Lycée J.P Vernant - spé TS — Année scolaire 2010-2011
Vendredi 4 février

DEVOIR SURVEILLE N° 4 (sujet a)

Le barême n'est pas définitif, il est seulement donné à titre indicatif

Exercice 1 : (9 points)

Les questions sont indépendantes les unes des autres

1. **Question de cours** : Soit a et b deux entiers naturels. Démontrer que l'ensemble des multiples communs à a et b est l'ensemble des multiples de $PPCM(a\,;b)$.

2. *Calcul de PPCM*
   (a) Décomposer le nombre $N = 2760$ en produit de facteurs premiers.
   (b) En déduire la décomposition en produit de facteurs premiers de $PPCM(N\,;2\times 3^2\times 7)$.

3. *A la manif !*
   Un dirigeant syndical essaie de créer des rangées de manifestants, il émet le constat suivant :
   "*Rangeons nous par 10, il en manquera 1 pour compléter la dernière ligne ; rangeons nous par 9, il en manquera un aussi. Par 8 aussi, par 7 aussi, par 6 aussi, par 5 aussi, par 4 aussi, par 3 aussi, par 2 aussi. Et pourtant, nous sommes assurément moins de 5000*"
   Combien y-a-t'il de manifestants ? (selon les syndicats !)

4. *PPCM et équations*
   On considère $n\in\mathbb{N}$ et on pose $a = 2n+3$ et $b = n+4$.
   (a) Déterminer $PPCM(a\,;b)$ en fonction de n.
   (b) Déterminer les entiers naturels n vérifiant $PPCM(a\,;b) = 600$.

5. *Vrai ou Faux ?*
   Dire si les phrases suivantes sont vraies ou fausses en ***justifiant*** *avec précision vos réponses*
   (a) Il existe un unique couple $(a\,;b)\in\mathbb{N}^2$ tels que $a<b$ et $PPCM(a\,;b) - PGCD(a\,;b) = 1$.
   (b) On considère l'équation (E') : $x^2 - 52x + 480 = 0$, où $x\in\mathbb{N}$.
   Il existe deux entiers naturels non nuls dont le $PGCD$ et le $PPCM$ sont solutions l'équation (E').

6. *Théorème de Wilson*
   Soit p un nombre premier et x un entier compris entre 1 et $p-1$.
   On considère les produits de x par 1, 2, ..., $p-1$ et les restes de ces produits dans la division par p.
   (a) Un de ces restes peut-il être nul ?
   (b) Démontrer que tous ces restes sont différents.
   (c) En déduire que, quelque soit x compris entre 1 et $p-1$, il existe un entier y et un seul compris entre 1 et $p-1$ tel que $xy\equiv 1\ [p]$.
   (d) Vérifier que pour $x = 1$ et $x = p-1$, on a $y = x$.
   (e) Démontrer que pour toutes les autres valeurs de x, on a $x\neq y$.
   (f) Déduire de ce qui précède que, si p est premier $(p-1)!\equiv -1\ [p]$ (*ceci est l'énoncé du théorème de Wilson*)
   (g) Pour $p = 7$:
   - vérifier que le théorème de Wilson est vérifié ;
   - déterminer pour chaque entier x compris entre 1 et 6, l'unique entier y compris entre 1 et 6 tel que $xy\equiv 1\ [7]$.

Exercice 2 : *Critères de divisibilité* (4 points)

On désigne par p un nombre entier premier supérieur ou égal à 7. Le but de l'exercice est de démontrer que l'entier $n = p^4 - 1$ est divisible par 240, puis d'appliquer ce résultat.

1. Montrer que p est congru à -1 ou 1 modulo 3. En déduire que n est divisible par 3.
2. Justifier qu'il existe $k \in \mathbb{N}$ tel que $p^2 - 1 = 4k(k+1)$ puis montrer que n est divisible par 16.
3. Démontrer que 5 divise n.
4. Conclure.
5. Existe-t-il quinze nombres premiers p_1, p_2, $\cdots$ p_{15} supérieurs ou égaux à 7 tels que le nombre entier $A = (p_1)^4 + (p_2)^4 + \cdots + (p_{15})^4$ soit un nombre premier ?

Exercice 3 : *Codage* (7 points)

PARTIE A

1. Résoudre dans $\mathbb{Z}^2$ l'équation $13x - 7y = 3$.
2. Un cryptanalyste doit déchiffrer le message suivant : $YM \quad QMGGKAM \quad MGN \quad GMYZMN$
   Il sait seulement qu'il s'agit d'un cryptage affine du type $y \equiv ax + b$ [26] où x est le rang de la lettre avant cryptage (A a le rang 0, B a le rang 1, ..., Z a le rang 25, les correspondances sont indiquées dans le tableau en fin d'exercice) et où y est le rang de la lettre obtenue après cryptage ; a et b étant deux **entiers naturels strictement inférieurs à 26**. .
   Sachant que les lettres les plus fréquentes en français sont le E, puis le S, il fait donc la conjecture que la lettre M correspond à E et la lettre G à S.
   (a) Démontrer que la conjecture émise revient à résoudre le système $\begin{cases} 12 \equiv 4a + b \ [26] \\ 6 \equiv 18a + b \ [26] \end{cases}$
   (b) On suppose que $PGCD(a\,;26) = 1$. Montrer que si $ax + b \equiv ax' + b$ [26] alors $x \equiv x'$ [26].
   Pour que deux lettres distinctes soient cryptées par deux lettres distinctes, on suppose donc dans la suite de l'exercice que a ***et 26 sont premiers entre eux***
   (c) Déterminer a puis b

PARTIE B

1. Déterminer $a' \in \mathbb{N}$ tel que $7a' \equiv 1$ [26].
2. Démontrer l'équivalence suivante : $y \equiv 7x + 10$ [26] $\Leftrightarrow$ $x \equiv a'y + 6$ [26]
3. Décoder le message donné dans la partie A.

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25