TP5 : Arithmétique modulaire et corps finis

1 Le théorème des restes chinois

Soient $n_1, ..., n_l$ des entiers deux à deux premiers entre eux. Notons $n = \prod_{i=1}^{l} n_i$.

1. Rappeler le théorème des restes chinois. Que se passe-t-il si les entiers ne sont pas premiers entre eux ?
2. Indiquer comment construire (algorithmiquement...) des entiers $e_1, ..., e_l$ tels que $\forall 1 \leq i \leq l$:
$$\begin{cases} e_i \equiv 1 \bmod n_i \\ e_i \equiv 0 \bmod n_j \quad \forall j \neq i \end{cases}$$
3. Expliquer comment, grâce à (2), pour tout l-uplet d'entiers $(a_1, ..., a_l)$, on peut construire l'unique $x \in \mathbb{Z}/n\mathbb{Z}$ tel que $\forall i \quad x \equiv a_i \bmod n_i$. À quel résultat cette méthode vous fait-elle penser ?
4. En déduire un algorithme `restes_chinois(A,N)` qui prend en entrée deux listes de même longueur et renvoie un entier x tel que $\forall i \; x \equiv A[i] \bmod N[i]$ lorsque les $N[i]$ sont deux à deux premiers entre eux. Tester et comparer votre fonction avec `crt`.
5. Quelles sont les solutions du système :
$$\begin{cases} x \equiv 1 \bmod 2 \\ x \equiv 2 \bmod 3 \\ x \equiv 3 \bmod 5 \\ x \equiv 4 \bmod 7 \end{cases}$$
6. En utilisant le théorème des restes Chinois, donner la liste des éléments inversibles de $\mathbb{Z}/136\mathbb{Z}$.

2 Arithmétique polynomiale en caractéristique 0

Dans $\mathbb{Q}[X]$, on considère les polynômes :

$$P = X^2 + X, \qquad Q = X^3 + 2X + 1 \qquad \text{et} \qquad R = 3X.$$

7. En réécrivant la division euclidienne, ou en utilisant les fonctions `%` et `//`, tester vos algorithmes d'Euclide, Euclide étendu et théorème chinois pour des polynômes de $\mathbb{Q}[X]$. En particulier, calculer $pgcd(P, Q)$ et $pgcd(P, R)$, une identité de Bézout pour Q et R, ainsi que deux polynômes $S1$ et $S2$ tels que :
$$\begin{cases} S1 \equiv 1 \bmod P \\ S1 \equiv X \bmod Q \end{cases}$$
et :
$$\begin{cases} S2 \equiv 1 \bmod P \\ S2 \equiv X \bmod Q \\ S2 \equiv 0 \bmod R \end{cases}$$
Vérifier vos résultats grâce aux fonctions SAGE correspondantes : `gcd`, `xgcd`, `crt`.

8. Proposer un algorithme pour calculer la partie sans carré d'un polynôme T.

On travaille à présent dans $\mathbb{Z}[X]$; P, Q et R sont en particulier vus comme des polynômes à coefficients entiers.

9. Dispose-t-on d'une division euclidienne dans $\mathbb{Z}[X]$? A quelle condition sur P et Q peut-on quand même effectuer la division euclidienne de P par Q ?
10. Reprendre les questions précédentes.

3 Construction de corps finis

♣ `Fp=GF(p)`, `Fq.<a>=GF(p**n)`, `Fq.<a>=GF(p**n,name='a',modulus=P)` ♣

11. Existe-t-il un corps fini à 1 élement, 2 élements, 4 éléments, 6 éléments, 9 éléments ?
12. Construire l'anneau `PolF2` des polynômes sur $F2$. Est-il euclidien ? Tester les fonctions `%`, `//`,`gcd`, `xgcd`, `crt`.
13. Montrer que dans F_2, le polynôme X^2+X+1 est irréductible. En déduire une construction de F_4. Ecrire, à la main, les tables d'addition et de multiplication de F_4. Vérifier vos calculs sur SAGE.
14. Ecrire un algorithme qui énumère les polynômes de F_2 de degré inférieur à 6.
15. En déduire un algorithme (naïf) qui énumère les polynômes irréductibles de F_2 de degré inférieur à 6.
16. D'après vos observations, tout corps fini peut-il [en théorie] être construit comme corps de rupture sur son corps premier ? Quel théorème vous l'assure ?
17. ♠ Tout corps fini peut-il *en pratique* (c'est-à-dire de façon effective et efficace) être obtenu comme corps de rupture sur son corps premier ?