Examen terminal du mercredi 6 janvier 2016
Durée : 2 h

Les documents de cours, calculatrices et téléphone portables ne sont pas autorisés.
Le sujet comporte SIX exercices.
Le barème est donné à titre indicatif.
Toutes les réponses doivent être justifiées.

Exercice 1 (3 points)

1. Montrer que dans un ensemble de cardinal 10, deux sous-ensembles de cardinal 7 ont une intersection non vide.
2. Dessiner (si possible) trois ensembles A, B et C avec cinq éléments chacun et dont la réunion $A \cup B \cup C$ a neuf éléments et l'intersection $A \cap B \cap C$ aucun.
3. Soient A, B et C trois sous-ensembles d'un ensemble E tels que $A \cup B = B \cap C$.
   Montrer que $A \subset B \subset C$.

Solution de l'exercice 1

1. Soient E un ensemble de cardinal 10 et A et B deux sous-ensembles de E de cardinal 7. On a
$$\text{card}(A \cup B) = \text{card}A + \text{card}B - \text{card}(A \cap B) = 14 - \text{card}(A \cap B)$$
   Or $A \cup B \subset E$ donc $\text{card}(A \cup B) \leqslant \text{card}E = 10$. On en déduit que $\text{card}(A \cap B) = 14 - \text{card}(A \cup B) \geqslant 14 - 10 = 4$. Donc $A \cap B$ est non vide.
2. Par exemple, $E = \mathbb{N}$, $A = \{1, 2, 3, 4, 5\}$, $B = \{4, 5, 6, 7, 8\}$ et $C = \{1, 2, 3, 6, 9\}$. Alors $A \cup B \cup C = \{1, 2, 3, 4, 5, 6, 7, 8, 9\}$ a pour cardinal 9 et $A \cap B \cap C = \emptyset$.
3. Soit $x \in A$. Alors $x \in A \cup B$. Or $A \cup B = B \cap C$ donc $x \in B \cap C \subset B$. On a montré que $A \subset B$. De même, soit $x \in B$. Alors $x \in A \cup B$. Or $A \cup B = B \cap C$ donc $x \in B \cap C \subset C$. On a montré que $B \subset C$.

Exercice 2 (2 points)

Trouver le reste de la division euclidienne de $2\,228^{5\,555}$ par 11.

Solution de l'exercice 2

On remarque que $2\,222$ est divisible par 11 donc $2\,228 \equiv 6 \pmod{11}$. On en déduit que $2\,228^{5\,555} \equiv 6^{5\,555} \pmod{11}$. Or 11 est un nombre premier et 6 est premier avec 11, donc, d'après le théorème de Fermat, $6^{10} \equiv 1 \pmod{11}$.
On a a alors $6^{5\,555} = 6^{10 \times 555 + 5} = (6^{10})^{555} \times 6^5 \equiv 6^5 \pmod{11}$.
Or $6^5 = 6^2 \times 6^2 \times 6 = 36 \times 36 \times 6 \equiv 3 \times 3 \times 6 \pmod{11} \equiv 9 \times 6 \pmod{11} \equiv 54 \pmod{11} \equiv -1 \pmod{11}$.
On en déduit que le reste de la division euclidienne de $2\,228^{5\,555}$ par 11 est 10.

Exercice 3 (3 points)

Soient E et F deux ensembles.

1. En utilisant les quantificateurs, donner la définition d'une fonction injective de E dans F.
2. Montrer que la fonction $f : \mathbb{R} \setminus \{3\} \to \mathbb{R}$ définie par $f(x) = \dfrac{x + 17}{x - 3}$ est injective.
3. Calculer l'image $f(\mathbb{R} \setminus \{3\})$. La fonction f est-elle surjective ?

Solution de l'exercice 3

1. La fonction f est injective de E dans F si une des propriétés suivantes est vérifiée :
   $\forall x \in E, \forall x' \in E, f(x) = f(x') \Longrightarrow x = x'$
   $\forall (x, x') \in A^2, \quad [x \neq x' \Longrightarrow f(x) \neq f(x')]$
2. Soient x et x' deux éléments de $\mathbb{R} \setminus \{3\}$ tels que $f(x) = f(x')$. On a alors $\dfrac{x+17}{x-3} = \dfrac{x'+17}{x'-3}$, soit en faisant le produit en croix $(x+17)(x'-3) = (x'+17)(x-3)$. En développant les facteurs, on obtient $x = x'$. Donc la fonction f est injective de $\mathbb{R} \setminus \{3\}$ dans $\mathbb{R}$.
3. On a $f(x) = 1 - \dfrac{20}{x-3}$, la fonction f est donc strictement croissante sur chacun des intervalles $]-\infty, 3[$ et $]3, +\infty[$. Or $\lim_{x \to +\infty} f(x) = \lim_{x \to -\infty} f(x) = 1$, $\lim_{x \to 3^-} f(x) = +\infty$ et $\lim_{x \to 3^+} f(x) = -\infty$. On en déduit que $f(\mathbb{R} \setminus \{3\}) = \mathbb{R} \setminus \{1\}$.
   La fonction f n'est donc pas surjective car 1 n'a pas d'antécédent par f.

Exercice 4 (2 points)

Résoudre sur $\mathbb{Z}$ l'équation $55n \equiv 9 \pmod{72}$.

Solution de l'exercice 4

Les décompositions en produit de facteurs premiers de 55 et 72 sont $55 = 5 \times 11$ et $72 = 2^3 3^2$ donc les entiers 55 et 72 sont premiers entre eux. On en déduit que 55 admet un inverse modulo 72.
L'algorithme d'Euclide s'écrit :

$$\begin{array}{rcl} 72 & = & 1 \times 55 + 17 \\ 55 & = & 3 \times 17 + 4 \\ 17 & = & 4 \times 4 + 1 \end{array}$$

(Ce qui permet également de montrer que 55 et 72 sont premiers entre eux).
En remontant l'algorithme d'Euclide (on peut aussi utiliser l'algorithme d'Euclide étendu), on obtient

$$\begin{array}{rcl} 1 & = & 17 - 4 \times 4 \\ & = & 17 - 4 \times (55 - 3 \times 17) = 13 \times 17 - 4 \times 55 \\ & = & 13 \times (72 - 55) - 4 \times 55 = 13 \times 72 - 17 \times 55 \end{array}$$

On en déduit que $-17 \times 55 \equiv 1 \pmod{72}$ donc -17 est un inverse de 55 modulo 72.
Alors, pour tout entier n :
$55n \equiv 9 \pmod{72}$ si, et seulement si, $-17 \times 55n \equiv -17 \times 9 \pmod{72}$. Cette dernière égalité se réécrit $n \equiv -153 \equiv -9 \pmod{72}$, donc les solutions sont les entiers de la forme $-9 + 72k$, pour $k \in \mathbf{Z}$.
Remarque : l'équivalence entre les deux équations aux congruences $55n \equiv 9 \pmod{72}$ et $-17 \times 55n \equiv -17 \times 9 \pmod{72}$ vient du fait qu'on retrouve la première en multipliant la seconde par 55.

Exercice 5 (6 points)

1. Soient p un nombre premier et $a \in \mathbb{Z}$.
   Montrer que $\text{pgcd}(a, p) = 1$ si, et seulement si, p ne divise pas a.
2. Soit $(a, b, c) \in \mathbb{Z}^3$.
   Montrer que, si $\text{pgcd}(a, b) = 1$ et $\text{pgcd}(a, c) = 1$, alors $\text{pgcd}(a, bc) = 1$.
   La réciproque est-elle vraie ? Justifier.
3. À l'aide d'une récurrence soigneusement écrite, montrer que
   $$\forall (a, b) \in \mathbb{Z}^2, \ (\text{pgcd}(a, b) = 1 \Longrightarrow \forall n \in \mathbb{N}, \ \text{pgcd}(a, b^n) = 1).$$
4. Montrer que, pour tout entier naturel n non nul, on a $\text{pgcd}(2, 4^n + 7^n) = \text{pgcd}(7, 4^n + 7^n) = 1$.
   On pourra utiliser les première et troisième questions.
5. Pour tout entier naturel n non nul, déterminer la valeur explicite de $\text{pgcd}(56, 4^n + 7^n)$.

Solution de l'exercice 5

1. p est premier et, par définition, $\text{pgcd}(a, p)$ est un diviseur de p. On en déduit que $\text{pgcd}(a, p)$ vaut 1 ou p. Alors, $\text{pgcd}(a, p) = p$ si, et seulement, si p divise a. Ainsi, $\text{pgcd}(a, p) = 1$ si, et seulement si, $\text{pgcd}(a, p) \neq p$, ce qui est équivalent à : p ne divise pas a.

2. On va montrer que $\text{pgcd}(a, b) = 1$ et $\text{pgcd}(a, c) = 1$ si, et seulement si, $\text{pgcd}(a, bc) = 1$. Il y a deux méthodes pour répondre à la question : on peut utiliser le théorème de Bézout, ou raisonner sur les facteurs premiers des pgcd qui entrent en jeux.
Avec les combinaisons de Bézout : Supposons $\text{pgcd}(a, b) = 1$ et $\text{pgcd}(a, c) = 1$, et soient u, v, u', v' des entiers tels que $au + bv = 1$ et $au' + cv' = 1$ (ils existent d'après le théorème de Bézout). Alors, en multipliant ces égalités, on a $(au + bv)(au' + cv') = 1$, soit :

$$a(auu' + ucv' + bvu') + bc(vv') = 1$$

ce qui montre que a et bc sont premiers entre eux, toujours par le théorème de Bézout.
Réciproquement, si a et bc sont premiers entre eux, on a des entiers u et v tels que $au + bcv = 1$. Cette identité de Bézout fournit une identité de Bézout entre a et b, ainsi qu'entre a et c, ce qui montre $\text{pgcd}(a, b) = 1$ et $\text{pgcd}(a, c) = 1$.
Avec les facteur premiers : On va montrer la contraposée de la première implication : supposons $\text{pgcd}(a, bc) \neq 1$, et considérons un facteur premier p de $\text{pgcd}(a, bc)$, ce qui est possible car tout entier naturel strictement plus grand que 1 admet un diviseur premier. Alors, p divise bc. Mais, par le lemme d'Euclide, si p divise bc, alors p divise b ou p divise c. Mais p divisant aussi a, on en déduit que p divise $\text{pgcd}(a, b)$, ou que p divise $\text{pgcd}(a, c)$. Dans tous les cas, l'assertion "$\text{pgcd}(a, b) = 1$ et $\text{pgcd}(a, c) = 1$" est fausse, car l'un de deux pgcd à un diviseur premier, d'où le résultat.
Réciproquement, supposons $\text{pgcd}(a, bc) = 1$. $\text{pgcd}(a, b)$ et $\text{pgcd}(a, c)$ sont des diviseurs de $\text{pgcd}(a, bc) = 1$ car tous deux divisent a et bc, donc $\text{pgcd}(a, b) = 1$ et $\text{pgcd}(a, c) = 1$.

3. Soient a et b deux entiers premiers entre eux. Montrons par récurrence sur l'entier n, que :

$$\forall n \in \mathbf{N}, \text{pgcd}(a, b^n) = 1$$

La propriété dépendant de l'entier n intervenant dans la récurrence, est donc (H_n) : $\text{pgcd}(a, b^n) = 1$.
Initialisation : Au rang 0, l'énoncé à montrer est : $\text{pgcd}(a, b^0) = 1$. Mais $b^0 = 1$, donc il faut montrer $\text{pgcd}(a, 1) = 1$ ce qui est vrai pour tout entier a.
Hérédité : Soit n un entier naturel, supposons que $\text{pgcd}(a, b^n) = 1$ (H_n) et montrons que a et b^{n+1} sont premiers entre eux (H_{n+1}). On sait que $\text{pgcd}(a, b) = 1$ (par hypothèse) et $\text{pgcd}(a, b^n) = 1$ (par hypothèse de récurrence). D'après la question précédente, on en déduit que $\text{pgcd}(a, bb^n) = 1$, i.e. que $\text{pgcd}(a, b^{n+1}) = 1$, ce qui est bien la propriété voulue au rang $n + 1$.
La propriété est héréditaire, donc par le principe de récurrence, on a bien montré que :

$$\forall n \in \mathbf{N}, \text{pgcd}(a, b^n) = 1$$

4. Soit n un entier strictement positif. L'entier 2 étant premier donc,pour montrer que $\text{pgcd}(2, 4^n + 7^n) = 1$, il suffit, d'après la question 1, de montrer que 2 ne divise pas $4^n + 7^n$ (et de même pour 7). On constate que 2 divise 4^n (n étant non nul, on peut écrire $4^n = 2(2.4^{n-1})$), et que 2 ne divise pas 7^n. En effet, 2 et 7 sont premiers entre eux (car $7 - 3 \times 2 = 1$, ou encore car deux nombres premiers distincts sont premiers entre eux), donc d'après la question précédente, 2 et 7^n sont aussi premiers entre eux. Raisonnons maintenant par l'absurde : si 2 divisait $4^n + 7^n$, puisque 2 divise aussi 4^n, on aurait que 2 divise la différence $4^n + 7^n - 4^n = 7^n$, mais on déjà prouvé le contraire, d'où une contradiction. On prouve ainsi que 2 et $4^n + 7^n$ sont premiers entre eux.
Le raisonnement est le même pour 7 : 7 divise 7^n, mais pas 4^n. Si par l'absurde, 7 n'était pas premier avec $4^n + 7^n$, alors par la question 1, 7 diviserait $4^n + 7^n$, donc aussi $4^n + 7^n - 7^n = 4^n$, ce qui est une contradiction.

5. D'après la question 4, $4^n + 7^n$ est premier avec 2 et 7, donc aussi avec $2^3 = 8$ (question 3). Mais alors, $4^n + 7^n$ étant premier avec 8 et 7, la question 1 montre que $4^n + 7^n$ est premier avec $8 \times 7 = 56$, ce qui répond à la question : $\text{pgcd}(56, 4^n + 7^n) = 1$.

Tourner la page S.V.P.

Exercice 6 (6 points)

Soient n un entier naturel et E un ensemble fini à n éléments.
On note X l'ensemble des couples (A, B) composés de deux parties de E telles que $A \subset B$.
L'objet de l'exercice est de montrer que $\text{card}(X) = 3^n$.

1. Donner le cardinal de l'ensemble $\mathcal{P}(E)$ des sous-ensembles de E. (*On ne demande pas de justification.*)
2. Dans cette question seulement, on suppose $n = 2$ et $E = \{1, 2\}$. Déterminer X.
3. Énoncer la formule du binôme de Newton pour deux réels x et y.
4. Soit $j \in \{0, \ldots, n\}$, on note X_j l'ensemble des paires $(A, B) \in X$ telles que $\text{card}(B) = j$. Montrer que $\{X_j\}_{0 \leqslant j \leqslant n}$ est une partition de X.
5. On veut choisir $(A, B) \in X_j$.
   Combien de choix possibles y a-t-il pour B ?
   Une fois B choisie, combien de choix possibles y a-t-il pour A ?
6. En déduire le cardinal de X_j, puis celui de X.

Solution de l'exercice 6

1. Si $\text{card}(E) = n$, alors $\text{card}(\mathcal{P}(E)) = 2^n$.
2. $X = \{(\emptyset, \emptyset), (\emptyset, \{1\}), (\emptyset, \{2\}), (\emptyset, E), (\{1\}, \{1\}), (\{2\}, \{2\}), (\{1\}, E), (\{2\}, E), (E, E)\}$
3. Soit x et y deux réels et n un entier naturel alors

$$(x+y)^n = \sum_{p=0}^{n} \binom{n}{p} x^p y^{n-p} = \sum_{p=0}^{n} \binom{n}{p} x^{n-p} y^p$$

4. Soient $j \in \{0, \ldots, n\}$ et B un sous-ensemble de E avec j éléments. Comme $B \subset B$, on a $(B, B) \in X_j$. Donc X_j est non vide.
   Soient $i \in \{0, \ldots, n\}$ et $j \in \{0, \ldots, n\}$ tels que $i \neq j$. Supposons que $X_i \cap X_j$ soit non vide. Il existe alors $(A, B) \in X_i \cap X_j$. On a donc, à la fois, $\text{card}(B) = i$ et $\text{card}(B) = j$. Or $i \neq j$. Absurde donc $X_i \cap X_j = \emptyset$.
   On a $\cup_j X_j \subset X$. Soit $(A, B) \in X$. B est un ensemble fini car inclus dans E. Posons $i = \text{card}(B)$, alors $0 \leqslant i \leqslant n$. On a montré que $(A, B) \subset X_i$. On a donc $\cup_j X_j = X$ et $\{X_j\}_{0 \leqslant j \leqslant n}$ est une partition de X.
5. B est un sous-ensemble à j éléments d'un ensemble à n éléments. Il y a donc $\binom{n}{j}$ choix pour B. Une fois B choisie, l'ensemble A est choisi comme étant un sous-ensemble de B. Or un ensemble de j éléments a 2^j sous-ensembles.
6. L'ensemble X_j a donc $2^j \times \binom{n}{j}$ éléments. Comme $\{X_j\}_{0 \leqslant j \leqslant n}$ est une partition de X, on a

$$\text{card} X = \sum_{j=0}^{n} \text{card} X_j = \sum_{j=0}^{n} 2^j \times \binom{n}{j}.$$

   Si on fait $x = 2$ et $y = 1$ dans la formule du binôme, on en déduit que $\text{card} X = 3^n$.