

NOM : Prénom :

Spé maths TS	<u>Devoir d'arithmétique</u>	Lundi 27 mars 2017
--------------	-------------------------------------	--------------------

- Calculatrice autorisée
- Durée : 1h15

Observations :

NOTE :

Exercice 1 : Questions de cours

1) Soient a , b , c , et d , quatre entiers tels que $a \equiv b [n]$ et $c \equiv d [n]$. Montrer que $ac \equiv bd [n]$

2) a) Énoncer le théorème de Bézout :

b) Énoncer le théorème de Gauss :

c) Démontrer le théorème de Gauss :

d) Démontrer la propriété suivante : *Si p est un nombre premier, a et b deux entiers naturels tels que $p \mid ab$, alors $p \mid a$ ou $p \mid b$*

NOM : Prénom :

3) Énoncer le petit théorème de Fermat :

4) a) Décomposer 140 en produit de facteurs premiers

b) À l'aide d'un arbre, déterminer tous les diviseurs de 140 :

Problème : (Sur votre copie)

Partie A :

On considère l'équation (E) : $25x - 108y = 1$, où x et y sont des entiers relatifs

- 1) Vérifier que le couple (13 ; 3) est solution de cette équation
- 2) En déduire la résolution de (E)

Partie B :

Dans cette partie, a désigne un entier naturel et les nombres c et g sont des entiers naturels vérifiant la relation : $25g - 108c = 1$

Dans cette partie, l'énoncé du petit théorème de Fermat est supposé connu

- 1) Soit x un entier naturel. Démontrer que si $x \equiv a [7]$ et $x \equiv a [19]$, alors $x \equiv a [133]$
- 2) a) On suppose que a n'est pas un multiple de 7.

Montrer que $a^6 \equiv 1 [7]$, puis que $a^{108} \equiv 1 [7]$

En déduire que $(a^{25})^g \equiv a [7]$

b) On suppose que a est un multiple de 7

Démontrer que $(a^{25})^g \equiv a [7]$

c) On admet que pour tout entier naturel a , $(a^{25})^g \equiv a [19]$

Démontrer que $(a^{25})^g \equiv a [133]$

Partie C :

On note A , l'ensemble des entiers naturels a tels que $1 \leq a \leq 26$

Un message, constitué d'entiers appartenant à A , est codé puis décodé.

- La phase de codage consiste à associer, à chaque entier a de A , l'entier r tel que :

$$a^{25} \equiv r [133] \text{ avec } 0 \leq r < 133$$

- La phase de décodage consiste à associer à r , l'entier r_1 tel que :

$$r^{13} \equiv r_1 [133] \text{ avec } 0 \leq r_1 < 133$$

- 1) Justifier que $r_1 \equiv a [133]$
- 2) Un message codé conduit à la suite des deux entiers suivants : 128 59
Décoder ce message.