UPEC
Licences d'Informatique et de Mathématiques
Mathématiques discrètes pour l'informatique

TD 2 - Eléments inversibles, indicatrice d'Euler, chiffrement affine

Exercice 1

1. Déterminer tous les éléments inversibles de $\mathbb{Z}/20\mathbb{Z}$.
2. Calculer $\varphi(20)$, puis comparer avec le résultat de la question précédente

Exercice 2

1. Démontrer que $\text{pgcd}(49, 72) = 1$ en utilisant l'algorithme d'Euclide
2. En utilisant l'algorithme d'Euclide étendu, trouver des coefficients entiers u et v tels que $49u + 72v = 1$.
3. En déduire la valeur de l'inverse de 49 dans $\mathbb{Z}/72\mathbb{Z}$.
4. Refaire les questions 1 et 2 avec 436 et 237, ainsi que 534 et 408.
5. Trouver les inverses de 169, 187, 338 et 209 dans $\mathbb{Z}/420\mathbb{Z}$.

Exercice 3

Résoudre dans $\mathbb{Z}$ les équations suivantes :

1. $7x \equiv 2 \pmod 9$.
2. $98x \equiv 79 \pmod{144}$.
3. $98x \equiv 4 \pmod{144}$.

Exercice 4

On considère le chiffrement affine dans $\mathbb{Z}/76\mathbb{Z}$.

1. Combien existe-t-il de clés valides ?
2. Supposons que la clé secrète est $k = (9, 3)$. Calculer la fonction de déchiffrement.

Exercice 5

On considère le chiffrement affine dans $\mathbb{Z}/26\mathbb{Z}$.

1. On dispose des couples clair/chiffré $(3, 10)$ et $(10, 21)$. Quelle est la clé utilisée ?
2. Même question avec les couples clair/chiffré $(3, 10)$ et $(11, 22)$.

Exercice 6

Démontrer que pour tout $n \geq 2$ on a

$$n = \sum_{d|n} \varphi(d)$$

Indice : si l'on met les n fractions $1/n$, $2/n$, …, n/n, sous forme irréductible, quels sont les dénominateurs possibles ?