

Examen du mardi 11 octobre 2022
Correction.

Exercice 1 a) Donner un exemple d'application injective $\mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$. Justifier votre exemple.

Par exemple, l'application $\mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$
 $(m, n) \mapsto 2^m 3^n$ est injective car 2 et 3 sont des nombres premiers distincts

b) Donner un exemple d'application injective $\mathbb{Q}_{\geq 0} \rightarrow \mathbb{N} \times \mathbb{N}$.

Tout nombre rationnel s'écrit $r = \frac{p}{q}$ pour un unique couple $(p, q) \in \mathbb{N} \times \mathbb{N}_{>0}$ d'entiers premiers entre eux.

c) Existe-t-il une d'application injective $\mathbb{Q}_{\geq 0} \rightarrow \mathbb{N}$?

Comme la composée de deux applications injectives est injective, l'application

$$\mathbb{Q}_{\geq 0} \xrightarrow{\frac{\cdot}{q}} \mathbb{N} \xrightarrow{2^{\cdot} 3^{\cdot}} \mathbb{N}$$

(si $p \in \mathbb{N}, q \in \mathbb{N}_{>0}, \text{pgcd}(p, q) = 1$) est injective.

l'application $\mathbb{Q}_{\geq 0} \rightarrow \mathbb{N} \times \mathbb{N}$
 $\frac{p}{q} \mapsto (p, q)$ est clairement injective
où $(p, q) \in \mathbb{N} \times \mathbb{N}_{>0}$
 $\text{pgcd}(p, q) = 1$

Exercice 2 a) Résoudre dans \mathbb{Z} :

$$\begin{cases} x = 0 [2] \\ x = 1 [5] \end{cases} \Leftrightarrow x = 6 [10]$$

et en déduire le dernier chiffre de

$$N = \underbrace{2^{2022}}_2 \dots 2$$

La nombre N est pair donc $N = 0 [2]$.

$$2^4 = 16 \equiv -1 [5] \Rightarrow 2^4 = 1 [5] \Rightarrow \forall n \in \mathbb{N}, 2^{4n} = 1 [5]$$

en écriture décimale.

Comme l'exposant ci-dessus est clairement multiple de 4, on a aussi $N = 1 [5]$. Donc d'après a), $N = 6 [10]$. Le dernier chiffre de N est 6.

b) Résoudre dans \mathbb{Z} :

$$(*) \begin{cases} x = 0 [4] \\ x = 1 [25] \end{cases}$$

On résout $4k = 1 [25]$, $k \in \mathbb{Z}$.

Si on multiplie par 6 :

$$24k = 6 [25]$$

$$\Leftrightarrow -k = 6 [25] \Leftrightarrow k = -6 [25]$$

$$\text{Donc } x = 4(-6 + 25n) \quad n \in \mathbb{Z}$$

$$\Leftrightarrow x = -24 + 100m, \quad m \in \mathbb{Z}$$

$$\Leftrightarrow x = -24 [100] = 76 [100]$$

et en déduire les deux derniers chiffres de

$$N = \underbrace{2^{2022}}_2 \dots 2$$

La nombre N est un multiple de 4.

$$\text{Donc } N = 0 [4].$$

Calculons quelques puissances de 2 modulo 25 : $2^4 = 16, 2^8 = 16^2 = 256 = 6 [25] \Rightarrow 2^{16} = 36 [25] = 11 [25] \Rightarrow 2^{32} = 11^2 = 121 = 1 [25]$

$$\text{Donc } 2^m = 2^{m'} \text{ si } m = m' [20]$$

$$\text{On voit que } 2^4 = 16 \equiv -9 [25] \Rightarrow e = -4 [20]$$

$$e = 2^4 = 16 \equiv 16 [25]$$

$$\text{Donc } N = 2^e = 2^{16} [100] = (2^8)^2 [100] = 36^2 [100] = 1296 [100] = 96 [100].$$

Donc les deux derniers chiffres de N sont 96.

Exercice 3 a) Donner la liste des nombres premiers $\leq \sqrt{641}$.

Comme $25^2 < 641 < 26^2$, il s'agit de donner la liste des nombres premiers ≤ 25 . La voici : 2, 3, 5, 7, 11, 13, 17, 19, 23.

b) Pour chaque nombre premier p dans la liste ci-dessus, trouver au moins un entier n_p tel que

~~$$pn_p \equiv 1 [p]$$~~

c) Justifier que le nombre 641 est premier.

Si 641 n'est pas premier, alors 641 a au moins deux nombres premiers dans sa factorisation $p_1 \leq p_2$

$$\Rightarrow 641 \geq p_1 p_2 \geq p_1^2$$

donc il existerait un nombre premier $p_1 \leq \sqrt{641}$ qui diviserait 641. C'est impossible car pour les nombres premiers de la liste a), on a :

$$641 = 4 [7], 641 = 3 [11], 641 = 4 [13], 641 = 12 [17],$$

$$641 = 4 [19], 641 = 20 [23]$$

Donc 641 est un nombre premier !

- d) Soient x, y des entiers. Soit p un nombre premier. On suppose que dans $\mathbb{Z}/p\mathbb{Z}$ on a les égalités :

$$x^4 + y^4 = 0 [p] \text{ et } x^7 y + 1 = 0 [p] .$$

Montrer que $x^{32} = -1 [p]$.

on peut calculer modulo p :

*$x^4 = -y^4 [p]$. Or $x^7 y = -1 [p]$
 $\Rightarrow x^7 = -\frac{1}{y} [p] \Rightarrow x^{28} = -\frac{1}{y^4} [p] \Rightarrow x^{28} = \frac{-1}{x^4} [p]$*

- e) Montrer que $2^4 + 5^4 = 0 [641]$. Montrer à l'aide des questions précédentes que $641 \mid 2^{2^5} + 1$.

On a: $2^4 + 5^4 = 16 + 625 = 641 = 0 [641]$

Posons $p = 641$ (c'est un nombre premier), $x = 2, y = 5$.

- f) Le nombre $2^{2^5} + 1$ est-il premier ?

On a $x^4 + y^4 = 0 [p]$ et $x^7 y + 1 = 2^7 \cdot 5 + 1 = 128 \cdot 5 + 1 = 641 = 0 [p]$

d'après la question précédente, on a alors:

Exercice 4 Soit $P(X) = 8X^3 + 4X^2 - 4X - 1$.

*$x^{32} = -1 [p] \Leftrightarrow 2^{2^5} = -1 [641]$
 $\Rightarrow 641 \mid 2^{2^5} + 1$. Or $2^{2^5} + 1 > 2^{10} + 1 = 1025$*

- a) Calculer $P(1)$ et $P(-1)$. En déduire que P n'a pas de racines dans \mathbb{Z} .
 c) $P(1) = 7, P(-1) = -1$. *Si $x \in \mathbb{Z}$ est racine de P , alors $P(x) = 0 \Leftrightarrow 8x^3 + 4x^2 - 4x - 1 = 0 \Rightarrow x \mid 1 \Rightarrow x = \pm 1$ donc $2^{2^5} + 1$ n'est pas premier.*
 b) Soit $r = \frac{a}{b} \in \mathbb{Q}$ où $a, b \in \mathbb{Z}$, a, b premiers entre eux. Montrer que si $P(r) = 0$, alors $b \mid 8$. En déduire que $2 \mid b$.
b) $P(\frac{a}{b}) = 0 \Rightarrow 8a^3 + 4a^2b - 4ab^2 - b^3 = 0 \Rightarrow b \mid 8a^3 \Rightarrow b \mid 8$ d'après le lemme de Gauss. Or $8 = 2^3$ donc $b = \pm 1, \pm 2, \pm 4$ ou ± 8 . Si $b = \pm 1$, alors $r = \pm a \in \mathbb{Z}$: impossible d'après a). Donc $2 \mid b$.

On suppose que $b = 2b'$ avec b' entier. Justifier que a, b' sont premiers entre eux et montrer que $b' = \pm 1$.

Comme $b = 2b'$, $\text{pgcd}(a, b') \mid \text{pgcd}(a, b) \Rightarrow \text{pgcd}(a, b') = 1$.

- c) Montrer que P n'a pas de racine dans \mathbb{Q} .

*On a donc $P(r) = 0 \Rightarrow 8a^3 + 4a^2b' - 4ab'^2 - b'^3 = 0$ donc $b' = \pm 2$.
 $\Rightarrow 8a^3 + 8a^2b' - 16ab'^2 - 8b'^3 = 0$ donc $r = \pm \frac{a}{2}$
 $\Rightarrow a^3 + a^2b' - 2ab'^2 - b'^3 = 0$
 $\Rightarrow b' \mid a \Rightarrow b' = \pm 1$ car $\text{pgcd}(a, b') = 1$.*

- c) Si $r \in \mathbb{Q}$ est une racine de P dans \mathbb{Q} , alors $r = \frac{a}{2}$ pour un $a \in \mathbb{Z}$ impair (quitte à changer a en $-a$).
 Mais alors $P(r) = 0 \Leftrightarrow a^3 + a^2 - 2a - 1 = 0 \Rightarrow a \mid 1 \Rightarrow a = \pm 1$.
 Or $1^3 + 1^2 - 2 \cdot 1 - 1 = -1 \neq 0 \neq 1 = (-1)^3 + (-1)^2 - 2 \cdot (-1) - 1$.

Donc pas de racine dans \mathbb{Q} pour P .