

QCM

Nom et prénom :

.....

.....

Durée/Duration : 15 minutes.

Aucun document n'est autorisé.

No document allowed.

L'usage de la calculatrice est interdit.

Using a calculator is forbidden.

Les questions faisant apparaître le symbole ♣ peuvent présenter une ou plusieurs bonnes réponses.

Questions with ♣ symbole may have one or several correct answers.

Les autres ont une unique bonne réponse.

The other ones have a unique correct answer.

- Si aucune réponse n'est cochée pour une question, alors aucun point n'y est attribué ni retranché.
If no answer is marked, then no point is earned nor removed.
- Sinon, si seules toutes les bonnes réponses sont cochées, alors un point y est attribué.
Otherwise, if only all the correct answers are marked, then one point is earned.
- Sinon un point y est retranché.
Otherwise a point is removed.

Question [Zcorps] \mathbb{Z} est un corps.

\mathbb{Z} is a field.

☐ Vrai/True.

☒ Faux/False.

Question [K(x)corps] Pour \mathbb{K} un corps, $\mathbb{K}(x)$ est un corps.

For \mathbb{K} a field, $\mathbb{K}(x)$ is a field.

☒ Vrai/True.

☐ Faux/False.

Question [Qcorps] \mathbb{Q} est un corps.

\mathbb{Q} is a field.

☒ Vrai/True.

☐ Faux/False.

Question [Z/9Zcorps] $\mathbb{Z}/9\mathbb{Z}$ est un corps.

$\mathbb{Z}/9\mathbb{Z}$ is a field.

☐ Vrai/True.

☒ Faux/False.

Question [Z/29Zcorps] $\mathbb{Z}/29\mathbb{Z}$ est un corps.

$\mathbb{Z}/29\mathbb{Z}$ is a field.

☒ Vrai/True.

☐ Faux/False.

Question [Z/31Zcorps] $\mathbb{Z}/31\mathbb{Z}$ est un corps.

$\mathbb{Z}/31\mathbb{Z}$ is a field.

☒ Vrai/True.

☐ Faux/False.

Question [Z/41Zcorps] $\mathbb{Z}/41\mathbb{Z}$ est un corps.

$\mathbb{Z}/41\mathbb{Z}$ is a field.

☒ Vrai/True.

☐ Faux/False.

Question [Z/51Zcorps] $\mathbb{Z}/51\mathbb{Z}$ est un corps.

$\mathbb{Z}/51\mathbb{Z}$ is a field.

☐ Vrai/True.

☒ Faux/False.

CATALOGUE

Question [corps25] Il existe deux corps non isomorphes à 25 éléments.
There exists two non isomorphic fields with 25 elements.

☐ Vrai/True. ☒ Faux/False.

Question [corps27] Il existe un corps à 27 éléments.
There exists a field with 27 elements.

☒ Vrai/True. ☐ Faux/False.

Question [corps36] Il existe un corps à 36 éléments.
There exists a field with 36 elements.

☐ Vrai/True. ☒ Faux/False.

Question [corps40] Il existe un corps à 40 éléments.
There exists a field with 40 elements.

☐ Vrai/True. ☒ Faux/False.

Question [corps45] Il existe un corps à 45 éléments.
There exists a field with 45 elements.

☐ Vrai/True. ☒ Faux/False.

Question [corps49] Il existe un corps à 49 éléments.
There exists a field with 49 elements.

☒ Vrai/True. ☐ Faux/False.

Question [corps81] Il existe un corps à 81 éléments.
There exists a field with 81 elements.

☒ Vrai/True. ☐ Faux/False.

Question [corps100] Il existe un corps à 100 éléments.
There exists a field with 100 elements.

☐ Vrai/True. ☒ Faux/False.

Question [corps4<32] Le corps à 4 éléments est inclus dans celui à 32 éléments.
The field with 4 elements is included in the one with 32 elements.

☐ Vrai/True. ☒ Faux/False.

Question [corps4<64] Le corps à 4 éléments est inclus dans celui à 64 éléments.
The field with 4 elements is included in the one with 64 elements.

☒ Vrai/True. ☐ Faux/False.

Question [corps25>5] Un corps à 25 éléments contient un sous-corps à 5 éléments.
A field with 25 elements contains a subfield with 5 elements.

☒ Vrai/True. ☐ Faux/False.

Question [corps25<125] Un corps à 25 éléments est toujours inclus dans un corps à 125 éléments.
A field with 25 elements is always included in a field with 125 elements.

☐ Vrai/True. ☒ Faux/False.

Question [corps25<625] Un corps à 25 éléments est toujours inclus dans un corps à 625 éléments.
A field with 25 elements is always included in a field with 625 elements.

☒ Vrai/True. ☐ Faux/False.

Question [corps121>11] Le corps à 121 éléments contient celui à 11 éléments.
The field with 121 elements contains the one with 11 elements.

☒ Vrai/True. ☐ Faux/False.

Question [corps121<1331] Le corps à 121 éléments est inclus dans celui à 1331 éléments.
The field with 121 elements contains the one with 1331 elements.

☐ Vrai/True. ☒ Faux/False.

Question [fakeF9] $\mathbb{F}_3[x]/\langle x^2 + x + 1 \rangle$ est un corps.
 $\mathbb{F}_3[x]/\langle x^2 + x + 1 \rangle$ is a field.

☐ Vrai/True. ☒ Faux/False.

Question [fakeF8] $\mathbb{F}_2[x]/\langle x^3 + x^2 + x + 1 \rangle$ est un corps.
 $\mathbb{F}_2[x]/\langle x^3 + x^2 + x + 1 \rangle$ is a field.

☐ Vrai/True. ☒ Faux/False.

Question [F25] $\mathbb{F}_5[x]/\langle x^2 + x + 1 \rangle$ est un corps.
 $\mathbb{F}_5[x]/\langle x^2 + x + 1 \rangle$ is a field.

☒ Vrai/True. ☐ Faux/False.

Question [F49] $\mathbb{F}_7[x]/\langle x^2 + 1 \rangle$ est un corps.
 $\mathbb{F}_7[x]/\langle x^2 + 1 \rangle$ is a field.

☒ Vrai/True. ☐ Faux/False.

Question [fakeF16] $\mathbb{F}_2[x]/\langle x^4 + x^2 + 1 \rangle$ est un corps.
 $\mathbb{F}_2[x]/\langle x^4 + x^2 + 1 \rangle$ is a field.

☐ Vrai/True. ☒ Faux/False.

Question [F16] $\mathbb{F}_2[x]/\langle x^4 + x + 1 \rangle$ est un corps.
 $\mathbb{F}_2[x]/\langle x^4 + x + 1 \rangle$ is a field.

☒ Vrai/True. ☐ Faux/False.

Question [F49] $\mathbb{F}_7[x]/\langle x^2 + 2 \rangle$ est un corps.
 $\mathbb{F}_7[x]/\langle x^2 + 2 \rangle$ is a field.

☒ Vrai/True. ☐ Faux/False.

Question [fakeF49] $\mathbb{F}_7[x]/\langle x^2 + 3 \rangle$ est un corps.
 $\mathbb{F}_7[x]/\langle x^2 + 1 \rangle$ is a field.

☐ Vrai/True. ☒ Faux/False.

Question [inv331] ♣ L'inverse de 3, s'il existe, dans \mathbb{F}_{31} est
The inverse of 3, if it exists, in \mathbb{F}_{31} is

☒ 21. ☐ 10.
☒ -10. ☐ -21.

CATALOGUE

Question [inv5mod31] ♣ L'inverse de 5, s'il existe, dans \mathbb{F}_{31} est
The inverse of 5, if it exists, in \mathbb{F}_{31} is

☒ 25.
☒ -6.

☐ 6.
☐ -25.

Question [inv3mod37] ♣ L'inverse de 3, s'il existe, dans \mathbb{F}_{37} est
The inverse of 3, if it exists, in \mathbb{F}_{37} is

☒ 25.
☒ -12.

☐ 12.
☐ -25.

Question [inv3mod61] ♣ L'inverse de 3, s'il existe, dans \mathbb{F}_{61} est
The inverse of 3, if it exists, in \mathbb{F}_{61} is

☒ 41.
☒ -20.

☐ 20.
☐ -41.

Question [inv6mod39] ♣ L'inverse de 6, s'il existe, dans $\mathbb{Z}/39\mathbb{Z}$ est
The inverse of 6, if it exists, in $\mathbb{Z}/39\mathbb{Z}$ is

☐ 33.
☐ 7.

☐ 0.
☒ Aucune de ces réponses n'est correcte.

Question [inv10mod48] ♣ L'inverse de 10, s'il existe, dans $\mathbb{Z}/48\mathbb{Z}$ est
The inverse of 10, if it exists, in $\mathbb{Z}/48\mathbb{Z}$ is

☐ 5.
☐ 38.

☐ 0.
☒ Aucune de ces réponses n'est correcte.

Question [inv8mod39] ♣ L'inverse de 8, s'il existe, dans $\mathbb{Z}/39\mathbb{Z}$ est
The inverse of 8, if it exists, in $\mathbb{Z}/39\mathbb{Z}$ is

☒ 5.
☐ 34.

☐ 0.
☐ Aucune de ces réponses n'est correcte.

Question [inv7mod48] ♣ L'inverse de 7, s'il existe, dans $\mathbb{Z}/48\mathbb{Z}$ est
The inverse of 7, if it exists, in $\mathbb{Z}/48\mathbb{Z}$ is

☒ 7.
☐ 41.

☐ 0.
☐ Aucune de ces réponses n'est correcte.

Question [inv10mod32] ♣ L'inverse de 10, s'il existe, dans $\mathbb{Z}/32\mathbb{Z}$ est
The inverse of 10, if it exists, in $\mathbb{Z}/32\mathbb{Z}$ is

☐ 22.
☐ 11.

☐ 0.
☒ Aucune de ces réponses n'est correcte.

Question [inv12mod32] ♣ L'inverse de 12, s'il existe, dans $\mathbb{Z}/32\mathbb{Z}$ est
The inverse of 12, if it exists, in $\mathbb{Z}/32\mathbb{Z}$ is

☐ 20.
☐ 3.

☐ 0.
☒ Aucune de ces réponses n'est correcte.

Question [inv11mod32] ♣ L'inverse de 11, s'il existe, dans $\mathbb{Z}/32\mathbb{Z}$ est
The inverse of 11, if it exists, in $\mathbb{Z}/32\mathbb{Z}$ is

☒ 3.
☐ 21.

☐ 0.
☐ Aucune de ces réponses n'est correcte.

Question [inv3mod32] ♣ L'inverse de 3, s'il existe, dans $\mathbb{Z}/32\mathbb{Z}$ est
The inverse of 3, if it exists, in $\mathbb{Z}/32\mathbb{Z}$ is

☒ 11.
☐ 29.

☐ 0.
☐ Aucune de ces réponses n'est correcte.

Question [invxmod5etx3+2x+4] ♣ L'inverse de x , s'il existe, dans $\mathbb{F}_5[x]/\langle x^3 + 2x + 4 \rangle$ est
The inverse of x , if it exists, in $\mathbb{F}_5[x]/\langle x^3 + 2x + 4 \rangle$ is

☒ $x^2 + 2$.
☐ $4x^2 + 3$.

☐ $-x$.
☐ Aucune de ces réponses n'est correcte.

Question [invxmod3etx3+2x+2] ♣ L'inverse de x , s'il existe, dans $\mathbb{F}_3[x]/\langle x^3 + 2x + 2 \rangle$ est
The inverse of x , if it exists, in $\mathbb{F}_3[x]/\langle x^3 + 2x + 2 \rangle$ is

☒ $x^2 + 2$.
☐ $2x^2 + 1$.

☐ $-x$.
☐ Aucune de ces réponses n'est correcte.

Question [invxmod5etx4+2x2+4] ♣ L'inverse de x , s'il existe, dans $\mathbb{F}_5[x]/\langle x^4 + 2x^2 + 4 \rangle$ est
The inverse of x , if it exists, in $\mathbb{F}_5[x]/\langle x^4 + 2x^2 + 4 \rangle$ is

☒ $x^3 + 2x$.
☐ $2x^3 + 4x$.

☐ $-x$.
☐ Aucune de ces réponses n'est correcte.

Question [invxmod2etx3+x+1] ♣ L'inverse de x , s'il existe, dans $\mathbb{F}_2[x]/\langle x^3 + x + 1 \rangle$ est
The inverse of x , if it exists, in $\mathbb{F}_2[x]/\langle x^3 + x + 1 \rangle$ is

☒ $x^2 + 1$.
☐ x^3 .

☐ $-x$.
☐ Aucune de ces réponses n'est correcte.

Question [K[[x]] corps] Si \mathbb{K} est un corps, alors $\mathbb{K}[[x]]$ est un corps.
If \mathbb{K} is a field, then $\mathbb{K}[[x]]$ is a field.

☐ Vrai/True.

☒ Faux/False.

Question [valz-adique] La valuation x -adique de $x^7 + 2x^5 \in \mathbb{F}_3[x]$ est
The x -adic valuation of $x^7 + 2x^5 \in \mathbb{F}_3[x]$ is

☒ 5.

☐ 7.

Question [normez-adique] Soient $A, B \in \mathbb{K}[z]$, la distance de A à B pour la norme z -adique $|\cdot|_z$ est au plus 1.

Let $A, B \in \mathbb{K}[z]$, the distance of A to B for the z -adic norm $|\cdot|_z$ is at most 1.

☒ Vrai/True.

☐ Faux/False.

Question [invK[[z]]] Le polynôme $2 + 3z$ est inversible dans $\mathbb{F}_5[[z]]$.
The polynomial $2 + 3z$ is invertible in $\mathbb{F}_5[[z]]$.

☒ Vrai/True.

☐ Faux/False.

Question [pasinvK[[z]]] Le polynôme $3z + 2z^2$ est inversible dans $\mathbb{F}_5[[z]]$.
The polynomial $3z + 2z^2$ is invertible in $\mathbb{F}_5[[z]]$.

☐ Vrai/True.

☒ Faux/False.

Question [Newtonop] L'opérateur de Newton pour F et une solution approchée y_k de $F(y) = 0$ est
The Newton operator for F and approximated solution y_k of $F(y) = 0$ is

☒ $y_{k+1} = y_k - \frac{F(y_k)}{F'(y_k)}$.

☐ $y_{k+1} = y_k - \frac{F'(y_k)}{F(y_k)}$.

Question [ratreconpossible] La reconstruction rationnelle $B = \frac{R}{V} \bmod z^n$ avec $\deg R < \deg B$ est toujours possible.

The rational reconstruction $B = \frac{R}{V} \bmod z^n$ with $\deg R < \deg B$ is always possible.

☐ Vrai/True.

☒ Faux/False.

Question [ratreconpossible2] La reconstruction rationnelle $B = \frac{R}{V} \bmod z^n$ avec $\deg R = \deg B$ est toujours possible.

The rational reconstruction $B = \frac{R}{V} \bmod z^n$ with $\deg R = \deg B$ is always possible.

☒ Vrai/True.

☐ Faux/False.

Question [ratreconalgo] ♣ La reconstruction rationnelle $B = \frac{R}{V} \bmod z^n$ peut être résolue via l'algorithme

The rational reconstruction $B = \frac{R}{V} \bmod z^n$ can be solved using the

☒ d'Euclide étendu/extended Euclidean algorithm.

☐ de division euclidien/Euclidean division al-

gorithm.

☐ de Bézout/Bézout algorithm.

☐ Aucune de ces réponses n'est correcte.