Algèbre et arithmétique 1 - Examen 2010-2011 1e session - corrigé

Exercice 1

1- a-

$$\begin{array}{r|l} 3673 & 8 \\ \cline{2-2} 47 & 459 \\ 73 & \\ 1 & \end{array} \qquad \begin{array}{r|l} 459 & 8 \\ \cline{2-2} 59 & 57 \\ 3 & \end{array} \qquad \begin{array}{r|l} 57 & 8 \\ \cline{2-2} 1 & 7 \end{array}$$

Le nombre 3673 s'écrit $\overline{7131}^{(8)}$ en base huit.

1- b-

On a : $\overline{3042}^{(5)} = ((3\times 5 + 0)\times 5 + 4)\times 5 + 2$

$= (15 \times 5 + 4)\times 5 + 2$

$= 79 \times 5 + 2$

$= 397$

Le nombre $\overline{3042}^{(5)}$ s'écrit 397 en base dix.

2-

On utilise l'algorithme d'Euclide étendu.

$$\begin{aligned} 1980 &= 1078 \times 1 + 902 \\ 1078 &= 902 \times 1 + 176 \\ 902 &= 176 \times 5 + 22 \\ 176 &= 22 \times 8 + 0 \end{aligned} \qquad \begin{aligned} 1980 &= 1980 \times 1 + 1078 \times 0 \\ 1078 &= 1980 \times 0 + 1078 \times 1 \\ 902 &= 1980 \times 1 + 1078 \times (-1) \\ 176 &= 1980 \times (-1) + 1078 \times 2 \\ 22 &= 1980 \times 6 + 1078 \times (-11) \end{aligned}$$

On a $\mathrm{pgcd}(1078, 1980) = 22$ (dernier reste non nul), et $1078 \times (-11) + 1980 \times 6 = 22$, donc les entiers $u = -11$ et $v = 6$ conviennent.

3-

Si $(x,y) \in \mathbb{R}^2$, on a : $(y-x)^6 = \sum_{k=0}^{6} \binom{6}{k} y^k (-x)^{6-k}$ (formule du binôme),

c'est-à-dire : $(y-x)^6 = x^6 - 6x^5y + 15x^4y^2 - 20x^3y^3 + 15x^2y^4 - 6xy^5 + y^6$.

1
1 1
1 2 1
1 3 3 1
1 4 6 4 1
1 5 10 10 5 1
1 6 15 20 15 6 1

4- a-

Théorème (petit théorème de Fermat) :

Soit p un nombre premier. Pour tout entier $a \in \mathbb{Z}$, on a $a^p \equiv a \pmod p$, et de plus, si a est premier à p, on a $a^{p-1} \equiv 1 \pmod p$.

4- b-

Comme x est premier à pq, l'entier x est premier à p, donc $x^{p-1} \equiv 1 \pmod p$ d'après le petit théorème de Fermat, donc $x^{(p-1)(q-1)} \equiv 1^{q-1} \equiv 1 \pmod p$, donc $p \mid x^{(p-1)(q-1)} - 1$.

De même, x est premier à pq donc à q, donc $x^{q-1} \equiv 1 \pmod q$, donc $x^{(p-1)(q-1)} \equiv 1 \pmod q$, donc $q \mid x^{(p-1)(q-1)} - 1$.

On a donc $\begin{cases} p \mid x^{(p-1)(q-1)} - 1 \\ q \mid x^{(p-1)(q-1)} - 1 \end{cases}$, et p et q sont premiers entre eux car ce sont des nombres premiers distincts,

donc $pq \mid x^{(p-1)(q-1)} - 1$ par le théorème de Gauss, c'est-à-dire $x^{(p-1)(q-1)} \equiv 1 \pmod{pq}$.

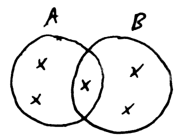
Exercice 2

Notons A, B, C, D les quatre ensembles. On a

$$\begin{cases} \operatorname{Card} A = \operatorname{Card} B = \operatorname{Card} C = \operatorname{Card} D = 3 \\ \operatorname{card}(A\cap B) = \operatorname{Card}(A\cap C) = \operatorname{Card}(A\cap D) = \operatorname{Card}(B\cap C) = \operatorname{Card}(B\cap D) = \operatorname{Card}(C\cap D) = 1 \\ \operatorname{card}(A\cup B\cup C\cup D) = 6 \end{cases}$$

On en déduit :

$\operatorname{Card}(A\setminus B) = \operatorname{Card}(A\setminus(A\cap B)) = \operatorname{Card} A - \operatorname{Card}(A\cap B) = 3-1 = 2$ (car $A\cap B \subset A$)



$\operatorname{card}(B\setminus A) = 2$ (de même)

$\operatorname{card}(A\cup B) = \operatorname{Card} A + \operatorname{Card} B - \operatorname{Card}(A\cap B) = 3+3-1 = 5$ (principe d'inclusion-exclusion)

Comme $A\cap B\cap C \subset A\cap B$ et $\operatorname{Card}(A\cap B) = 1$, on a $\operatorname{card}(A\cap B\cap C) \in \{0,1\}$.

Le principe d'inclusion-exclusion appliqué à $A\cap C$ et $B\cap C$ donne alors

$$\begin{aligned} \operatorname{Card}\big((A\cap C)\cup(B\cap C)\big) &= \operatorname{Card}(A\cap C) + \operatorname{Card}(B\cap C) - \operatorname{Card}(A\cap B\cap C) \\ &= 1+1 - \operatorname{Card}(A\cap B\cap C) \\ &\in \{1,2\}. \end{aligned}$$

Le principe d'inclusion-exclusion appliqué à $A\cup B$ et C donne :

$\operatorname{Card}((A\cup B)\cap C) + \operatorname{Card}(A\cup B\cup C) = \operatorname{card}(A\cup B) + \operatorname{Card} C = 5+3 = 8$,

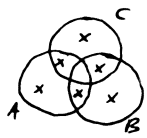
or $(A\cup B)\cap C = (A\cap C)\cup(B\cap C)$ donc $\operatorname{Card}((A\cup B)\cap C) = \operatorname{Card}((A\cap C)\cup(B\cap C)) \in \{1,2\}$

et $A\cup B \subset A\cup B\cup C \subset A\cup B\cup C\cup D$ donc $5 \leq \operatorname{Card}(A\cup B\cup C) \leq 6$.

Pour avoir $\operatorname{Card}((A\cup B)\cap C) + \operatorname{Card}(A\cup B\cup C) = 8$, on a nécessairement $\operatorname{Card}((A\cup B)\cap C) = 2$ et $\operatorname{Card}(A\cup B\cup C) = 6$.

On en déduit $\operatorname{Card}(A\cap B\cap C) = 2 - \operatorname{Card}((A\cap C)\cup(B\cap C)) = 2-2 = 0$, et $A\cup B\cup C = A\cup B\cup C\cup D$ donc $D\subset A\cup B\cup C$.

De plus, $\begin{cases} \operatorname{Card}(C\setminus(A\cup B)) = \operatorname{Card}(C\setminus((A\cup B)\cap C)) = 3-2 = 1. \\ \operatorname{card}((A\cap B)\setminus C) = \operatorname{Card}((A\cap B)\setminus(A\cap B\cap C)) = 1-0 = 1 \end{cases}$



Enfin, $A\cap B\cap D = A\cap C\cap D = B\cap C\cap D = \emptyset$ (comme pour $A\cap B\cap C = \emptyset$),

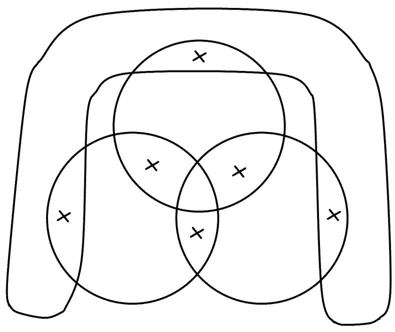
donc $D\cap A\cap(B\cup C) = (A\cap B\cap D)\cup(A\cap C\cap D) = \emptyset$, $D\cap B\cap(A\cup C) = \emptyset$, $D\cap C\cap(A\cup B) = \emptyset$, **or $D\subset A\cup B\cup C$**,

donc $D\subset (A\setminus(B\cup C))\cup(B\setminus(A\cup C))\cup(C\setminus(A\cup B))$, or $\operatorname{Card}(A\setminus(B\cup C)) = \operatorname{Card}(B\setminus(A\cup C)) = \operatorname{Card}(C\setminus(A\cup B)) = 1$,

et les ensembles $A\setminus(B\cup C)$, $B\setminus(A\cup C)$, $C\setminus(A\cup B)$ sont deux à deux disjoints, et $\operatorname{Card} D = 3$,

donc $D = (A\setminus(B\cup C))\cup(B\setminus(A\cup C))\cup(C\setminus(A\cup B))$.

On trouve donc la figure suivante, qui vérifie bien toutes les propriétés demandées par l'énoncé.



Exercice 3

Si $A = \emptyset$ et $B = \emptyset$, on a

$A \triangle B = (A \setminus B) \cup (B \setminus A) = (\emptyset \setminus \emptyset) \cup (\emptyset \setminus \emptyset) = \emptyset \cup \emptyset = \emptyset$

$A \cap B = \emptyset \cap \emptyset = \emptyset$

donc $A \triangle B = A \cap B$.

Si $A \triangle B = A \cap B$, alors :

- si $x \in A$, alors :
  - si $x \in B$, on a $x \in A \cap B = A \triangle B = (A \setminus B) \cup (B \setminus A)$,
    donc $x \in A \setminus B$ ou $x \in B \setminus A$,
    or $x \notin A \setminus B$ car $x \in B$, et $x \notin B \setminus A$ car $x \in A$,
    donc c'est impossible ;
  - si $x \notin B$, alors $x \in A \setminus B$ donc $x \in A \triangle B = A \cap B$,
    donc $x \in B$, donc c'est impossible ;

  donc on trouve une contradiction, donc $A = \emptyset$;
- si $x \in B$, alors :
  - si $x \in A$, alors $x \in A \cap B = A \triangle B$,
    donc $x \in A \setminus B$ ou $x \in B \setminus A$, ce qui est impossible car $x \in B$ et $x \in A$;
  - si $x \notin A$, alors $x \in B \setminus A \subset A \triangle B = A \cap B$ donc $x \in A$,
    ce qui est impossible ;

  donc $B = \emptyset$,

donc $A = \emptyset$ et $B = \emptyset$.

On a donc $A \triangle B = A \cap B$ si et seulement si $A = \emptyset$ et $B = \emptyset$.

Exercice 4

1-

Soit $k \in \mathbb{N}$. On a
$$\begin{aligned} 3^{3(k+1)} &\equiv 27^{k+1} \pmod{13} && \text{car } 3^3 = 27 \\ &\equiv 1^{k+1} \pmod{13} && \text{car } 27 \equiv 1 \pmod{13} \\ &\equiv 1 \pmod{13} \end{aligned}$$

donc : $\forall k \in \mathbb{N} \quad 13 \mid 3^{3(k+1)} - 1$.

2 -

Notons, pour tout entier $n \in \mathbb{N}$, $\mathcal{P}(n)$ la propriété : $169 \mid 3^{3(n+1)} - 26n - 27$.

• La propriété $\mathcal{P}(0)$ est vraie. En effet, on a

$$3^{3\cdot(0+1)} - 26\cdot 0 - 27 = 3^3 - 27 = 0,$$

et 0 est bien divisible par 169.

• Supposons que la propriété $\mathcal{P}(n)$ est vérifiée pour un certain entier $n \in \mathbb{N}$.
On a alors $3^{3(n+1)} - 26n - 27 \equiv 0 \pmod{169}$,

donc
$$\begin{aligned} 3^{3(n+2)} - 26(n+1) - 27 &\equiv \left(3^{3(n+2)} - 26(n+1) - 27\right) - \left(3^{3(n+1)} - 26n - 27\right) \pmod{169} \\ &\equiv 3^3\cdot 3^{3(n+1)} - 3^{3(n+1)} - 26 \pmod{169} \\ &\equiv 26\cdot 3^{3(n+1)} - 26 \pmod{169} \\ &\equiv 2\cdot 13\cdot\left(3^{3(n+1)} - 1\right) \pmod{169}, \end{aligned}$$

or $13 \mid 3^{3(n+1)} - 1$ d'après la question 1,

donc $13^2 \mid 13\cdot(3^{3(n+1)} - 1)$, or $13^2 = 169$,

donc $3^{3(n+2)} - 26(n+1) - 27 \equiv 2\cdot 0 \equiv 0 \pmod{169}$,

donc $\mathcal{P}(n+1)$ est vraie.

Par récurrence, on en déduit donc : $\forall n \in \mathbb{N} \quad 169 \mid 3^{3(n+1)} - 26n - 27$

Exercice 5

1 -

On a $7 = 3\times 2 + 1$, donc $3\times 2 \equiv -1 \pmod 7$,

donc $3\cdot(-2) \equiv 1 \pmod 7$,

donc -2 est un inverse de 3 modulo 7.

2 -

Si $x \in \mathbb{Z}$, on a : $3x \equiv 2 \pmod 7 \iff x \equiv (-2)\cdot 2 \pmod 7$

(par multiplication par -2 dans le sens $\Rightarrow$,
et par multiplication par 3 dans le sens $\Leftarrow$,
en utilisant $3\cdot(-2) \equiv 1 \pmod 7$)

donc
$$\begin{aligned} 3x \equiv 2 \pmod 7 &\iff x \equiv -4 \pmod 7 \\ &\iff x \equiv 3 \pmod 7. \end{aligned}$$

Les solutions de $3x \equiv 2 \pmod 7$ sont donc les entiers $x \in \mathbb{Z}$ qui sont congrus à 3 modulo 7.

4-

Si $x \in \mathbb{Z}$, on a

$$\begin{cases} 3x \equiv 2 \pmod 7 \\ x \equiv 1 \pmod 5 \\ x \equiv 5 \pmod{12} \end{cases} \iff \begin{cases} x \equiv 3 \pmod 7 \\ x \equiv 1 \pmod 5 \\ x \equiv 5 \pmod{12} \end{cases}$$ d'après la question 2.

Les entiers 5 et 12 sont premiers entre eux, donc le théorème chinois s'applique au système

$$(a) \begin{cases} x \equiv 1 \pmod 5 \\ x \equiv 5 \pmod{12} \end{cases}.$$

Cherchons une relation de Bézout par l'algorithme d'Euclide étendu.

$$\begin{array}{ll} & 12 = 12\times 1 + 5\times 0 \\ & 5 = 12\times 0 + 5\times 1 \\ 12 = 5\times 2 + 2 & 2 = 12\times 1 + 5\times(-2) \\ 5 = 2\times 2 + 1 & 1 = 12\times(-2) + 5\times 5 \end{array}$$

Une solution particulière du système (a) est alors $12\times(-2)\times 1 + 5\times 5\times 5 = -24 + 125 = 101$,

donc (a) $\iff x \equiv 101 \pmod{5\times 12}$

$\iff x \equiv 41 \pmod{60}$,

donc $\begin{cases} 3x \equiv 2 \pmod 7 \\ x \equiv 1 \pmod 5 \\ x \equiv 5 \pmod{12} \end{cases} \iff \begin{cases} x \equiv 3 \pmod 7 \\ x \equiv 41 \pmod{60} \end{cases}$

Les entiers 7 et 60 sont premiers entre eux, donc le théorème chinois s'applique au système

$$(b) \begin{cases} x \equiv 3 \pmod 7 \\ x \equiv 41 \pmod{60} \end{cases}.$$

Cherchons une relation de Bézout par l'algorithme d'Euclide étendu.

$$\begin{array}{ll} & 60 = 60\times 1 + 7\times 0 \\ & 7 = 60\times 0 + 7\times 1 \\ 60 = 7\times 8 + 4 & 4 = 60\times 1 + 7\times(-8) \\ 7 = 4\times 1 + 3 & 3 = 60\times(-1) + 7\times 9 \\ 4 = 3\times 1 + 1 & 1 = 60\times 2 + 7\times(-17) \end{array}$$

Une solution particulière du système (b) est alors $60\times 2\times 3 + 7\times(-17)\times 41 = 360 - 4879 = -4519$,

donc $\begin{cases} 3x \equiv 2 \pmod 7 \\ x \equiv 1 \pmod 5 \\ x \equiv 5 \pmod{12} \end{cases} \iff \begin{cases} x \equiv 3 \pmod 7 \\ x \equiv 41 \pmod{60} \end{cases}$

$\iff x \equiv -4519 \pmod{7\times 60}$ (par le théorème chinois)

$\iff x \equiv -4519 \pmod{420}$

$\iff x \equiv 101 \pmod{420}$,

donc les solutions du système $\begin{cases} 3x \equiv 2 \pmod 7 \\ x \equiv 1 \pmod 5 \\ x \equiv 5 \pmod{12} \end{cases}$ sont les entiers $x \in \mathbb{Z}$ qui sont

congrus à 101 modulo 420.