Examen de mi-parcours - Arithmétique

18/03/2024 - Durée : 2h15

Documents interdits, Calculatrice interdite

La qualité de la présentation et le soin apporté à la rédaction seront pris en compte dans la notation. Il est demandé d'encadrer vos résultats à la fin de chaque question (en-dehors des questions de cours).

Exercice n°1 : (Questions de cours)
1. Soit $n \in \mathbb{N}$. Soient a et b deux entiers relatifs. Que signifie :

$$a \equiv b\,[n]$$

(a est congru à b modulo n) ?
Donner une définition mathématique précise.

2. Soient a et b deux entiers relatifs. Que signifie : "a et b sont premiers entre eux " ?

3. Énoncer le théorème de Bézout.

4. Énoncer le théorème de Gauss.

5. Énoncer le petit théorème de Fermat.

Exercice n°2 : (Équation diophantienne)
Résoudre l'équation (E) dans $\mathbb{Z}^2$:

$$(E) \quad 4x - 3y = 1$$

Exercice n°3 : (Raisonnement)
Soit p un nombre premier tel que $p \neq 2$.
Démontrer que $p + 3$ n'est pas un nombre premier.

Exercice n°4 : (Problème)
Bob choisit les paramètres suivants : $N = 91$ et $e = 5$. Il déclare que tout le monde peut lui envoyer des messages chiffrés à l'aide de la fonction de chiffrement :

$$f : x \longmapsto y$$

où y est le reste de la division euclidienne de x^e par N. On a donc : $y \equiv x^e\,[N]$, c'est-à-dire que $y \equiv x^5\,[91]$.
Alice souhaite envoyer un message à Bob. Pour cela, elle choisit un message x et elle envoie y sur le réseau.
Vous êtes Charlie et vous interceptez le message chiffré y sur le réseau. Vous voyez que $y = 2$. Vous souhaitez décrypter y.

1. Écrire la décomposition en facteurs premiers de $N = 91$, sous la forme $N = p \times q$, avec p et q deux nombres premiers tels que $p < q$.

2. On note désormais $n = (p-1)(q-1)$. Calculer n.

3. Justifier qu'il existe $(u, v) \in \mathbb{Z}^2$ tel que :

$$5u + nv = 1$$

4. À l'aide de l'algorithme d'Euclide étendu, déterminer la valeur de u et de v, puis en déduire l'inverse modulaire de 5 modulo n, noté d (vérifier que : $1 \leq d \leq 90$).

5. On admet que la fonction de déchiffrement est :

$$f^{-1} : y \longmapsto z$$

où z est le reste de la division euclidienne de y^d modulo N. Autrement dit, $z \equiv y^d\ [N]$, c'est-à-dire que $z \equiv 2^d\ [91]$.
Comme $x = f^{-1}(y)$, on peut donc écrire que : $x \equiv 2^d [91]$.

a) Donner l'écriture de d en base binaire.
(Exemples d'écriture en base binaire :

- $23 = 2^4 + 2^2 + 2^1 + 2^0$, que l'on peut aussi écrire $23 = 16 + 4 + 2 + 1$;
- $35 = 2^5 + 2^1 + 2^0$, que l'on peut aussi écrire $35 = 32 + 2 + 1$)

b) La table de congruences suivante a été pré-calculée.

Puissance	Calcul modulo 91
0	$2^0 \equiv 1\ [91]$
1	$2^1 \equiv 2\ [91]$
2	$2^2 \equiv 4\ [91]$
4	$2^4 \equiv 16\ [91]$
8	$2^8 \equiv 74\ [91]$
16	$2^{16} \equiv 16\ [91]$
32	$2^{32} \equiv 74\ [91]$
64	$2^{64} \equiv 16\ [91]$

En utilisant l'écriture de d en base binaire obtenue dans la question a), déchiffrer le message envoyé par Alice (c'est-à-dire : retrouver la valeur de x).

Aide au calcul :
$16 \times 74 \equiv 1\ [91]$