# Arithmétique pour la cryptographie

Exercices de Révision pour l'Examen Final

EPITA Cyber 1 2024-2025

Ce document comprend des exercices de révision pour l'examen final.

## 1 Congruence

**Exercice 1 :** Soit un entier relatif $n$.

1. Déterminer les valeurs de n telles que $10n^2 - n + 1$ soit divisible par 3.
2. Déterminer les valeurs de n telles que $n^3 + 2n + 2$ soit divisible par 5.

## 2 Inverse Modulaire et Coefficient de Bézout

**Exercice 2 :**

1. Montrer que 4 est un inverse modulaire de 13 pour la multiplication modulo 17.
2. Montrer que 6 est un inverse modulaire de 21 pour la multiplication modulo 25.
3. Déterminer un inverse modulaire de 5 pour la multiplication modulo 12.
4. Déterminer un inverse modulaire de 3 pour la multiplication modulo 17.

**Exercice 3 :**

1. Les coefficients de Bézout de 25 et 21 sont $-5$ et 6.
   En déduire un inverse modulaire positif de 21 modulo 25.
   En déduire un inverse modulaire positif de 25 modulo 21.
2. Déterminer un inverse modulaire positif de 17 modulo 53, à l'aide des coefficients de Bézout entre 17 et 53.
3. Déterminer un inverse modulaire positif de 7 modulo 81, à l'aide des coefficients de Bézout entre 7 et 81.

## 3 Gauss / Equation Diophantienne

**Exercice 4 :**

1. Déterminer les entiers relatifs $x$ et $y$ tels que
$$3x - 2y = 1$$
2. Déterminer les entiers relatifs $x$ et $y$ tels que
$$5x - 2y = 6$$

# 4 Protocole RSA

**Exercice 5 :**
Attention : Dans cet exercice, ne pas calculer directement $m^e$ car ce nombre peut être très grand. Calculez itérativement $m^{i+1} \equiv m * m^i \pmod{n}$, avec $e$ étapes de calcul.

Exemple : Nous souhaitons calculer $9^5 \equiv c \pmod{35}$.

- Nous calculons d'abord $9^2 \equiv 81 \equiv 11 \pmod{35}$.
- Puis, nous calculons $9^3 \equiv 9 * 9^2 \equiv 9 * 11 \equiv 99 \equiv 29 \pmod{35}$.
- Puis, nous calculons $9^4 \equiv 9 * 9^3 \equiv 9 * 29 \equiv 261 \equiv 16 \pmod{35}$.
- Puis, nous calculons $9^5 \equiv 9 * 9^4 \equiv 9 * 16 \equiv 4 \pmod{35}$.

  $\rightarrow$ Notre message chiffré est donc $c = 4$.

1. Soit le module de chiffrement $n = 33$, l'exposant de chiffrement $e = 5$.
   (a) Soit le message $m = 6$. Calculer le message chiffré correspondant.
   (b) Soit le message $m = 3$. Calculer le message chiffré correspondant.
2. Soit le module de chiffrement $n = 55$, l'exposant de déchiffrement $d = 3$.
   (a) Soit le message chiffré $c = 7$. Calculer le message initial correspondant.
   (b) Soit le message chiffré $c = 10$. Calculer le message initial correspondant.

## Source :

**Éric Barbazo**, **Christophe Barnet**, **Martial Baheux**, **Dominique Grihon**, *Barbazo Mathématiques Expertes Terminale*, édition 2020, Hachette Éducation.

## Exercices supplémentaires :

`https://www.bibmath.net/ressources/index.php?action=affiche&quoi=bde/arithm/congruence&type=fexo`