

Révision du 08 juin 2018

EXERCICE 1

Cours

- 1) Trouver tous les diviseurs de 96. Vérifier votre résultats en calculant le nombre de diviseurs.
- 2) d divise $5n + 1$ et $3n - 4$. Montrer que d divise 23. Valeurs possibles pour d ?
- 3) L'égalité $1600 = 17 \times 93 + 19$ correspond-elle à la division de 1600 par 17?
- 4) Démontrer que $2011^{2011} \equiv 2 \pmod{7}$.
- 5) Déterminer, par l'algorithme d'Euclide, le pgcd de 935 et 517.
- 6) Démontrer le théorème de Bézout : $\text{pgcd}(a, b) = 1 \Leftrightarrow \exists (u, v) \in \mathbb{Z}^2, au + bv = 1$
- 7) Déterminer, en remontant l'algorithme d'Euclide, un solution à l'équation $59x + 27y = 1$.
En déduire toutes les solution dans \mathbb{N}^2
- 8) Démontrer le théorème de Gauss : Si a divise bc et $\text{pgcd}(a, b) = 1$ alors, a divise c .
- 9) Démontrer la factorisation standard pour $n \in \mathbb{N}^*$ et $x \in \mathbb{R}$:

$$x^n - 1 = (x - 1)(x^{n-1} + x^{n-2} + \dots + 1)$$
 En déduire que si n n'est pas premier, les nombres de la forme $2^n - 1$, avec $n \geq 2$, ne sont pas premier. La réciproque est-elle vraie?

EXERCICE 2

Pondichéry mai 2018

À toute lettre de l'alphabet on associe un nombre entier x compris entre 0 et 25 comme indiqué dans le tableau ci-dessous :

Lettre	A	B	C	D	E	F	G	H	I	J	K	L	M
x	0	1	2	3	4	5	6	7	8	9	10	11	12
Lettre	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
x	13	14	15	16	17	18	19	20	21	22	23	24	25

Le « chiffre de RABIN » est un dispositif de cryptage asymétrique inventé en 1979 par l'informaticien Michael Rabin.

Alice veut communiquer de manière sécurisée en utilisant ce cryptosystème. Elle choisit deux nombres premiers distincts p et q . Ce couple de nombres est sa clé privée qu'elle garde secrète.

Elle calcule $n = p \times q$ et elle choisit un nombre entier naturel B tel que $0 \leq B \leq n - 1$.

Si Bob veut envoyer un message secret à Alice, il le code lettre par lettre.

Le codage d'une lettre représentée par le nombre entier x est le nombre y tel que :

$$y \equiv x(x + B) \pmod{n} \text{ avec } 0 \leq y \leq n.$$

Dans tout l'exercice on prend $p = 3$, $q = 11$ donc $n = p \times q = 33$ et $B = 13$.

Partie A : Cryptage

Bob veut envoyer le mot « NO » à Alice.

- 1) Montrer que Bob code la lettre « N » avec le nombre 8.
- 2) Déterminer le nombre qui code la lettre « O ».

Partie B : Décryptage

Alice a reçu un message crypté qui commence par le nombre 3.

Pour décoder ce premier nombre, elle doit déterminer le nombre entier x tel que :

$$x(x + 13) \equiv 3 \pmod{33} \quad \text{avec } 0 \leq x < 26.$$

- 1) Montrer que $x(x + 13) \equiv 3 \pmod{33}$ équivaut à $(x + 23)^2 \equiv 4 \pmod{33}$.
- 2) a) Montrer que si $(x+23)^2 \equiv 4 \pmod{33}$ alors le système $\begin{cases} (x+23)^2 \equiv 4 \pmod{3} \\ (x+23)^2 \equiv 4 \pmod{11} \end{cases}$ est vérifié.
 b) Réciproquement, montrer que si $\begin{cases} (x + 23)^2 \equiv 4 \pmod{3} \\ (x + 23)^2 \equiv 4 \pmod{11} \end{cases}$ alors $(x + 23)^2 \equiv 4 \pmod{33}$.
 c) En déduire que $x(x + 13) \equiv 3 \pmod{33} \Leftrightarrow \begin{cases} (x + 23)^2 \equiv 1 \pmod{3} \\ (x + 23)^2 \equiv 4 \pmod{11} \end{cases}$
- 3) a) Déterminer les nombres entiers naturels a tels que $0 \leq a < 3$ et $a^2 \equiv 1 \pmod{3}$.
 b) Déterminer les nombres entiers naturels b tels que $0 \leq b < 11$ et $b^2 \equiv 4 \pmod{11}$.
- 4) a) En déduire que $x(x + 13) \equiv 3 \pmod{33}$ équivaut aux quatre systèmes suivants :

$$\begin{cases} x \equiv 2 \pmod{3} \\ x \equiv 8 \pmod{11} \end{cases} \quad \text{ou} \quad \begin{cases} x \equiv 0 \pmod{3} \\ x \equiv 1 \pmod{11} \end{cases} \quad \text{ou} \quad \begin{cases} x \equiv 2 \pmod{3} \\ x \equiv 1 \pmod{11} \end{cases} \quad \text{ou} \quad \begin{cases} x \equiv 0 \pmod{3} \\ x \equiv 8 \pmod{11} \end{cases}$$

- b) On admet que chacun de ces systèmes admet une unique solution entière x telle que $0 \leq x < 33$.
 Déterminer, sans justification, chacune de ces solutions.
- 5) Compléter l'algorithme suivant pour qu'il affiche les quatre solutions trouvées dans la question précédente.

```

Traitement
|
|  pour ... allant de ... à ... faire
|   |
|   |  si le reste de la division de ... par ... est égal à ... alors
|   |   |
|   |   |  Afficher ...
|   |   |
|   |   |  fin
|   |
|   |  fin
|

```

- 6) Alice peut-elle connaître la première lettre du message envoyé par Bob ?
 Le « chiffre de RABIN » est-il utilisable pour décoder un message lettre par lettre ?