

Note :

20

Appréciation du correcteur (uniquement s'il s'agit d'un examen) :

* Uniquement s'il s'agit d'un examen.

Q07.5 : $n \in \mathbb{N}, n \geq 2$

$$\begin{cases} m = p_1^{\alpha_1} \times \dots \times p_m^{\alpha_m} \\ n = q_1^{\beta_1} \times \dots \times q_r^{\beta_r} \end{cases}$$

1. $i \in \llbracket 1, m \rrbracket, j \in \llbracket 1, r \rrbracket$ (a) Supposons $p_i \neq q_j$. Soit d diviseur commun $\geq p_i^{\alpha_i}$ et $q_j^{\beta_j}$. $d \mid p_i^{\alpha_i}$ et p_i premier $\Rightarrow d \mid p_i \Rightarrow d=1$ ou $d=p_i$ $d \mid q_j^{\beta_j}$ et q_j premier $\Rightarrow d \mid q_j \Rightarrow d=1$ ou $d=q_j$ Or $p_i \neq q_j$, donc $d=1$ Leur seul diviseur commun est 1, donc $p_i^{\alpha_i}$ et $q_j^{\beta_j}$ sont premiers entre eux.

(par l'abs.)

(b) Soit $i \in \llbracket 1, m \rrbracket$. Si $\forall j \in \llbracket 1, r \rrbracket, p_i \neq q_j$, alors $\forall j \in \llbracket 1, r \rrbracket, p_i^{\alpha_i}$ est premier avec $q_j^{\beta_j}$ Donc $p_i^{\alpha_i}$ est premier avec $\prod_{j=1}^r q_j^{\beta_j}$, i.e. $p_i^{\alpha_i}$ est premier avec n , contradiction.Il existe $j \in \llbracket 1, r \rrbracket$ t. q. $p_i = q_j$.(c) Ainsi, à chaque $i \in \llbracket 1, m \rrbracket$ correspond au moins un $j \in \llbracket 1, r \rrbracket$,donc : cardinal $(\llbracket 1, r \rrbracket) \geq$ cardinal $(\llbracket 1, m \rrbracket)$

$$r \geq m.$$

Comme i, j, p_i, q_j jouent des rôles symétriques, on montre de la même manière que $m \geq r$.Il faut finalement, $m = r$.

$$\text{donc } \{p_1, p_2, \dots, p_m\} = \{q_1, q_2, \dots, q_r\}$$

$$\text{Par suite, } \min\{p_1, p_2, \dots, p_m\} = \min\{q_1, q_2, \dots, q_r\}$$

$$\text{Donc } p_1 = q_1$$

N°

.../...

Il vient $\{p_2, p_3, \dots, p_m\} = \{q_2, q_3, \dots, q_r\}$

Donc $\min\{p_2, p_3, \dots, p_m\} = \min\{q_2, q_3, \dots, q_r\}$

|| i.e. $p_2 = q_2$

De la même manière, on montre que $\forall k \in \llbracket 1, m \rrbracket$,

|| $p_k = q_k$

2°) On a $p_1^{d_1} \times p_2^{d_2} \times \dots \times p_m^{d_m} = q_1^{\beta_1} \times q_2^{\beta_2} \times \dots \times q_m^{\beta_m}$ (*)

Supposons $d_1 < \beta_1$. Alors $\exists d_1' \mid q_1$ tq $\beta_1 = d_1 + d_1'$

Donc (*) devient: $p_1^{d_1} \times p_2^{d_2} \times \dots \times p_m^{d_m} = q_1^{d_1 + d_1'} \times q_2^{\beta_2} \times \dots \times q_m^{\beta_m}$

En divisant membre à membre par $p_1^{d_1}$, il vient:

$$p_2^{d_2} \times \dots \times p_m^{d_m} = q_1^{d_1'} \times q_2^{\beta_2} \times \dots \times q_m^{\beta_m}$$

Or $q_1^{d_1'}$ est premier avec p_i , $\forall i \in \llbracket 1, m \rrbracket$.

Donc $q_1^{d_1'} = 1$, i.e. $d_1' = 0$, ce qui contredit $d_1 < \beta_1$.

On montrerait de même qu'en supposant $\beta_1 < d_1$, on aboutit à une contradiction.

|| Donc $d_1 = \beta_1$.

On montrerait de même que $\forall i \in \llbracket 1, m \rrbracket$, $d_i = \beta_i$.

Donc $r = m$, et $\forall i \in \llbracket 1, m \rrbracket$, $p_i = q_i$ et $d_i = \beta_i$, i.e.

|| les deux décompositions en facteurs premiers sont identiques, d'où l'unicité.

Ex 7.6

Soient $x, y \in \mathbb{N}^*$ tq $x < y$. $S = \{(x, y) \mid \text{pgcd}(x, y) = y - x\}$.

1°)

a)

$$\begin{array}{r|l} 363 & 3 \\ \hline 121 & 11 \\ \hline 11 & 11 \\ \hline 1 & 1 \end{array}$$

$$\begin{array}{r|l} 486 & 2 \\ \hline 242 & 2 \\ \hline 121 & 11 \\ \hline 11 & 11 \\ \hline 1 & 1 \end{array}$$

$$\text{pgcd}(363; 486) = 121$$

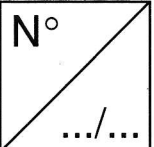
b) $486 - 363 = 121$, donc $(363; 486) \in S$.

2°)

Soit $m \in \mathbb{N}^*$. $(m, m+1) \in S$ si $\text{pgcd}(m, m+1) = m+1 - m = 1$,

i.e. si m et $m+1$ sont premiers entre eux.

Or si on note d un diviseur de m ,



$d \mid m+1$ si $d \mid 1$, donc d est un diviseur commun à m et $m+1$ si $d=1$.

Donc m et $m+1$ sont premiers entre eux, et le couple $(m, m+1)$ appartient bien à S .

3°) ~~Supposons $\exists k \in \mathbb{N}^* \text{ tq } \begin{cases} x = k(y-x) \\ y = (k+1)(y-x) \end{cases}$~~

Alors $(y-x) \mid x$

Nq. $(x, y) \in S$ si $\exists k \in \mathbb{N}^* \text{ tq } \begin{cases} x = k(y-x) \\ y = (k+1)(y-x) \end{cases}$

$\Leftrightarrow$ Sat. $(x, y) \in S$.

$$\text{pgcd}(x, y) = y - x$$

$$x = (y-x)k_1$$

$$y = (y-x)k_2$$

$$y-x = (y-x)(k_2 - k_1)$$

$$\text{Donc } k_2 - k_1 = 1, \quad k_2 = k_1 + 1.$$

$$\text{Notons } k = k_1, \quad \text{on a } x = k(y-x)$$

$$\text{et } y = (k+1)(y-x)$$

$\Leftrightarrow$ Supposons $\exists k \in \mathbb{N}^* \text{ tq } \begin{cases} x = k(y-x) \\ y = (k+1)(y-x) \end{cases}$

$$\text{pgcd}(x, y) \mid x \quad \text{et} \quad \text{pgcd}(x, y) \mid y$$

$$\text{Donc } \text{pgcd}(x, y) \mid k(y-x) \quad \text{et} \quad \text{pgcd}(x, y) \mid (k+1)(y-x)$$

Car $(y-x)$ est un diviseur commun à y et x ,

$$(y-x) \mid \text{pgcd}(x, y), \exists p \in \mathbb{N}^* \text{ tq } \text{pgcd}(x, y) = p(y-x).$$

$$p(y-x) \mid k(y-x) \quad \text{et} \quad p(y-x) \mid (k+1)(y-x)$$

$$\Rightarrow p \mid k \quad \text{et} \quad p \mid (k+1)$$

or k et $(k+1)$ premiers entre eux, donc $p=1$.

$$\text{Donc } \text{pgcd}(x, y) = (y-x).$$

$$\text{Donc } (x, y) \in S.$$

$d \mid m+1$ si $d \mid 1$, donc d est un diviseur commun à m et $m+1$ si $d=1$.

Donc m et $m+1$ sont premiers entre eux, et le couple $(m, m+1)$ appartient bien à S .

3°) ~~Supposons $\exists k \in \mathbb{N}^* \text{ tq } \begin{cases} x = k(y-x) \\ y = (k+1)(y-x) \end{cases}$~~

Alors $(y-x) \mid x$
 Nq $(x, y) \in S$ si $\exists k \in \mathbb{N}^* \text{ tq } \begin{cases} x = k(y-x) \\ y = (k+1)(y-x) \end{cases}$

($\Rightarrow$) Soit $(x, y) \in S$.

$$\begin{aligned} \text{pgcd}(x, y) &= y - x \\ x &= (y-x)k_1 \\ y &= (y-x)k_2 \end{aligned}$$

$$y - x = (y-x)(k_2 - k_1)$$

$$\text{Donc } k_2 - k_1 = 1, \quad k_2 = k_1 + 1.$$

$$\text{Notons } k = k_1, \text{ on a } \begin{cases} x = k(y-x) \\ y = (k+1)(y-x) \end{cases}$$

($\Leftarrow$) Supposons $\exists k \in \mathbb{N}^* \text{ tq } \begin{cases} x = k(y-x) \\ y = (k+1)(y-x) \end{cases}$

$$\text{pgcd}(x, y) \mid x \text{ et } \text{pgcd}(x, y) \mid y$$

Donc $\text{pgcd}(x, y) \mid k(y-x)$ et $\text{pgcd}(x, y) \mid (k+1)(y-x)$

Comme $(y-x)$ est un diviseur commun à y et x ,

$$(y-x) \mid \text{pgcd}(x, y), \exists p \in \mathbb{N}^* \text{ tq } \text{pgcd}(x, y) = p(y-x).$$

$$p(y-x) \mid k(y-x) \text{ et } p(y-x) \mid (k+1)(y-x)$$

$$\Rightarrow p \mid k \text{ et } p \mid (k+1)$$

or k et $(k+1)$ premiers entre eux, donc $p=1$.

$$\text{Donc } \text{pgcd}(x, y) = (y-x).$$

$$\text{Donc } (x, y) \in S.$$

N°

.../...

Ex 7.6

1. a) $\text{pgcd}(363; 486) = 121$
 b) $486 - 363 = 121$, donc $(363; 486) \in S$.

2. Deux entiers consécutifs sont premiers entre eux.
 En effet, si $m = p_1^{\alpha_1} \dots p_r^{\alpha_r}$

alors si $p_i | m$ et $p_i | m+1$,
 alors $p_i | 1$, chaque sauf si $p_i = 1$.

Donc $\text{pgcd}(m; m+1) = 1$.

De plus, $m+1 - m = 1$, donc les couples $(m; m+1)$ appartiennent à S .

3. $\text{Pg}(x; y) \in S \Leftrightarrow \exists k \in \mathbb{N}^* \text{ tq } \begin{cases} x = k(y-x) \\ \text{et} \\ y = (k+1)(y-x) \end{cases}$

$(\Rightarrow)$ Si $\text{pgcd}(x; y) = y - x$, alors $(y-x) | x : \exists k \in \mathbb{N}^* : x = k(y-x)$
 $(y-x) | y : \exists k' \in \mathbb{N}^* : y = k'(y-x)$

En soustrayant membre à membre il vient

$y - x = (k' - k)(y - x)$, d'où $k' - k = 1$, or $k' = k + 1$.

$(\Leftarrow) \text{pgcd}(x; y) = \text{pgcd}(k(y-x); (k+1)(y-x)) \stackrel{\text{pgcd}}{=} (y-x) \text{pgcd}(k; k+1)$
 $\stackrel{\text{entiers consécutifs}}{=} (y-x) \times 1 = y - x$

Donc $(x; y) \in S$.

Ex 7.7 ~~à~~ page suivante

Ex 7.8

1')
$$\begin{array}{r|l} 66 & 15 \\ -60 & 4 \\ \hline 6 & \end{array}$$

$$\begin{array}{r|l} 15 & 6 \\ -12 & 3 \\ \hline 3 & \end{array}$$

$$\begin{array}{r|l} 6 & 3 \\ 0 & 2 \\ \hline \end{array}$$

Donc $\text{pgcd}(66; 15) = 3$.

division reste non nul.

2') $15 = 6 \times 2 + 3$

$3 = 15 - 6 \times 2$

$3 = 15 \times \underline{1} + 6 \times \underline{(-2)} \quad , \quad a = 1 \text{ et } b = -2 \quad (E_1)$

$$3^c) \quad 66 = 15 \times 4 + 6$$

$$6 = 66 \times 1 - 15 \times 4$$

$$6 = 66 \times 1 + 15 \times (-4) \quad (E_2) \quad a' = 1, \quad b' = -4$$

$$4^c) \quad \text{Dans } (E_1): \quad 3 = 15 \times 1 + \underbrace{(66 \times 1 + 15 \times (-4))}_{6} \times (-2)$$

$$3 = 15 \times 1 - 2 \times 66 + 15 \times 8$$

$$3 = 15 \times (1+8) - 66 \times 2$$

$$\textcircled{3} = 15 \times 9 + 66 \times (-2)$$

} c'est l'identité de Bézout
(PTh 3.6)

Ex 7.7

$m \in \mathbb{N}, n \geq 2$

$\text{pgcd}(a, b)$

$\text{pgcd}(66, 15)$

1°) Soit $d \in \mathbb{N}$ tq $d|m$

Alors $d|2m$.

Si $d|2m+1$, comme $d|2m$, alors $d|1$, donc $d=1$.

Le seul diviseur commun à m et $2m+1$ est 1.

$\text{pgcd}(m, 2m+1) = 1$.

$$2) \quad \alpha = m+3; \quad \beta = 2m+1. \quad \delta = \text{pgcd}(\alpha, \beta)$$

$$(a) \quad 2\alpha - \beta = 2m+6 - 2m-1 = 5$$

$$\delta|\alpha \Rightarrow \delta|2\alpha; \quad \text{or } \delta|\beta, \text{ donc } \delta|2\alpha - \beta$$

$$\text{Ainsi } \delta|5, \text{ donc } \delta \in \{1, 5\}.$$

$$(b) \quad \text{Iq } (5|\alpha \text{ et } 5|\beta) \Leftrightarrow 5|(m-2)$$

$$(\Rightarrow) \quad 5|\alpha \text{ et } 5|\beta \Rightarrow 5|\beta - \alpha$$

$$\text{or } \beta - \alpha = 2m+1 - m-3 = m-2$$

$$\text{Donc } 5|(m-2)$$

$$(\Leftarrow) \quad \text{Supp. } 5|(m-2)$$

$$\text{Alors } \exists k \in \mathbb{N} \text{ tq } m-2 = 5k, \text{ or } m = 5k+2$$

$$\text{Il vient } \alpha = 5k+2+3 = 5(k+1), \text{ donc } 5|\alpha$$

$$\text{et } \beta = 2(5k+2)+1 = 5(2k+1), \text{ donc } 5|\beta.$$

3) $a = m^3 + 2m^2 - 3m$

$$\begin{array}{r|l} m^3 + 2m^2 - 3m & m-1 \\ - (m^3 - m^2) & \\ \hline 0 + 3m^2 - 3m & m^2 + 3m \\ - (3m^2 - 3m) & \\ \hline 0 & \end{array}$$

Donc $a = (m-1)(m^2 + 3m) = m(m-1)(m+3) = (m-1) \times m(m+3)$

$b = 2m^2 - m - 1$

$$\begin{array}{r|l} 2m^2 - m - 1 & m-1 \\ - (2m^2 - 2m) & \\ \hline 0 + m - 1 & 2m + 1 \\ \hline 0 & \end{array}$$

Donc $b = (m-1)(2m+1)$

6) (a) $d = \text{pgcd}(m(m+3), (2m+1))$

Or $\delta = \text{pgcd}(m+3, 2m+1)$

Si $(d/m+3)$ et $(d/2m+1)$,
alors $(d/m(m+3))$ et $(d/2m+1)$.

Alors l'ensemble D_1 des diviseurs communs à $\frac{(m+3)}{\alpha}$ et $\frac{(2m+1)}{\beta}$ est inclus dans l'ensemble D_2 des diviseurs communs

à $m(m+3)$ et $(2m+1)$.

Donc $\text{pgcd}(m+3, (2m+1)) \in D_2$

i.e. $\delta \in D_2$

Or tous les diviseurs communs divisent le pgcd,

donc δ/d , a fortiori $\delta \leq d$.

$\text{pgcd}(m+3, 2m+1)$ $\text{pgcd}(m(m+3), (2m+1))$

Or $m \nmid d/m$, $d \nmid m$ et donc $d \nmid (2m+1)$ (deux entiers consécutifs ont pour diviseurs communs 1).

Contradiction car $d = \text{pgcd}(m(m+3), 2m+1)$. Or $d=1$

Donc $d \nmid m$, par suite d est un diviseur commun à $(m+3)$ et $(2m+1)$,

donc $d \leq \delta$ - finalement, $d = \delta$.

le pgcd d'entre eux.

On a : $a = (m-1) \cdot m(m+3)$

et $b = (m-1) \cdot (2n+1)$

Donc les diviseurs communs à a et b sont

- les diviseurs communs à $m(m+3)$ et $(2n+1)$
- et les diviseurs de $m-1$.

Donc $\Delta = \text{pgcd}(a, b) = \cancel{\max((m-1), d)}$
 $= \cancel{\max((m-1), 5)}$

or $\delta \in \{1, 5\}$. $\Delta = (m-1)$

autres cas : Si $\delta = 1$, alors $\Delta = \max(m-1, 1) = m-1$ car $m \geq 2$.

$m = 5k+2$ (2b) Si $\delta = 5$, alors :
 Si $m < 6$, $\Delta = 5$ cas exclu car $m = 5k+2$ sauf $k=0, m=2$
 Si $m \geq 6$, $\Delta = m-1$.
 par $(m-2)$ multiple de 5 (q'2b)
 or $m = 5k+2$
 $\Delta = 5(m-1)$

- Si $m = 5k+2$, alors :
 - Si $m = 2$, $\Delta = 5$
 - Si $m > 2$, $\Delta = m-1$
- Sinon, $\Delta = m-1$.

Enfinement, Si $m = 2$, $\Delta = 5$
 Sinon, $\Delta = m-1$.

b) (c) $m = 2001 = \cancel{600 \times 5} + 1$ [5], donc $\Delta = 2000$.

(d) $m = 2002 = \cancel{600 \times 5} + 2$ [5] donc $\Delta = \cancel{2001}$
 $5 \times 2001 = 10005$.

à vérifier
 ???
 !