# TD1 - correction

September 2022

## 1 Introduction

**Objectif:** appliquer de manière approfondie les concepts et méthodes vues durant le cours.
**Prérequis:** les bases de l'arithmétique modulaire, la compréhension des méthodes de chiffrement symétrique vues en cours.
**Connaissances à acquérir:** comprendre les congruences, appliquer les algorithmes de Polybe, César et Vigenère.

## 2 Arithmétique modulaire

### 2.1 Relation de congruence

Ces congruences sont-elles vraies ?

- $100 \equiv 5$ [5] : VRAI
- $1024 \equiv 16$ [16] : VRAI
- $102 \equiv$ -23 [98] : FAUX
- $49 \equiv 70$ [7] : VRAI (49 et 70 sont de la table de 7)
- $8 + 31 \equiv 7$ [4] : VRAI
- $305 + 950 \equiv 100$ [200] : FAUX
- $15472 + 15489 \equiv 1$ [15480] : VRAI (15489 % 15480 = 9. 15472 + 9 = 15481)
- $8 * 15 \equiv$ -1 [11] : VRAI (15 % 11 = 4. 8 * 4 = 32. 32 = -1 + 3 * 11)
- $10 * 13 \equiv 20$ [11] : FAUX (même technique que le précédent)
- $5^3 \equiv 5$ [3] : VRAI (5 % 3 = 2. $2^3 = 8$. 8 = 5 + 1 * 3.)
- $94^{10} \equiv 1020$ [92] : FAUX (94 % 92 = 2. $2^{10} = 1024$)
- $12^{100} \equiv 2$ [11] : VRAI (même technique que le précédent)

### 2.2 Z/nZ

Calculez les exponentiations suivantes:

- $c \equiv 10^5 \pmod{500}$:
  $10^5 \pmod{500} \equiv 10^2 * 10^3 \pmod{500}$
  Or $10^3 \pmod{500} \equiv 1000 \pmod{500} = 0$
  Donc $10^5 \pmod{500} \equiv 10^2 * 0 \pmod{500} = 0 \pmod{500}$
  $c = 0$

- $c \equiv 10^5 \pmod{495}$:
  $10^5 \pmod{495} \equiv 10^2 * 10^3 \pmod{495}$
  Or $10^3 \pmod{495} \equiv 1000 \pmod{495} = 10$
  Et $10^2 \pmod{495} \equiv 100 \pmod{495} = 100$
  Donc $10^5 \pmod{495} \equiv 100 * 10 \pmod{495} = 10 \pmod{495}$
  Donc $c = 10$

- $c \equiv 3^{17} \pmod{26}$
  $3^3 \pmod{26} \equiv 27 \pmod{26} \equiv 1 \pmod{26}$
  Or $3^{17} = 3^3 * 3^3 * 3^3 * 3^3 * 3^3 * 3^2$
  $3^{17} \pmod{26} \equiv 1 * 1 * 1 * 1 * 1 * 3^2 \pmod{26}$
  Et $3^2 \pmod{26} \equiv 9 \pmod{26}$
  Donc $3^{17} \pmod{26} \equiv 1 * 9 \pmod{26} = 9 \pmod{26}$
  Donc $c = 9$

  Les autres exponentiations se font de la même manière.

- $c \equiv 4^9 \pmod{48}$ — solution: 16
- $c \equiv 9^9 \pmod{79}$ — solution: 65
- $c \equiv 2^{11} \pmod{1998}$ — solution: 50
- $c \equiv 5^5 \pmod{26}$ — solution: 5
- $c \equiv 7^6 \pmod{40}$ — solution: 9
- $c \equiv 8^5 \pmod{63}$ — solution: 8

# 3 Chiffrement par substitution

## 3.1 Polybe

Correction des mots à chiffrer:

| | | |
|---|---|---|
| 3515434415 | 421124432433 | 113333245115424311244215 |
| 152121421154113344 | 3443241542 | 13344513231543 |
| 3111441553 | 21243143 | 1334423315 |

Correction des mots à déchiffrer:

| | | |
|---|---|---|
| ordinateur | camion | chiffrement |
| python | message | route |
| Nenuphar | antilope | gnou |

### 3.2 César

Le message décodé est: *Je rentre chez moi. Sur le trottoir, un homme se promene, ses deux musettes remplies de legumes entre ses doigts.*

## 4 Chiffrement par bloc

La clé permet de chiffrer 3 lettres à la fois. La taille des blocs sont donc de 3.

Il faut vérifier avec chaque groupe d'étudiants que le message décodé est le même que le message initial.