Master CSI 2 2018-2019

Cryptanalyse — 4TCY902U
Responsable : G. Castagnos

TP 1 — Initiation à Sage, révisions sur les corps finis

1 Que fait la fonction `xgcd` ? Appliquez-la à des entiers puis à des polynômes et vérifiez le résultat.

2 Faire la liste des carrés des nombres premiers compris entre 0 et 20.

3 Quel est l'ordre multiplicatif de 25 modulo 1000003 ? Cherchez-le par une boucle puis par une fonction de Sage en créant l'anneau $\mathbf{Z}/1000003\mathbf{Z}$.

4 Trouvez tous les entiers inférieurs ou égaux à 1000 qui sont égaux à la somme de leurs diviseurs stricts (utilisez la méthode `.divisors()`).

5 Une matrice de Vandermonde est une matrice de la forme

$$\mathrm{M} = \begin{pmatrix} 1 & 1 & 1 & \dots & 1 \\ a_1 & a_2 & a_3 & \dots & a_n \\ a_1^2 & a_2^2 & a_3^2 & \dots & a_n^2 \\ \vdots & \vdots & \vdots & & \vdots \\ a_1^{n-1} & a_2^{n-1} & a_3^{n-1} & \dots & a_n^{n-1} \end{pmatrix}$$

- Faire une fonction qui prend en argument des rationnels $[a_1, a_2, a_3, a_4]$ et rend la matrice associée M.
- Modifier votre fonction afin qu'elle accepte des suites de a_i de taille arbitraire.
- Modifier encore votre fonction afin qu'elle accepte des a_i de n'importe quel type.
- Enfin calculez et factorisez le déterminant dans le cas de 4 variables (on pourra travailler avec des variables formelles, dans l'anneau symbolique de Sage, déclarées comme suit : `x=var('x')`). Quelle est la formule ?

6 Caractéristique, corps premier (cf. fiche Rappels corps finis, Définition 1)

- Soit $n = 25$. Créer l'anneau $\mathrm{A} = \mathbf{Z}/n\mathbf{Z}$ avec Sage. Quel est sa caractéristique ? Donner la liste de ses éléments inversibles. L'anneau est-il un corps ?

- Mêmes questions avec $n = 13$.

7 Le corps $\mathbf{F}_8$ (cf. fiche Rappels corps finis, Proposition 1, Remarque 1, et section réalisation)

- Créer le corps $\mathbf{F}_8$ avec Sage. Donner une base de $\mathbf{F}_8$, et lister tous les éléments en utilisant cette base.
- Vérifier l'identité $(x+y)^2 = x^2 + y^2$ sur les éléments de $\mathbf{F}_8$ avec Sage.
- Lister les éléments tels que $x^2 = x$.

8 Calculs dans $\mathbf{F}_8$ (cf. fiche Rappels corps finis, section réalisation)

- Quel est le polynôme P(X) utilisé par Sage pour construire l'extension ? Vérifier qu'il est bien irréductible sur F_2 (par le calcul et avec Sage). On note $a = \mathrm{X} \pmod{\mathrm{P(X)}}$ de telle sorte que a que $\mathrm{P}(a) = 0$. Quelles sont les autres racines dans $\mathbf{F}_8$ (par Sage et par le calcul) ?

  Tout élément de $\mathbf{F}_8$ s'écrit $v_0 + v_1\mathrm{X} + v_2\mathrm{X}^2$ modulo P(X) : On note juste les coordonnées (v_0, v_1, v_2) : cette chaîne de 3 bits permet de représenter chaque élément de $\mathbf{F}_8$.

- Faire le calcul $(1,0,1) + (0,1,1)$ dans $\mathbf{F}_8$ avec Sage : en utilisant le corps $\mathbf{F}_8$ et en utilisant la notation polynomiale. De manière générale comment se fait l'addition ?
- Calculer $(1,1,1) \times (0,1,1)$ en utilisant la notation polynomiale. Calculer ensuite l'inverse de $(0,0,1)$ toujours via les polynômes (utiliser une identité de Bézout). Vérifier le résultat en utilisant directement les opérations `*` et `^(-1)`.

9 Polynômes minimaux et ordres dans $\mathbf{F}_8$ (cf. fiche Rappels corps finis, sections ordres et section polynôme minimal)

- Lister les polynômes minimaux de tous les éléments de $\mathbf{F}_8$ (par le calcul et avec Sage)
- Quels sont les éléments primitifs ?
- On note $b = a + 1$. Établir la correspondance entre les éléments exprimés en base $(1, a, a^2)$ et comme puissance de a, ainsi que comme puissance de b.

10 $\mathbf{F}_{16}$, $\mathbf{F}_{256}$ et $\mathbf{F}_{2^{100}}$

- Trouver, grâce à un élément de $\mathbf{F}_{2^4}$, un polynôme irréductible de degré 4, non primitif.
- Trouver de diverses façons les éléments de $\mathbf{F}_{2^8}$ qui forment $\mathbf{F}_{2^4}$.
- De même lister les éléments de $\mathbf{F}_{2^{100}}$ qui forment $\mathbf{F}_{2^4}$.