Licence 2 - 2018/2019

HLMA304 : Arithmétique

Thierry Mignon

Janvier 2019

Examen de première session

Durée : 2h – Documents, calculatrices et téléphones interdits

Exercice 1. *(Cours)* Soit m, n deux entiers premiers entre eux et $(a, b) \in \mathbb{Z}$. On considère le système d'équation de congruence en x :

$$(\star) \qquad \begin{cases} x \equiv a\ [m] \\ x \equiv b\ [n] \end{cases} \quad , \quad x \in \mathbb{Z}$$

Montrer que le système $(\star)$ possède une solution.

Exercice 2. Au cours d'une partie de poker, Zoé souhaite compter combien elle possède de jetons. Elle sait qu'elle possède entre 300 et 400 jetons. Si elle les regroupe par 17, il lui en reste 9. Si elle les regroupe par 5, il lui en reste 3. Combien de jetons possède-t-elle ?

Indication : On pourra utiliser le théorème des restes chinois.

Exercice 3.

(1) Calculer, à l'aide du petit théorème de Fermat, le reste de la division euclidienne de 4^{2019} par 7.

(2) Pour quelles valeurs de l'entier n, le nombre $4^n + 2^n + 1$ est-il divisible par 7 ?

Exercice 4. Soit $a = c_n \cdots c_2 c_1$ un nombre écrit en base dix (où chaque c_i est l'un des chiffres $0, 1, \ldots, 9$).

(1) Calculer l'inverse de 10 dans $\mathbb{Z}/7\mathbb{Z}$.

(2) Montrer que a est multiple de 7 si et seulement si $c_n \cdots c_2 - 2c_1$ l'est. (*Par exemple, si* $a = 28$*, alors* $n = 2$*,* $c_2 = 2$*,* $c_1 = 8$*, et* a *est multiple de* 7 *car* $c_2 - 2c_1 = 2 - 2.8 = -14$ *l'est*).

(3) Montrer que a est multiple de 13 si et seulement si $c_n \cdots c_2 + 4c_1$ l'est.

(4) Généraliser à tout nombre premier autre que 2 et 5, et donner explicitement un test de divisibilité par 17.

Exercice 5. Soit p un nombre premier impair.

(1) Montrer que

$$\left(\left(\frac{p-1}{2}\right)!\right)^2 \equiv (-1)^{\frac{p-1}{2}}(p-1)!\ [p]$$

Indication : On peut transformer le produit $1 \times 2 \times \cdots \times (p-2) \times (p-1)$ *en un produit calculant* $\left(\left(\frac{p-1}{2}\right)!\right)^2$ *modulo* p *en effectuant des modifications de certains termes qui ne changent pas leur valeur modulo* p.

(2) Énoncer le théorème de Wilson.

(3) Déduire des questions précédente que, si $p \equiv 3[4]$

$$\left(\frac{p-1}{2}\right)! \equiv \pm 1[p].$$

Est-ce toujours le cas si $p \equiv 1[4]$?
(on pourra admettre la formule de la question (1)*).*

1 Session 2

Exercice 6. Soit $a \in \mathbb{N}$ tel que $a^n + 1$ soit premier, montrer que

$$\exists k \in \mathbb{N}, n = 2^k.$$

Que penser de la conjecture :

$$\forall n \in \mathbb{N}, 2^{2^n} + 1 \text{ est premier ?}$$

Exercice 7. Soient $a, b \in \mathbb{N}^* \setminus \{-1\}$ tels que $\text{pgcd}(a, b) = 1$. Soient $m, n \in \mathbb{N}^*$ et posons $\text{pgcd}(m, n) = d$. Montrer que $\text{pgcd}(a^n - b^n, a^m - b^m) = a^d - b^d$.

Exercice 8. Le but de l'exercice est de montrer que : si $(a, b) \in \mathbb{N}^*$ est un couple d'entier positifs tel que $ab + 1$ divise $a^2 + b^2$, alors le quotient

$$k = \frac{a^2 + b^2}{ab + 1}$$

est un carré parfait (le carré d'un nombre entier).

(1) Montrer que si $a = b$ alors $ab + 1$ ne divise pas $a^2 + b^2$.
Dans la suite On pose :

$$S = \{(a, b) \in \mathbb{N}^*, a < b, (ab + 1)|(a^2 + b^2)\}$$

(2) Montrer que S est non vide.

Dans la suite on note (a,b) un élément de S tel que $b = \min\{b', \quad (a',b') \in S\}$.

(3) Posons $k = \frac{a^2+b^2}{ab+1}$ Montrer que b est racine du polynôme :

$$P = X^2 - akX + (a^2 - k)$$

Soit b' la deuxième racine de ce polynôme.

(4) En considérant les relations coefficients/racines pour P, montrer que b' est entier.

(5) Montrer qu'on a : $k = \frac{a^2+b'^2}{ab'+1}$
a. En déduire que, si $b' = 0$, alors k est un carré.
b. En déduire que si $b' < 0$, alors $k < 0$.
On a donc : $b' \in \mathbb{N}^*$.

(6) En considérant les relations coefficients/racines pour P, montrer que $b' < a$. En déduire que le couple $(b', a) \in S$.
Conclure.

Exercice 9. Déterminer la parité des solutions entières de l'équation $x^3+6x^2+4x-9 = 0$

(1) Ces solutions sont-elles divisibles par 3 ?

(2) On note $P(x) = x^3 + 6x^2 + 4x - 9$. Montrer que – si $x \geq 1$, alors $P(x) \geq 1$. – si $x \leq 0$, alors $P(x) \leq x^2(x+6)$

(3) En déduire l'ensemble des solutions entières de l'équation $x^3 + 6x^2 + 4x - 9 = 0$.

Exercice 10. Soit $n \in \mathbb{N}$, $n \geq 2$. Soient $a, b \in \mathbb{Z}$ tels que $a \equiv b[n]$. Montrer que pour tout $k \in \mathbb{N}$, $a^{n^k} \equiv b^{n^k}[n^{k+1}]$.

Exercice 11.

(1) Soit a un entier. Soit m tel que $2^m \leq n \leq 2^{m+1}$. Montrer que le seul entier de $\{1, 2, \dots, n\}$ qui est divisible par 2^m est 2^m lui même.

(2) Montrer que $1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n}$ n'est pas entier (multiplier par 2^{m-1} et par un entier impair bien choisi, de sorte que tous les termes sauf un soient entiers.)

Exercice 12. Montrer que si $n \in \mathbb{N}^* \setminus \{1\}$, alors $n^4 + 4$ n'est jamais premier.

Exercice 13. Soient $p, n \in \mathbb{N}^*$ tels que $p, p + 2(n^2 + 1)$ et $p + 4(n^2 + 1)$ sont tous les trois premiers. Montrer que $p = 3$. (restes modulo...?)