Tableur 02 : Cryptographie ASCII/Affine/Congruence

Partie II : Justification du cryptage.

Pour le codage ASCII, deux lettres de l'alphabet sont codées par deux nombres différents. Il faut s'assurer que le cryptage choisi ensuite au I2. Code deux nombres n et p distincts, compris entre 0 et 255, par deux nombres distincts.

On veut donc démontrer que :

« Si $n \neq p$ alors ..... » avec $n > p$

a. Explique pourquoi, pour tout n du code ASCII, il existe un entier k tel que : $7n = 256k + f(n)$

b. Montrer que si $f(n) = f(p)$ alors 256 divise $7(n-p)$

c. On admet le résultat suivant (Théorème de **Gauss**) :

Si *un nombre n divise un produit de facteurs entiers et que l'un des facteurs est premiers avec n, alors n divise l'autre facteur.*

A l'aide de ce résultat, en déduire que $n = p$. Justifier alors que le codage est valide.

PARTIE III : Le décryptage

Message crypté :

20/185/37 251/167/44/216/95/251/167/44/223/23/51/195/37 181 195/37/44/224/251/167/209/2/223/202/223/23/51/195

Pour décrypter ce message, on note g la fonction de décryptage qui, à tout entier k appartenant à [0;255] associe le reste de la division de $183k$ par 256. On note $g(k)$ ce reste.

Entrer, dans une nouvelle feuille de tableur, le message codé ci-dessus puis construire le tableau permettant de décoder le message, comme dans le tableau ci-dessous :

	A	B	C	D	E
1	Message Codé f(n)	195	1	4	23
2	183*f(n)	35685	183	732	4209
3	Reste par 256	101	183	220	113
4	Lettre	e	·	Ü	q

PARTIE IV : Justification du décodage

a. Vérifier que le reste de la division euclidienne de 183×7 par 256 est 1

b. En déduire que le reste de la division euclidienne de $183 \times 7n$ par 256 est n (si $n < 256$)

c. Le but de cette question est d'expliquer pourquoi la fonction g, qui à k associe g(k) le reste de la division de 183k par 256, assure le décryptage attendu.

- Par rapport à la partie I, que représente k ?
- Quelle égalité faut-il donc démontrer ?
- En utilisant le fait que f(n) est le reste de la division de 7n par 256, démontrer alors l'égalité et conclure.

Evaluation

Tableur02			
AA	A	EA	NA
SEI06			
AA	A	EA	NA

Vocabulaire

ASCII

American Standard Code for Informatique Interchange.

Tableur

« **=code(L)** » donne le code ASCII de la lettre L

« **=car(*n*)** » donne la lettre dont le code ASCII est *n*.

« **=mod(a;b)** » donne le reste de la division euclidienne de a par b

Histoire

Johann Carl Friedrich Gauss
(1777-1855)
Mathématicien, astronome et physicien allemand