S1 B2 Correction examen ARITH

Exercice 1 : autour des nombres premiers

Soient $a = 4500$ *et* $b \in \mathbb{N}$.

1. *Décomposer* a *en produit de facteurs premiers.*

   $a = 2^2 \times 3^2 \times 5^3$.

2. *On suppose que :* $\forall\, d \in \mathbb{N}^*,\ d \mid b \iff d = 2^i \times 3^j \times 5^k \times 7^l$ *avec* $i \in [\![0,3]\!]$, $j \in [\![0,1]\!]$, $k \in [\![0,2]\!]$ et $l \in [\![0,2]\!]$.

   (a) *Combien* b *a-t-il de diviseurs positifs ? Justifier brièvement.*

   Il y a 4 possibilités pour les puissances de 2 (2^0, 2^1, 2^2 et 2^3), 2 possibilités pour les puissances de 3, 3 pour les puissances de 5 et 3 pour les puissances de 7.

   Ainsi, b admet $4 \times 2 \times 3 \times 3 = 72$ diviseurs positifs.

   (b) *Donner la décomposition en facteurs premiers de* b*. Justifier.*

   Le plus grand diviseur de b est b. On prend donc pour chaque facteur premier la puissance la plus grande.

   Ainsi, $b = 2^3 \times 3^1 \times 5^2 \times 7^2$ $(= 29400)$.

   (c) *Calculer* $a \wedge b$*. Vous expliquerez comment vous l'obtenez.*

   On prend la plus petite puissance des facteurs premiers en commun à a et b.

   Ainsi, $a \wedge b = 2^2 \times 3^1 \times 5^2 \times 7^0 = 300$.

   (d) *Donner la décomposition en facteurs premiers d'un entier naturel* $c \geq 200$ *tel que* $a \wedge c = 90$*. Expliquez votre raisonnement.*

   On a $90 = 2 \times 3^2 \times 5$. On peut prendre $c = 2 \times 3^2 \times 5 \times 11 = 990$ par exemple.

Exercice 2 : équation diophantienne

On considère l'équation $(E) : 102x + 27y = 6$ *d'inconnues* $(x, y) \in \mathbb{Z}^2$.

1. *Via l'algorithme d'Euclide, trouver* $102 \wedge 27$*. En déduire que* (E) *admet des solutions.*

   $$\begin{aligned} 102 &= 27 \times 3 + 21 \quad (3) \\ 27 &= 21 \times 1 + 6 \quad (2) \\ 21 &= 6 \times 3 + 3 \quad (1) \\ 6 &= 3 \times 2 + 0 \end{aligned}$$

   Ainsi, $102 \wedge 27 = 3$. Comme 6 est un multiple de 3, (E) admet bien des solutions.

2. *Via la question précédente, trouver une solution particulière* (x_0, y_0) *de* (E).

   On a, en remontant l'algorithme :

   $$3 \underset{(1)}{=} 21 - 6 \times 3 \underset{(2)}{=} 21 - (27 - 21) \times 3 = 21 \times 4 + 27 \times (-3) \underset{(3)}{=} (102 - 27 \times 3) \times 4 + 27 \times (-3) = 102 \times 4 + 27 \times (-15).$$

   Ainsi, $6 = 3 \times 2 = 102 \times 8 + 27 \times (-30)$. Le couple $(x_0, y_0) = (8, -30)$ est une solution particulière de (E).

3. *Trouver toutes les solutions de (E). Vous devez faire un raisonnement détaillé et ne pas parachuter la réponse.*

   • Soit $(x, y) \in \mathbb{Z}^2$ une solution de (E). On a : $102x + 27y = 6$. Ainsi, $102x + 27y = 102x_0 + 27y_0$.

   $\implies 102(x - x_0) = 27(y_0 - y)$.

   En divisant par $102 \wedge 27 = 3$, $102(x - x_0) = 27(y_0 - y) \implies 34(x - x_0) \underset{(\star)}{=} 9(y_0 - y) \implies 34 \,|\, 9(y_0 - y)$. Or $34 \wedge 9 = 1$.

   Ainsi, par Gauss : $34 \,|\, (y_0 - y) \implies \exists\, k \in \mathbb{Z},\ y_0 - y = 34k \implies \exists\, k \in \mathbb{Z},\ y = y_0 - 34k = -30 - 34k$.

   En réinjectant dans $(\star)$, $34(x - x_0) = 9 \times 34k$. D'où, $x - x_0 = 9k \implies x = x_0 + 9k = 8 + 9k$.

   • Réciproquement supposons que $x = 8 + 9k$ et $y = -30 + 34k$ avec $k \in \mathbb{Z}$. On a alors :

   $102x + 24y = 102(8+9k) + 27(-30-34k) = 102 \times 8 + 27 \times (-30) + 102 \times 9k - 27 \times 34k = 6 + 3 \times 34 \times 9k - 3 \times 9 \times 34k = 6$

   Ainsi, (x, y) est solution de (E).

   • En conclusion : $S = \{(8 + 9k, -30 - 34k);\ k \in \mathbb{Z}\}$.

Exercice 3 : autour du cours

1. *Soient $(a, b, n) \in \mathbb{Z}^3$. En utilisant les quantificateurs, montrer que si $n \,|\, a$ et $n \,|\, b$ alors $\forall\, (k, k') \in \mathbb{Z}^2$, $n \,|\, ka + k'b$*

   Supposons que $n \,|\, a$ et $n \,|\, b$. $\exists\, (q, q') \in \mathbb{Z}^2$, $a = nq$ et $b = nq'$.

   Soit $(k, k') \in \mathbb{Z}^2$. On a $ka + k'b = knq + k'nq' = n(kq + k'q')$. Or $kq + k'q' \in \mathbb{Z}$. Donc, $n \,|\, ka + k'b$.

2. *Théorème de Bézout*

   (a) *Soit $(a, b) \in \mathbb{Z}^2$ non nuls. Énoncer les deux versions du théorème de Bézout.*

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

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

   (b) ***Application** : soit $(a, b) \in \mathbb{N}^2$ tel que $a \wedge b = 1$. Soit $d \in \mathbb{N}^*$ un diviseur commun de $3a$ et de $3b$.*

   i. *Montrer que $d \,|\, 3$.*

   Soit $d \in \mathbb{N}^*$ tel que $d \,|\, 3a$ et $d \,|\, 3b$. On sait que $a \wedge b = 1$, d'où, par le théorème de Bézout, $\exists\, (u, v) \in \mathbb{Z}^2$ tel que $au + bv = 1$. Ainsi, en multipliant par 3 : $3au + 3bv = 3$.

   Or $d \,|\, 3a$ et $d \,|\, 3b \implies d \,|\, (3au + 3bv)$ par la question 1.(avec $k = u$ et $k' = v$). Donc, $d \,|\, 3$.

   ii. *En déduire que $3a \wedge 3b = 3$. Justifier.*

   $3a \wedge 3b$ est un diviseur commun de $3a$ et de $3b$. Par la question précédente, $3a \wedge 3b \,|\, 3$. Ainsi, $3a \wedge 3b = 1$ ou 3. Or 3 est un diviseur commun de $3a$ et $3b$ et $3a \wedge 3b$ est le plus grand diviseur commun de $3a$ et $3b$. On en déduit que $3a \wedge 3b \geq 3$. Donc, $3a \wedge 3b = 3$.

3. *Lemme de Gauss*

   (a) *Énoncer le lemme de Gauss.*

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

   (b) *Soient a, b et c trois entiers non nuls. On suppose que $a \,|\, c$, $b \,|\, c$ et $a \wedge b = 1$.*

   i. *En traduisant les deux divisibilités $a \,|\, c$ et $b \,|\, c$, montrer qu'il existe $(k, k') \in \mathbb{Z}^2$ tel que $ka = k'b$. En déduire que a divise k'.*

   • $a \,|\, c$ et $b \,|\, c \implies \exists\, (k, k') \in \mathbb{Z}^2$ tel que $c = ak$ et $c = bk'$. Ainsi, $ak = bk'$.

   • On en déduit que $a \,|\, bk'$. Or $a \wedge b = 1$, ainsi, par le lemme de Gauss, $a \,|\, k'$.

   ii. *En déduire que $ab \,|\, c$.*

   $a \,|\, k' \implies \exists\, k'' \in \mathbb{Z}$ tel que $k' = ak''$. Ainsi, $c = bk' = bak''$. Donc, $ab \,|\, c$.

Exercice 4 : congruence

Les deux questions sont indépendantes. La fin de la deuxième question est un bonus.

1. *Énoncer les deux versions du petit théorème de Fermat pour tout $n \in \mathbb{N}$.*

   • Soit p un nombre premier. $\forall\, n \in \mathbb{Z}$, $n^p \equiv n\,[p]$.

   • Soient p un nombre premier et $n \in \mathbb{Z}$ tel que p ne divise pas n. Alors, $n^{p-1} \equiv 1\,[p]$.

   (a) ***Application 1*** *: soit p un nombre premier. Montrer que, pour tout $n \in \mathbb{N}$, $3^{n+p} - 3^{n+1}$ est un multiple de p.*

   Soit $n \in \mathbb{N}$. p est premier, d'où par Fermat, $3^p \equiv 3\,[p]$.

   Ainsi, $3^{n+p} - 3^{n+1} = 3^n \times 3^p - 3^n \times 3 \equiv 3^n \times 3 - 3^n \times 3\,[p] \equiv 0\,[p]$. Donc, $3^{n+p} - 3^{n+1}$ est bien un multiple de p.

   (b) ***Application 2*** *: soit $n \in \mathbb{N}$. Trouver le reste de la division euclidienne de $N = 3^{12n} + 18^{37}$ par 7.*

   • 7 est premier et 7 ne divise pas 3, d'où par Fermat, $3^6 \equiv 1\,[7]$. Ainsi, $3^{12n} = \left(3^6\right)^{2n} \equiv 1^{2n}\,[7] \equiv 1\,[7]$.

   • $18 \equiv 4\,[7]$, d'où, $18^{37} \equiv 4^{37}\,[7]$. Or 7 est premier et 7 ne divise pas 4, d'où par Fermat, $4^6 \equiv 1\,[7]$. Ainsi, $4^{37} = 4^{6\times 6+1} = (4^6)^6 \times 4 \equiv 1^6 \times 4\,[7] \equiv 4\,[7]$.

   • Ainsi, $N \equiv 1 + 4\,[7] \equiv 5\,[7]$. Or $0 \leq 5 < 7$. Donc, 5 est le reste de la division euclidienne de N par 7.

2. (a) *Soit $n \in \mathbb{Z}$. Remplir le tableau suivant modulo 7 et en déduire les valeurs possibles du reste de la division euclidienne de n^2 par 7.*

$n\,[7]$	0	1	2	3	4	5	6
$n^2\,[7]$	0	1	4	2	2	4	1

   Les valeurs possibles du reste de la divsion euclidienne de n^2 par 7 sont : 0, 1, 2 ou 4.

   (b) *Soit $(x, y) \in \mathbb{Z}^2$. À l'aide d'un tableau à double entrée, donner les valeurs possibles du reste de la division euclidienne de $x^2 + y^2$ par 7 en fonction de ceux de x^2 et y^2.*
   Par la question précédente, on construit le tableau suivant qui donne les valeurs possibles du reste de $x^2 + y^2$ par 7 en fonction de ceux de x^2 et de y^2.

$x^2 + y^2$	$x^2 = 0$	$x^2 = 1$	$x^2 = 2$	$x^2 = 4$
$y^2 = 0$	0	1	2	4
$y^2 = 1$	1	2	3	5
$y^2 = 2$	2	3	4	6
$y^2 = 4$	4	5	6	1

   (c) **(Question bonus)** *En déduire que que si $(x, y) \in \mathbb{Z}^2$ est une solution de l'équation $x^2 + y^2 = 7^{2026}$ alors 7 divise x et 7 divise y.*

   Supposons que $(x, y) \in \mathbb{Z}^2$ est une solution de l'équation $x^2 + y^2 = 7^{2026}$. Ainsi, $x^2 + y^2 \equiv 0\,[7]$.

   Par le tableau précédent, cela donne $x^2 \equiv 0\,[7]$ et $y^2 \equiv 0\,[7]$. On réutilise alors le premier tableau fait, on obtient $x \equiv 0\,[7]$ et $y \equiv 0\,[7]$, c'est-à-dire 7 divise x et 7 divise y.