Contrôles Finaux et Rattrapages (2019-2022)

Ali Ouadfel et Azzouz Cherrabi

Université Mohammed V-Rabat
Faculté des Sciences
Département de Mathématiques

Première partie

Epreuves

Contrôle Final 2019-2020

Exercice 1. *Soit A, B et C des parties d'un ensemble E. Montrer que :*

1) $A \cup B = A \cap C$ *si, et seulement si,* $B \subset A \subset C$.

2) $\begin{cases} A \cup B &= A \cup C \\ A \cap B &= A \cap C \end{cases}$ *si, et seulement si,* $B = C$.

Exercice 2. *On considère la suite réelle* $(u_n)_{n\in\mathbb{N}}$ *définie par* $u_0 = 3$, $u_1 = 4$ *et pour tout* $n \in \mathbb{N}^\star$, $u_{n+1} = u_{n-1}^2 - nu_n$. *Montrer que pour tout* $n \in \mathbb{N}$, $u_n = n + 3$.

Exercice 3. *On considère* $a_n = 4 \times 10^n - 1$, $b_n = 2 \times 10^n + 1$ *et* $c_n = 2 \times 10^n - 1$, *où* $n \in \mathbb{N}^\star$.

1) Vérifier que pour tout $n \in \mathbb{N}^\star$, 3 *divise* a_n *et* b_n.

2) Vérifier que pour tout $n \in \mathbb{N}^\star$, $b_n \times c_n = a_{2n}$.

3) Factoriser a_6 *(On admet que* 1999 *est un nombre premier).*

4) a) Montrer que pour tout $n \in \mathbb{N}^\star$, $b_n \wedge c_n = c_n \wedge 2$.

b) En déduire que pour tout $n \in \mathbb{N}^\star$, b_n *et* c_n *sont premiers entre eux.*

Exercice 4.

1) On considère la relation $\mathcal{R}$ *définie sur* $\mathbb{R}^\star$ *par* $x\mathcal{R}y$ *si il existe* $\alpha \in \mathbb{R}^{+\star}$ *tel que* $y = \alpha x$.

a) Montrer que $\mathcal{R}$ *est une relation d'équivalence.*

b) Soit $x \in \mathbb{R}^\star$.

i) Montrer que si $x > 0$, *alors* $\overline{x} = \overline{1}$.

ii) Montrer que si $x < 0$, *alors* $\overline{x} = \overline{-1}$.

c) En déduire que $\mathbb{R}^\star/\mathcal{R} = \{\overline{-1}, \overline{1}\}$.

2) On considère l'application $f : \mathbb{R}^\star \to \mathbb{R}$, $x \mapsto \begin{cases} -1 & si\ x < 0 \\ 1 & si\ x > 0 \end{cases}$

a) Déterminer $f(\mathbb{R}^\star)$. f *est-elle surjective ?*

b) f *est-elle injective ?*

c) Montrer que la relation $\mathcal{R}$ *est la relation associée à l'application* f.

d) Donner une bijection de $\mathbb{R}^\star/\mathcal{R}$ *vers* $\{-1, 1\}$.

Rattrapage 2019-2020

Exercice 5. *Montrer que :*

1) $\{(x,y) \in \mathbb{R}^2 / \exists t \in \mathbb{R} : x = 2t \text{ et } y = t^2 + 1\} \subset \{(x,y) \in \mathbb{R}^2 / x \leq y\}$.

2) $\{z \in \mathbb{C} / |z-1| = |z+1|\} = \{z \in \mathbb{C} / Re(z) = 0\}$.

Exercice 6. *Soit E, F deux ensembles tels que $E \cap F = \emptyset$. Soit A et B deux parties respectivement de E et F. Montrer que si $A \cup B = E \cup F$, alors $A = E$ et $B = F$.*

Exercice 7. *On se propose de résoudre dans $\mathbb{Z}$ l'équation $x^{29} \equiv 2 \pmod{53}$ (*). (On rappelle que 53 est un nombre premier).*

1) a) Déterminer le reste de la division euclidienne de $29 \times 9 = 261$ par 52.

b) En déduire que 2^9 est solution de (*).

2) Soit x_0 une solution de (*).

a) Montrer que x_0 et 53 sont premiers entre eux.

b) Montrer que $x_0^{261} \equiv x_0 \pmod{53}$.

c) En déduire que $x_0 \equiv 2^9 \pmod{53}$.

d) Vérifier que $2^9 \equiv 35 \pmod{53}$.

3) En utilisant 1) et 2), résoudre dans $\mathbb{Z}$ l'équation (*).

Exercice 8. *On considère l'application $f : \mathbb{R}^2 \to \mathbb{R}, (x,y) \mapsto x^2 + y^2$.*

1) Déterminer $f^{-1}(\mathbb{R}^-)$ et $f(\mathbb{R}^2)$. f est-elle surjective ?

2) f est-elle injective ?

3) On considère la relation d'équivalence $\mathcal{R}$ associée à l'application f.

a) Déterminer $\overline{(0,0)}$ et $\overline{(1,0)}$.

b) Soit $(x,y) \in \mathbb{R}^2$. Montrer que $\overline{(x,y)} = \{(z,t) \in \mathbb{R}^2 / z^2 + t^2 = x^2 + y^2\}$.

c) Donner une bijection de $\mathbb{R}^2/\mathcal{R}$ vers $\mathbb{R}^+$.

Contrôle Final 2020-2021

Exercice 9. *Soit $n \in \mathbb{N}$ tel que $n \geq 4$. Montrer que $n^2 \leq 2^n$.*

Exercice 10. *Soit E, F deux ensembles, A, B deux parties de E et $f : E \to F$ une application.*

1) Montrer que $f(A \cap B) \subset f(A) \cap f(B)$.

2) Donner un contre-exemple pour montrer qu'en général $f(A \cap B) \neq f(A) \cap f(B)$.

Exercice 11. *Soit E un ensemble et A une partie non vide de E telle que $A \neq E$. On considère la relation $\mathcal{R}$ définie dans E par $\forall (x, y) \in E^2$, $x\mathcal{R}y$ si $\{x, y\} \subset A$ ou $\{x, y\} \subset \overline{A}$, où $\overline{A}$ désigne le complémentaire de A dans E. On note χ_A la fonction caractéristique de la partie A, i.e., c'est l'application $\chi_A : E \to \{0, 1\}$, $x \mapsto \begin{cases} 1 & si \quad x \in A \\ 0 & si \quad x \notin A \end{cases}$*

1) Montrer que $\forall (x, y) \in E^2$, $x\mathcal{R}y$ si, et seulement si, $\chi_A(x) = \chi_A(y)$.

2) Montrer que $\mathcal{R}$ est une relation d'équivalence.

3) a) Soit $x \in A$. Déterminer $\overline{x}$, où $\overline{x}$ est la classe d'équivalence de x.

b) Soit $x \notin A$. Déterminer $\overline{x}$.

c) En déduire que $E/\mathcal{R} = \{A, \overline{A}\}$.

Exercice 12.

1) Soit $a \in \mathbb{Z}$ tel que $a \equiv 1 \pmod{10}$.

a) Soit $x \in \mathbb{Z}$ tel que $x \equiv 1 \pmod{n}$, où n est un entier ≥ 2. Montrer que $\forall k \in \mathbb{N}^\star, x^k \equiv 1 \pmod{n}$ (On pourra utiliser l'égalité $x^k - 1 = (x-1)(x^{k-1} + x^{k-2} + \cdots + x + 1)$).

b) En déduire que $a^9 + a^8 + \cdots + a + 1 \equiv 0 \pmod{10}$

c) Montrer que $a^{10} \equiv 1 \pmod{10^2}$.

2) Soit $b \in \mathbb{Z}$ et r le reste dans la division euclidienne de b par 10.

a) Déterminer les restes possibles de b^4 dans la division euclidienne par 10.,

b) Montrer que b et 10 sont premiers entre eux si, et seulement si, $r \in \{1, 3, 7, 9\}$.

c) En déduire que $b^4 \equiv 1 \pmod{10}$ si, et seulement si, b et 10 sont premiers entre eux.

3) Soit $b \in \mathbb{Z}$ tel que b et 10 sont premiers entre eux.

a) Montrer que $b^{40} \equiv 1 \pmod{10^2}$.

*b) **(Bonus)** Déterminer le reste de la division euclidienne de 67^{41} par 100.*

Rattrapage 2020-2021

Exercice 13. *Soit A et B deux parties d'un ensemble E et $f : \mathcal{P}(E) \to \mathcal{P}(A) \times \mathcal{P}(B), X \mapsto (X \cap A, X \cap B)$. Montrer que :*

1) f est injective si, et seulement si, $A \cup B = E$.

2) f est surjective si, et seulement si, $A \cap B = \emptyset$.

3) En déduire une condition nécessaire et suffisante pour que f soit bijective.

Exercice 14. *On considère l'ensemble $E = \{a + ib / a, b \in \mathbb{Z}\}$ et la relation $\mathcal{R}$ définie dans E par $\forall (x, y) \in E^2$, $x\mathcal{R}y$ si il existe $(h, k) \in \mathbb{Z}^2$ tel que $x - y = 2h + 2ki$ (i est le nombre complexe $i^2 = -1$).*

1) Montrer que $\mathcal{R}$ est une relation d'équivalence.

2) Montrer que les classes d'équivalence $cl(0), cl(1), cl(i)$ et $cl(1+i)$ sont deux à deux disjointes.

3) Déterminer $cl(0), cl(1), cl(i)$ et $cl(1 + i)$.

4) En déduire que $E/\mathcal{R} = \{cl(0), cl(1), cl(i), cl(1 + i)\}$.

Exercice 15. *Soit dans $\mathbb{Z}$ l'équation (E) : $x^{19} \equiv -2 \pmod{29}$.*

1) a) Justifier que $2^{28} \equiv 1 \pmod{29}$.

b) En déduire que -8 est une solution de (E).

2) Soit x_0 une solution de (E).

a) Montrer que $x_0^{28} \equiv 1 \pmod{29}$.

b) Montrer que $x_0^{57} \equiv -8 \pmod{29}$.

c) En déduire que $x_0 \equiv -8 \pmod{29}$.

3) En déduire l'ensemble des solutions dans $\mathbb{Z}$ de l'équation (E).

*4) **(Bonus)** Résoudre dans $\mathbb{Z}$ le système* $\begin{cases} (x-3)^{19} \equiv -2 \pmod{29} \\ (x-3)^{13} \equiv -2 \pmod{13} \end{cases}$.

Contrôle Final 2021-2022

Exercice 16.

1) *Soit* $E = \{n \in \mathbb{Z}/\exists k \in \mathbb{Z} : n = 6k + 12\}$ *et* $F = \{n \in \mathbb{Z}/\exists k \in \mathbb{Z} : n = 3k\}$. *Montrer que* $E \subset F$. *A-t-on* $E = F$ *?*
2) *Soit* $E = \{n \in \mathbb{Z}/\exists k \in \mathbb{Z} : n = 6k\}$ *et* $F = \{n \in \mathbb{Z}/\exists k \in \mathbb{Z} : n = 6k - 18\}$. *Montrer que* $E = F$.

Exercice 17. *Soit* E *un ensemble et* A, B *deux parties de* E. *On considère l'application* $f : \mathcal{P}(E) \to \mathcal{P}(E), X \mapsto (X \cap A) \cup B$.

1) *Calculer* $f(\emptyset)$, $f(A)$, $f(B)$ *et* $f(E)$.
2) *Montrer que si* f *est injective, alors* $f = id_{\mathcal{P}(E)}$.

Exercice 18. *On considère la relation* $\mathcal{R}$ *définie dans* $\mathbb{Z}$ *par* $x\mathcal{R}y$ *si, et seulement si,* $7x - 5y$ *est pair.*

1) *Montrer que* $\mathcal{R}$ *est une relation d'équivalence. Pour tout* $x \in \mathbb{Z}$, $cl(x)$ *désigne la classe d'équivalcence de* x *modulo la relation* $\mathcal{R}$.
2) *Vérifier que* $cl(0) \neq cl(1)$.
3) *Soit* $n \in \mathbb{Z}$.
   a) *Montrer que si* n *est pair, alors* $cl(n) = cl(0)$.
   b) *Montrer que si* n *est impair, alors* $cl(n) = cl(1)$.
4) *En déduire que* $\mathbb{Z}/\mathcal{R} = \{cl(0), cl(1)\}$.

Exercice 19.

1) *Soit* $x \in \mathbb{Z}$. *Montrer que si* $\begin{cases} x \equiv 1 \pmod 8 \\ x \equiv 7 \pmod{125} \end{cases}$, *alors* $x \equiv 257 \pmod{1000}$.
2) *On considère la suite* $(u_n)_{n\in\mathbb{N}}$ *définie sur* $\mathbb{N}$ *par :* $u_n = 2 \times 5^n + 7$.
   a) *Soit* $n \in \mathbb{N}$. *Montrer que* 5^n *est congru à* 1 *ou* 5 *modulo* 8. *(ind : distinguer les cas :* n *est pair ;* n *est impair).*
   b) *Montrer que pour tout* $n \in \mathbb{N}$, $u_n \equiv 1 \pmod 8$.
   c) *Montrer que si* $n \geq 3$, *alors* $u_n \equiv 257 \pmod{1000}$ *(ind : utiliser 1)).*
   d) *Soit* $n \in \mathbb{N}$ *et* $d = u_{2n} \wedge u_{2n+1}$.
      i) *Vérifier* $5u_{2n} - u_{2n+1} = 28$.
      ii) *Justifier que* d *est impair.*
      iii) *Montrer que* $d \neq 7$.
      iv) *Calculer* d.

Rattrapage 2021-2022

Exercice 20. *Soit E et A deux ensembles. Montrer que les propositions suivantes sont équivalentes :*

(a) $A \subset E$

(b) $A \cap E = A$

(c) $A \cup E = E$.

Exercice 21. *On considère l'ensemble* $E = \{x \in \mathbb{Z} / \forall n \in \mathbb{N}, x^n \equiv 1 + n(x-1) \pmod{100}\}$.

1) Soit $k \in \mathbb{Z}$. *Montrer par récurrence que pour tout* $n \in \mathbb{N}$, $(1+10k)^n \equiv 1+10nk \pmod{100}$.

2) Soit $a \in E$.

a) Montrer $(a-1)^2 \equiv 0 \pmod{10}$.

b) En déduire que $a \equiv 1 \pmod{10}$.

3) Montrer que $E = \{x \in \mathbb{Z} / x \equiv 1 \pmod{10}\}$.

Exercice 22. *On considère la relation binaire $\mathcal{R}$ définie sur $\mathbb{Z}$ par $x\mathcal{R}y$ si, et seulement si,* 5 *divise* $x^2 - y^2$.

1) Montrer que $\mathcal{R}$ est une relation d'équivalence. Pour tout $x \in \mathbb{Z}$, $cl(x)$ désigne la classe d'équivalence de x modulo la relation $\mathcal{R}$ et $\overline{x}$ est la classe de congruence de x modulo 5.

2) Montrer que $cl(0) = \overline{0}$, $cl(1) = \overline{1} \cup \overline{4}$ *et* $cl(2) = \overline{2} \cup \overline{3}$.

3) Montrer que $\mathbb{Z}/\mathcal{R} = \{\overline{0}, \overline{1} \cup \overline{4}, \overline{2} \cup \overline{3}\}$.

Exercice 23. *Soit E un ensemble et A, B deux parties de E. On considère l'application* $f : \mathcal{P}(E) \to \mathcal{P}(E), X \mapsto (\overline{X} \cup A) \cap B$, *où $\overline{X}$ est le complémentaire de X dans E.*

1) Calculer $f(\emptyset)$ *et* $f(E)$.

2) Montrer que f est une application constante si, et seulement si, $B \subset A$.

3) On suppose que f est surjective .

a) Montrer que $B = E$ *et* $A = \emptyset$.

b) En déduire que f est bijective et déterminer f^{-1} *(ind : on pourra calculer* $f \circ f$.*)*

Contrôle Final 2022-2023

Exercice 24. *On considère la suite* $(u_n)_{n\in\mathbb{N}}$ *définie par :* $u_0 = u_1 = 1$ *et* $\forall n \in \mathbb{N}, u_{n+2} = u_{n+1} + u_n$. *Montrer que* $\forall n \in \mathbb{N}, u_n \leq (\frac{5}{3})^n$.

Exercice 25. *Soit* E *et* F *deux ensembles. Montrer que* $E \subset F$ *si, et seulement si,* $\mathcal{P}(E) \subset \mathcal{P}(F)$.

Exercice 26. *On considère la relation binaire* $\mathcal{R}$ *définie sur* $\mathbb{Z}^2$ *par* $(x, y)\mathcal{R}(z, t)$ *si* $x - z \equiv 3(y - t) \pmod 5$, *où* $(x, y), (z, t) \in \mathbb{Z}^2$.

1) *Vérifier que* $\mathcal{R}$ *est une relation d'équivalence. Pour tout* $(x, y) \in \mathbb{Z}^2$, $cl((x, y))$ *désigne la classe d'équivalence de* (x, y) *modulo la relation* $\mathcal{R}$.
2) *Montrer que* $cl((0, 0)) = \{(x, 2x + 5k)/(x, k) \in \mathbb{Z}^2\}$.
3) *Soit* $q, r \in \mathbb{Z}$. *Montrer que* $cl((5q + r, 0)) = cl((r, 0))$.
4) *Soit* $(x, y) \in \mathbb{Z}^2$. *Montrer que* $cl((x, y)) = cl((x + 2y, 0))$.
5) *Soit* $(x, y) \in \mathbb{Z}^2$. *Montrer que* $cl((x, y)) = cl((r, 0))$, *avec* $r \in \{0, 1, 2, 3, 4\}$. *(Ind : On pourra utiliser 4) et 3)).*
6) *On considère la correspondance* $f : \mathbb{Z}_5 \to (\mathbb{Z} \times \mathbb{Z})/\mathcal{R}$, $\overline{x} \mapsto cl((x, 0))$, *où* $\overline{x}$ *est la classe de congruence de* x *modulo* 5.
   a) *Montrer que* f *est une application bien définie.*
   b) *Montrer que* f *est bijective.*

Exercice 27.

I) *On se propose de montrer par l'absurde que la congruence* $x^2 \equiv -1 \pmod{43}$ *ne possède pas de solutions dans* $\mathbb{Z}$. *Supposons que* $x_0 \in \mathbb{Z}$ *est solution de* $x^2 \equiv -1 \pmod{43}$. *(On rappelle que* 43 *est un nombre premier).*
   1) *Montrer que* 43 *ne divise pas* x_0.
   2) *En déduire que* $(x_0^2)^{21} \equiv 1 \pmod{43}$.
   3) *Conclure.*

II) *Soit* $a, b \in \mathbb{Z}$ *tels que* 43 *divise* $a^2 + b^2$. *On se propose de montrer par l'absurde que* 43 *divise* a *et* b. *Supposons alors que* 43 *ne divise pas* a.
   1) *Montrer qu'il existe* $u \in \mathbb{Z}$ *tel que* $ua \equiv 1 \pmod{43}$.
   2) *Montrer que* $(ub)^2 \equiv -1 \pmod{43}$.
   3) *En déduire que* 43 *divise* a *et qu'ainsi* 43 *divise aussi* b *(Ind : Utiliser 1)).*

Rattrapage 2022-2023

Exercice 28.

1) Montrer que la correspondance $f : \mathbb{Z}/4\mathbb{Z} \to \mathbb{Z}/8\mathbb{Z}$, $\overline{x} \mapsto \overline{3x}$ *n'est pas une application.*

2) On considère l'application $g : \mathbb{Z}/10\mathbb{Z} \to \mathbb{Z}/10\mathbb{Z}$, $\overline{x} \mapsto \overline{7x}$. *Montrer que* g *est bijective.*

Exercice 29. *Soit* E *un ensemble et* A, B, X *des parties de* E. *Montrer que si* $X \cap A \subset X \cap B$ *et* $X \cup A \subset X \cup B$, *alors* $A \subset B$.

Exercice 30. *Soit* $n \in \mathbb{N} \setminus \{0, 1\}$ *et* $a \in \mathbb{Z}$. *On considère la relation binaire* $\mathcal{R}$ *définie sur* $\mathbb{Z}^2$ *par* $(x, y)\mathcal{R}(z, t)$ *si* $x - z \equiv a(y - t) \pmod{n}$, *où* $(x, y), (z, t) \in \mathbb{Z}^2$.

1) Vérifier que $\mathcal{R}$ *est une relation d'équivalence. Pour tout* $(x, y) \in \mathbb{Z}^2$, $cl((x, y))$ *désigne la classe d'équivalence de* (x, y) *modulo la relation* $\mathcal{R}$.

2) Vérifier que pour tout $(x, y) \in \mathbb{Z}^2$, $cl((x, y)) = cl((x - ay, 0))$.

3) Soit $r, s \in \{0, 1, \ldots, n-1\}$. *Montrer que si* $cl((r, 0)) = cl((s, 0))$, *alors* $r = s$ *et qu'ainsi les classes* $cl((0, 0)), cl((1, 0)), \ldots, cl((n-1, 0))$ *sont deux à deux distinctes.*

4) Montrer que $\mathbb{Z}^2/\mathcal{R} = \{cl((0, 0)), cl((1, 0)), \ldots, cl((n-1, 0))\}$ *(Ind : on pourra remarquer que si* $q, r \in \mathbb{Z}$, *alors* $cl((qn + r, 0)) = cl((r, 0))$*).*

Exercice 31.

I) Soit $a \in \mathbb{Z}$.

1) Montrer que si a *est impair, alors* $a \equiv 1 \pmod{4}$ *ou* $a \equiv 3 \pmod{4}$.

2) Montrer que $a^2 \equiv 0 \pmod{4}$ *ou* $a^2 \equiv 1 \pmod{4}$.

II) On se propose de montrer par l'absurde que l'équation $(E) : x^2 = y^3 + 7$ *n'a pas de solutions dans* $\mathbb{Z} \times \mathbb{Z}$. *On suppose qu'elle possède une solution* (a, b).

1) Montrer que b *est impair et en déduire que* $a^2 + 1$ *est impair.(Ind : on suppose que* b *est pair et on utilise I)2)).*

2) Montrer qu'il existe $m \in \mathbb{Z}$ *tel que* $a^2 + 1 = (b + 2)(4m^2 + 3)$ *(Ind : on rappelle que* $b^3 + 8 = (b + 2)(b^2 - 2b + 4)$*).*

3) Justifier que $4m^2 + 3 = p_1^{k_1} \ldots p_r^{k_r}$, *où* $p_1, \ldots, p_r \in \mathbb{N}$ *sont des nombres premiers impairs et* $k_1, \ldots, k_r \in \mathbb{N}^*$.

4) Montrer qu'il existe $p \in \{p_1, \ldots, p_r\}$ *tel que* $p \equiv 3 \pmod{4}$ *(Ind : utiliser I)1)).*

5) Montrer que p *ne divise pas* a *et en déduire que* $a^{p-1} \equiv 1 \pmod{p}$.

6) Justifier que $\frac{p-1}{2}$ *est un entier naturel impair et qu'ainsi* $a^{p-1} \equiv -1 \pmod{p}$ *et conclure.*

Corrigé du Contrôle Final 2019-2020

Exercice 1

1) Supposons que $B \subset A \subset C$. Alors, $A \cup B = A$ car $B \subset A$ et $A \cap C = A$ car $A \subset C$ donc $A \cup B = A \cap C$.
Réciproquement, supposons que $A \cup B = A \cap C$. Puisque $A \subset A \cup B$, alors $A \subset A \cap C$ et comme $A \cap C \subset C$, alors $A \subset C$. Aussi, Puisque $B \subset A \cup B$, alors $B \subset A \cap C$ et comme $A \cap C \subset A$, alors $B \subset A$.

2) Il est évident que si $B = C$, alors $\begin{cases} A \cup B &= A \cup C \\ A \cap B &= A \cap C \end{cases}$. Réciproquement, supposons que $\begin{cases} A \cup B &= A \cup C \\ A \cap B &= A \cap C \end{cases}$ Montrons que $B \subset C$ (de même pour $C \subset B$) : Soit $x \in B$. On distingue les deux cas : le cas où $x \in A$ et le cas où $x \notin A$: Si $x \in A$, alors $x \in A \cap B = A \cap C$ d'où $x \in C$. Si $x \notin A$, on a $x \in A \cup B = A \cup C$ d'où $x \in C$ car $x \notin A$.

Exercice 2 Pour tout $n \in \mathbb{N}$, $P(n)$ désigne la propriété $u_n = n + 3$. On a $P(0)$ est vraie car $u_0 = 3 = 0 + 3$ et $P(1)$ est vraie car $u_1 = 4 = 1 + 3$. Supposons que $P(n)$ et $P(n + 1)$ sont vraies. Montrons que $P(n + 2)$ est vraie : On a $u_{n+2} = u_n^2 - (n + 1)u_{n+1}$ et, d'après l'hypothèse de réccurence, $u_{n+1} = (n + 1) + 3 = n + 4$ et $u_n = n + 3$, ainsi on obtient $u_{n+2} = (n + 3)^2 - (n + 1)(n + 4) = n + 5 = (n + 2) + 3$ donc $P(n + 2)$ est vraie et par suite $\forall n \in \mathbb{N}$, $u_n = n + 3$.

Exercice 3

On considère $a_n = 4 \times 10^n - 1$, $b_n = 2 \times 10^n + 1$ et $c_n = 2 \times 10^n - 1$, où $n \in \mathbb{N}^\star$.

1) On a $10 \equiv 1 \pmod 3$ d'où $10^n \equiv 1 \pmod 3$ ainsi $a_n = 4 \times 10^n - 1 \equiv 4 - 1 \equiv 0 \pmod 3$ donc 3 divise a_n. Aussi, on a $b_n = 2 \times 10^n + 1 \equiv 2 + 1 \equiv 0 \pmod 3$ donc 3 divise b_n.

2) Soit $n \in \mathbb{N}^\star$. On a $b_n \times c_n = (2 \times 10^n + 1)(2 \times 10^n - 1) = (2 \times 10^n)^2 - 1$ alors $b_n \times c_n = 4 \times 10^{2n} - 1 = a_{2n}$.

3) On a, d'après 2), $a_6 = a_{2.3} = b_3.c_3$. On a $c_3 = 1999$ est premier. Par ailleurs, on a $3 \mid b_3 = 2001$ et en divisant b_3 par 3, on obtient $b_3 = 3.667$. Pour factoriser 667, on a $[\sqrt{667}] = 25$ et si 667 est composé, alors il existe p premier ≤ 25. En essayant les divisions successives de 667 par $2, 3, 5, 7, 11, 13, 17, 19, 23$, on obtient $667 = 23.29$ (voir crible d'Eratosthène dans exercices corrigé, Arithmétique) alors $b_3 = 3.23.29$ et donc $a_6 = 3.23.29.1999$.

4) a) Soit $n \in \mathbb{N}^\star$. On a $b_n = c_n + 2$ d'où $b_n \wedge c_n = c_n \wedge 2$.

   b) On a c_n est impair, alors $c_n \wedge 2 = 1$ d'où b_n et c_n sont premiers entre eux.

Exercice 4

1) On considère la relation $\mathcal{R}$ définie sur $\mathbb{R}^\star$ par $x\mathcal{R}y$ si il existe $\alpha \in \mathbb{R}^{+\star}$ tel que $y = \alpha x$.

   a) On a $\mathcal{R}$ est réflexive. En effet, soit $x \in \mathbb{R}^\star$. Alors, il existe $\alpha = 1 \in \mathbb{R}^{+\star}$ tel que $x = \alpha x$. ainsi $x\mathcal{R}x$. La relation $\mathcal{R}$ est symétrique. En effet, soit $x, y \in \mathbb{R}^\star$: $x\mathcal{R}y$. Alors, il existe $\alpha \in \mathbb{R}^{+\star}$ tel que $y = \alpha x$ ainsi il existe $\frac{1}{\alpha} \in \mathbb{R}^{+\star}$ tel que $x = \frac{1}{\alpha} y$ et par suite $y\mathcal{R}x$. Aussi, $\mathcal{R}$ est transitive. En effet, soit $x, y, z \in \mathbb{R}^\star$: $x\mathcal{R}y$ et $y\mathcal{R}z$. Alors, il existe $\alpha \in \mathbb{R}^{+\star}$ tel que $y = \alpha x$ et il existe $\beta \in \mathbb{R}^{+\star}$ tel que $z = \beta y$ ainsi il existe $\alpha\beta \in \mathbb{R}^{+\star}$ tel que $z = \alpha\beta x$ d'où $x\mathcal{R}z$ donc $\mathcal{R}$ est une relation d'équivalence.

   b) Soit $x \in \mathbb{R}^\star$.

i) Supposons que $x > 0$. On a $1\mathcal{R}x$ car il existe $\alpha = x \in \mathbb{R}^{+\star}$ tel que $x = \alpha.1$ donc $\overline{x} = \overline{1}$.

ii) Supposons que $x < 0$. On a $(-1)\mathcal{R}x$ car il existe $\alpha = -x \in \mathbb{R}^{+\star}$ tel que $x = \alpha.(-1)$ donc $\overline{x} = \overline{-1}$.

c) On a $\{\overline{-1}, \overline{1}\} \subset \mathbb{R}^{\star}/\mathcal{R}$. Inversement, Soit $x \in \mathbb{R}^{\star}$. Alors, d'après b), on a $\overline{x} = \overline{1}$ ou $\overline{x} = \overline{-1}$ donc $\mathbb{R}^{\star}/\mathcal{R} \subset \{\overline{-1}, \overline{1}\}$.

2) a) On a $\forall x \in \mathbb{R}^{\star}, f(x) = \pm 1$ d'où $f(\mathbb{R}^{\star}) \subset \{-1, 1\}$. Inversemnet, on a $1 = f(1)$ et $-1 = f(-1)$ d'où $f(\mathbb{R}^{\star}) = \{-1, 1\}$.
On a f n'est pas surjective car, par exemple, 2 n'a pas d'antécédent.

b) On $f(1) = 1 = f(2)$ d'où f n'est pas injective.

c) Soit $\mathcal{S}$ la relation associée à l'application f, i.e., la relation définie par $x\mathcal{S}y$ si, et seulement si, $f(x) = f(y)$, avec $x, y \in \mathbb{R}^{\star}$, i.e., $x\mathcal{S}y$ si, et seulement si, x et y ont le même signe si, et seulement si, il existe $\alpha = \frac{y}{x} \in \mathbb{R}^{+\star}$ tel que $y = \alpha x$ si, et seulement si, $x\mathcal{R}y$. ainsi $\mathcal{S} = \mathcal{R}$.

d) D'après le cours, on a $g : \mathbb{R}^{\star}/\mathcal{R} \to f(\mathbb{R}^{\star}) = \{-1, 1\}$, $\overline{x} \mapsto f(x)$ est une bijection

Corrigé du Rattrapage 2019-2020

Exercice 5 Voir Exercice 1 du polycopié des exercices corrigés (Ensembles, applications et Relations binaires).

Exercice 6

On a $A \subset E$; alors il suffit de vérifier que $E \subset A$ (de même pour $F = B$). Soit $x \in E$. Alors $x \in E \cup F = A \cup B$ et comme $x \notin B$ (sinon, $x \in F$, contradiction car $E \cap F = \emptyset$) doc $x \in A$.

Exercice 7

On se propose de résoudre dans $\mathbb{Z}$ l'équation $x^{29} \equiv 2 \pmod{53}$ (*). (On rappelle que 53 est un nombre premier).

1) a) On a $261 = 5.52 + 1$ d'où le reste de la division euclidienne de $29 \times 9 = 261$ par 52 est 1.

   b) On a $(2^9)^{29} = 2^{261} = (2^{52})^5.2^1$ et puisque $2 \wedge 53 = 1$ et 53 est un nombre premier, alors, d'après le petit théorème de Fermat, $2^{52} \equiv 1 \pmod{53}$ ainsi $(2^9)^{29} \equiv 1^5.2 \pmod{53}$ par suite $(2^9)^{29} \equiv 2 \pmod{53}$ donc 2^9 est solution de (*).

2) a) On a $53 \nmid x_0$; sinon $x_0 \equiv 0 \pmod{53}$ d'où $x_0^{29} \equiv 0 \pmod{53}$, ce qui est faux car $x_0^{29} \equiv 2 \pmod{53}$. Alors, x_0 et 53 sont premiers entre eux car 53 est un nombre premier.

   b) Puisque x_0 et 53 sont premiers entre, alors, d'après le petit théorème de Fermat, $x_0^{52} \equiv 1 \pmod{53}$ d'où $x_0^{261} = (x_0^{52})^5.x_0 \equiv 1^5.x_0 \pmod{53}$ donc $x_0^{261} \equiv x_0 \pmod{53}$.

   c) Puisque x_0 est une solution de (*), alors $x_0^{29} \equiv 2 \pmod{53}$ d'où $(x_0^{29})^9 \equiv 2^9 \pmod{53}$ ainsi $x_0^{261} \equiv 2^9 \pmod{53}$ donc, d'après 2)b), $x_0 \equiv 2^9 \pmod{53}$.

   d) On a $2^2 \equiv 4 \pmod{53}$, $2^3 \equiv 8 \pmod{53}$, $2^4 \equiv 16 \pmod{53}$, $2^5 \equiv 32 \pmod{53}$, $2^6 \equiv 11 \pmod{53}$, $2^7 \equiv 22 \pmod{53}$, $2^8 \equiv 44 \pmod{53}$, $2^2 \equiv 35 \pmod{53}$.

3) D'après 1), 2^9 est solution de $(*)$ et d'après 2), si x_0 est solution de $(*)$, alors $x_0 \equiv 2^9 \pmod{53}$ et on a $2^9 \equiv 35 \pmod{53}$ donc x est solution de $(*)$ si, et seulement si, $x \equiv 35 \pmod{53}$ ainsi l'ensemble des solutions de $(*)$ est $S = \{35 + 53k / k \in \mathbb{Z}\}$.

Exercice 8

1) Puisque $\forall (x, y) \in \mathbb{R}^2, f(x, y) = x^2 + y^2 \geq 0$, alors $f^{-1}(\mathbb{R}^-) = \emptyset$.
   Soit $(x, y) \in \mathbb{R}^2$. Alors, $f(x, y) = x^2 + y^2 \in \mathbb{R}^+$ d'où $f(\mathbb{R}^2) \subset \mathbb{R}^+$. Inversement, soit $z \in \mathbb{R}^+$. Alors, il existe $(x, y) = (\sqrt{z}, 0) \in \mathbb{R}^2 : f(x, y) = (\sqrt{z})^2 = z$ donc $f(\mathbb{R}^2) = \mathbb{R}^+$.
   Puisque $f(\mathbb{R}^2) = \mathbb{R}^+ \neq \mathbb{R}$, alors f n'est pas surjective.

2) On a f n'est pas injective car, par exemple, $f(-1, 0) = 1 = f(1, 0)$ mais $(-1, 0) \neq (1, 0)$.

3) La relation d'équivalence $\mathcal{R}$ est définie dans $\mathbb{R}^2$ par $(x, y)\mathcal{R}(z, t)$ si, et seulement si, $f(x, y) = f(z, t)$, avec $(x, y), (z, t) \in \mathbb{R}^2$.

   a) Soit $(x, y) \in \mathbb{R}^2$.
   On a $(x, y) \in \overline{(0, 0)}$ si, et seulement si, $(x, y)\mathcal{R}(0, 0)$ si, et seulement si, $x^2 + y^2 = 0$ si, et seulement si, $x = y = 0$ si, et seulement si, $(x, y) = (0, 0)$ ainsi $\overline{(0, 0)} = \{(0, 0)\}$.
   On a $(x, y) \in \overline{(1, 0)}$ si, et seulement si, $(x, y)\mathcal{R}(1, 0)$ si, et seulement si, $x^2 + y^2 = 1$ ainsi $\overline{(1, 0)} = \{(x, y) \in \mathbb{R}^2 / x^2 + y^2 = 1\}$.

   b) Soit $(z, t) \in \mathbb{R}^2$. On a $(z, t) \in \overline{(x, y)}$ si, et seulement si, $(z, t)\mathcal{R}(x, y)$ si, et seulement si, $z^2 + t^2 = x^2 + y^2$ ainsi $\overline{(x, y)} = \{(z, t) \in \mathbb{R}^2 / z^2 + t^2 = x^2 + y^2\}$.

c) D'après le cours, l'application $g : \mathbb{R}^2/\mathcal{R} \to f(\mathbb{R}^2) = \mathbb{R}^+$, $\overline{(x,y)} \mapsto f(x,y) = x^2 + y^2$ est bijective.

Corrigé du Contrôle Final 2020-2021

Exercice 9 Voir Exercice 2)1) du plycopié des exercices corrigé (Arithmétique dans $\mathbb{Z}$)..
Exercice 10 Voir le cours.
Exercice 11

1) Soit $(x, y) \in E^2$. Supposons que $x\mathcal{R}y$. Alors, $\{x, y\} \subset A$ ou $\{x, y\} \subset \overline{A}$. Si $\{x, y\} \subset A$, alors $x, y \in A$ d'où $\chi_A(x) = 1$ et $\chi_A(y) = 1$ ainsi $\chi_A(x) = \chi_A(y)$. Aussi, si $\{x, y\} \subset \overline{A}$, alors $x, y \notin A$ d'où $\chi_A(x) = 0$ et $\chi_A(y) = 0$ ainsi $\chi_A(x) = \chi_A(y)$.
   Réciproquement, supposons que $\chi_A(x) = \chi_A(y)$. Alors, $\chi_A(x) = \chi_A(y) = 0$ ou $\chi_A(x) = \chi_A(y) = 1$ ainsi $x, y \notin A$ ou $x, y \in A$, i.e., $\{x, y\} \subset \overline{A}$ ou $\{x, y\} \subset A$ d'où $x\mathcal{R}y$.
2) La relation $\mathcal{R}$ est réflexive, en effet, soit $x \in E$. On a $\chi_A(x) = \chi_A(x)$ d'où $x\mathcal{R}x$. Aussi, $\mathcal{R}$ est symétrique, en effet, soit $x, y \in E$ tels que $x\mathcal{R}y$. Alors, $\chi_A(x) = \chi_A(y)$, i.e., $\chi_A(y) = \chi_A(x)$ donc $y\mathcal{R}x$. La relation $\mathcal{R}$ est transitive, en effet, soit $x, y, z \in E$ tels que $x\mathcal{R}y$ et $y\mathcal{R}z$. Alors, $\chi_A(x) = \chi_A(y)$ et $\chi_A(y) = \chi_A(z)$ d'où $\chi_A(x) = \chi_A(z)$ ainsi $x\mathcal{R}z$. Alors, $\mathcal{R}$ est une relation d'équivalence.
3) a) Soit $x \in A$ et $y \in E$. On a $y \in \overline{x}$ si, et seulement si, $y\mathcal{R}x$ si, et seulement si, $\chi_A(y) = \chi_A(x)$ si, et seulement si, $\chi_A(y) = 1$ (car $x \in A$) si, et seulement si, $y \in A$. Ainsi, $\overline{x} = A$.
   b) Soit $x \notin A$ et $y \in E$. On a $y \in \overline{x}$ si, et seulement si, $y\mathcal{R}x$ si, et seulement si, $\chi_A(y) = \chi_A(x)$ si, et seulement si, $\chi_A(y) = 0$ (car $x \notin A$) si, et seulement si, $y \notin A$ si, et seulement si, $y \in \overline{A}$. Ainsi, $\overline{x} = \overline{A}$.
   c) Puisque $A \neq \emptyset$, il existe $x \in E$ tel que $x \in A$ et comme $\overline{x} = A$, $A \in E/\mathcal{R}$. Aussi, puique $A \neq E$, il existe $x \in E$ tel que $x \notin A$ d'où $\overline{x} = \overline{A}$ et par suite $\overline{A} \in E/\mathcal{R}$ ainsi $\{A, \overline{A}\} \subset E/\mathcal{R}$. Inversement, si $x \in E$, $x \in A$ ou $x \notin A$ alors $\overline{x} = A$, ou $\overline{x} = \overline{A}$ ainsi $E/\mathcal{R} = \{A, \overline{A}\}$.
   Remarque : Pour justifier que $E/\mathcal{R} \subset \{A, \overline{A}\}$, on peut aussi remarquer que, d'après 3)a) et b), A et $\overline{A}$ sont des classes d'équivalence et que $(A, \overline{A})$ forme une partition de E.

Exercice 12

1) Soit $a \in \mathbb{Z}$ tel que $a \equiv 1 \pmod{10}$.
   a) Puisque $x \equiv 1 \pmod{10}$, $10 \mid x - 1$ d'où $10 \mid (x-1)(x^{k-1} + x^{k-2} + \cdots + x + 1)$ alors $10 \mid x^k - 1$ (car $x^k - 1 = (x-1)(x^{k-1} + x^{k-2} + \cdots + x + 1)$) donc $x^k \equiv 1 \pmod{10}$.
   b) Puisque $a \equiv 1 \pmod{10}$, alors $\forall n \in \{1, \cdots, 9\}$, $a^n \equiv 1 \pmod{10}$ d'où $a^9 + a^8 + \cdots + a + 1 \equiv \overbrace{1 + 1 + \cdots + 1 + 1}^{10 \text{ fois}} \equiv 10 \equiv 0 \pmod{10}$
   c) On a $a \equiv 1 \pmod{10}$ d'où $10 \mid a-1$ et d'après b), on a $a^9 + a^8 + \cdots + a + 1 \equiv 0 \pmod{10}$ d'où $10 \mid a^9 + a^8 + \cdots + a + 1$ ainsi $10^2 = 10.10 \mid (a-1)(a^9 + a^8 + \cdots + a + 1) = a^{10} - 1$ donc $a^{10} \equiv 1 \pmod{10^2}$.
2) Soit $b \in \mathbb{Z}$.
   a) Soit r le reste de la division euclidienne de b par 10. Alors, $r \in \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$.
      - Si $r = 0$, alors $b \equiv 0 \pmod{10}$ d'où $b^4 \equiv 0 \pmod{10}$.
      - Si $r = 1$, alors $b \equiv 1 \pmod{10}$ d'où $b^4 \equiv 1 \pmod{10}$
      - Si $r = 2$, alors $b \equiv 2 \pmod{10}$ d'où $b^4 \equiv 2^4 \equiv 6 \pmod{10}$

- Si $r = 3$, alors $b \equiv 3 \pmod{10}$ d'où $b^4 \equiv 3^4 \equiv 1 \pmod{10}$
- Si $r = 4$, alors $b \equiv 4 \pmod{10}$ d'où $b^4 \equiv 4^4 \equiv 6 \pmod{10}$
- Si $r = 5$, alors $b \equiv 5 \pmod{10}$ d'où $b^4 \equiv 5^4 \equiv 5 \pmod{10}$
- Si $r = 6$, alors $b \equiv 6 \pmod{10}$ ainsi $b \equiv -4 \pmod{10}$ d'où $b^4 \equiv (-4)^4 \equiv 6 \pmod{10}$
- Si $r = 7$, alors $b \equiv 7 \pmod{10}$ ainsi $b \equiv -3 \pmod{10}$ d'où $b^4 \equiv (-3)^4 \equiv 1 \pmod{10}$
- Si $r = 8$, alors $b \equiv 8 \pmod{10}$ ainsi $b \equiv -2 \pmod{10}$ d'où $b^4 \equiv (-2)^4 \equiv 6 \pmod{10}$
- Si $r = 9$, alors $b \equiv 9 \pmod{10}$ ainsi $b \equiv -1 \pmod{10}$ d'où $b^4 \equiv (-1)^4 \equiv 1 \pmod{10}$.

Ainsi, les restes possibles de b^4 dans la division euclidienne par 10 sont $0, 1, 5$ et 6.

b) Soit r le reste de la division euclidienne de b par 10. Alors, $b = 10q+r$, où $q \in \mathbb{Z}$. d'après le cours, on a $b \wedge 10 = 1$ si, et seulement si, $r \wedge 10 = 1$ et comme $r \in \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$, alors $r \wedge 10 = 1$ si, et seulement si, $r \in \{1, 3, 7, 9\}$.

c) D'après la question précédente, on a $r \in \{1, 3, 7, 9\}$ si, et seulement si, $b \wedge 10 = 1$ et d'après les calculs de 2)a), $r \in \{1, 3, 7, 9\}$ si, et seulement si, $b^4 \equiv 1 \pmod{10}$ ainsi $b^4 \equiv 1 \pmod{10}$ si, et seulement si, $b \wedge 10 = 1$.

3) Soit $b \in \mathbb{Z}$ tel que b et et 10 sont premiers entre eux.

a) Puisque b et 10 sont premiers entre eux, on a, d'après la question précédente, $b^4 \equiv 1 \pmod{10}$ d'où, d'après 1), $(b^4)^{10} \equiv 1 \pmod{10^2}$, i.e., $b^{40} \equiv 1 \pmod{10^2}$.

b) **(Bonus)** On a $67 \wedge 10 = 1$ d'où, d'après la question précédente, $67^{40} \equiv 1 \pmod{10^2}$ ainsi $67^{41} = 67^{40}.67 \equiv 1.67 = 67 \pmod{10^2}$ donc le reste de la division euclidienne de 67^{40} par 100 est 67.

Corrigé du Rattrapage 2020-2021

Exercice 13 Voir Exercice 15 du polycopié des exercices corrigés (Ensembles, Applications et Relations binaires).

Exercice 14 Voir Exercice 27 du polycopié des exercices corrigés (Ensembles, Applications et Relations binaires).

Exercice 15 Soit dans $\mathbb{Z}$ l'équation (E) : $x^{19} \equiv -2 \pmod{29}$.

1) a) On a 29 est premier et $2 \wedge 29 = 1$, alors, d'après le petit théorème de Fermat, $2^{28} \equiv 1 \pmod{29}$.

   b) On a $(-2)^{56} = 2^{56}$ d'où, d'après a), $(-2)^{56} = (2^{28})^2 \equiv 1 \pmod{29}$ ainsi $(-8)^{19} = (-2)^{57} = (-2)^{56}.(-2) \equiv -2 \pmod{29}$ donc -8 est une solution de (E).

2) Soit x_0 une solution de (E).

   a) On a $x_0 \wedge 29 = 1$ sinon $29 \mid x_0$ d'où $x_0 \equiv 0 \pmod{29}$ et par suite $x_0^{19} \equiv 0 \pmod{29}$, contradiction. Alors, d'après le petit théorème de Fermat, $x_0^{28} \equiv 1 \pmod{29}$.

   b) On a $x_0^{19} \equiv -2 \pmod{29}$ d'où $(x_0^{19})^3 \equiv (-2)^3 \pmod{29}$, i.e., $x_0^{57} \equiv -8 \pmod{29}$.

   c) D'après a), on a $x_0^{28} \equiv 1 \pmod{29}$ d'où $x_0^{57} = (x_0^{28})^2.x_0 \equiv x_0 \pmod{29}$ donc, d'après b), $x_0 \equiv -8 \pmod{29}$.

3) On a, d'après 1), -8 est une solution de (E) et d'après 2), si x_0 est solution de (E), alors $x_0 \equiv -8 \pmod{29}$ d'où x est une solution de (E) si, et seulement si, $x \equiv -8 \pmod{29}$ si, et seulement si, il existe $k \in \mathbb{Z} : x = -8 + 29k$ ainsi l'ensemble des solutions de (E) est $S = \{-8 + 29k / k \in \mathbb{Z}\}$.

4) **(Bonus)** Soit $x \in \mathbb{Z}$. Posons $y = x - 3$. Puisque 13 est premier, alors $y^{13} \equiv y \pmod{13}$. Ainsi, on a $\begin{cases} (x-3)^{19} \equiv -2 \pmod{29} \\ (x-3)^{13} \equiv -2 \pmod{13} \end{cases}$ si, et seulement si, $\begin{cases} y^{19} \equiv -2 \pmod{29} \\ y \equiv -2 \pmod{13} \end{cases}$. Aussi, on a, d'après 3), $y^{19} \equiv -2 \pmod{29}$ ssi $y \equiv -8 \pmod{29}$ alors on a $\begin{cases} (x-3)^{19} \equiv -2 \pmod{29} \\ (x-3)^{13} \equiv -2 \pmod{13} \end{cases}$ si, et seulement si, $\begin{cases} y \equiv -8 \pmod{29} \\ y \equiv -2 \pmod{13} \end{cases}$. Alors, il existe $h \in \mathbb{Z}$ tel que $y = -8 + 29h$. Aussi, on a $y \equiv -2 \pmod{13}$ d'où $-8 + 29h \equiv -2 \pmod{13}$ ainsi $3h \equiv 6 \pmod{13}$, i.e., $13 \mid 3(h-2)$ d'où $13 \mid h - 2$ (car $13 \wedge 3 = 1$) alors il existe $k \in \mathbb{Z}$ tel que $h - 2 = 13k$ ainsi $h = 2 + 13k$ par suite $y = -8 + 29(2 + 13k) = 50 + 377k$et par suite $x = 53 + 377k$ avec $k \in \mathbb{Z}$. Réciproquement, si $x = 53 + 377k$, avec $k \in \mathbb{Z}$, alors $\begin{cases} x - 3 \equiv -8 \pmod{29} \\ x - 3 \equiv -2 \pmod{)9} \end{cases}$ donc $\begin{cases} (x-3)^{19} \equiv -2 \pmod{29} \\ (x-3)^{13} \equiv -2 \pmod{13} \end{cases}$ ainsi $S = \{53 + 377k / k \in \mathbb{Z}\}$.

   Remarque : Pour une deuxième méthode, voir exercice 20 du polycopié des exercices corrigés (Arithmétique).

Corrigé du Contrôle Final 2021-2022

Exercice 16 Voir exercice 2 du polycopié des exercices corrigés (Ensembles, Applications et Realtions binaires).

Exercice 17

1) On a $f(\emptyset) = (\emptyset \cap A) \cup B = \emptyset \cup B = B$; $f(A) = (A \cap A) \cup B = A \cup B$; $f(B) = (B \cap A) \cup B = B$ car $B \cap A \subset B$. Aussi, on a $f(E) = (E \cap A) \cup B = A \cup B$.
2) Supposons que f est injective. Alors, d'après 1), on a $f(\emptyset) = B = f(B)$ et comme f est injective, alors $B = \emptyset$. Aussi, d'après 1), on a $f(A) = A \cup B = f(E)$ donc $A = E$ car f est injective. Comme $B = \emptyset$ et $A = E$, alors pour tout $X \in \mathcal{P}(E)$, $f(X) = (X \cap E) \cup \emptyset = X \cup \emptyset = X$ donc $f = id_{\mathcal{P}(E)}$.

Exercice 18

1) On a $\mathcal{R}$ est réflexive. En effet, $\forall x \in \mathbb{Z}, 7x - 5x = 2x$ est pair d'où $x\mathcal{R}x$. Aussi, $\mathcal{R}$ est symétrique. En effet, soit $x, y \in \mathbb{Z} : x\mathcal{R}y$. Alors, $7x - 5y$ est pair d'où $7y - 5x = 7x - 5y + 2(6y - 6x)$ est pair ainsi $y\mathcal{R}x$. Montrons que $\mathcal{R}$ est transitive : soit $x, y, z \in \mathbb{Z} : x\mathcal{R}y$ et $y\mathcal{R}z$ d'où $2/7x - 5y$ et $2/7y - 5z$ alors $2/(7x - 5y) + (7y - 5z) = 7x - 5z + 2y$ et comme $2/2y$, alors $2/(7x - 5z + 2y) - 2y = 7x - 5y$ ainsi $x\mathcal{R}z$.
   Puisque $\mathcal{R}$ est réflexive, symétrique et transitive, alors $\mathcal{R}$ est une relation d'équivalence.
2) On a $1 \not\mathcal{R}0$ car $7.1 - 5.0 = 7$ est impair donc $cl(0) \neq cl(1)$
3) Soit $n \in \mathbb{Z}$.
   (a) Si n est pair, alors $7n = 7n - 5 \times 0$ est pair d'où $n\mathcal{R}0$ et ainsi $cl(n) = cl(0)$.
   (b) Si n est impair, alors $7n$ est impair d'où $7n - 5 \times 1 = 7n - 5$ est pair d'où $n\mathcal{R}1$ et ainsi $cl(n) = cl(1)$.
4) On a $cl(0), cl(1) \in \mathbb{Z}/\mathcal{R}$ d'où $\{cl(0), cl(1)\} \subset \mathbb{Z}/\mathcal{R}$. Inversement, soit $cl(n) \in \mathbb{Z}/\mathcal{R}$. Alors, d'après 3), si n est pair, alors $cl(n) = cl(0)$ et si n est impair, alors $cl(n) = cl(1)$ ainsi $\mathbb{Z}/\mathcal{R} \subset \{cl(0), cl(1)\}$ donc $\mathbb{Z}/\mathcal{R} = \{cl(0), cl(1)\}$.

Remarque : On peut aussi remarquer que la relation $\mathcal{R}$ n'est autre que la congruence modulo 2. En effet, soit $x, y \in \mathbb{Z}$. On a $x\mathcal{R}y$ si, et seulement si, $7x - 5y \equiv 0 \pmod 2$ si, et seulement si, $x - y \equiv 0 \pmod 2$ (car $7 \equiv 5 \equiv frm[o] - -Mod2$) si, et seulement si, $x \equiv y \pmod 2$.

Exercice 19

1) Soit $x \in \mathbb{Z}$. Supposons que $\begin{cases} x \equiv 1 \pmod 8 \\ x \equiv 7 \pmod{125} \end{cases}$. Alors, $125 \mid x - 7$ d'où il existe $h \in \mathbb{Z}$: $x - 7 = 125h$ ainsi $x = 7 + 125h$. Aussi, on a $x \equiv 1 \pmod 8$ d'où $7 + 125h \equiv 1 \pmod 8$, i.e., $7 + 5h \equiv 1 \pmod 8$ (car $125 \equiv 5 \pmod 8$) d'où $-6 - 5h \equiv 0 \pmod 8$, i.e., $-6 + 3h \equiv 0 \pmod 8$ alors $8 \mid 3(h-2)$ donc $8 \mid h-2$ (car 8 et 3 sont premiers entre eux) ainsi $h = 2+8k$, où $k \in \mathbb{Z}$ et par suite $x = 7 + 125(2 + 8k) = 257 + 1000k$ donc $x \equiv 257 \pmod{1000}$.
2) On considère la suite $(u_n)_{n\in\mathbb{N}}$ définie sur $\mathbb{N}$ par : $u_n = 2 \times 5^n + 7$.
   a) On a $5^2 = 25 \equiv 1 \pmod 8$. Si $n = 2k$, où $k \in \mathbb{N}$ (i.e., si n est pair), alors $5^n = (5^2)^k \equiv 1^k \equiv 1 \pmod 8$. Si $n = 2k + 1$, où $k \in \mathbb{N}$ (i.e., si n est impair), alors $5^n = (5^2)^k \times 5 \equiv 1^k \times 5 \equiv 5 \pmod 8$.
   b) Soit $n \in \mathbb{N}$. Si n est pair, alors $u_n = 2 \times 5^n + 7 \equiv 2 \times 1 + 7 \equiv 1 \pmod 8$. Aussi, si n est impair, alors $u_n = 2 \times 5^n + 7 \equiv 2 \times 5 + 7 \equiv 1 \pmod 8$ ainsi pour tout $n \in \mathbb{N}$, $u_n \equiv 1 \pmod 8$.

c) Soit $n \in \mathbb{N} : n \geq 3$. Alors, $125 = 5^3 \mid 5^n$ et comme $5^n \mid u_n - 7$ alors $125 \mid u_n - 7$ donc $u_n \equiv 7 \pmod{125}$ et on a, d'après 2)b) $u_n \equiv 1 \pmod 8$ donc, d'après 1), $u_n \equiv 257 \pmod{1000}$.

d) Soit $n \in \mathbb{N}$ et $d = u_{2n} \wedge u_{2n+1}$.

i) Soit $n \in \mathbb{N}$. Alors, $5u_{2n} - u_{2n+1} = 5(2 \times 5^{2n} + 7) - (2 \times 5^{2n+1} + 7) = 10 \times 5^{2n} + 35 - 10 \times 5^{2n} - 7 = 28$.

ii) On a d est impair car si d est pair, alors u_{2n} est pair ce qui est faux (car $u_{2n} = 2 \times 5^{2n} + 7 \equiv 1 \pmod 2$).

iii) Supposons que $d = 7$. Alors, $7 = d \mid u_{2n} = 2 \times 5^{2n} + 7$ d'où $7 \mid 2 \times 5^{2n}$ alors $7 \mid 2$ ou $7 \mid 5$ (car 7 est premier), ce qui est faux ; donc $d \neq 7$.

iv) Puisque $d \mid u_{2n}$ et $d \mid u_{2n+1}$, alors $d \mid 5u_{2n} - u_{2n+1} = 28$ donc $d \in \{1, 2, 4, 7, 14, 28\}$ et coome d est impair et $d \neq 7$, alors $d = 1$.

Corrigé du Rattrapage 2021-2022

Exercice 20 $(a) \Rightarrow (b)$: Supposons que $A \subset E$. On a $A \cap E \subset A$. Soit $x \in A$. Alors $x \in E$ car $A \subset E$ d'où $x \in A \cap E$ ainsi $A \subset A \cap E$ et donc $A \cap E = A$.
$(b) \Rightarrow (c)$:Supposons que $A \cap E = A$ et montrons que $A \cup E = E$: On a $E \subset A \cup E$. Inversement, soit $x \in A \cup E$. Alors, $x \in E$ ou $x \in A$. Si $x \in A$, alors $x \in A \cap E$ car $A \cap E = A$ d'où $x \in E$ et donc, dans les deux cas, on a $x \in E$.
$(c) \Rightarrow (a)$: Supposons que $A \cup E = E$ et montrons que $A \subset E$: On a $A \subset A \cup E$ et donc $A \subset E$ car $A \cup E = E$.

Exercice 21

1) Soit $k \in \mathbb{Z}$. Pour tout entier $n \in \mathbb{N}$, $P(n)$ désigne la propriété : $(1 + 10k)^n \equiv 1 + 10nk \pmod{100}$.
On a $P(0)$ est vraie car $(1 + 10k)^0 = 1$ et $1 = 1 + 10k \times 0$.
Supposons que $P(n)$ est vraie à un certain rang n, i.e., $(1 + 10k)^n \equiv 1 + 10nk \pmod{100}$.
Montrons que $P(n + 1)$ est vraie : Puisque $(1 + 10k)^n \equiv 1 + 10nk \pmod{100}$, alors $(1 + 10k)^{n+1} = (1 + 10k)(1 + 10k)^n \equiv (1 + 10k)(1 + 10nk) \pmod{100}$ d'où $(1 + 10k)^{n+1} \equiv 1 + 10nk + 10k \pmod{100}$ (car $100nk^2 \equiv 0 \pmod{100}$) ainsi $(1 + 10k)^{n+1} \equiv 1 + 10k(n + 1) \pmod{100}$, i.e., $P(n + 1)$ est vraie et donc $\forall n \in \mathbb{N}$, $(1 + 10k)^n \equiv 1 + 10nk \pmod{100}$.

2) Soit $a \in E$.

   a) Puisque $a \in E$, alors $\forall n \in \mathbb{N}, a^n \equiv 1 + n(a - 1) \pmod{100}$. En particulier, pour $n = 2$, on obtient $a^2 \equiv 1 + 2(a - 1) \pmod{100}$ d'où $a^2 - 1 - 2(a - 1) \equiv 0 \pmod{100}$, i.e., $(a - 1)^2 \equiv 0 \pmod{100}$ alors $100 \mid (a - 1)^2$ d'où $10 \mid (a - 1)^2$ (car $10 \mid 100$) et par suite $(a - 1)^2 \equiv 0 \pmod{10}$.

   b) Puisque $(a - 1)^2 \equiv 0 \pmod{10}$, alors $10 \mid (a - 1)^2$ ainsi $2 \mid (a - 1)^2$ (car $2 \mid 10$) donc $2 \mid a - 1$ (car 2 est premier). Aussi, puisque $10 \mid (a - 1)^2$, alors $5 \mid (a - 1)^2$ (car $5 \mid 10$) donc $5 \mid a - 1$ (car 5 est premier). Comme $2 \mid a - 1$ et $5 \mid a - 1$ et $2 \wedge 5 = 1$, alors $10 = 2.5 \mid a - 1$ donc $a - 1 \equiv 0 \pmod{10}$, i.e., $a \equiv 1 \pmod{10}$.

3) Soit $x \in \mathbb{Z}$ tel que $x \equiv 1 \pmod{10}$. Alors, il existe $k \in \mathbb{Z} : x = 1 + 10k$. Alors, d'après 1), $\forall n \in \mathbb{N}$, $x^n = (1 + 10k)^n \equiv 1 + 10nk \pmod{100}$ et comme $10k = x - 1$, alors $x^n \equiv 1 + n(x - 1) \pmod{100}$ donc $x \in E$. Inversement, soit $x \in E$, alors, d'après 2), $x \equiv 1 \pmod{10}$ donc $E = \{x \in \mathbb{Z} / x \equiv 1 \pmod{10}\}$.

Exercice 22

1) On a $\mathcal{R}$ est réflexive. En effet, $\forall x \in \mathbb{Z}, 5/0 = x^2 - x^2$, alors $x\mathcal{R}x$. Aussi, $\mathcal{R}$ est symétrique. En effet, soit $x, y \in \mathbb{Z} : x\mathcal{R}y$. Alors, $5/x^2 - y^2$ d'où $5/y^2 - x^2$ ainsi $y\mathcal{R}x$. Montrons que $\mathcal{R}$ est transitive : soit $x, y, z \in \mathbb{Z} : x\mathcal{R}y$ et $y\mathcal{R}z$ d'où $5/x^2 - y^2$ et $5/y^2 - z^2$ ainsi $5/(x^2 - y^2) + (y^2 - z^2) = x^2 - z^2$ alors $x\mathcal{R}z$. Puisque $\mathcal{R}$ est réflexive, symétrique et transitive, alors $\mathcal{R}$ est une relation d'équivalence.

2) Soit $x \in \mathbb{Z}$.
On a $x \in cl(0)$ si, et seulement si, $x\mathcal{R}0$ si, et seulement si, $5/x^2 - 0^2 = x^2$ si, et seulement si, $5/x$ (on a $5/x^2 \Rightarrow 5/x$ car 5 est premier) si, et seulement si, $x \equiv 0 \pmod{5}$ si , et seulement si, $x \in \overline{0}$ et ainsi $cl(0) = \overline{0}$.
On a $x \in cl(1)$ si, et seulement si, $x\mathcal{R}1$ si, et seulement si, $5/x^2 - 1^2 = x^2 - 1 = (x - 1)(x + 1)$ si, et seulement si, $5/x - 1$ ou $5/x + 1$ (on a $5/(x - 1)(x + 1) \Rightarrow 5/x - 1$ ou $5/x + 1$ car 5

est premier) si, et seulement si, $x \equiv 1 \pmod 5$ ou $x \equiv -1 \equiv 4 \pmod 5$ si , et seulement si, $x \in \overline{1}$ ou $x \in \overline{4}$ si, et seulement si, $x \in \overline{1} \cup \overline{4}$ et ainsi $cl(1) = \overline{1} \cup \overline{4}$.
On a $x \in cl(2)$ si, et seulement si, $x\mathcal{R}2$ si, et seulement si, $5/x^2 - 2^2 = (x-2)(x+2)$ si, et seulement si, $5/x-2$ ou $5/x+2$ (on a $5/(x-2)(x+2) \Rightarrow 5/x-2$ ou $5/x+2$ car 5 est premier)si, et seulement si, $x \equiv 2 \pmod 5$ ou $x \equiv -2 \equiv 3 \pmod 5$ si , et seulement si, $x \in \overline{2}$ ou $x \in \overline{3}$ si, et seulement si, $x \in \overline{2} \cup \overline{3}$ et ainsi $cl(2) = \overline{2} \cup \overline{3}$.

3) On a $\overline{0} = cl(0), \overline{1} \cup \overline{4} = cl(1), \overline{2} \cup \overline{3} = cl(2) \in \mathbb{Z}/\mathcal{R}$. Inversement, soit $cl(x) \in \mathbb{Z}/\mathcal{R}$, où $x \in \mathbb{Z}$. Puisque $x \in \mathbb{Z}$, $x \in \overline{0} \cup \overline{1} \cup \overline{2} \cup \overline{3} \cup \overline{4}$ car $\mathbb{Z} = \overline{0} \cup \overline{1} \cup \overline{2} \cup \overline{3} \cup \overline{4}$. Alors,
   — Si $x \in \overline{0}$, alors, d'après 2), $x \in cl(0)$ d'où $x\mathcal{R}0$ et donc, d'après le cours, $cl(x) = cl(0)$.
   — Si $x \in \overline{1}$ ou $x \in \overline{4}$, alors, d'après 2), $x \in cl(1)$ d'où $x\mathcal{R}1$ et donc, d'après le cours, $cl(x) = cl(1)$.
   — Si $x \in \overline{2}$ ou $x \in \overline{3}$, alors, d'après 2), $x \in cl(2)$ d'où $x\mathcal{R}2$ et donc, d'après le cours, $cl(x) = cl(2)$.
   Ainsi, $cl(x) = cl(0) = \overline{0}$ ou $cl(x) = cl(1) = \overline{1} \cup \overline{4}$ ou $cl(x) = cl(2) = \overline{2} \cup \overline{3}$ donc $\mathbb{Z}/\mathcal{R} = \{\overline{0}, \overline{1} \cup \overline{4}, \overline{2} \cup \overline{3}\}$.

Exercice 23 Soit E un ensemble et A, B deux parties de E. On considère l'application $f : \mathcal{P}(E) \to \mathcal{P}(E), X \mapsto (\overline{X} \cup A) \cap B$.

1) On a $f(\emptyset) = (\overline{\emptyset} \cup A) \cap B = (E \cup A) \cap B = E \cap B = B$. Aussi, on a $f(E) = (\overline{E} \cup A) \cap B = (\emptyset \cup A) \cap B = A \cap B$.

2) Supposons que f est constante.. Alors, $f(\emptyset) = f(E)$ d'où $B = A \cap B$ ainsi $B \subset A$. Réciproquement, supposons que $B \subset A$. On a $\forall X \in \mathcal{P}(E)$, $f(X) = (\overline{X} \cup A) \cap B$ et comme $B \subset A \subset \overline{X} \cup A$, alors $f(X) = B$ donc f est constante.

3) Supposons que f est surjective.
   (a) On a $E \in \mathcal{P}(E)$ possède un antécédent par f, i.e., il existe $X \in \mathcal{P}(E) : (\overline{X} \cup A) \cap B = E$ d'où $E \subset (\overline{X} \cup A) \cap B \subset B$ et comme $B \subset E$, alors $B = E$. Aussi, puisque f est surjective, alors $\emptyset \in \mathcal{P}(E)$ possède un antécédent par f, i.e., il existe $X \in \mathcal{P}(E) : (\overline{X} \cup A) \cap B = \emptyset$ et comme $B = E$, alors $(\overline{X} \cup A) \cap E = \emptyset$ d'où $\overline{X} \cup A = \emptyset$ donc $A = \emptyset$.
   (b) On a $\forall X \in \mathcal{P}(E)$, $f(X) = (\overline{X} \cup A) \cap B = (\overline{X} \cup \emptyset) \cap E = \overline{X} \cap E = \overline{X}$. Alors, $\forall X \in \mathcal{P}(E)$, $f \circ f(X) = f(f(X)) = f(\overline{X}) = \overline{\overline{X}} = X$ donc $f \circ f = id_{\mathcal{P}(E)}$ et ainsi il existe une application $g = f$ telle que $f \circ g = id_{\mathcal{P}(E)}$ et $g \circ f = id_{\mathcal{P}(E)}$ donc f est bijective et $f^{-1} = g = f$.

Corrigé du Contrôl Final 2022-2023

Exercice 24 Voir exercice 2)2) du polycopié des exercices corrigés (Arithmétique). La seule différence est que pour cet exercice, on doit vérifier que $P(0)$ et $P(1)$ sont vraies (au lieu de $P(1)$ et $P(2)$).

Exercice 25 Voir exercice 3)2) du polycopié des exercices corrigés (Ensembles, Applications et Realtions binaires).

Exercice 26 On considère la relation binaire $\mathcal{R}$ définie sur $\mathbb{Z}^2$ par $(x,y)\mathcal{R}(z,t)$ si $x-z \equiv 3(y-t) \pmod 5$, où $(x,y),(z,t) \in \mathbb{Z}^2$.

1) Soit $(x,y) \in \mathbb{Z}^2$. On a $x-x=0 \equiv 0 = 3(y-y) \pmod 5$ d'où $(x,y)\mathcal{R}(x,y)$ et ainsi $\mathcal{R}$ est réflexive.
   Soit $(x,y),(z,t) \in \mathbb{Z}^2$ tels que $(x,y)\mathcal{R}(z,t)$. Alors, $x-z \equiv 3(y-t) \pmod 5$ d'où $z-x \equiv 3(t-y) \pmod 5$ ainsi $(z,t)\mathcal{R}(x,y)$ et donc $\mathcal{R}$ est symétrique.
   Soit $(x,y),(z,t),(u,v) \in \mathbb{Z}^2$ tels que $(x,y)\mathcal{R}(z,t)$ et $(z,t)\mathcal{R}(u,v)$. Alors, $x-z \equiv 3(y-t) \pmod 5$ et $z-u \equiv 3(t-v) \pmod 5$ ainsi $(x-z)+(z-u) \equiv 3(y-t)+3(t-v) \pmod 5$ d'où $x-u \equiv 3(y-v)$ alors $(x,y)\mathcal{R}(u,v)$ donc $\mathcal{R}$ est transitive.
   Puisque $\mathcal{R}$ est réflexive, symétrique et transitive, alors $\mathcal{R}$ est une relation d'équivalence.

2) Soit $(x,y) \in \mathbb{Z}^2$. On a $(x,y) \in cl((0,0))$ si, et seulement si, $x-0 \equiv 3(y-0) \pmod 5$ si, et seulement si, $x \equiv 3y \pmod 5$ si, et seulement si, $2x \equiv y \pmod 5$ (pour $\Rightarrow$) il suffit de multiplier les deux membres de la congruence par 2 et pour $\Leftarrow$) on les multiplie par 3). Ainsi, $(x,y) \in cl((0,0))$ si, et seulement si, il existe $k \in \mathbb{Z} : y = 2x+5k$ si, et seulement si, $(x,y) = (x, 2x+5k)$, où $k \in \mathbb{Z}$. Alors, $cl((0,0)) = \{(x,2x+5k)/(x,k) \in \mathbb{Z}^2\}$.

3) Soit $q,r \in \mathbb{Z}$. On a $5q+r-r = 5q \equiv 0 \pmod 5$ et $3(0-0) \equiv 0 \pmod 5$ d'où $5q+r-r \equiv 0-0 \pmod 5$ ainsi $(5q+r,0)\mathcal{R}(r,0)$ donc $cl((5q+r,0)) = cl((r,0))$.

4) Soit $(x,y) \in \mathbb{Z}^2$. On a $x-(x+2y) = -2y \equiv 3y \pmod 5$ alors $(x,y)\mathcal{R}(x+2y,0)$ donc $cl((x,y)) = cl((x+2y,0))$.

5) Soit $(x,y) \in \mathbb{Z}^2$. D'après 4), on a $cl((x,y)) = cl((x+2y,0))$ et en effectuant la division euclidienne de $x+2y$ par 5, on obtient $x+2y = 5q+r$, avec $q \in \mathbb{Z}$ et $r \in \{0,1,2,3,4\}$. Alors, $cl((x,y)) = cl((x+2y,0)) = cl((5q+r,0))$ et d'après 3), $cl((5q+r,0)) = cl((r,0))$ donc $cl((x,y)) = cl((r,0))$ avec $r \in \{0,1,2,3,4\}$.

6) On considère la correspondance $f : \mathbb{Z}_5 \to (\mathbb{Z}\times\mathbb{Z})/\mathcal{R}$, $\overline{x} \mapsto cl((x,0))$, où $\overline{x}$ est la classe de congruence de x modulo 5.

   a) Soit $\overline{x} \in \mathbb{Z}_5$, avec $x \in \mathbb{Z}$. Alors, $(x,0) \in \mathbb{Z}^2$ d'où $cl((x,0)) \in (\mathbb{Z}\times\mathbb{Z})/\mathcal{R}$.
      Soit $x,y \in \mathbb{Z}$ tels que $\overline{x} = \overline{y}$ dans $\mathbb{Z}_5$. Alors, il existe $q \in \mathbb{Z}$ tel que $y-x = 5q$. Alors, $(y,0) = (5q+x,0)$ d'où, d'après 3) , $cl((y,0)) = cl((5q+x,0)) = cl((x,0))$, i.e., $f(\overline{y}) = f(\overline{x})$.

   b) On a f est injective. En effet, soit $\overline{x},\overline{y} \in \mathbb{Z}_5$ tels que $f(\overline{x}) = f(\overline{y})$. Alors, $cl((x,0)) = cl((y,0))$ d'où $(x,0)\mathcal{R}(y,0)$ ainsi $x-y \equiv 3.(0-0) \pmod 5$ donc $x \equiv y \pmod 5$ et par suite $\overline{x} = \overline{y}$.
      Aussi, on a f est surjective. En effet, soit $cl((x,y)) \in (\mathbb{Z}\times\mathbb{Z})/\mathcal{R}$, avec $x,y \in \mathbb{Z}$. On a, d'après 4), $cl((x,y)) = cl((x+2y,0))$ ainsi il existe $\overline{z} = \overline{x+2y} \in \mathbb{Z}_5$ tel que $f(\overline{z}) = f(\overline{x+2y}) = cl((x+2y,0)) = cl((x,y))$. Ainsi, puisque f est injective et surjective, alors f est bijective.

Exercice 27

I) On se propose de montrer par l'absurde que la congruence $x^2 \equiv -1 \pmod{43}$ ne possède pas de solutions dans $\mathbb{Z}$. Supposons que $x_0 \in \mathbb{Z}$ est solution de $x^2 \equiv -1 \pmod{43}$.

1) Supposons que 43 divise x_0. Alors, $43 \mid x_0^2$. D'autre part, puisque $x_0^2 \equiv -1 \pmod{43}$, alors $43 \mid x_0^2 + 1$ ainsi $43 \mid 1$, ce qui est faux et donc 43 ne divise pas x_0.

2) Puisque 43 ne divise pas x_0 et 43 est un nombre premier, alors, d'après le petit théorème de Fermat, $x_0^{42} \equiv 1 \pmod{43}$, i.e., $(x_0^2)^{21} \equiv 1 \pmod{43}$.

3) On a $x_0^2 \equiv -1 \pmod{43}$ d'où $(x_0^2)^{21} \equiv (-1)^{21} \pmod{43}$ donc $(x_0^2)^{21} \equiv -1 \pmod{43}$. Aussi, on a, d'après 2), $(x_0^2)^{21} \equiv 1 \pmod{43}$. Alors, $-1 \equiv 1 \pmod{43}$ donc 43 divise 2, ce qui est faux et donc la congruence $x^2 \equiv -1 \pmod{43}$ ne possède pas de solutions dans $\mathbb{Z}$.

II) Soit $a, b \in \mathbb{Z}$ tels que 43 divise $a^2 + b^2$. On se propose de montrer par l'absurde que 43 divise a et b. Supposons alors que 43 ne divise pas a.

1) Puisque 43 ne divise pas a, alors $43 \wedge a = 1$ d'où il existe $u, v \in \mathbb{Z} : ua + 43v = 1$ donc il existe $u \in \mathbb{Z} : ua \equiv 1 \pmod{43}$.

2) On a $43 \mid a^2+b^2$. Alors, $43 \mid u^2(a^2+b^2)$ d'où $(ua)^2+(ub)^2 \equiv 0 \pmod{43}$. D'autre part, puisque $ua \equiv 1 \pmod{43}$, alors $(ua)^2 \equiv 1 \pmod{43}$ et ainsi $(ub)^2 \equiv -1 \pmod{43}$.

3) Puisque $(ub)^2 \equiv -1 \pmod{43}$, alors la congruence $x^2 \equiv -1 \pmod{43}$ possède des solutions, ce qui contredit I), donc 43 divise a. Puisque 43 divise a, alors 43 divise a^2 et comme 43 divise $a^2 + b^2$, alors 43 divise b^2 et donc 43 divise aussi b car 43 est premier.

Corrigé du Rattrapage 2022-2023

Exercice 28

1) Voir exercice 23)1) du polycopié des exercices corrigés (Arithmétique).
2) On a g est injective. En effet, soit $\overline{x}, \overline{y} \in \mathbb{Z}/10\mathbb{Z} : g(\overline{x}) = g(\overline{y})$. Alors, $\overline{7x} = \overline{7y}$ dans $\mathbb{Z}/10\mathbb{Z}$ d'où, en multipliant les deux membres de l'égalité par $\overline{3}$, on obtient $\overline{x} = \overline{y}$.
Montrons que g est surjective : soit $\overline{y} \in \mathbb{Z}/10\mathbb{Z}$. Alors, il existe $\overline{x} = \overline{3y}$ dans $\mathbb{Z}/10\mathbb{Z}$ tel que $g(\overline{x}) = g(\overline{3y}) = \overline{7.3y} = \overline{y}$.

Exercice 29 Supposons que $X \cap A \subset X \cap B$ et $X \cup A \subset X \cup B$. Soit $a \in A$.
— Si $a \in X$, alors $a \in X \cap A$ d'où $a \in X \cap B$ car $X \cap A \subset X \cap B$ et ainsi $a \in B$.
— Si $a \notin X$: on a $a \in X \cup A$ car $a \in A$ d'où $a \in X \cup B$ car $X \cup A \subset X \cup B$ et ainsi $a \in B$ car $a \notin X$.

Exercice 30 On considère la relation binaire $\mathcal{R}$ définie sur $\mathbb{Z}^2$ par $(x, y)\mathcal{R}(z, t)$ si $x - z \equiv a(y - t) \pmod{n}$, où $(x, y), (z, t) \in \mathbb{Z}^2$.

1) Soit $(x, y) \in \mathbb{Z}^2$. On a $x - x = 0 \equiv 0 = a(y - y) \pmod{n}$ d'où $(x, y)\mathcal{R}(x, y)$ et ainsi $\mathcal{R}$ est réflexive.
Soit $(x, y), (z, t) \in \mathbb{Z}^2$ tels que $(x, y)\mathcal{R}(z, t)$. Alors, $x - z \equiv a(y - t) \pmod{n}$ d'où $z - x \equiv a(t - y) \pmod{n}$ ainsi $(z, t)\mathcal{R}(x, y)$ et donc $\mathcal{R}$ est symétrique.
Soit $(x, y), (z, t), (u, v) \in \mathbb{Z}^2$ tels que $(x, y)\mathcal{R}(z, t)$ et $(z, t)\mathcal{R}(u, v)$. Alors, $x - z \equiv a(y - t) \pmod{n}$ et $z - u \equiv a(t - v) \pmod{n}$ ainsi $(x - z) + (z - u) \equiv a(y - t) + a(t - v) \pmod{n}$ d'où $x - u \equiv a(y - v) \pmod{n}$ alors $(x, y)\mathcal{R}(u, v)$ donc $\mathcal{R}$ est transitive.
Puisque $\mathcal{R}$ est réflexive, symétrique et transitive, alors $\mathcal{R}$ est une relation d'équivalence.
2) Soit $(x, y) \in \mathbb{Z}^2$. On a $x - (x - ay) \equiv a(y - 0) \pmod{n}$ alors $(x, y)\mathcal{R}(x - ay, 0)$ donc $cl((x, y)) = cl((x - ay, 0))$.
3) Soit $r, s \in \{0, 1, \ldots, n - 1\}$ tels que $cl((r, 0)) = cl((s, 0))$. Alors, $(r, 0)\mathcal{R}(s, 0)$ d'où $r - s \equiv 0 \pmod{n}$ ainsi $n \mid r - s$ et par suite $n \mid |r - s|$. D'autre part, on a $0 \leq r \leq n - 1$ et $-(n - 1) \leq -s \leq 0$ d'où $-(n - 1) \leq r - s \leq (n - 1)$ ainsi $|r - s| \leq n - 1 < n$. Comme $n \mid |r - s|$ et $|r - s| < n$, alors $|r - s| = 0$ donc $r = s$. Ainsi, puisque $0, 1, \ldots, n - 1$ sont deux à deux distincts, alors les classes $cl((0, 0)), cl((1, 0)), \ldots, cl((n - 1, 0))$ sont deux à deux distinctes.
4) Il est évident que $\{cl((0, 0)), cl((1, 0)), \ldots, cl((n-1, 0))\} \subset \mathbb{Z}^2/\mathcal{R}$. Inversement, soit $cl((x, y)) \in \mathbb{Z}^2/\mathcal{R}$. On a, d'après 2), $cl((x, y)) = cl((x - ay, 0))$. En effectuant la division euclidienne de $x - ay$ par n, on obtient $x - ay = qn + r$, avec $r \in \{0, 1, \ldots, n - 1\}$. Alors, $cl((x - ay, 0)) = cl((qn + r, 0))$ et en remarquant que $(qn + r) - r \equiv 0 \equiv a(0 - 0) \pmod{n}$, on obtient $(qn + r, 0)\mathcal{R}(r, 0)$ ainsi $cl((qn + r, 0)) = cl((r, 0)))$ alors $cl((x, y)) = cl((r, 0))$ avec $r \in \{0, 1, \ldots, n - 1\}$ et par suite $\mathbb{Z}^2/\mathcal{R} \subset \{cl((0, 0)), cl((1, 0)), \ldots, cl((n - 1, 0))\}$ donc $\mathbb{Z}^2/\mathcal{R} = \{cl((0, 0)), cl((1, 0)), \ldots, cl((n - 1, 0))\}$.

Exercice 31

1) On a 3 ne divise pas $2 - 1$, alors $2 \in A$ et donc $A \neq \emptyset$. (On peut aussi remarquer que $3 \in A$ car 3 ne divise pas $3 - 1$.
2) Soit $p \in A$ tel que $p \not\equiv 2 \pmod{3}$. Puisque $p \in A$, alors 3 ne divise pas $p - 1$ d'où $p - 1 \not\equiv 0 \pmod{3}$ ainsi $p \not\equiv 1 \pmod{3}$ et comme $p \not\equiv 2 \pmod{3}$, alors $p \equiv 0 \pmod{3}$ d'où $3 \mid p$ donc $p = 3$ car p est premier.
On suppose que A est fini et on pose $A = \{p_1, \ldots, p_m\}$. Soit $N = (3p_1 \ldots p_m) - 1$.

3) On a N est une entier > 2 d'où, d'après le théorème fondamental d'arithmétique, $N = q_1 \dots q_r$, où $q_1, \dots, q_r$ sont des nombres premiers.

4) Pour tout $i \in \{1, \dots, m\}$, on a p_i divise $3p_1 \dots p_m$ d'où p_i ne divise pas $N = (3p_1 \dots p_m) - 1$ car si p_i ne divise pas $N = (3p_1 \dots p_m) - 1$, alors p_i divise $(3p_1 \dots p_m) - N = 1$ ce qui est faux. Comme p_i est premier et p_i ne divise pas N, alors $p_i \wedge N = 1$.

   On peut aussi remarquer que $p_i(p_1 \dots p_{i-1}p_{i+1} \dots p_m) + (-1).N = 1$ alors, d'après le théorème de Bezout, $p_i \wedge N = 1$.

5) Soit $j \in \{1, \dots, r\}$. On a $q_j \notin A$. En effet, supposons que $q_j \in A$, alors il existe $i \in \{1, \dots, m\} : q_j = p_i$ d'où p_i divise N donc $p_i \wedge N = p_i \neq 1$, ce qui est faux. Puisque $q_j \notin A$, alors 3 divise $q_j - 1$ d'où $q_j \equiv 1 \mod 3$.

6) Puisque $N + 1 = 3p_1 \dots p_m$, alors 3 divise $N + 1$ d'où $N + 1 \equiv 0 \pmod 3$ ainsi $N \equiv -1 \pmod 3$. D'autre part, on a $N = q_1 \dots q_r$ et, d'après ..., $\forall j = 1, \dots, r$, $q_j \equiv 1 \mod 3$ donc $N \equiv 1 \pmod 3$. Ainsi, on obtient $-1 \equiv 1 \pmod 3$ d'où 3 divise 2, contradiction. Alors, A est un ensemble infini, i.e., il existe une infinité de nombres premiers p tels que 3 ne divise pas $p - 1$ ainsi il existe une infinité de nombres premiers p tels que $p \not\equiv 1 \pmod 3$ et comme $q = 3$ est l'unique nombre premier vérifiant $q \equiv 0 \pmod{}$, alors il existe une infinité de nombres premiers p tels que $p \equiv 2 \pmod 3$, i.e., il existe une infinité de nombres premiers p de la forme $3k + 2$, avec $k \in \mathbb{N}$.