S2PA B4 Correction ARITH

Exercice 1 : décomposition des entiers

1. *Trouver la décomposition en produits de facteurs premiers de $a = 792$.*

   $a = 2 \times 396 = 2 \times 2 \times 198 = 2 \times 2 \times 2 \times 99 = 2^3 \times 9 \times 11 = 2^3 \times 3^2 \times 11.$

2. *Soit $d \in \mathbb{N}^*$ tel que d divise a. Quelle est la forme générale de la décomposition en facteurs premiers de d ? (Vous pouvez vous aider au brouillon en faisant un arbre par exemple).*

   Tout diviseur positif de a est de la forme $d = 2^i \times 3^j \times 11^k$ avec $i \in [\![0, 3]\!]$, $j \in [\![0, 2]\!]$ et $k \in [\![0, 1]\!]$.

3. *En utilisant la question précédente, donner le nombre de diviseurs positifs de a. (Vous pouvez vous aider au brouillon en faisant un arbre par exemple).*

   Pour les puissances de 2, il y a 4 possibilités, pour les puissances de 3, on en a 3 et pour 11, on en a 2. Au total, il y a donc $4 \times 3 \times 2 = 24$ diviseurs positifs de a possibles.

4. *Décomposer* 36 *en produits de facteurs premiers.*

   $36 = 2^2 \times 3^2$.

5. Trouver un $b \in \mathbb{N}$, $b > 100$ tel que $a \wedge b = 36$. Justifiez votre choix.

   b doit avoir comme diviseurs au moins 2^2 et 3^2 mais pas 11. On peut prendre par exemple, $b = 2^5 \times 3^4 = 576$.

Exercice 2 : congruence

Les questions sont indépendantes.

1. Remplir le tableau suivant, sachant que dans chaque case, votre réponse doit être un entier entre 0 et 10.

a	-2	1	28	36	35
b	3	4	14	-4	49
$a[11]$	9	1	6	3	2
$b[11]$	3	4	3	7	5
$a^3 - 2b[11]$	8	4	1	2	9

2. *Énoncer rigoureusement les deux versions du petit théorème de Fermat.*

   Soit p un nombre premier. On a
   — $\forall n \in \mathbb{N}$, $n^p \equiv n\,[p]$
   — $\forall n \in \mathbb{N}$ tel que p ne divise pas n, $n^{p-1} \equiv 1\,[p]$

3. *Le nombre $N = 4 \times 6^{43} - 128$ est-il divisible par 7 ? Justifier.*

   • $128 = 7 \times 18 + 2$ donc, $128 \equiv 2\,[7]$.

   • 7 est premier et 7 ne divise pas 6, donc par le petit théorème de Fermat, $6^6 \equiv 1\,[7]$.
   Ainsi, $6^{43} = 6^{6\times 7+1} = (6^6)^7 \times 6 \equiv 1^6 \times 6\,[7] \equiv 6[7]$. Par conséquent, $4 \times 6^{43} \equiv 24\,[7] \equiv 3\,[7]$.

   En conclusion $N \equiv 3 - 2\,[7] \equiv 1\,[7]$. N n'est donc pas congru à 0 modulo 7. Donc, 7 ne divise pas N.

Exercice 3 : autour de Bézout et Gauss

Soit a et b deux entiers non nuls.

1. *Énoncer le théorème de Bézout, d'une part pour $a \wedge b = d$ quelconque et d'autre part pour $a \wedge b = 1$.*

   — $\forall (a,b) \in \mathbb{Z}^2$, $\exists (u,v) \in \mathbb{Z}^2$ tel que $au + bv = a \wedge b$.
   — $\forall (a,b) \in \mathbb{Z}^2$, $a \wedge b = 1 \iff \exists (u,v) \in \mathbb{Z}^2$ tel que $au + bv = 1$.

2. *Énoncer ET démontrer le théorème de Gauss.*

   Théorème : $\forall (a,b,c) \in \mathbb{Z}^3$, $a \mid bc$ et $a \wedge b = 1 \implies a \mid c$.

   Preuve : soit $(a,b,c) \in \mathbb{Z}^3$ tel que $a \mid bc$ et $a \wedge b = 1$. On a alors : $\exists k \in \mathbb{Z}$ tel que $bc = ak$ et, par le théorème de Bézout, $\exists (u,v) \in \mathbb{Z}^2$ tel que $au + bv = 1$. Ainsi

   $$c = c \times 1 = c \times (au + bv) = cau + cbv = cau + akv = a \times (cu + kv)$$

   Comme $cu + kv \in \mathbb{Z}$, on conclut $a \mid c$.

3. *En utilisant obligatoirement l'algorithme d'Euclide, trouver un couple $(u,v) \in \mathbb{Z}^2$ tel que $50u + 18v = 2$.*

   $$\begin{array}{lcl} 50 & = & 18 \times 2 + 14 \\ 18 & = & 14 \times 1 + 4 \\ 14 & = & 4 \times 3 + 2 \\ 4 & = & 2 \times 2 + 0 \end{array}$$

   On en déduit donc que $50 \wedge 18 = 2$. De plus, en remontant l'algorithme :

   $$2 = 14 - 4 \times 3 = 14 - (18 - 14) \times 3 = 14 \times 4 - 18 \times 3 = (50 - 18 \times 2) \times 4 - 18 \times 3 = 50 \times 4 + 18 \times (-11)$$

   Ainsi, le couple $(u,v) = (4, -11)$ convient.

4. *Soit (E) $25x + 9y = 6$ d'inconnues $(x,y) \in \mathbb{Z}^2$. En utilisant le théorème de Gauss, trouver toutes les solutions de (E).*

   Soit $(x,y) \in \mathbb{Z}^2$ tel que $50x + 18y = 2$.

   Comme on a aussi $2 = 50u + 18v$, on a $50x + 18y = 50u + 18v$. On divise par $2 = 50 \wedge 18$. On a $25x + 9y = 25u + 9v$.

   Cela donne $25(x - u) = 9(v - y)$ $(\star)$. Ainsi, $9 \mid 25(x - u)$. Or $25 \wedge 9 = 1$, d'où par le théorème de Gauss, $9 \mid x - u$. Cela nous donne : $\exists k \in \mathbb{Z}$ tel que $x - u = 9k$, d'où $x = u + 9k = 4 + 9k$.

   En reportant dans $(\star)$, $25 \times 9k = 9 \times (v - y)$, d'où $v - y = 25k$, ce qui donne $y = v - 25k = -11 - 25k$.

   Réciproquement, supposons que $x = 4 + 9k$ et $y = -11 - 25k$ avec $k \in \mathbb{Z}$. On a

   $$50x + 18y = 50 \times 4 + 50 \times 9k + 18 \times (-11) - 18 \times 25k = 2 + 2 \times 25 \times 9k - 2 \times 9 \times 25k = 2 + 0 = 2$$

   En conclusion, $S = \{(4 + 9k, -11 + 25k);\ k \in \mathbb{Z}\}$.

Exercice 4 : polynômes

Les questions sont indépendantes.

1. *Soient un entier $n \geq 2$ et le polynôme $A_n(X) = 5X^{2n+1} - X^3 - 4X$. Montrer que $X^2 + X \mid A_n$.*

   $A_n(0) = 0$, d'où $X \mid A_n$. De plus, $A_n(-1) = 5 \times (-1)^{2n+1} - (-1)^3 - 4 \times (-1) = -5 + 1 + 4 = 0$. Ainsi, $X + 1 \mid A_n$. On a donc $X(X+1) \mid A_n$ ce qui donne $X^2 + X \mid A_n$.

2. *Soit $B(X) = X^4 + X^3 + aX^2 + bX + 1$ avec $(a,b) \in \mathbb{R}^2$. Trouver a et b pour que -1 soit une racine d'ordre de multiplicité au moins 2 de B.*

   -1 racine d'ordre au moins 2 de $B \Longleftarrow B(-1) = 0$ et $B'(-1) = 0$. Or

   $$\left\{ \begin{array}{lcl} B(-1) & = & 0 \\ B'(-1) & = & 0 \end{array} \right. \iff \left\{ \begin{array}{lcl} a - b + 1 & = & 0 \\ -1 - 2a + b & = & 0 \end{array} \right. \iff \left\{ \begin{array}{lcl} a & = & 0 \\ b & = & 1 \end{array} \right.$$

   Ainsi, -1 d'ordre au 2 de B si et seulement si $B = X^4 + X^3 + X + 1$.

3. *Soit* $P(X) = X^4 + 4X^3 + 5X^2 + 4X + 4$.

   (a) *Montrer que* -2 *est une racine d'ordre de multiplicité exactement* 2 *de* P.

   - $P(-2) = 16 - 32 + 20 - 8 + 4 = 0$.
   - $P'(X) = 4X^3 + 12X^2 + 10X + 4$. Ainsi, $P'(-2) = -32 + 48 - 20 + 4 = 0$.
   - $P''(X) = 12X^2 + 24X + 10$. Ainsi, $P''(-2) = 48 - 48 + 10 = 10 \neq 0$.

   On en déduit que -2 est une racine d'ordre exactement 2 de P.

   (b) *Interpréter le résultat précédent en terme de divisibilité.*

   -2 est une racine d'ordre exactement 2 de P signifie $(X+2)^2 \mid P$ et $(X+2)^3$ ne divise pas P.

   (c) *En ne vous aidant que d'une seule division euclidienne écrire* P *comme produits de polynômes irréductibles dans* $\mathbb{R}[X]$ *et dans* $\mathbb{C}[X]$. *Justifiez.*

   On fait donc la division euclidienne de P par $(X+2)^2 = X^2 + 4X + 4$. On trouve $P(X) = (X+2)^2 \times (X^2 + 1)$. Ainsi, dans $\mathbb{R}[X]$, comme le discriminant de $X^2 + 1$ est strictement négatif, la décomposition de P en polynômes irréductibles de $\mathbb{R}[X]$ est $P(X) = (X+2)^2 \times (X^2 + 1)$.

   Dans $\mathbb{C}[X]$, les racines de $X^2 + 1$ sont i et $-i$. D'où, $P(X) = (X+2)^2(X-i)(X+i)$.