distincts]
Soit p un nombre premier. Programmer l'algorithme de factorisation en degrés distincts sur $\mathbb{F}_p[x]$. L'essayer sur $x^6 + 2x^5 + x^4 + x^3 + 2x$ dans $\mathbb{F}_3[x]$, puis sur d'autres polynômes sans facteurs carrés dans $\mathbb{F}_p[x]$, où vous ferez varier p à votre convenance.

Exercice 2 – [Algorithme de Cantor-Zassenhaus]
Le programmer sur $\mathbb{F}_p$, où p est un nombre premier impair. et l'essayer sur des polynômes produits de polynômes irréductibles de même degré. Par exemple, l'essayer sur $x^8+8x^6+9x^4+6x^2+4 \in \mathbb{F}_{11}[x]$. Ici, le degré des polynômes irréductibles est égal à 2.

Exercice 3 – [Factorisation complète dans $\mathbb{F}_p[x]$]
Ici, p désigne toujours un nombre premier impair. Les polynômes sont dans $\mathbb{F}_p[x]$.

1) Écrire une fonction qui, étant donné un polynôme sans facteur carré dont tous les facteurs irréductibles sont de degré d, rend ces facteurs irréductibles. Cette fonction utilisera l'algorithme de Cantor-Zassenhaus de la question précédente, et s'appellera elle-même récursivement.

2) Écrire une fonction qui, étant donné un polynôme quelconque, donne sa décomposition complète.

Exercice 4 – [Racines dans $\mathbb{F}_p$ d'un polynôme de $\mathbb{F}_p[x]$]
Pour calculer ces racines, il suffit d'appliquer la méthode de “factorisation en degrés distincts” pour “$d = 1$”, puis d'appliquer l'algorithme de la question 1 de l'exercice précédent. Programmer cette fonction.

Exercice 5 – [Algorithme de Berlekamp]
Le programmer.