

TD1 - Arithmétique - Congruences

Exercice 1. Calculer le reste de 7^8 modulo 6 puis celui de 3^{15} modulo 11 (On ne calculera pas explicitement la puissance).

Exercice 2. Montrer que $2x + 9y \equiv 0 \pmod{8}$ implique $10x - 3y \equiv 0 \pmod{8}$.

Exercice 3. Trouver tous les entiers y tels que $2y \equiv 5 \pmod{7}$.

Exercice 4. Trouver tous les entiers y tels que $3y \equiv 12 \pmod{33}$.

Exercice 5. Trouver tous les entiers x tels que

$$\begin{cases} x \equiv 3 \pmod{11} \\ x \equiv 5 \pmod{7}. \end{cases}$$

Arithmétique - Congruences

Exercice 6. a) Montrer que 223 est un nombre premier.

b) Calculer 1998^{1998} modulo 223.

Exercice 7. Trouver tous les entiers x tels que

$$\begin{cases} x \equiv -1 [8] \\ x \equiv 7 [13]. \end{cases}$$

Exercice 8. a) Factoriser 455 en produit de nombres premiers.

b) Soient a et n des entiers naturels. Montrer que l'on a $a^n \equiv 1 [455]$ si et seulement si $a^n \equiv 1 [5]$, $a^n \equiv 1 [7]$ et $a^n \equiv 1 [13]$.

c) Soit a un entier tel que $\text{pgcd}(a, 455) = 1$. Montrer que l'on a $a^{12} \equiv 1 [455]$.

Arithmétique - Congruences

Exercice 9. Soient p un nombre premier et a un entier positif non multiple de p .

a) Montrer qu'il existe un plus petit entier positif k tel que $a^k \equiv 1 [p]$.

Soit $n \in \mathbb{N}$. Notons r le reste de la division euclidienne de n par k .

b) Montrer que l'on a $a^n \equiv 1 [p]$ si et seulement si n est multiple de k .

c) Soit $p = 5$ et $a = 4$. Vérifiez que $a^{p-1} \equiv 1 [5]$. Chercher le plus petit entier k tel que $a^k \equiv 1 [5]$.

Exercice 10. a) Soit $a \in \mathbb{Z}$. Montrer que a^2 est congru à 0, 1 ou 4 modulo 8.

b) Soit n un entier positif. Montrer que $a^2 + b^2 + c^2 \neq 8n - 1$, pour tous $a, b, c \in \mathbb{Z}$. (On interprétera cette dernière équation dans le langage de la congruence).

Arithmétique - Congruences

Exercice 11. a) Factoriser 1729 en produit de nombres premiers.

b) Soient a et n des entiers positifs. Montrer que l'on a $a^n \equiv 1 \pmod{1729}$ si et seulement si $a^n \equiv 1 \pmod{7}$, $a^n \equiv 1 \pmod{13}$ et $a^n \equiv 1 \pmod{19}$.

c) Soit a un entier positif tel que $\text{pgcd}(a, 1729) = 1$. Démontrer que l'on a $a^{1728} \equiv 1 \pmod{1729}$.

Exercice 12. Trouver tous les entiers x tels que

$$\begin{cases} 7x \equiv 5 \pmod{19} \\ 3x \equiv 1 \pmod{11}. \end{cases}$$

Cryptologie

Exercice 1 – Chiffrement de Polybe

On considère l'alphabet privé du W, soit 25 lettres. Polybe (200–125 av J.C.) a proposé le mécanisme suivant : on range les lettres dans un tableau 5×5 , en commençant par le mot clé (et en supprimant les doublons), puis on continue avec les lettres restantes de l'alphabet, dans l'ordre. Par exemple, avec le mot-clé MYSTERE, on construit le tableau suivant :

	1	2	3	4	5
1	M	Y	S	T	E
2	R	A	B	C	D
3	F	G	H	I	J
4	K	L	N	O	P
5	Q	U	V	X	Z

Le chiffrement s'effectue alors en remplaçant chaque lettre par les deux chiffres : ligne + colonne qui indiquent sa position dans la grille. Par exemple, F est chiffré par 31.

Q1. Expliquer comment on peut cryptanalyser un tel système : par une attaque à clair connu, puis dans une attaque simple (seulement un chiffré).

Raoul envoie un message à Anna pour lui fixer un rendez-vous. Le cryptogramme est le suivant :

123222	512215	424215	512242	242255	534352	111524	225254
322252	512211	515222	532251	142251	154352	21	

Q2. Décrypter ce message.

Cryptologie

Exercice 2 – Chiffrement de Hill

Dans le chiffrement de Hill, chaque lettre de l'alphabet est représentée par un entier compris entre 0 et 25. L'algorithme est un chiffrement par blocs de m lettres, qui transforme un bloc $(x_1, x_2, \dots, x_m)$ en un bloc $(y_1, y_2, \dots, y_m)$ défini par la relation algébrique :

$$(y_1, y_2, \dots, y_m) = (x_1, x_2, \dots, x_m) \cdot A$$

où A est une matrice carrée d'ordre m à coefficients dans $\mathbb{Z}_{26}$, tous les calculs étant faits modulo 26. Par exemple avec $m = 2$ et $A = \begin{pmatrix} 5 & 1 \\ 12 & 3 \end{pmatrix}$, le message $(10, 21)$ est chiffré en $(10, 21) \cdot A = (10 \times 5 + 21 \times 12, 10 \times 1 + 21 \times 3) = (16, 21)$

Le déchiffrement d'un bloc se fait en multipliant le bloc chiffré par la matrice inverse de A . Une matrice carrée à coefficient dans $\mathbb{Z}_{26}$ est inversible si et seulement si son déterminant est inversible modulo 26.

- Q1. Quelle est la formule donnant la matrice inverse lorsque $m = 2$?
- Q2. Calculer la matrice inverse de celle donnée en exemple.
- Q3. Décrire une méthode permettant d'attaquer le chiffrement de Hill « à clair connu »
- Q4. Application : on dispose des couples $((2\ 9), (11\ 11))$ et $((7\ 3), (11\ 23))$.

Cryptologie

Exercice 3 – Crytanalyse

Soit le chiffrement par flot asynchrone suivant : $k_1 = K \in \mathbb{Z}_{26}$ et $k_i = x_{i-1}$ pour tout message $x = (x_1, x_2, \dots)$. On définit $\mathcal{E}_k(x) = x + k \bmod 26$ et $\mathcal{D}_k(y) = y - k \bmod 26$.

Q1. Décrypter le chiffré suivant :

MALVVMAFBHBUQPTSOXALTGVWWRG