RELATIONS
CORRECTION

Exercice 1

Soient E un ensemble non vide et $\mathscr{R}$ une relation sur E. La relation $\mathscr{R}^2$ sur E est définie par $\forall x, y \in E,\ \big(x\mathscr{R}^2\, y\big) \iff \big(\exists u \in E,\ x\mathscr{R}\, u \text{ et } u\mathscr{R}\, y\big)$.

1. *Soit la relation $\ll$ sur $\mathbb{R}^2$ définie par $\forall (x,y),(a,b) \in \mathbb{R}^2,\ \big((x,y) \ll (a,b)\big) \iff \big(x \leqslant a \text{ ou } y \leqslant b\big)$. Démontrer que $\ll^2$ est la relation pleine sur $\mathbb{R}^2$.*

   Soient $(x,y),(a,b) \in \mathbb{R}^2$. Par définition de $\ll$, on a $(x,y) \ll (x,b)$ et $(x,b) \ll (a,b)$, ce qui implique, d'après la définition de $\ll^2$, que $(x,y) \ll^2 (a,b)$. Par conséquent,

   $$\boxed{\ll^2 \text{ est la relation pleine sur } \mathbb{R}^2.}$$

2. *On suppose que $\mathscr{R}$ est réflexive et transitive. Démontrer que $\mathscr{R}^2 = \mathscr{R}$. Donner, en conséquence, deux grands types de relations $\mathscr{R}$ vérifiant $\mathscr{R}^2 = \mathscr{R}$.*

   Démontrer que $\mathscr{R}^2 = \mathscr{R}$ revient à démontrer que $\forall x, y \in E,\ \big(x\mathscr{R}\, y\big) \iff \big(x\mathscr{R}^2\, y\big)$.
   Soient $x, y \in E$. On procède par double implication.

   - $\Rightarrow$ Supposons que $x\mathscr{R}\, y$. Comme $\mathscr{R}$ est réflexive, on a $x\mathscr{R}\, x$. En associant $x\mathscr{R}\, x$ et $x\mathscr{R}\, y$ et la définition de $\mathscr{R}^2$ (avec $u = x$), on obtient $x\mathscr{R}^2\, y$.
   - $\Leftarrow$ Supposons que $x\mathscr{R}^2\, y$. Par définition de $\mathscr{R}^2$, il existe $u \in E$ tel que $x\mathscr{R}\, u$ et $u\mathscr{R}\, y$. Par transitivité de $\mathscr{R}$, on a alors $x\mathscr{R}\, y$.

   En conclusion,

   $$\boxed{\text{si } \mathscr{R} \text{ est réflexive et transitive, alors } \mathscr{R}^2 = \mathscr{R}.}$$

   Les relations d'équivalence et les relations d'ordre étant réflexives et transitives, on en déduit que

   $$\boxed{\text{si } \mathscr{R} \text{ est une relation d'ordre ou d'équivalence, alors } \mathscr{R}^2 = \mathscr{R}.}$$

3. *Démontrer que si $\mathscr{R}$ est réflexive, alors $\mathscr{R}^2$ l'est aussi.*

   Soit $x \in E$. Comme $\mathscr{R}$ est réflexive, on a $x\mathscr{R}\, x$. Par définition de $\mathscr{R}^2$, on a donc $x\mathscr{R}^2\, x$ (en prenant $u = x$), ce qui prouve que $\mathscr{R}^2$ est réflexive. En conclusion,

   $$\boxed{\text{si } \mathscr{R} \text{ est réflexive, alors } \mathscr{R}^2 \text{ l'est aussi.}}$$

4. *Démontrer que si $\mathscr{R}$ est transitive, alors $\mathscr{R}^2$ l'est aussi.*

   Soient $x, y, z \in E$ tels que $x\mathscr{R}^2\, y$ et $y\mathscr{R}^2\, z$. Il existe alors $u_1, u_2 \in E$ tels que d'une part $x\mathscr{R}\, u_1$ et $u_1\mathscr{R}\, y$ et d'autre part $y\mathscr{R}\, u_2$ et $u_2\mathscr{R}\, z$. Comme $\mathscr{R}$ est transitive, cela implique d'une part que $x\mathscr{R}\, y$ et d'autre part que $y\mathscr{R}\, z$. Par définition de $\mathscr{R}^2$, on a $x\mathscr{R}^2\, z$. Donc $\mathscr{R}^2$ est transitive. En conclusion,

   $$\boxed{\text{si } \mathscr{R} \text{ est transitive, alors } \mathscr{R} \circ \mathscr{R} \text{ l'est aussi.}}$$

5. *Démontrer que si $\mathscr{R}$ est symétrique, alors $\mathscr{R}^2$ l'est aussi.*

   Soient $x, y \in E$ tels que $x\mathscr{R}^2\, y$. Il existe alors $u \in E$ tel que $x\mathscr{R}\, u$ et $u\mathscr{R}\, y$. Comme $\mathscr{R}$ est symétrique, on en déduit que $u\mathscr{R}\, x$ et $y\mathscr{R}\, u$. Par définition de $\mathscr{R}^2$, on a alors $y\mathscr{R}^2\, x$.. Cela prouve que $\mathscr{R}^2$ est symétrique. En conclusion,

   $$\boxed{\text{si } \mathscr{R} \text{ est symétrique, alors } \mathscr{R}^2 \text{ l'est aussi.}}$$

6. *Démontrer que si $\mathscr{R}$ est antisymétrique et transitive, alors $\mathscr{R}^2$ est antisymétrique.*

   Soient $x, y \in E$ tels que $x\mathscr{R}^2\, y$ et $y\mathscr{R}^2\, x$. Il existe alors $u_1, u_2 \in E$ tels que d'une part $x\mathscr{R}\, u_1$ et $u_1\mathscr{R}\, y$ et d'autre part $y\mathscr{R}\, u_2$ et $u_2\mathscr{R}\, x$. Comme $\mathscr{R}$ est transitive, cela implique d'une part que $x\mathscr{R}\, y$ et d'autre part que $y\mathscr{R}\, x$. Comme $\mathscr{R}$ est antisymétrique, il s'ensuit que $x = y$. Donc $\mathscr{R}^2$ est antisymétrique. En conclusion,

   $\boxed{\text{si } \mathscr{R} \text{ est antisymétrique et transitive, alors } \mathscr{R}^2 \text{ est antisymétrique.}}$

Exercice 2

Soient $n \in \mathbb{N}$ et p un diviseur impair de n^2+1. On considère la relation $\sim$ sur $[\![1; p-1]\!]$ définie par $\forall x, y \in [\![1; p-1]\!]\,,\ (x \sim y) \iff (\exists k \in [\![0; 3]\!]\,,\ y \equiv n^k x\ [p])$.

1. a) *Quelle est la valeur de n^4 modulo p ?*

   Comme p divise n^2+1, on a $n^2 \equiv -1\ [p]$. En élevant au carré, on obtient

   $$\boxed{n^4 \equiv 1\ [p].}$$

   b) *Démontrer que $\sim$ est une relation d'équivalence sur $[\![1; p-1]\!]$.*

   Réflexivité :
   Soit $x \in [\![1; p-1]\!]$. On a clairement $x \equiv n^0 x\ [p]$ donc $x \sim x$.

   Transitivité :
   Soient $x, y, z \in [\![1; p-1]\!]$ tels que $x \sim y$ et $y \sim z$. Il existe $k, \ell \in [\![0; 3]\!]$ tels que $y \equiv n^k x\ [p]$ et $z \equiv n^\ell y\ [p]$. Cela donne $z = n^{k+\ell} x\ [p]$.
   Comme $k, \ell \in [\![0; 3]\!]$, on a $k + \ell \in [\![0; 6]\!]$.
   Si $\ell + k \in [\![0; 3]\!]$, la relation $z = n^{k+\ell} x\ [p]$ nous dit que $x \sim z$.
   Si $\ell + k \in [\![4; 6]\!]$, on utilise le fait que $n^4 \equiv 1\ [p]$ (démontré à la question précédente) pour écrire que $z = n^{k+\ell-4} x\ [p]$. Comme $k + \ell - 4 \in [\![0; 2]\!]$, cela nous dit que $x \sim z$.
   Dans tous les cas, on a $x \sim z$.

   Symétrie :
   Soient $x, y \in [\![1; p-1]\!]$ tels que $x \sim y$. Il existe $k \in [\![0; 3]\!]$ tels que $y \equiv n^k x\ [p]$.
   Si $k = 0$, on a $y \equiv x\ [p]$, c'est-à-dire $x \equiv n^0 y\ [p]$, donc $y \sim x$.
   Si $k \in [\![1; 3]\!]$, on multiplie la relation $y \equiv n^k x\ [p]$ par n^{4-k}, ce qui donne $n^{4-k} y \equiv n^4 x\ [p]$. Comme $n^4 \equiv 1\ [p]$, on en déduit que $n^{4-k} y \equiv x\ [p]$. Comme $4 - k \in [\![1; 3]\!]$, on en déduit que $y \sim x$.
   Dans tous les cas, on a $y \sim x$.

   En conclusion,

   $\boxed{\sim \text{ est une relation d'équivalence sur } [\![1; p-1]\!].}$

2. a) *Démontrer que p ne divise ni $n-1$, ni n^2-1, ni n^3-1.*

   Par l'absurde : Supposons que p divise $n-1$, c'est-à-dire $n \equiv 1\ [p]$. Alors $n^2 \equiv 1\ [p]$. Comme on sait que $n^2 \equiv -1\ [p]$ puisque p divise n^2+1, on en déduit que $1 \equiv -1\ [p]$, c'est-à-dire $p = 2$. C'est absurde !

   Par l'absurde : Supposons que p divise n^2-1, c'est-à-dire $n^2 \equiv 1\ [p]$. D'après le cas précédent, c'est absurde !

   Par l'absurde : Supposons que p divise n^3-1, c'est-à-dire $n^3 \equiv 1\ [p]$. En élevant au carré, on obtient $n^6 \equiv 1\ [p]$, c'est-à-dire $n^2 \equiv 1\ [p]$ puisque $n^4 \equiv 1\ [p]$. D'après le cas précédent, c'est absurde !

   On en conclut que

   $\boxed{p \text{ ne divise ni } n-1, \text{ ni } n^2-1, \text{ ni } n^3-1.}$

b) *En déduire que chaque classe d'équivalence de* $[\![1;p-1]\!]$ *pour la relation* $\sim$ *est un ensemble à quatre éléments.*

Soit $x \in [\![1;p-1]\!]$. On note $\widehat{x}$ la classe d'équivalence de x pour la relation $\sim$.
Posons $x_0 = x$. Notons x_1 le reste de la division euclidienne de nx par p, x_2 le reste de la division euclidienne de n^2x par p et x_3 le reste de la division euclidienne de n^3x par p.
D'après la définition de la relation $\sim$, on a $\widehat{x} = \{x_0, x_1, x_2, x_3\}$.
Pour démontrer que $\widehat{x}$ est de cardinal 4, il faut démontrer que x_0, x_1, x_2, x_3 sont distincts deux à deux.
Par l'absurde : supposons l'existence de $0 \leqslant k < \ell \leqslant 3$ tels que $x_k = x_\ell$. Par définition de x_k et x_ℓ, on a $x_k \equiv n^k x\ [p]$ et $x_\ell \equiv n^\ell x\ [p]$. Par conséquent, on a $n^k x \equiv n^\ell x\ [p]$, ce qui donne $(n^{\ell-k}-1)x \equiv 0\ [p]$. Comme p est premier, on en déduit que p divise $n^{\ell-k}-1$ ou x. Comme ce ne peut pas être x (puisque $x \in [\![1;p-1]\!]$), on sait que p divise $n^{\ell-k}-1$. Or $\ell - k \in [\![1;3]\!]$, donc p divise $n-1$ ou n^2-1 ou n^3-1. On a démontré au début de cette question que c'est absurde !
Les nombres x_0, x_1, x_2, x_3 sont donc bien distincts deux à deux, ce qui démontre que l'ensemble $\widehat{x} = \{x_0, x_1, x_2, x_3\}$ est de cardinal 4.
En conclusion,

chaque classe d'équivalence de $[\![1;p-1]\!]$ pour la relation $\sim$ est un ensemble à quatre éléments.

c) *En conclure que* $p \equiv 1\ [4]$.

On sait que les classes d'équivalence de $\sim$ forment une partition de $[\![1;p-1]\!]$. Comme chaque classe d'équivalence est de cardinal 4, on en déduit que le cardinal de $[\![1;p-1]\!]$ est un multiple de 4. Autrement dit, $p-1$ est un multiple de 4. Cela signifie que

$$\boxed{p \equiv 1\ [4].}$$

Remarque culturelle :

Nous venons de démontrer que si -1 est un carré modulo p alors nécessairement p est congru à 1 modulo 4. En fait, la condition est aussi suffisante.

Nous verrons plus tard que l'on peut obtenir le résultat de cet exercice à l'aide du petit théorème de Fermat.