Spé TS — Corrigé du DS — (Faut le 27/03/17)

Arithmétique

Exercice 1 : /10

1) a, b, c, d, 4 entiers tels que : $a \equiv b[n]$ et $c \equiv d[n]$

$a \equiv b[n] \iff n \mid a-b$ ~~$\iff \exists k_1 \in \mathbb{Z},\ a-b = nk_1$~~

~~$\iff \exists k_1$~~

$c \equiv d[n] \iff n \mid c-d$ (1)

D'où n divise toute combinaison linéaire à coefficients entiers de $a-b$ et $c-d$.

En particulier, $n \mid c \times (a-b) + b(c-d) = ac - \cancel{bc} + \cancel{bc} - bd$

$= ac - bd$

$\iff \underline{ac \equiv bd[n]}$

2) a) Théorème de Bézout :

Soient a et b, deux entiers relatifs tels que $\text{pgcd}(a;b) = 1$.

On a alors l'équivalence suivante : (1)

$\underline{\text{pgcd}(a;b) = 1 \iff \exists (u;v) \in \mathbb{Z}^2,\ au + bv = 1}$

b) Soient a, b, deux entiers tels que $\text{pgcd}(a;b) = 1$.
Soit c, un entier tel que $a \mid bc$
alors $\underline{a \mid c}$ (Théorème de Gauss) (1,5)

c) Démonstration : Comme $\text{pgcd}(a;b) = 1$, d'après le théorème de Bézout : $\exists (u;v) \in \mathbb{Z}^2,\ au + bv = 1$

d'où en multipliant cette égalité par c :

$acu + bcv = c$

or, $a \mid ac$ (évident) et $a \mid bc$ (2)

D'où a divise toute combinaison linéaire à coefficients entiers de ac et bc, d'où en particulier $acu + bcv$

c'est-à-dire : $a \mid c$

d) Soit p nombre premier, $(a, b) \in \mathbb{N}^2$ tels que $p \mid ab$.

- Soit $p \mid a$ et c'est fini
- Soit $p \nmid a$:

② Comme p est premier, $\text{pgcd}(p; a) = 1$ et $p \mid ab$
D'après le théorème de Gauss, $p \mid b$.

Donc : $p \mid a$ ou $p \mid b$

3) Petit théorème de Fermat :
Soit p entier premier et $a \in \mathbb{Z}$ tel que $p \nmid a$

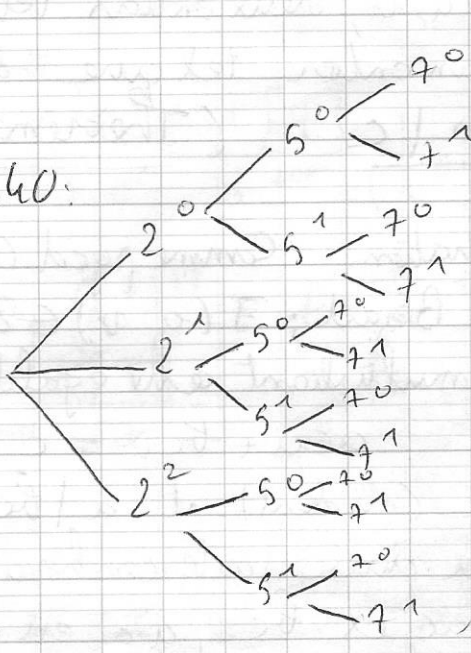
④ alors : $a^{p-1} \equiv 1 \ [p]$

4) a) $140 = 2^2 \times 5 \times 7$

140	2
70	2
35	5
7	7
1	

① d'où $140 = 2^2 \times 5 \times 7$

b) Diviseurs de 140 :



① Il y a 12 diviseurs de 140 en tout :
$\{1; 7; 5; 35; 2; 14; 10; 70; 4; 28; 20; 140\}$

Problème /10

$(E) : 25x - 108y = 1$, $(x;y) \in \mathbb{Z}^2$

1)

$25 \times 13 - 108 \times 3 = 325 - 324 = 1$

(1) Donc $(13;3)$ est une solution particulière de (E)

2) Soit $(x;y)$ solution de (E) :

$$\begin{cases} 25x - 108y = 1 \\ 25 \times 13 - 108 \times 3 = 1 \end{cases}$$

$\Leftrightarrow 25x - 108y = 25 \times 13 - 108 \times 3$

$\Leftrightarrow 25(x-13) = 108(y-3)$

$25 \mid 108(y-3)$ et $\text{Pgcd}(108;25) = 1$ (108 et 25 sont premiers entre eux)

(1,5) } D'après le théorème de Gauss, $25 \mid y-3$

$\Leftrightarrow \exists k \in \mathbb{Z}$, $y - 3 = 25k$

$\Leftrightarrow \exists k \in \mathbb{Z}$, $y = 25k + 3$

De même, $108 \mid 25(x-13)$ avec $\text{Pgcd}(108;25) = 1$ } D'après le théorème de Gauss, $108 \mid x-13$

$\Leftrightarrow \exists k' \in \mathbb{Z}$, $x - 13 = 108k'$

$\Leftrightarrow \exists k' \in \mathbb{Z}$, $x = 108k' + 13$

Réciproquement :

$25 \times 108k' = 108 \times 25k$

$k' = k$

Donc les solutions de (E) sont :

$$S = \{(108k + 13; 25k + 3), k \in \mathbb{Z}\}$$

Partie (B).

1) Soit $x \in \mathbb{N}$.

$x \equiv a\,[7]$ et $x \equiv a\,[19]$

On a : $x \equiv a\,[7] \iff 7 \mid x-a$

$\iff \exists k \in \mathbb{Z},\ x-a = 7k$

de même :

$x \equiv a\,[19] \iff 19 \mid x-a$

$\iff \exists k' \in \mathbb{Z},\ x-a = 19k'$ (1)

d'où :

$7k = 19k'$

Or, 7 et 19 sont premiers entre eux

$7 \mid 19k'$, d'après le théorème de Gauss,

$7 \mid k'$.

d'où : $\exists k'' \in \mathbb{Z},\ k' = 7k''$

d'où $19k' = 19 \times 7k'' = 133k'' = x-a$

Donc : $x - a = 133k'' \iff \underline{x \equiv a\,[133]}$

2) a) a n'est pas multiple de 7 $\iff 7 \nmid a$

Comme 7 est un nombre premier, d'après le petit théorème de Fermat, $a^{7-1} \equiv 1\,[7]$

c'est-à-dire :

$$\underline{a^6 \equiv 1\,[7]} \quad (1)$$

Or, $108 = 6 \times 18$, d'où : $a^{108} = (a^6)^{18}$

Comme $18 \in \mathbb{N}$,

$$(a^6)^{18} \equiv 1^{18}\,[7]$$

Donc : $\underline{a^{108} \equiv 1\,[7]}$ (1)

Comme $25g - 108c = 1 \iff 108c = 25g - 1$

Or, $a^{108c} \equiv 1\,[7]$ $(c \in \mathbb{N})$

c'est-à-dire $a^{25g-1} \equiv 1\,[7]$ d'où en multipliant par a.

(5)

(1) $a^{25g} \equiv a\ [7]$ c'est-à-dire $\underline{(a^{25})^g \equiv a\ [7]}$

B) Supposons a multiple de 7 :
c'est-à-dire $a \equiv 0\ [7]$
d'où $(a^{25})^g \equiv 0\ [7]$

(1) Donc : $\underline{(a^{25})^g \equiv a\ [7]}$.

c) $(a^{25})^g \equiv a\ [19]$ (admis)

(1) D'après la question 1) de la partie (B), comme $(a^{25})^g \equiv a\ [7]$
et $(a^{25})^g \equiv a\ [19]$
Par conséquent : $\underline{(a^{25})^g \equiv a\ [133]}$

Partie (C) :

$A = \{ a \in \mathbb{N},\ 1 \leq a \leq 26 \}$
- codage : $a^{25} \equiv r\ [133]$, $0 \leq r < 133$
- décodage : $r^{13} \equiv r_1\ [133]$, $0 \leq r_1 < 133$

1) On a : $r_1 \equiv r^{13}\ [133]$
$\equiv (a^{25})^{13}\ [133]$.

(1) $\equiv \underline{a\ [133]}$ (d'après partie (B))
(car $13 = 0k + 13$, $g = 13$)

2) 128 59
On a : $128 \equiv -5\ [133]$
d'où $128^{13} \equiv (-5)^{13}\ [133]$
$\equiv -131\ [133]$
$\equiv 2\ [133]$

$59^4 \equiv 130\ [133]$
$\equiv -3\ [133]$
donc $59^{13} = (59^4)^3 \times 59$
$\equiv (-3)^3 \times 59\ [133]$
$\equiv -130\ [133]$
$\equiv 3\ [133]$

(0,5) Le message initial était donc | 2 3 |