Terminales S spé - DS3

MATHEMATIQUES

Vendredi 21 janvier 2015

Partie A Cours

Citer le théorème de Bézout et le théorème de Gauss et démontrer le théorème de Gauss.

Partie B une équation diophantienne

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

1. A l'aide de l'algorithme d'Euclide prouver que le couple (13 ; 3) est solution de cette équation.
2. Utiliser le couple (13 ; 3) pour déterminer l'ensemble des couples d'entiers relatifs solutions de l'équation (E).

Partie C Fermat et des nombres premiers

Dans cette partie, a désigne un entier naturel ;
les nombres c et g sont des entiers naturels vérifiant la relation $25g - 108c = 1$.
On pourra utiliser le petit théorème de Fermat qui s'énonce ainsi :

> Si p est un nombre premier et a un entier non divisible par p,
> alors a^{p-1} est congru à 1 modulo p, ce que l'on note $a^{p-1} \equiv 1\ [p]$.

1. Soit x un entier naturel. Démontrer que si $x \equiv a\ [7]$ et $x \equiv a\ [19]$, alors $x \equiv a\ [133]$.
2. On suppose que a n'est pas un multiple de 7. Démontrer que $a^6 \equiv 1\ [7]$.
   En déduire que $a^{108} \equiv 1\ [7]$; et que $\left(a^{25}\right)^g \equiv a\ [7]$.
3. On suppose que a est un multiple de 7. Démontrer que $\left(a^{25}\right)^g \equiv a\ [7]$.
4. On admet que pour tout entier naturel a, $\left(a^{25}\right)^g \equiv a\ [19]$. Démontrer que $\left(a^{25}\right)^g \equiv a\ [133]$.

Partie D le code secret

On note A l'ensemble des entiers naturels a tels que : $1 \leqslant a \leqslant 26$.
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 $a^{25} \equiv r\ [133]$ avec $0 \leqslant r < 133$.
> r est donc le reste de la division euclidienne de a^{25} par 133

La phase de décodage consiste à associer à r ,

> l'entier s tel que $r^{13} \equiv s\ [133]$ avec $0 \leqslant s < 133$.
> s est donc le reste de la division euclidienne de r^{13} par 133

1. Justifier que $s \equiv a\ [133]$.
2. Décoder le message suivant : 128 59.

Partie A Cours

Théorème de Bézout :
2 entiers a et b sont premiers entre eux si et seulement si il existe 2 entiers u et v tels que $au+bv=1$**.**
Théorème de Gauss :
Soit a,b,c **3 entiers. Si a divise bc et que a est premier avec b alors a divise c.**
Preuve : Si $a\wedge b=1$ alors d'après Bézout il existe $(u;v)$ tels que $au+bv=1$.
donc $auc+bvc=c$ or $a|bc$ et $a|auc$ donc $a|auc+bvc$ d'où $a|c$.

Partie B une équation diophantienne

1. $108=25*4+8$; $25=8*3+1$ donc $1=25-3*8=25-3*(108-25*4)=13*25-3*108$
   donc (13;3) est une solution de (E).
2. $25x-108y=25*13-108*3\Rightarrow 25(x-13)=108(y-3)$ or $25\wedge 108=1$ donc $25|y-3$
   soit $y=25k+3, k\in\mathbb{Z}$ d'où $2(x-13)=108*25k$ et $x=108k+13, k\in\mathbb{Z}$
   Réciproquement : $\forall k\in\mathbb{Z}, 25*(108k+13)-108*(25k+3)=1$
   donc $\forall k\in\mathbb{Z}$, **(108k + 13 ; 25k + 3)** est bien solution de (E).

Partie C Fermat et des nombres premiers

1. $x-a$ est un multiple de 7 et de 19 or $7\wedge 19=1$ donc $x-a$ est un multiple de 7×19 soit $x\equiv a[133]$.
   Plus précisément $7|x-a$ donc $\exists k\in\mathbb{Z}: x-a=7k$ or $19|x-a$ et $19\wedge 7$
   donc d'après Gauss $19|k$ soit $\exists k'\in\mathbb{Z}: x-a=7\times 19\times k'=133\times k'$. QED.
2. 7 est premier et ne divise pas a, donc $a^6=a^{7-1}\equiv 1$ [7] d'après le Th. de Fermat.
   alors $a^{108}=\left(a^6\right)^{18}\equiv 1^{18}=1$ [7] et $a^{108c}\equiv 1$ [7] soit $a^{25g-1}\equiv 1$ [7] ou $a^{25g}\equiv 1$ [7]
3. Si a est un multiple de 7, $(a^{25})^g$ aussi donc $\left(a^{25}\right)^g\equiv a\equiv 0$ [7].
4. On applique **C.1.** avec $x=(a^{25})^g$,d'où $\left(a^{25}\right)^g\equiv a$ [133].

Partie D le code secret

1. $s\equiv r^{13}$ [133] $\equiv\left(a^{25}\right)^{13}$ [133] avec $(g\ ,\ c)=(13\ ;\ 3)$ vérifiant la relation $25g-108c=1$ d'après **A.**
   D'où d'après **B.2.c.**, $\left(a^{25}\right)^{13}\equiv a$ [133], donc finalement on bien $s\equiv a$ [133].
2. $128\equiv -5$ [133] or $(-5)^{13}=-1220703125=2-9178219\times 133$ donc $128^{13}\equiv -5^{13}\equiv 2$ [133]
   $59^4=12117361=91108\times 133-3\equiv -3$ [133] donc $59^{13}=\left(59^4\right)^3\times 59\equiv(-3)^3\times 59$ [133]
   or $(-3)^3\times 59=-1593=3-12*133$ donc $59^{13}\equiv 3$ [133]
   Le message initial était donc : **2 3**.