L.KAYRIDINE JANOURA
MR : AMMAR BOUAJILA
GSM :92 741 567

CORRECTION SERIE N°12

$4^{éme}$ MATHS | ARITHMETIQUE

EXERCICE 1

Indiquer si la proposition suivante est vraie ou fausse et donner une démonstration de la réponse choisie.

"Il existe un seul couple $(a\,;b)$ de nombres entiers naturels, tel que :
$a < b \quad ; \quad PPCM(a\,;\,b) - PGCD(a\,;\,b) = 1$"

Correction

En notant $d = \text{pgcd}\,(a\,;b)$, il existe k et k' deux entiers premiers entre eux tels que :
$a = k{\cdot}d \quad ; \quad b = k'{\cdot}d$

On en déduit l'écriture : $\text{ppcm}\,(a\,;b) = k{\cdot}k'{\cdot}d$

L'égalité recherchée devient alors :
$\text{ppcm}\,(a\,;b) - \text{pgcd}\,(a\,;b) = 1$

$$k{\cdot}k'{\cdot}d - d = 1$$
$$d{\cdot}(k{\cdot}k' - 1) = 1$$

De cette égalité, on en déduit des conditions sur les facteurs du produit du membre de gauche :
$d = 1 \quad \Big| \quad k{\cdot}k' - 1 = 1$
$\qquad\qquad\;\; k{\cdot}k' = 2$

On en déduit que les deux entiers a et b sont premiers entre eux et que $k{\cdot}k' = 2$. De l'hypothèse que $a < b$, on en déduit :
$k = 1$ et $k' = 2$.

Il n'existe qu'un couple de solution $(1\,;2)$

EXERCICE 2

Indiquer si la proposition suivante est vraie ou fausse et donner une démonstration de la réponse choisie.

"On considère l'équation :
$(E) : \; x^2 - 52x + 480 = 0$
où x est un entier naturel.
Il existe deux entiers naturels non nuls dont le $PGCD$ et le $PPCM$ sont solutions de l'équation (E)."

Correction

Le polynôme $x^2 - 52{\cdot}x + 480$ a pour discriminant :
$\Delta = b^2 - 4{\cdot}a{\cdot}c = 52^2 - 4{\times}1{\times}480 = 784$
On a la simplification suivante : $\sqrt{784} = 28$

Le discriminant étant strictement positif, ce polynôme admet les deux racines suivantes :

$$x_1 = \frac{-b - \sqrt{\Delta}}{2{\cdot}a} = \frac{52 - 28}{2} = \frac{24}{2} = 12 \qquad x_2 = \frac{-b + \sqrt{\Delta}}{2{\cdot}a} = \frac{52 + 28}{2} = \frac{80}{2} = 40$$

Il ne peux exister deux entiers a et b tels que :
$\text{pgcd}\,(a\,;b) = 12 \quad ; \quad \text{ppcm}\,(a\,;b) = 40$
car le $PPCM$ n'est pas divisible par le $PGCD$.

On ne précise pas dans l'énoncé si les deux entiers sont distincts, il est donc possible de choisir :
$a = 12 \quad ; \quad b = 12$

www.devoirat.net 2015

EXERCICE 3

Le but de l'exercice est d'étudier certaines propriétés de divisibilité de l'entier $4^n - 1$, lorsque n est un entier naturel.

On rappelle la propriété connue sous le nom de petit théorème de Fermat : "*Si p est un nombre entier premier et a un entier naturel premier avec p, alors $a^{p-1} - 1 \equiv 0 \pmod{p}$*"

Partie A. Quelques exemples.

1. Démontrer que, pour tout entier naturel n, 4^n est congru à 1 modulo 3.
2. Prouver à l'aide du petit théorème de Fermat, que $4^{28}-1$ est divisible par 29.
3. Pour $1 \leqslant n \leqslant 4$, déterminer le reste de la division de 4^n par 17. En déduire que, pour tout entier k, le nombre $4^{4k} - 1$ est divisible par 17.
4. Pour quels entiers naturels n le nombre $4^n - 1$ est-il divisible par 5 ?
5. A l'aide des questions précédentes, déterminer quatre diviseurs premiers de $4^{28} - 1$.

Partie B. Divisibilité par un nombre premier

Soit p un nombre premier différent de 2.

1. Démontrer qu'il existe un entier $n \geqslant 1$ tel que : $4^n \equiv 1 \pmod{p}$.
2. Soit $n \geqslant 1$ un entier naturel tel que $4^n \equiv 1 \pmod{p}$. On note b le plus petit entier strictement positif tel que $4^b \equiv 1 \pmod{p}$ et r le reste de la division euclidienne de n par b :
   a. Démontrer que $4^r \equiv 1 \pmod{p}$. En déduire que $r = 0$.
   b. Prouver l'équivalence : $4^n - 1$ est divisible par p si, et seulement si, n est multiple de b.
   c. En déduire que b divise $p - 1$.

Correction :

Partie A

1. Montrons la relation suivante par récurrence : "*Pour tout entier entier naturel n, 4^n est congru à 1 modulo 3*"
   - Initialisation :
     Pour $n = 0$, on a :$4^n = 4^0 = 1$ qui est bien congru à 1 modulo 3.
   - Hérédité :
     Supposons que pour une valeur de n, on a : $4^n \equiv 1 \pmod{3}$
     Montrons que cette relation reste vraie au rang $(n+1)$:
     $$4^{n+1} = 4 \cdot 4^n \equiv 1 \cdot 1 \equiv 1 \pmod{3}$$
     Ainsi, la relation est également vraie au rang $(n+1)$.

   On vient ainsi de montrer la relation par un raisonnement par récurrence.

2. Pour $n = 29$ et $a = 2$, le petit théorème de Fermat permet d'écrire :
$$2^{29-1} - 1 \equiv 0 \pmod{29}$$
$$2^{28} - 1 \equiv 0 \pmod{29}$$
En élevant les deux membres au carré, on a :
$$(2^{28} - 1)^2 \equiv 0^2 \pmod{29}$$
$$(2^{28})^2 - 2 \cdot 2^{28} \cdot 1 + 1 \equiv 0 \pmod{29}$$
$$4^{28} - 2 \cdot 2^{28} + 1 \equiv 0^2 \pmod{29}$$
$$4^{28} - 2 \cdot \left(2^{28} - 1\right) + 1 - 2 \equiv 0 \pmod{29}$$
D'après le résultat obtenu par le petit théorème de Fermat :
$$4^{28} - 2 \cdot 0 + 1 - 2 \equiv 0 \pmod{29}$$
$$4^{28} - 1 \equiv 0 \pmod{29}$$
Ainsi, on vient de montrer que $4^{28} - 2$ est divisible par 29.

3. On a le tableau suivant présentant les restes de 4^n par 17 :

n	1	2	3	4
4^n	4	16	64	256
$4^n \pmod{17}$	4	16	13	1

On a l'égalité suivante :
$$4^{4k} - 1 = \left(4^4\right)^k - 1 \equiv 1^k - 1 \equiv 1 - 1 \equiv 0 \pmod{17}$$
Ainsi, le nombre $4^{4k} - 1$ est divisible par 17.

4. Montrons que le nombre $(4^n - 1)$ est divisible par 5 lorsque le nombre n est pair ; supposons n est pair, il existe un entier naturel k tel que :
$$n = 2 \cdot k$$
$$4^n = 4^{2 \cdot k}$$
$$4^n - 1 = 4^{2 \cdot k} - 1$$
$$4^n - 1 \equiv \left(4^2\right)^k - 1 \pmod{5}$$
$$4^n - 1 \equiv 16^k - 1 \pmod{5}$$
$$4^n - 1 \equiv 1^k - 1 \pmod{5}$$
$$4^n - 1 \equiv 1 - 1 \pmod{5}$$
$$4^n - 1 \equiv 0 \pmod{5}$$
Montrons que pour n impair, 4^n n'est pas divisible par 5 ; supposons n impair, il existe un entier naturel k tel que :
$$n = 2 \cdot k + 1$$
$$4^n = 4^{2 \cdot k + 1}$$
$$4^n - 1 = 4^{2 \cdot k + 1} - 1$$
$$4^n - 1 equiv 16^k - 3 \pmod{5}$$
$$4^n - 1 equiv 1^k - 3 \pmod{5}$$
$$4^n - 1 equiv 1 - 2 \pmod{5}$$
$$4^n - 1 equiv 3 \pmod{5}$$
Le nombre $4^n - 1$ n'est pas divisible par 5 lorsque n est impair.

5. En se servant des questions précédentes :
   - D'après la question 1., le nombre 4^{28} est congru à 1 modulo 3 ; ainsi, on a : $4^{28} - 1 \equiv 0 \pmod{3}$
   - D'après la question 2., $4^{28} - 1$ est divisible par 29.

www.devoirat.net 2015

- En remarquant l'égalité suivante :
  $4^{28}-1=4^{4\cdot7}-1$
  En utilisant la question 3., le nombre $4^{28}-1$ est divisible par 17.
- 28 étant un nombre pair, d'après la question 4., $(4^{28}-1)$ est divisible par 5.

Ainsi, on vient de montrer que le nombre $4^{28}-1$ est divisible par les nombres :
3 ; 5 ; 17 ; 29

Partie B

1. Puique p est un nombre premier différent de 2, les nombres 2 et p sont premiers entre eux ; ainsi, d'après le petit théorème de Fermat, on a :

$$\begin{aligned}
2^{p-1}-1 &\equiv 0 \pmod{p}\\
\left(2^{p-1}-1\right)^2 &\equiv 0^2 \pmod{p}\\
\left(2^{p-1}\right)^2-2\cdot2^{p-1}\cdot1+1 &\equiv 0 \pmod{p}\\
2^{2\cdot(p-1)}-2\cdot2^{p-1}+1 &\equiv 0 \pmod{p}\\
4^{p-1}-2\cdot\left(2^{p-1}-1\right)-2+1 &\equiv 0 \pmod{p}\\
4^{p-1}-2\cdot0-1 &\equiv 0 \pmod{p}\\
4^{p-1} &\equiv 1 \pmod{p}
\end{aligned}$$

Ainsi, la valeur de n recherchée est $n=p-1$.

2. a. En effectuant la division euclidienne de n par b, on obtient l'existence des entiers q et r tels que :
$n=q\cdot b+r$
De l'égalité vérifiant n, on a :

$$\begin{aligned}
4^n &\equiv 1 \pmod{p}\\
4^{q\cdot b+r} &\equiv 1 \pmod{p}\\
4^{q\cdot b}\cdot4^r &\equiv 1 \pmod{p}\\
\left(4^b\right)^q\cdot4^r &\equiv 1 \pmod{p}\\
1\cdot4^r &\equiv 1 \pmod{p}\\
4^r &\equiv 1 \pmod{p}
\end{aligned}$$

Or, le nombre b est définie comme étant le plus petit entier strictement positif tel que $4^b\equiv1 \pmod{p}$. Or, r étant le reste par une division euclidienne par b, r est strictement inférieur à b et r vérifie également la relation :
$4^r\equiv1 \pmod{p}$
Ainsi, r est nécessairement nul pour ne pas contredire que b est le plus petit entier strictement positif :
$r=0$

b. - $\Longrightarrow$:
Prenons n tel que 4^n-1 soit divisible par p :
$\Longrightarrow 4^n-1\equiv0 \pmod{p}$
$\Longrightarrow 4^n\equiv1 \pmod{p}$
D'après la question précédente :
Le reste de la division de n par b est nul
n est un multiple de b.

- $\Longleftarrow$:
Supposons que le nombre n est un multiple de b ainsi, il existe un entier naturel k tel que :
$n=k\cdot b$
Ainsi, on a :

$$\begin{aligned}
4^n-1 &\equiv 4^{k\cdot b}-1 \pmod{p}\\
&\equiv \left(4^b\right)^k-1 \pmod{p}\\
&\equiv 1^k-1 \pmod{p}\\
&\equiv 1-1 \pmod{p}\\
&\equiv 0 \pmod{p}
\end{aligned}$$

c. La question 1. nous a permis de montrer que le nombre $p-1$ vérifie la relation :
$4^{p-1}-1\equiv0 \pmod{p}$
Ainsi, on a : $4^{p-1}\equiv1 \pmod{p}$
D'après la question précédente, le nombre b est le plus petit des entiers vérifiant la relation $4^n\equiv1 \pmod{p}$ et divise chacun des nombres *(d'après la question b.)* vérifiant cette relation :
Le nombre b divise $(p-1)$.

www.devoirat.net 2015

EXERCICE 4

1. On considère l'équation (E) :

$$109x - 226y = 1$$

où x et y sont des entiers relatifs.

a. Déterminer le *pgcd* de 109 et 226. Que peut-on en conclure pour l'équation (E) ?

b. Montrer que l'ensemble des solutions de (E) est l'ensemble des couples de la forme $(141 + 226k\,;68 + 109k)$, où k appartient à $\mathbb{Z}$.
En déduire qu'il existe un unique entier naturel non nul d inférieur ou égal à 226 et un unique entier naturel non nul e tels que $109d = 1 + 226e$.
(On précisera les valeurs des entiers d et e)

2. Démontrer que 227 est un nombre premier.

3. On note A l'ensemble des 227 entiers naturels a tels que $a \leqslant 226$.
On considère les deux fonctions f et g de A dans A définies de la manière suivante :
- à tout entier de A, f associe le reste de la division euclidienne de a^{109} par 227 ;
- à tout entier de A, g associe le reste de la division euclidienne de a^{141} par 227.

a. Vérifier que $g[f(0)] = 0$.
On rappelle le résultat suivant appelé petit théorème de Fermat :
Si p est un nombre premier et a un entier non divisible par p alors $a^{p-1} \equiv 1 \pmod{p}$

b. Montrer que, quel que soit l'entier non nul a de A, $a^{226} \equiv 1 \pmod{227}$.

c. En utilisant 1. b. , en déduire que, quel que soit l'entier non nul a de A $g[f(a)] = a$.
Que peut-on dire de $f[g(a)] = a$?

Correction

1. a. L'algorithme d'Euclide donne les divisions euclidiennes suivantes :
- $226 = 2\times 109 + 8$
- $109 = 13\times 8 + 5$
- $8 = 1\times 5 + 3$
- $5 = 1\times 3 + 2$
- $3 = 1\times 2 + 1$
- $2 = 2\times 1 + 0$

On en déduit : $PGCD(226\,;109) = 1$.
Les nombres 226 et 109 étant premier entre eux, on en déduit d'après le théorème de Bezout qu'il existe au moins un couple d'entiers $(x\,;y)$ vérifiant :
$$109\cdot x - 226\cdot y = 1$$
L'équation (E) admet au moins une solution.

b. Montrons que le couple $(141\,;68)$ est solution de (E) :
$$109\cdot x - 226\cdot y = 109\times 141 - 226\times 68$$
$$= 15\,369 - 15\,368 = 1$$
Notons $(x\,;y)$ un couple de solution de (E), on a :
$$109\cdot x - 226\cdot y = 1$$
Or, on a : $109\times 141 - 226\times 68 = 1$
$$109\cdot x - 226\cdot y = 109\times 141 - 226\times 68$$
$$109\cdot(x - 141) = 226\cdot(y - 68)$$
- De l'égalité précédente, on déduit que le nombre 109 divise le produit $226\cdot(y - 68)$; or, les nombres 109 et 226 sont premiers entre eux, d'après le théorème de Gauss, on en déduit :
  109 divise $(y-68)$.
  On en déduit l'existence d'un entier relatif k' vérifiant l'égalité :
  $$y - 68 = k'\cdot 109$$
  $$y = 68 + k'\cdot 109$$
- Le nombre 226 divise le produit $109\cdot(x - 141)$; or, les nombres 226 et 109 sont premiers entre eux, on en déduit à l'aide du théorème de Gauss :
  226 divise $(x - 141)$
  Il existe $k \in \mathbb{Z}$ vérifiant :
  $$x - 141 = k\cdot 226$$
  $$x = 141 + 226\cdot k$$

Ainsi, les couples de solutions de l'équation (E) sont de la forme :
$$\big(141 + 226\cdot k\,;68 + k'\cdot 109\big)$$
Cherchons les couples solutions parmi les couples présentés précédemment :
$$109\cdot x - 226\cdot y = 1$$
$$109\cdot(141 + 226\cdot k) - 226\cdot(68 + k'\cdot 109) = 1$$
$$109\times 141 + 109\times 226\cdot k - 226\times 68 - 226\times k'\cdot 109 = 1$$
$$(109\times 141 - 226\times 68) + (109\times 226\cdot k - 226\times k'\cdot 109) = 1$$
$$1 + 109\times 226\times(k - k') = 1$$
$$109\times 226\times(k - k') = 0$$
Ainsi, on a l'égalité :
$$k - k' = 0 \Longrightarrow k = k'$$
Ainsi, l'ensemble des couples de solutions sont de la forme :
$$\Big\{(141 + 226\cdot k\,;68 + k\cdot 109)\ \Big|\ k \in \mathbb{Z}\Big\}$$
Soit $(d\,;e)$ un couple de solution vérifiant :
$$109\cdot d = 1 + 226\cdot e \quad ; \quad 0 < d \leqslant 226$$
On en déduit que ce couple vérifie l'équation (E) :
$$109\cdot d - 226\cdot e = 1$$
On en déduit l'existence d'un entier relatif k vérifiant :
$$d = 141 + 226\cdot k \quad ; \quad e = 68 + 109\cdot k$$
Vérifions qu'il existe un seul entier vérifiant l'encadrement :
$$0 < 141 + 226\cdot k \leqslant 226$$
$$-141 < 226\cdot k \leqslant 85$$
$$-\frac{141}{226} < k \leqslant \frac{85}{226}$$
Ainsi, k ne peut prendre que la valeur 0.

2. Si 227 est non-premier alors, il admet un diviseur premier inférieur à :
$$\sqrt{227} \simeq 15{,}1$$
On vérifie facilement que 227 n'admet aucun diviseur parmi les entiers premiers inférieurs à 15 :
$$2 \;;\; 3 \;;\; 5 \;;\; 7 \;;\; 11 \;;\; 13$$

3. a. On a : $0^{109} = 0$. Le reste de la division euclidienne de 0 par 227 est 0 ; on en déduit :
$$f(0) = 0$$
On a $0^{141} = 0$. Le reste de la division euclidienne de 0

www.devoirat.net 2015

par 227 vaut 0 ; on en déduit :

$g(0) = 0$

On a l'égalité suivante :

$g[f(0)] = 0$

b. D'après la question 2., le nombre 227 est premier. D'après le petit théorème de Fermat, pour tout entier a non divisible par 227, on a l'équivalence suivante :

$a^{227-1} \equiv 1 \pmod{227}$

$a^{226} \equiv 1 \pmod{227}$

Or, les entiers appartenant à l'ensemble a sont inférieurs ou égaux à 226 : ils ne peuvent pas être divisible par 227 ; on en déduit que les entiers a non-nul appartenant à l'ensemble A vérifient :

$a^{226} \equiv 1 \pmod{227}$

c. D'après la question 1. b. , le couple $(141\,;68)$ est solution de l'équation (E), on a :

$109\times 141 - 226\times 68 = 1$

$109\times 141 = 1 + 226\times 68$

$f(a)$ est le reste de la division euclidienne de a par 227, on a donc l'équivalence suivante :

$f(a) \equiv a^{109} \pmod{227}$

$g[f(a)] \equiv g(a^{109}) \pmod{227}$

En utilisant le définition de la fonction g, on a :

$$\begin{aligned} g[f(a)] &\equiv g(a^{109}) \equiv (a^{109})^{141} \pmod{227} \\ &\equiv a^{109\cdot 141} \pmod{227} \\ &\equiv a^{1+226\times 68} \pmod{227} \\ &\equiv a^{1}\cdot a^{226\times 68} \pmod{227} \\ &\equiv a\cdot(a^{226})^{68} \pmod{227} \\ &\equiv a\cdot 1^{68} \pmod{227} \\ &\equiv a \pmod{227} \end{aligned}$$

De même, on montre que $f[g(a)] = a$

EXERCICE 6

On rappelle la propriété, connue sous le nom de petit théorème de Fermat : "*soit p un nombre premier et a un entier naturel premier avec p ; alors $a^{p-1} - 1$ est divisible par p*".

1. Soit p un nombre premier impair.

   a. Montrer qu'il existe une entier naturel k, non nul, tel que :

   $2^k \equiv 1 \pmod{p}$.

   b. Soit k un entier naturel non nul tel que $2^k \equiv 1 \pmod{p}$ et soit n un entier naturel. Montrer que, si k divise n, alors :

   $2^n \equiv 1 \pmod{p}$.

   c. Soit b tel que $2^b \equiv 1 \pmod{p}$, b étant le plus petit entier non nul vérifiant cette propriété.
   Montrer, en utilisant la division euclidienne de n par b, que :

   si $2^n \equiv 1 \pmod{p}$ alors b divise n.

2. Soit q un nombre premier impair et le nombre $A = 2^q - 1$. On prend pour p un facteur premier de A.

   a. Justifier que :

   $2^q \equiv 1 \pmod{p}$

   b. Montrer que p est impair.

   c. Soit b tel que $2^b \equiv 1 \pmod{p}$, b étant le plus petit entier non nul vérifiant cette propriété.
   Montrer, en utilisant 1., que b divise q. En déduire que $b = q$.

   d. Montrer que q divise $p-1$, puis montrer que $p \equiv 1 \pmod{2q}$.

3. Soit $A_1 = 2^{17} - 1$. Voici la liste des nombres premiers inférieurs à 400 et qui sont de la forme $34m + 1$, avec m entier non nul : 103, 137, 239, 307. En déduire que A_1 est premier.

Correction

1. a. p étant impair, on en déduit que les nombres 2 et p sont premiers entre eux :

   $PGCD(2\,;p) = 1$

   D'après le petit théorème de Fermat, on a l'égalité suivante :

   $2^{p-1} \equiv 1 \pmod{p}$

   Ainsi, il existe k tel que $2^k \equiv 1 \pmod{p}$; il suffit de prendre :

   $k = p - 1$

   b. Si k divise n, alors il existe k' tel que :

   $n = k\cdot k'$

   Ainsi, on a :

   $2^n = 2^{k\cdot k'} = (2^k)^{k'} \equiv 1^{k'} \equiv 1 \pmod{p}$

   c. La division euclidienne de n par b donne l'existence du couple $(q\,;r)$ vérifiant :

   $n = q\cdot b + r \quad ; \quad 0 \leqslant r < b$

   Supposons que l'entier n vérifie :

   $$\begin{aligned} 2^n &\equiv 1 \pmod{p} \\ 2^{q\cdot b + r} &\equiv 1 \pmod{p} \\ 2^{q\cdot b}\cdot 2^r &\equiv 1 \pmod{p} \\ (2^b)^q \cdot 2^r &\equiv 1 \pmod{p} \\ 1^q \cdot 2^r &\equiv 1 \pmod{p} \\ 2^r &\equiv 1 \pmod{p} \end{aligned}$$

   r vérifie la propriété $2^r \equiv 1 \pmod{p}$ et $0 \leqslant r < b$; or, b est le plus entier non-nul vérifiant cette propriété : $r = 0$.

   On a :

   $n = q\cdot b$

   On en déduit : b divise n.

2. a. p est un facteur du nombre A ; cela signifie qu'il existe k tel que :

   $A = p\cdot k$

www.devoirat.net 2015

On en déduit les égalités et équivalences suivantes :

$$A = p\cdot k$$
$$2^q - 1 = p\cdot k$$
$$2^q - 1 \equiv 0 \pmod{p}$$
$$2^q \equiv 1 \pmod{p}$$

b. De l'équivalence $2^q \equiv 1 \pmod{p}$, on en déduit l'existence d'un entier k vérifiant l'égalité suivante :

$$2^q = 1 + k\cdot p$$
$$2^q - 1 = k\cdot p$$

Il est clair que pour tout entier naturel q, le nombre $2^q - 1$ est impair. Sachant qu'un produit de deux nombres est impair si, et seulement si, les deux facteurs sont impairs, on en déduit que :

k est impair ; p est impair.

c. p est un entier premier impair et q est un entier naturel vérifiant :

$$2^q \equiv 1 \pmod{p}$$

D'après la question 1. c., on en déduit que :

b divise q.

Or, q étant un entier premier, il n'a pour diviseur que 1 et q ; on a :

$b = 1$ ou $b = q$

Supposons que $b = 1$, alors $2^b = 2^1 = 2$. Or p est un entier premier :

- si $p = 2$, $2^b \equiv 0 \not\equiv 1 \pmod{p}$
- si $p > 2$, $2^b = 2 \equiv 2 \not\equiv 1 \pmod{p}$

Ce qui est absurde.

On en déduit que $b = q$.

d. L'entier p est un nombre premier impair ; on en déduit que 2 et p sont premiers entre eux. D'après le petit théorème de Fermat, on en déduit que :

$$2^{p-1} \equiv 1 \pmod{p}$$

Or, q est le plus entier non nul vérifiant la propriété $2^q \equiv 1 \pmod{p}$; on en déduit, d'après la question 1. c., que q divise $p - 1$.

Ainsi, on a l'existence d'un entier k vérifiant l'égalité :

$$p - 1 = k\cdot q$$

p étant impair, on a $p-1$ qui est un entier pair :

2 divise $p-1$ $\Longrightarrow$ 2 divise $k\cdot q$

Or, q étant un entier premier impair donc premier avec 2, d'après le théorème de Gauss, on en déduit que 2 divise k. Il existe un entier k' tel que :

$$k = 2\cdot k'$$
$$k\cdot q = 2\cdot k'\cdot q$$
$$p - 1 = 2\cdot k'\cdot q$$

On a l'équivalence suivante :

$$p - 1 \equiv 0 \pmod{2q}$$
$$p \equiv 1 \pmod{2q}$$

3. Supposons que A_1 est non-premier, ainsi, il admet un facteur premier p vérifiant :

$$p \leqslant \sqrt{2^{17} - 1}$$
$$p \leqslant 362{,}04$$

soit p un facteur premier de A_1 d'après la question 2. d. doit vérifier :

$$p \equiv 1 \pmod{34}$$

Cela entraîne que tout facteur premier p de A_1 admet l'écriture :

$$p = 34\cdot k + 1 \text{ où} k \in \mathbb{N}$$

D'après l'énoncé, seul les entiers premiers 103, 137, 239 et 307 vérifient ces deux conditions mais aucun de ces entiers ne sont des diviseurs de A_1 ce qui est absurdent.

Le nombre A_1 est un entier premier.

www.devoirat.net 2015

EXERCICE 9

Dans tout l'exercice x et y désignent des entiers naturels non nuls vérifiant $x < y$. S est l'ensemble des couples $(x\,;y)$ tels que $PGCD\,(x\,;y) = y - x$

1. **a.** Calculer le $PGCD(363\,;\,484)$.

b. Le couple $(363\,;484)$ appartient-il à S ?

2. Soit n un entier naturel non nul ; le couple $(n\,;n+1)$ appartient-il à S
Justifier votre réponse.

3. **a.** Montrer que $(x\,;y)$ appartient à S si, et seulement si, il existe un entier naturel k non nul tel que :
$x = k{\cdot}(y-x) \quad ; \quad y = (k+1)(y-x)$

b. En déduire que pour tout couple $(x\,;y)$ de S, on a :
$PPCM\,(x\,;y) = k{\cdot}(k+1){\cdot}(y-x)$

4. **a.** Déterminer l'ensemble des entiers naturels diviseurs de 228.

b. En déduire l'ensemble des couples $(x\,;y)$ de S tels que :
$PPCM(x\,;\,y) = 228$

Correction

1. **a.** Déterminons le $PGCD$ des nombres 363 et 484 à l'aide de l'algorithme d'Euclide :
- $484 = 1{\times}363 = 121$
- $363 = 3{\times}121 + 0$

On en déduit que $PGCD(363\,;\,484) = 121$

b. On a les deux égalités suivantes :
$PGCD(363\,;\,484) = 121 \quad ; \quad 484 - 363 = 121$

2. Soit n un entier naturel non-nul ; notons d le $PGCD$ de n et de $n{+}1$. d divise alors $n+1$ et n, on en déduit que d divise leur différence :
d divisant 1, on en déduit que : $d = 1$
C'est à dire : $PGCD(n\,;n+1) = 1$

Ainsi, on a les deux égalités suivantes :
$PGCD(n\,;n+1) = 1 \quad ; \quad (n+1) - n = 1$

3. **a.**
- $\Longrightarrow$: supposons que $(x\,;y) \in S$:
On en déduit :
$PGCD(x\,;\,y) = y - x$
On en déduit l'existence de deux entiers k et k' premiers entre eux tels que :
$x = k{\cdot}(y-x) \quad ; \quad y = k'{\cdot}(y-x)$
Partons de l'égalité suivante :

$$y = k'{\cdot}(y-x)$$
$$k{\cdot}y = k{\cdot}k'{\cdot}(y-x)$$
$$k{\cdot}y = k'{\cdot}\big[k{\cdot}(y-x)\big]$$
$$k{\cdot}y = k'{\cdot}x$$
$$k{\cdot}y - k{\cdot}x = k'{\cdot}x - k{\cdot}x$$
$$k{\cdot}(y-x) = k'{\cdot}x - k{\cdot}x$$
$$x - k'{\cdot}x + k{\cdot}x = 0$$
$$x{\cdot}(k+1-k') = 0$$

x étant un entier non-nul, cela entraîne que le second facteur est nul :
$$k+1-k' = 0 \Longrightarrow k+1 = k'$$
$$\Longrightarrow y = (k+1){\cdot}(y-x)$$

- $\Longleftarrow$: supposons qu'il existe un entier k non nul tel que :
$x = k{\cdot}(y-x) \quad ; \quad y = (k+1){\cdot}(y-x)$

Notons d le $PGCD$ de x et de y. Ainsi, d divise x et y, il divise donc leur différence :
$y - x = (k+1){\cdot}(y-x) - k{\cdot}(y-x) = y - x$
On en déduit que d divise $(y{-}x)$.
En utilisant les deux écritures de x définies dans l'hypothès, il est clair que l'entier $(y{-}x)$ divise x et y ; $(y{-}x)$ est un diviseur commun à x et à y : $(y{-}x)$ divise d.

On en déduit l'égalité :
$d = PGCD(x\,;\,y) = y - x.$

b. La relation entre le $PPCM$ et le $PGCD$ de deux nombres permet d'écrire :
$PPCM(x\,;\,y){\cdot}PGCD(x\,;\,y) = x{\cdot}y$

Puisque $(x\,;y) \in S$:
$PPCM(x\,;\,y){\cdot}(y-x) = x{\cdot}y$

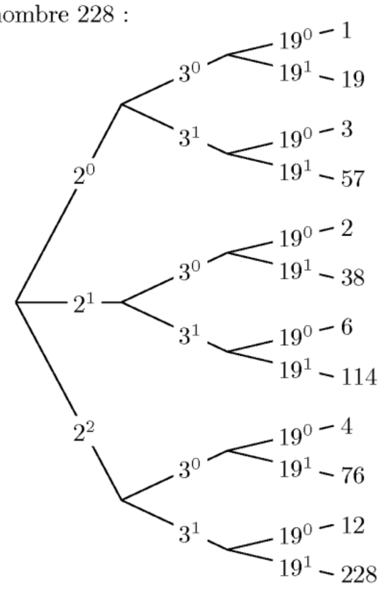
Avec les relations obtenues à la question **a.** et **b.** :
$$PPCM(x\,;\,y){\cdot}(y-x) = \big[k{\cdot}(y-x)\big]{\cdot}\big[(k+1){\cdot}(y-x)\big]$$
$$PPCM(x\,;\,y){\cdot}(y-x) = k{\cdot}(k+1){\cdot}(y-x)^2$$
$$PPCM(x\,;\,y) = k{\cdot}(k+1){\cdot}(y-x)$$

4. **a.** L'algorithme de décomposition d'un nombre en produit de facteurs premiers donne :

$$\begin{array}{r|l} 228 & 2 \\ 114 & 2 \\ 57 & 3 \\ 19 & 19 \\ 1 & \end{array}$$

Ainsi, le nombre 228 admet pour décomposition en produit de facteurs premiers :
$228 = 2^2{\times}3{\times}19$

On en déduit l'arbre des diviseurs suivant pour le nombre 228 :



L'ensemble des diviseurs de 228 sont :
1 ; 2 ; 3 ; 4 ; 6 ; 12 ; 19
38 ; 57 ; 76 ; 114 ; 228

b. D'après la question **3. b.**, le couple $(x\,;y)$ appartenant à l'ensemble S, on a :
$PPCM(x\,;\,y) = k{\cdot}(k+1){\cdot}(y-x)$

www.devoirat.net 2015

Ainsi, le $PPCM$ doit pouvoir s'écrire comme un produit où deux de ses facteurs sont des entiers consécutifs. Parmi, les diviseurs de 228, voici ceux qui réalisent cette contrainte :

- $2\times3\times38$: ainsi, on a les identifications suivantes :
  $k=2 \quad ; \quad k+1=3 \quad ; \quad y-x=38$
  On en déduit les valeurs de x et de y :
  $x=k\cdot(y-x)=76 \quad ; \quad y=(k+1)\cdot(y-x)=114$
- $3\times4\times19$: ainsi, on a les identifications suivantes :
  $k=3 \quad ; \quad k+1=4 \quad ; \quad y-x=19$
  On en déduit les valeurs de x et de y :
  $x=k\cdot(y-x)=57 \quad ; \quad y=(k+1)\cdot(y-x)=76$

Ainsi, deux couples appartenant à S vérifient $PPCM(x\,;y)=228$:
$(76\,;114) \quad ; \quad (57\,;76)$

www.devoirat.net 2015