HLMA304, Arithmétique
Examen, Première session, janvier 2017

— Durée : 2h —
Documents, calculatrices et téléphones portables sont interdits durant l'examen.

Les exercices pourront être traités dans n'importe quel ordre. On pourra admettre le résultat d'une question pour aborder les suivantes.

Exercice 1. Résoudre le système de congruence suivant :

$$\begin{cases} x \equiv 9 \quad [21] \\ x \equiv 11 \quad [25] \end{cases}$$

Correction : Appliquons l'algorithme d'Euclide étendu à 21 et 25 :

$$25 = 1.21 + 4, \qquad 21 = 5.4 + 1$$

donc $21 \wedge 25 = 1$ et,

$$1 = 21 - 5.4, \quad 1 = 21 - 5.(25 - 21), \quad 1 = 6.21 - 5.25$$

D'après la preuve du lemme théorème des restes chinois, on connait une solution particulière du système :

$$x_0 = 11.6.21 - 9.5.25 = 1386 - 1125 = 261$$

et les autres solutions sont congru à x_0 modulo $21.25 = 525$

$$S = \{261 + 525k, k \in \mathbb{Z}\}$$

Exercice 2.

(1) A l'aide de l'algorithme d'Euclide, trouver un inverse de 47 modulo 89.

Correction : Appliquons l'algorithme d'Euclide étendu à 47 et 89 :

$$89 = 1.47 + 42, \qquad 47 = 1.42 + 5 \qquad 42 = 8.5 + 2 \qquad 5 = 2.2 + 1$$

donc $89 \wedge 47 = 1$ et,

$$1 = 5 - 2.2, \quad 1 = 5 - 2.(42 - 8.5) = 17.5 - 2.42 \quad 1 = 17.(47 - 42) - 2.42 = 17.47 - 19.42$$
$$1 = 17.47 - 19.(89 - 47) = 36.47 - 19.89$$

Donc $36.47 \equiv 1[89]$ et $\overline{36}$ est un inverse de $\overline{47}$ dans $\mathbb{Z}/89\mathbb{Z}$.

(1) Résoudre l'équation :

$$47x \equiv 3[89]$$

Correction : On cherche les $x \in \mathbb{Z}$ tels que, dans $\mathbb{Z}/89\mathbb{Z}$, $\overline{47}.\overline{x} = \overline{3}$. On a, en utilisant le résultat de la question précédente :

$$\begin{aligned} & \overline{47}.\overline{x} = \overline{3} \\ \iff & \overline{36}.\overline{47}.\overline{x} = \overline{36}.\overline{3} \\ \iff & \overline{x} = \overline{108} = \overline{19} \end{aligned}$$

L'ensemble des solutions est donc :

$$S = \{19 + k89,\ k \in \mathbb{Z}\}$$

Exercice 3.

(1) Soient n, a, b, c trois entiers positifs tels que $4n = a^2 + b^2 + c^2$. Montrer que n est aussi une somme de trois carrés

Indication : on pourra considérer les parités respectives de a, b et c.

Correction : On peut travailler dans $\mathbb{Z}/4\mathbb{Z}$ et considérer les carrés de $\mathbb{Z}/4\mathbb{Z}$ qui sont $\overline{0}$ et $\overline{1}$.

Voici une autre preuve sans passage au quotient :
La parité d'un entier ne change pas par élévation au carré. La somme de trois entiers ne peut être paire que si les trois entiers sont pairs ou si un seul est pair et les deux autres impairs.
Considérons ce dernier cas. A permutation près, on peut supposer que $a = 2a' + 1, b = 2b' + 1, c = 2c'$. On a alors :

$$4n = 4a'^2 + 4a' + 1 + 4b'^2 + 4b' + 1 + 4c'^2 \implies 4(n - a'^2 - a' - b'^2 - b' - c'^2) = 2$$

Donc 4 divise 2, ce qui est impossible.
Ainsi, a, b et c sont tous les trois pairs ; on peut écrire $a = 2a', b = 2b', c = 2c'$ et on obtient :

$$n = a'^2 + b'^2 + c'^2.$$

(1) Montrer qu'aucun entier de la forme $4^m(8k + 7)$ n'est somme de trois carrés.

Indication : on pourra réduire le problème à l'aide du (1), puis travailler dans $\mathbb{Z}/8\mathbb{Z}$.

Correction : Supposons que $d = 4^m(8k + 7)$ est somme de trois carrés. D'après la question précédente, si $m \geq 1$, $4^{m-1}(8k + 1)$ est aussi somme de trois carrés. On recommence si nécessaire, et on en déduit que $8k + 1$ est aussi somme de trois carrés.
Calculons les carrés de $\mathbb{Z}/8\mathbb{Z}$:

$$\overline{0}^2 = \overline{0} \qquad (-\overline{1})^2 = \overline{1}^2 = \overline{1} \qquad (-\overline{2})^2 = \overline{2}^2 = \overline{4} \qquad (-\overline{3})^2 = \overline{3}^2 = \overline{1} \qquad \overline{4}^2 = \overline{0}$$

L'ensemble des carrés de $\mathbb{Z}/8\mathbb{Z}$ est donc : $\{\overline{0}, \overline{1}, \overline{4}\}$.

CORRECTION : Les sommes possibles de trois éléments de cet ensemble sont :

$$\begin{array}{lll} \overline{0}+\overline{0}+\overline{0}=\overline{0}, & \overline{0}+\overline{0}+\overline{1}=\overline{1}, & \overline{0}+\overline{0}+\overline{4}=\overline{4} \\ \overline{0}+\overline{1}+\overline{1}=\overline{2}, & \overline{0}+\overline{1}+\overline{4}=\overline{5}, & \overline{0}+\overline{4}+\overline{4}=\overline{0} \\ \overline{1}+\overline{1}+\overline{1}=\overline{3}, & \overline{1}+\overline{1}+\overline{4}=\overline{6}, & \overline{1}+\overline{4}+\overline{4}=\overline{1}, \quad \overline{4}+\overline{4}+\overline{4}=\overline{4} \end{array}$$

On observe que le seul éléments de $\mathbb{Z}/8\mathbb{Z}$ qui ne peut être écrit de cette façon est $\overline{7}$. Donc, $8k+7$ n'est pas somme de trois carrés.

Exercice 4. Soit X l'ensemble des nombres premiers de la forme $4k+3$ avec $k \in \mathbb{N}$.

(1) Montrer que X est non vide.

CORRECTION : $3 = 4.0 + 3$

(1) Montrer que le produit de nombres de la forme $4k+1$ est encore de cette forme.

CORRECTION : Les entiers de cette forme sont des entiers congru à 1 modulo 4. Dans $\mathbb{Z}/4\mathbb{Z}$, $\overline{1}.\overline{1} = \overline{1}$: le produit de deux entiers congru à 1 modulo 4 est encore congru à 1 modulo 4.

(1) On suppose que X est fini et on l'écrit alors $X = \{p_1, \ldots, p_n\}$. Soit

$$a = 4p_1p_2 \cdots p_n - 1.$$

Montrer par l'absurde que a admet un diviseur premier de la forme $4k+3$.

CORRECTION : Puisque a est impair, tous ses diviseurs premiers le sont.
Un nombre premier impair est soit congru à 1, soit congru à 3 modulo 4. Supposons que a ne possède que des diviseurs congru à 1 modulo 4. On peut écrire :

$$a = \prod_{i=1}^{r} q_i$$

où les q_i sont des nombres premiers tel que $\overline{q_i} = \overline{1}$ dans $\mathbb{Z}/4\mathbb{Z}$ (un même nombre premier peut être répété plusieurs fois dans ce produit).
On voit que $\overline{a} = \prod_{i=1}^{r} \overline{q_i} = \prod_{i=1}^{r} \overline{1} = \overline{1}$. Ce n'est pas possible puisque, dans $\mathbb{Z}/4\mathbb{Z}$,

$$\overline{a} = \overline{4\overline{p_1p_2\cdots p_n}} - \overline{1} = -\overline{1}, \text{ et } -\overline{1} \neq \overline{1} \text{ dans } \mathbb{Z}/4\mathbb{Z}.$$

L'entier a possède donc au moins un diviseur premier congru à 3 modulo 4.

(1) Montrer que ceci est impossible et donc que X est infini.

CORRECTION : L'un des éléments de X divise a. On peut supposer que c'est p_1. On peut donc écrire : $kp_1 = 4p_1p_2 \ldots p_n - 1$ (avec $k \in \mathbb{Z}$), donc p_1 divise 1 : contradiction.

Exercice 5.

(1) On souhaite démontrer que 2017 est un nombre premier.

a. Soit $X = \{p_1, \ldots, p_n\}$ l'ensemble des nombres premiers inférieurs ou égaux à $\sqrt{2017}$. Montrer que, si 2017 n'est divisible par aucun élément de X, c'est un nombre premier.

CORRECTION : Supposons que 2017 n'est pas premier. Soit p un diviseur premier de 2017, alors $b = 2017/p \geq 2$. Soit q un diviseur premier de b. Alors pq divise 2017 ce qui implique :

$$pq \leq 2017.$$

Mais puisque p, q ne sont pas éléments de X, on a : $p > \sqrt{2017}$, $q > \sqrt{2017}$, donc :

$$pq > 2017.$$

Contradiction

b. Trouver l'ensemble X.

CORRECTION : On observe (éventuellement par tâtonnement que : $44^2 = 1936$, $45^2 = 2025$. Puisque 44 est pair et n'est pas premier, L'ensemble X est donc l'ensemble des entiers premiers inférieurs ou égaux à 43.
On peut utiliser le crible d'Eratosthène en écrivant la liste des entiers entre 2 et 43.

		2	3	~~4~~	5	~~6~~	7	~~8~~	~~9~~
~~10~~	11	~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19
~~20~~	~~21~~	~~22~~	23	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	29
~~30~~	31	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~	37	~~38~~	~~39~~
~~40~~	41	~~42~~	43						

On obtient :

$$X = \{2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43\}$$

c. On admettra que 2017 n'est divisible par aucun des entiers 13, 17, 19, 23, 29, 31, 37, 41, 43. Montrer que 2017 est un nombre premier.

CORRECTION : Au vu de l'ensemble X ci-dessus, il reste à s'assurer que 2017 n'est divisible par aucun des entiers $2, 3, 5, 7, 11$.
Puisque 2017 ne se termine pas par un nombre pair, il n'est pas divisible par 2. Puisqu'il ne se termine pas par 0 ou 5, il n'est pas divisible par 5. La somme de ses chiffres vaut $2+0+1+7 = 10$ qui n'est pas un multiple de 3, donc 2017 n'est pas divisible par 3. La somme alternée de ses chiffres vaut : $2 - 0 + 1 - 7 = -4$ et n'est pas nulle, donc 2017 n'est pas divisible par 11.
Pour la divisibilité par 7, nous ne possédons pas de critère rapide, nous effectuons la division euclidienne :

$$2017 = 288.7 + 1$$

le reste n'est pas nul, donc 2017 n'est pas non plus divisible par 7, et est premier.

(1) Donner le reste de la division euclidienne de 2015^{2016} par 2017.

CORRECTION : D'après le petit théorème de Fermat, ce reste vaut 1.