Correction S1B2 ARITH

Exercice 1 : nombres premiers et pgcd

On se donne trois entiers naturels : $a = 300$, $b = 2^2 \times 3^3 \times 5 \times 11$ et $c = 2 \times 5^2 \times 9 \times 11$.

1. *Donner la décomposition de a en produit de facteurs premiers.*

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

2. *Soit $d \in \mathbb{N}^*$ un diviseur de b. Quelle est la forme générale de la décomposition de d en facteurs premiers ? En déduire, le nombre de diviseurs positifs distincts de b.*

   En utilisant la décomposition de b, on sait que tout diviseur de b est de la forme $d = 2^i \times 3^j \times 5^k \times 11^r$ avec $i = 0, 1$ ou 2, $j = 0, 1, 2$ ou 3 ; $k = 0$ ou 1 et $r = 0$ ou 1.

   Ainsi, b a $3 \times 4 \times 2 \times 2$ diviseurs possibles (nombre de possibilités pour i, nombre de possibilités pour j etc). Donc b a 48 diviseurs positifs distincts.

3. *Trouver $b \wedge c$. Vous détaillerez votre calcul.*

   $c = 2 \times 3^2 \times 5^2 \times 11$. En prenant les plus petites puissances communes à b et c, on a $b \wedge c = 2 \times 3^2 \times 5 \times 11 = 990$.

Exercice 2 : congruence

Les questions 1. et 2. sont indépendantes.

1. *Soit n un entier naturel non nul* ***premier avec*** *4, c'est-à-dire $n \wedge 4 = 1$.*

   (a) *Quels sont les valeurs possibles du reste de la division euclidienne de n par 4 ? Justifier.*

   Par propriété du reste r de la division euclidienne de n par 4, on sait déjà que $r = 0, 1, 2$ ou 3.

   Si $r = 0$, n est un multiple de 4 donc n et 4 ne seraient pas premiers entre eux. Donc $r \neq 0$.

   Si $r = 2$, on a $n = 4q + 2$ où q est le quotient de la division. Ainsi, $n = 2(2q + 1)$ et $2|n$. 2 est donc un diviseur commun de n et 4. Cela contredit $n \wedge 4 = 1$. Donc, $r \neq 2$.

   Ainsi, $r = 1$ ou 3.

   (b) *En déduire que $n^2 - 1 \equiv 0[4]$.*

   • Si $r = 1$, on a $n \equiv 1[4]$. D'où, $n^2 - 1 \equiv 1^2 - 1[4] \equiv 0[4]$.

   • Si $r = 3$, $n \equiv 3[4]$ d'où $n^2 \equiv 9[4] \equiv 1[4]$. Ainsi, $n^2 - 1 \equiv 1 - 1[4] \equiv 0[4]$.

2. *Quel est le reste de la division euclidienne de $N = 17^9 - 8^{2023}$ par 7 ? Justifier.*

   • $8 \equiv 1[7]$ donc $8^{2023} \equiv 1^{2023}[7] \equiv 1[7]$.

   • $17 \equiv 3[7]$ ainsi, $17^9 \equiv 3^9[7]$. Or 7 est premier et $3 \wedge 7 = 1$, ainsi par le petit théorème de Fermat, $3^6 \equiv 1[7]$. D'où, $3^9 = 3^6 \times 3^3 \equiv 1 \times 27[7] \equiv 6[7]$.

   • En conclusion $N \equiv 6 - 1[7] \equiv 5[7]$. Comme $0 \leq 5 < 7$, 5 est le reste de la division euclidienne de N par 7.

Exercice 3 : autour de Bézout et Gauss (9 points)

1. **Théorème de Bézout.** Soit $(a, b) \in \mathbb{Z}^2$.

   Les questions (b) et (c) sont indépendantes.

   (a) *Énoncer rigoureusement les deux versions du théorème de Bézout (d'une part quand $a \wedge b$ est quelconque et, d'autre part quand $a \wedge b = 1$).*

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

(b) *L'affirmation « Si a et b sont premiers entre eux alors $\exists\,(u,v)\in\mathbb{Z}^2$ tel que $au+bv=2$ » est-elle vraie ou fausse ? Justifier.*

Supposons $a\wedge b=1$. Par la version 2 de Bézout, $\exists\,(u_0,v_0)\in\mathbb{Z}^2$ tel que $au_0+bv_0=1$. En multipliant la dernière égalité par 2, on a $a(2u_0)+b(2v_0)=2$. On a bien trouvé un couple $(u,v)=(2u_0,2v_0)\in\mathbb{Z}^2$ tel que $au+bv=2$. L'affirmation est donc vraie.

(c) *En utilisant obligatoirement l'algorithme d'Euclide, montrer que 39 et 47 sont premiers entre eux. Trouver alors $(u,v)\in\mathbb{Z}^2$ tel que $39u+47v=1$*

$$\begin{aligned} 47 &= 39\times 1+8\\ 39 &= 8\times 4+7\\ 8 &= 7\times 1+1\\ 7 &= 1\times 7+0 \end{aligned}$$

Ainsi, on a bien $47\wedge 39=1$. De plus

$$1=8-7=8-(39-8\times 4)=8\times 5-39=(47-39)\times 5-39=39\times(-6)+47\times 5$$

Le couple $(u,v)=(-6,5)$ convient.

2. **Lemme de Gauss.** *Soit $(a,b,c)\in\mathbb{Z}^3$*

(a) *Montrer que $a\,|\,bc$ et $a\wedge b=1\Longrightarrow a\,|\,c$ (lemme de Gauss)*

cf. pdf "Démonstrations à connaitre "

(b) *On considère l'équation (E) : $5(x-1)=7y$ d'inconnues $(x,y)\in\mathbb{Z}^2$. À l'aide de la question précédente, montrer que si (x,y) est solution de (E) alors $x=1+7k$ et $y=5k$ avec $k\in\mathbb{Z}$.*

Supposons que (x,y) est solution de (E). Ainsi, $5(x-1)=7y$. Comme $x-1\in\mathbb{Z}$, on en déduit : $5\,|\,7y$. Comme $5\wedge 7=1$, on a par le lemme de Gauss que $5|y$ ce qui revient à dire : $\exists\,k\in\mathbb{Z}$ tel que $y=5k$. En reportant dans l'équation, on a $5(x-1)=7\times 5k$, ce qui équivaut à $x-1=7k$. Donc $x=1+7k$.

3. *Soit $(a,b,c)\in\mathbb{Z}^3$. En utilisant soit le théorème de Bézout, soit le lemme de Gauss, montrer que si $a\,|\,c$, $b\,|\,c$ et $a\wedge b=1$ alors $ab\,|\,c$.*

Supposons que $a|c$, $b|c$ et $a\wedge b=1$.

On a alors : $\exists\,(k_1,k_2)\in\mathbb{Z}^2$ tel que $c=ak_1$ et $c=bk_2$. De plus, par le théorème de Bézout : $\exists\,(u,v)\in\mathbb{Z}^2$ tel que $au+bv=1$. Ainsi,

$$c(au+bv)=c \iff cau+cbv=c \iff bk_2au+ak_1bv=c \iff ab(uk_2+k_1v)=c$$

Comme $uk_2+k_1v\in\mathbb{Z}$, on en déduit que $ab|c$.

Remarque : via Gauss, cela donne : $a|c$ d'où $\exists\,k\in\mathbb{Z}$ tel que $c=ak$. Or $b|c$ d'où $b|ak$. Comme $a\wedge b=1$, on obtient par le lemme de Gauss : $b|k$ c'est-à-dire : $\exists\,k'\in\mathbb{Z}$ tel que $k=bk'$. Ainsi, $c=ak=abk'$. Donc $ab|c$.