03

ARITHMÉTIQUE DANS $\mathbb{Z}$

1 Divisibilité dans $\mathbb{Z}$:

a- Définition

Soient a et b deux éléments de $\mathbb{Z}$ tels que $a \neq 0$

On dit que a divise b et on écrit $a|b$, s'il existe un nombre entier relatif k tel que : $b = ka$

$$a|b \Leftrightarrow (\exists k \in \mathbb{Z}) \quad b = ka$$

On dit aussi que a est un diviseur de b ou b est divisible par a ou b est un multiple de a

b- Propriétés

Pour tous a, b, c et d de $\mathbb{Z}^*$:

- 1, (-1), a et $(-a)$ sont des diviseurs de a

Un diviseur de a autre que ces quatre nombres s'appelle un diviseur propre de a

- Tout nombre entier non nul est un diviseur de zéro
- Si $d|a$ alors : $|d| \leq |a|$
- Si $a|b$ et $b|c$ alors : $a|c$
- Si $a|b$ alors : $(\forall n \in \mathbb{Z}^*) \quad a|nb$ et $na|nb$ et $(\forall n \in \mathbb{N}^*) \quad a^n|b^n$
- Si $d|a$ et $d|b$ alors : $(\forall (\alpha, \beta) \in \mathbb{Z}^2) \quad d|(\alpha a + \beta b)$
- Si $a|b$ et $c|d$ alors : $ac|bd$

2 Division euclidienne dans $\mathbb{Z}$

Soient a et b deux entiers tels que $a \neq 0$

Il existe un couple unique (q,r) de $\mathbb{Z} \times \mathbb{N}$ tel que : $b = qa + r$ et $0 \leq r < |a|$

L'opération qui permet de déterminer q et r s'appelle la division euclidienne de b par a

b est le dividende, a le diviseur, q le quotient et r est le reste.

3 Congruence modulo n

a- Définition

Soient $n \in \mathbb{N}^*$ et $(a,b) \in \mathbb{Z}^2$

On dit que a est congru à b modulo n et on écrit $a \equiv b[n]$ si n divise $(a-b)$

$$a \equiv b[n] \Longleftrightarrow n|(a-b)$$

b- Propriétés

Soit n un nombre entier naturel non nul

- $(\forall a \in \mathbb{Z}) \quad a \equiv a[n]$
- $(\forall (a,b) \in \mathbb{Z}^2) \quad a \equiv b[n] \Longrightarrow b \equiv a[n]$
- $(\forall (a,b,c) \in \mathbb{Z}^3) \quad (a \equiv b[n]$ et $b \equiv c[n]) \Longrightarrow a \equiv c[n]$
- $(\forall (a,b,c,d) \in \mathbb{Z}^4) \quad (a \equiv b[n]$ et $c \equiv d[n]) \Longrightarrow \begin{cases} a+c \equiv b+d[n] \\ ac \equiv bd[n] \end{cases}$
- $(\forall (a,b) \in \mathbb{Z}^2) \ (\forall p \in \mathbb{N}^*) \quad a \equiv b[n] \Longrightarrow a^p \equiv b^p[n]$
- $(\forall (a,b) \in \mathbb{Z}^2)(\forall p \in \mathbb{N}^*) \quad pa \equiv pb[pn] \Longrightarrow a \equiv b[n]$
- $(\forall a \in \mathbb{Z}) \quad a \equiv r[n]$ où r est le reste de la division euclidienne de a par n
- Pour tout $(a,b) \in \mathbb{Z}^2$; $a \equiv b[n]$ si et seulement si a et b ont le même reste dans la division euclidienne par n

c- L'ensemble $\mathbb{Z}/n\mathbb{Z}$

On considère la congruence modulo $n \ (n \in \mathbb{N}^* - \{1\})$

Pour tout $a \in \{0, 1, \cdots, n-1\}$, on note $\bar{a}$ l'ensemble $\{x \in \mathbb{Z} / x \equiv a[n]\}$

$\bar{a}$ s'appelle la classe d'équivalence de a modulo n

L'ensemble $\{\bar{0}, \bar{1}, \cdots, \overline{(n-1)}\}$ est noté $\mathbb{Z}/n\mathbb{Z}$

$\left(\forall (\bar{a}, \bar{b}) \in \left(\mathbb{Z}/n\mathbb{Z}\right)^2\right) \quad \overline{a+b} = \bar{a} + \bar{b}$ et $\overline{a \times b} = \bar{a} \times \bar{b}$

4 Plus grand diviseur commun

a- Définition

Soit $(a,b) \in (\mathbb{Z}^*)^2$

Le plus grand diviseur commun de a et b noté $a \wedge b$ est le plus grand élément de l'ensemble $D_a \cap D_b$: $a \wedge b = \max(D_a \cap D_b)$

b- Remarques

- $a \wedge b$ est un nombre entier naturel
- $a \wedge b$ divise a et divise b
- Si $c|a$ et $c|b$ alors $c \leq a \wedge b$
- $a \wedge b = |a| \wedge |b|$
- Pour tout $(a,b) \in (\mathbb{N}^*)^2$: $a \wedge b = b \wedge a$, $a \wedge a = a$, $a \wedge b = a \Longleftrightarrow a|b$

c- Algorithme d'Euclide

Propriété

Soit $(a,b) \in (\mathbb{N}^*)^2$ tel que b ne divise pas a

Si r est le reste de la division euclidienne de a par b alors : $a \wedge b = b \wedge r$

Corollaire

Soit $(a,b) \in (\mathbb{N}^*)^2$ tel que b ne divise pas a

$a \wedge b$ est le dernier reste non nul dans «les divisions successives de a par b»

d- Propriétés

Pour tout $(a,b,c) \in (\mathbb{Z}^*)^3$

- Si $a \wedge b = d$ alors : $(\exists (u,v) \in \mathbb{Z}^2) \quad d = au + bv$
- Pour tout $\alpha \in \mathbb{Z}^*$, si $\alpha | a$ et $\alpha | b$ alors : $\alpha | a \wedge b$
- $ca \wedge cb = |c|(a \wedge b)$
- $(a \wedge b) \wedge c = a \wedge (b \wedge c)$

5 Nombres premiers entre eux

a- Définition

Soit $(a,b) \in (\mathbb{Z}^*)^2$

On dit que a et b sont premiers entre eux si $a \wedge b = 1$

b- Théorème de Bezout

Soit $(a,b) \in (\mathbb{Z}^*)^2$

$a \wedge b = 1 \Longleftrightarrow (\exists (u,v) \in \mathbb{Z}^2) \quad au + bv = 1$

c- Théorème de Gauss

Soient a, b et c trois éléments de $\mathbb{Z}^*$

Si $a | bc$ et $a \wedge b = 1$ alors $a | c$

d- Corollaires

- Soient a et b deux éléments de $\mathbb{Z}^*$ et d un élément de $\mathbb{N}^*$

On a : $a \wedge b = d \Longleftrightarrow \dfrac{a}{d} \wedge \dfrac{b}{d} = 1$

- Soient a, b et c trois éléments de $\mathbb{Z}^*$

Si $a | c$ et $b | c$ et $a \wedge b = 1$ alors : $ab | c$

- Soient $n \in \mathbb{N}^*$ et $(a,b,c) \in (\mathbb{Z}^*)^3$

Si $ab \equiv ac\,[n]$ et $a \wedge n = 1$ alors : $b \equiv c\,[n]$

- Soit $(a,b,c) \in (\mathbb{Z}^*)^3$

Si $a \wedge b = 1$ et $a \wedge c = 1$ alors : $a \wedge bc = 1$

- Soit $(a,b) \in (\mathbb{Z}^*)^2$

Si $a \wedge b = 1$ alors : $(\forall (m,n) \in (\mathbb{N}^*)^2) \quad a^m \wedge b^n = 1$

6 Équations $ax + by = c$ dans $\mathbb{Z}^2$

Soit $(a,b,c) \in \mathbb{Z}^3$

L'équation $ax + by = c$ admet des solutions dans $\mathbb{Z}^2$ si et seulement si : $a \wedge b | c$

7 Plus petit multiple commun

a- Définition

Soit $(a,b) \in (\mathbb{Z}^*)^2$

Le plus petit multiple commun de a et b noté $a \vee b$ est le plus petit élément de l'ensemble $(|a|\mathbb{N}^*) \cap (|b|\mathbb{N}^*)$:

$$a \vee b = \min(|a|\mathbb{N}^* \cap |b|\mathbb{N}^*)$$

Remarques

$a \vee a = |a|$; $a \vee b = |a| \vee |b|$; $a \vee b = |a| \Leftrightarrow b | a$

b- Propriétés

- Soit $(a,b) \in (\mathbb{Z}^*)^2$ et soit $m = a \vee b$

Pour tout $\alpha \in \mathbb{Z}^*$, si α est un multiple commun de a et b

alors α est un multiple de m

Autrement dit: $(a|\alpha$ et $b|\alpha) \Longrightarrow m|\alpha$ ou $\alpha \in (a\mathbb{Z} \cap b\mathbb{Z}) \Longrightarrow \alpha \in m\mathbb{Z}$

Corollaires

- $(\forall (a,b) \in (\mathbb{Z}^*)^2)$ $\quad (a \wedge b) \times (a \vee b) = |a| \times |b|$
- $(\forall (a,b) \in (\mathbb{Z}^*)^2)$ $\quad a \wedge b = 1 \Leftrightarrow a \vee b = |a| \times |b|$
- $(\forall (a,b,c) \in (\mathbb{Z}^*)^3)$ $\quad ca \vee cb = |c|(a \vee b)$

8 Nombres premiers

a- Définition

Soit $p \in \mathbb{Z}^* - \{-1, 1\}$

On dit que le nombre p est premier s'il admet exactement quatre diviseurs: 1, -1, p et $-p$

Autrement dit: p est premier s'il n'admet pas de diviseur propre.

Remarque

Si le nombre p est premier alors le nombre $(-p)$ est premier

b- Propriétés

- Soit $n \in \mathbb{N}^* - \{1\}$ tel que n n'est pas premier

Le plus petit diviseur positif de n différent de 1 est un nombre premier

- Soit $n \in \mathbb{N}^* - \{1;2;3\}$ tel que n n'est pas premier

Il existe un nombre premier positif p tel que : $p|n$ et $p \leq \sqrt{n}$

- Si p et q sont deux nombres premiers positifs distincts Alors : $p \wedge q = 1$
- Soit $n \in \mathbb{Z}^*$

Si p est un nombre premier qui ne divise pas n alors $p \wedge n = 1$

- Soit $(a,b) \in (\mathbb{Z}^*)^2$ et soit $p \in \mathbb{N}^*$

Si $p|ab$ et p premier alors $p|a$ ou $p|b$

- Soient $a \in \mathbb{Z}^*$ et $n \in \mathbb{N}^*$

Si $p|a^n$ et p premier alors $p|a$

- Soient $p_1, \cdots$ et p_n des nombres premiers

Si p est un nombre premier tel que $p | p_1 p_2 \cdots p_n$

Alors il existe i tel que $p = p_i$

c- Théorème de Fermat

Si p est un nombre premier positif

Alors $(\forall n \in \mathbb{Z})$ $n^p \equiv n[p]$, et si p ne divise pas n, alors $n^{p-1} \equiv 1[p]$

9 Systèmes de numération

Soit b un élément de $\mathbb{N}^* - \{1\}$

Tout nombre entier naturel non nul n peut s'écrire d'une façon unique sous la forme : $n = a_m b^m + \cdots + a_2 b^2 + a_1 b + a_0$ où $a_0, a_1, \cdots$ et a_m sont des nombres entiers tels que $0 \leq a_i \leq b-1$ pour tout i de $\{0, 1, \cdots, m\}$ et $a_m \neq 0$

On écrit : $n = \overline{a_m a_{m-1} \cdots a_1 a_0}^{(b)}$

et on dit qu'on a écrit le nombre n dans le système de numération de base b

Exercice 1 Juin 2003

On considère dans $(\mathbb{N}^*)^2$ l'équation suivante :

$$(E) : x^2(x^2+7) = y(2x+y)$$

Soit (x,y) un élément de $(\mathbb{N}^*)^2$ et soit d le plus grand diviseur commun de x et y

On pose : $x = da$ et $y = db$

1) On suppose que (x,y) est une solution de l'équation (E)

a- Vérifier que : $a^2(d^2a^2+7) = b(2a+b)$

b- En déduire qu'il existe un nombre entier naturel k tel que : $d^2a^2+7 = kb$ et $2a+b = ka^2$

c- Montrer que : $a = 1$

d- En déduire que : $(b+1)^2 = d^2+8$

2) Résoudre dans $(\mathbb{N}^*)^2$ l'équation (E)

Solution

1) a- On a : (x,y) est une solution de l'équation (E)

Donc : $x^2(x^2+7) = y(2x+y)$ c'est-à-dire $d^2a^2(d^2a^2+7) = db(2da+db)$

D'où : $a^2(d^2a^2+7) = b(2a+b)$

b- On a : $x \wedge y = d$ et $x = da$ et $y = db$, Donc : $a \wedge b = 1$

Et puisque $a^2(d^2a^2+7) = b(2a+b)$ alors $b \mid a^2(d^2a^2+7)$

Et puisque $b \wedge a^2 = 1$ (car $b \wedge a = 1$)

alors : $b \mid (d^2a^2+7)$ (d'après le théorème de Gauss)

par suite, il existe un nombre entier naturel k tel que: $d^2a^2+7 = kb$

Donc : $a^2 \times bk = b(2a+b)$ (d'après le résultat de la question 1) a))

D'où : $2a+b = a^2k$

c- On a : $2a+b = ka^2$, Donc $b = a(ka-2)$

par suite, $a \mid b$, D'où : $a \wedge b = a$

Et puisque : $a \wedge b = 1$, alors : $a = 1$

d- On a : $a^2(d^2a^2+7)=b(2a+b)$ et $a=1$
Donc : $d^2+7=2b+b^2$ c'est-à-dire : $d^2+7+1=b^2+2b+1$
D'où : $(b+1)^2=d^2+8$

2) On a : $(E) \Leftrightarrow \begin{cases} x\wedge y=d \\ x=da \\ y=db \\ a^2(d^2a^2+7)=b(2a+b) \end{cases}$

$\Rightarrow \begin{cases} a=1 \\ (b+1)^2=d^2+8 \end{cases}$

$\Rightarrow \begin{cases} a=1 \\ (b+1-d)(b+1+d)=8 \end{cases}$

$\Rightarrow \begin{cases} a=1 \\ b-d+1=1 \\ b+d+1=8 \end{cases}$ ou $\begin{cases} a=1 \\ b-d+1=2 \\ b+d+1=4 \end{cases}$ (car $b+d+1>b-d+1$)

$\Rightarrow a=1$ et $b=2$ et $d=1$

$\Rightarrow x=1$ et $y=2$

et on vérifie que le couple $(1;2)$ est bien une solution de l'équation (E)
Donc l'ensemble de solutions de l'équation (E) est $S=\{(1;2)\}$

Exercice 2 Juin 2006

On considère dans $(\mathbb{N}^*)^2$ l'équation $(E): x^2(x+y)=y^2(x-y)^2$
1) Soit (x,y) une solution de l'équation (E)
On pose : $d=x\wedge y$, $x=ad$ et $y=bd$
a- Vérifier que : $db^2(a-b)^2=(a+b)a^2$
b- En déduire que : $b=1$
c- Montrer que : $a\neq 1$ et que $(a-1)$ divise $(a+1)$
d- En déduire que : $a=2$ ou $a=3$
2) Résoudre dans $(\mathbb{N}^*)^2$ l'équation (E)

Solution

1) a- On a : $x^2(x+y)=y^2(x-y)^2 \Leftrightarrow a^2d^2(ad+bd)=b^2d^2(ad-bd)^2$
$\Leftrightarrow a^2d^3(a+b)=b^2d^4(a-b)^2$
$\Leftrightarrow a^2(a+b)=b^2d(a-b)^2$ (car $d\neq 0$)

b- On a : $a^2(a+b)=b^2d(a-b)^2$, Donc : $b\,|\,a^2(a+b)$
et puisque : $x\wedge y=d$, alors : $a\wedge b=1$, par suite : $a^2\wedge b=1$
Donc : $b\,|\,(a+b)$ (d'après le théorème de Gauss)
Et puisque : $b\,|\,b$ alors : $b\,|\,(a+b-b)$ c'est-a-dire : $b\,|\,a$

d'où : $a \wedge b = b$
Et puisque : $a \wedge b = 1$ alors : $b = 1$
c- • On a : $d(a-1)^2 = (a+1)a^2$ car $b = 1$
Supposons que : $a = 1$, Donc : $0 = 2$ ce qui est faux
Donc : $a \neq 1$
• On a : $d(a-1)^2 = (a+1)a^2$ et $a \neq 1$
Donc : $(a-1) | a^2(a+1)$
Et puisque : $(a-1) \wedge a = 1$ (car $a-(a-1)=1$)
alors : $(a-1) \wedge a^2 = 1$
par suite, $(a-1) | (a+1)$ (d'après le théorème de Gauss)
d- On a : $(a-1) | (a+1)$
et on a : $(a-1) | (a-1)$
Donc : $(a-1) | (a+1)-(a-1)$
c'est-à-dire : $(a-1) | 2$
par suite, $a-1 = 1$ ou $a-1 = 2$ c'est-à-dire : $a = 2$ ou $a = 3$
2) • Soit (x,y) une solution de l'équation (E) dans $(\mathbb{N}^*)^2$
Si on pose : $x \wedge y = d$
Alors d'après ce qui précède ($x = 2d$ et $y = d$) ou ($x = 3d$ et $y = d$)
c'est-à-dire : $x = 2y$ ou $x = 3y$
si $x = 2y$ alors : $4y^2 \times 3y = y^2 \times y^2$ c'est-à-dire : $y = 12$ D'où : $x = 24$
si $x = 3y$ alors : $9y^2 \times 4y = y^2 \times 4y^2$ c'est-à-dire : $y = 9$ D'où : $x = 27$
• Réciproquement, vérifier que les couples $(24;12)$ et $(27;9)$ sont des solutions de l'équation (E)
Donc: $S = \{(24;12),(27;9)\}$

Exercice 3 Juin 2004

1) Soit n un élément de $\mathbb{N}$
a- Montrer que si n est impair alors $n^2 \equiv 1[8]$
b- Montrer que si n est pair alors $n^2 \equiv 0[8]$ ou $n^2 \equiv 4[8]$
2) Soient a, b et c des nombres entiers naturels impairs
a- Montrer que : $a^2+b^2+c^2$ n'est pas un carré parfait
b- Montrer que : $2(ab+bc+ca) \equiv 6[8]$
(Remarquer que : $(a+b+c)^2 = a^2+b^2+c^2+2ab+2bc+2ac$)
c- En déduire que $2(ab+bc+ac)$ n'est pas un carré parfait
d- Montrer que $(ab+bc+ca)$ n'est pas un carré parfait

Solution

1) a- Soit n un nombre entier naturel impair

Donc : $n \equiv 1[8]$ ou $n \equiv 3[8]$ ou $n \equiv 5[8]$ ou $n \equiv 7[8]$
par suite, $n^2 \equiv 1[8]$ ou $n^2 \equiv 9[8]$ ou $n^2 \equiv 25[8]$ ou $n^2 \equiv 49[8]$
Dans tous ces cas: $n^2 \equiv 1[8]$

b- Soit n un nombre entier naturel pair
Donc : $n \equiv 0[8]$ ou $n \equiv 2[8]$ ou $n \equiv 4[8]$ ou $n \equiv 6[8]$
par suite, $n^2 \equiv 0[8]$ ou $n^2 \equiv 4[8]$ ou $n^2 \equiv 16[8]$ ou $n^2 \equiv 36[8]$
Dans tous ces cas: $n^2 \equiv 0[8]$ ou $n^2 \equiv 4[8]$

Remarque : à partir des résultats de ces deux questions, un carré parfait est congru soit à 0 ou à 1 ou à 4 modulo 8

2) a- Soient a, b et c des nombres entiers naturels impairs
supposons que $a^2+b^2+c^2$ est un carré parfait
D'après le résultat de la question 1) a) On a : $a^2 \equiv 1[8]$ et $b^2 \equiv 1[8]$ et $c^2 \equiv 1[8]$
Donc : $a^2+b^2+c^2 \equiv 3[8]$ $(*)$
Et d'après les résultats des questions 1) a) et 1) b), la proposition $(*)$ est fausse
par suite, $a^2+b^2+c^2$ n'est pas un carré parfait.

b- On a : $2(ab+bc+ca)=(a+b+c)^2-(a^2+b^2+c^2)$
Et on sait que la somme de trois nombres entiers naturels impairs est un nombre impair
Donc : $a+b+c$ est un nombre impair
par suite : $(a+b+c)^2 \equiv 1[8]$
Et on a vu que : $a^2+b^2+c^2 \equiv 3[8]$
Donc : $2(ab+bc+ca) \equiv (1-3)[8]$ c'est-à-dire : $2(ab+bc+ca) \equiv -2[8]$
par suite: $2(ab+bc+ca) \equiv 6[8]$

c- Supposons que $2(ab+bc+ca)$ est un carré parfait
Donc : $(\exists n \in \mathbb{N})\quad 2(ab+bc+ca)=n^2$
Le nombre n^2 est pair, d'où n est pair
et d'après **1) b-** on a : $n^2 \equiv 0[8]$ ou $n^2 \equiv 4[8]$
cette proposition est fausse car d'après 2) b) on a : $n^2 \equiv 6[8]$
Conclusion : $2(ab+bc+ca)$ n'est pas un carré parfait.

d- Supposons que $ab+bc+ca$ est un carré parfait
Donc : $(\exists n \in \mathbb{N})\quad ab+bc+ca=n^2$
par suite, $2(ab+bc+ca)=2n^2$
Et puisque : $2(ab+bc+ca) \equiv 6[8]$ alors $2n^2 \equiv 6[8]$
Et puisque : $ab+bc+ca$ est un nombre impair alors n^2 est impair
par suite n est impair
Et d'après 1) a) on a : $n^2 \equiv 1[8]$, donc : $2n^2 \equiv 2[8]$
On a : $2n^2 \equiv 6[8]$ et $2n^2 \equiv 2[8]$, donc : $0 \equiv 4[8]$, ce qui est faux
par suite, $(ab+bc+ca)$ n'est pas un carré parfait.

Exercice 4 Juin 2005

I. Soit p un nombre entier naturel premier tel que $p \geq 5$

1) Montrer que $p^2 \equiv 1[3]$

2) a- Montrer qu'il existe un entier naturel q tel que: $p^2 - 1 = 4q(q+1)$

b- En déduire que $p^2 \equiv 1[8]$

3) Montrer que $p^2 \equiv 1[24]$

II. Soit a un nombre entier naturel tel que $a \wedge 24 = 1$

1) Montrer que $a^2 \equiv 1[24]$

2) Existe-t-il des entiers naturels $a_1, \cdots, a_{23}$ tels que $a_1^2 + \cdots + a_{23}^2 = 23997$ et $(\forall k \in \{1, \cdots, 23\})$ $a_k \wedge 24 = 1$?

Solution

I. 1) p est un nombre premier tel que $p \geq 5$
donc le nombre p n'est pas divisible par 3
et puisque 3 est un nombre premier
Alors d'après, le théorème de Fermat: $p^{3-1} \equiv 1[3]$ c'est-à-dire $p^2 \equiv 1[3]$

2) a- Le nombre p est impair
Donc : $(\exists q \in \mathbb{N})$ $p = 2q + 1$
D'où : $p^2 - 1 = (2q+1)^2 - 1 = 4q^2 + 4q = 4q(q+1)$

b- On sait que le produit de deux nombres entiers consécutifs est un nombre pair
Donc : $(\exists k \in \mathbb{N})$ $q(q+1) = 2k$
par suite : $p^2 - 1 = 8k$, d'où : $p^2 \equiv 1[8]$

3) On a : $p^2 \equiv 1[3]$ et $p^2 \equiv 1[8]$
Donc : $3 | (p^2 - 1)$ et $8 | (p^2 - 1)$
et comme $3 \wedge 8 = 1$, alors $(3 \times 8) | (p^2 - 1)$ c'est-à-dire $24 | (p^2 - 1)$
par suite, $p^2 \equiv 1[24]$

II. 1) Soit a un nombre entier naturel tel que $a \wedge 24 = 1$
et soit $a = p_1^{\alpha_1} \cdots p_n^{\alpha_n}$ la décomposition de a en facteurs premiers
Et puisque : $a \wedge 24 = 1$
Alors : $(\forall i \in \{1, \cdots, n\})$ $p_i \wedge 24 = 1$ et $p_i \geq 5$ (2 et 3 sont des diviseurs de 24)
Donc, d'après le résultat de la partie I): $p_i^2 \equiv 1[24]$ pour tout $i \in \{1, \cdots, n\}$
et par suite : $a^2 \equiv (p_1^2)^{\alpha_1} \cdots (p_n^2)^{\alpha_n} [24]$

$$\equiv 1 \times 1 \times \cdots \times 1 [24]$$

D'où : $a^2 \equiv 1[24]$

2) Supposons qu'il existe des entiers naturels $a_1, \cdots, a_{23}$ tels que
$a_1^2 + \cdots + a_{23}^2 = 23997$ et $a_k \wedge 24 = 1$ pour tout $k \in \{1, \cdots, 23\}$
D'après la résultat de la question précèdente: $(\forall k \in \{1, \cdots, 23\})$ $a_k^2 \equiv 1[24]$
Donc : $a_1^2 + \cdots + a_{23}^2 \equiv 23[24]$
c'est-à-dire : $23997 \equiv 23[24]$

c'est-à-dire : $23974 \equiv 0[24]$

donc : 24 divise 23974, ce qui est faux

par suite, il n'existe pas des nombres $a_1, \cdots, a_{23}$ tels que :

$a_1^2 + \cdots + a_{23}^2 = 23997$ et $(\forall k \in \{1, \cdots, 23\})$ $a_k \wedge 24 = 1$

Exercice 5 Juin 2010

1) Déterminer les nombres entiers naturels m tels que : $m^2 + 1 \equiv 0[5]$

2) Soit p un nombre premier tel que : $p = 3 + 4k$ où $k \in \mathbb{N}$

et soit n un nombre entier naturel tel que : $n^2 + 1 \equiv 0[p]$

a- Vérifier que : $(n^2)^{1+2k} \equiv -1[p]$

b- Montrer que les nombres n et p sont premiers entre eux.

c- En déduire que : $(n^2)^{1+2k} \equiv 1[p]$

d- En déduire, de ce qui précède, qu'il n'existe pas un nombre entier naturel n qui vérifie $n^2 + 1 \equiv 0[p]$

Solution

1) Pour déterminer les nombres entiers naturels m tels que $m^2 + 1 \equiv 0[5]$, on va utiliser le tableau suivant de la congruence modulo 5 :

$m \equiv$	0	1	2	3	4
$m^2 \equiv$	0	1	4	4	1
$m^2+1 \equiv$	1	2	0	0	2

D'où : $m^2 + 1 \equiv 0[5] \Longleftrightarrow m \equiv 2[5]$ ou $m \equiv 3[5]$

$\Longleftrightarrow m = 2 + 5k$ ou $m = 3 + 5k \quad (k \in \mathbb{N})$

Autre méthode :

On a : $m^2 + 1 \equiv 0[5] \Longleftrightarrow m^2 - 4 \equiv 0[5]$

$\Longleftrightarrow 5 \mid (m-2)(m+2)$

$\Longleftrightarrow 5 \mid (m-2)$ ou $5 \mid (m+2)$ (car 5 est un nombre premier)

$\Longleftrightarrow m \equiv 2[5]$ ou $m \equiv 3[5]$

$\Longleftrightarrow m = 2 + 5k$ ou $m = 5k + 3 \quad (k \in \mathbb{N})$

2) a- On a : $n^2 + 1 \equiv 0[p]$

Donc : $n^2 \equiv -1[p]$

D'où : $(n^2)^{1+2k} \equiv (-1)^{1+2k}[p]$

par suite, $(n^2)^{1+2k} \equiv -1[p]$

b- On a : $n^2 + 1 \equiv 0[p] \Longleftrightarrow (\exists k \in \mathbb{N}) \quad n^2 + 1 = kp$

$\Longleftrightarrow (\exists k \in \mathbb{N}) \quad kp - n^2 = 1$

$\Longleftrightarrow (\exists k \in \mathbb{N}) \quad k \times p - n \times n = 1$

Donc : $p \wedge n = 1$ (d'après le théorème de Bezout)

Autre méthode :

On a : $n^2 \equiv -1[p]$, donc p ne divise pas n^2, par suite p ne divise pas n

et comme p est un nombre premier, alors $p \wedge n = 1$

c- On a : p est premier et $p \wedge n = 1$, donc d'après le théorème de Fermat on a :

$n^{p-1} \equiv 1[p]$

Et puisque : $p = 3 + 4k$

alors : $n^{3+4k-1} \equiv 1[p]$

par suite, $n^{2(1+2k)} \equiv 1[p]$

D'où : $(n^2)^{1+2k} \equiv 1[p]$

d- S'il existe un nombre entier naturel n tel que $n^2 + 1 \equiv 0[p]$

alors : $(n^2)^{1+2k} \equiv 1[p]$ et $(n^2)^{1+2k} \equiv -1[p]$

par suite, $1 \equiv -1[p]$

D'où : $2 \equiv 0[p]$

Donc : $p|2$ ce qui est faux car p est de la forme $(4k+3)$

Conclusion : Donc, il n'existe pas un nombre entier naturel n qui vérifie $n^2 + 1 \equiv 0[p]$

Remarque :

Un nombre premier est soit de la forme $(4k+1)$ ou de la forme $(4k+3)$

Dans la question 1), le nombre premier 5 est de la forme $(4k+1)$ et on a vu qu'il existe des entiers n tels que $n^2 + 1 \equiv 0[5]$

Exercice 6 Juillet 2011

Soit x un nombre entier naturel qui vérifie $10^x \equiv 2[19]$

1) a- Vérifier que $10^{x+1} \equiv 1[19]$

b- Montrer que $10^{18} \equiv 1[19]$

2) Soit d le plus grand diviseur commun des deux nombres 18 et $(x+1)$

a- Montrer que : $10^d \equiv 1[19]$

b- Montrer que : $d = 18$

c- En déduire que : $x \equiv 17[18]$

Solution

1) a- On a : $10^x \equiv 2[19]$

Donc : $10 \times 10^x \equiv 10 \times 2[19]$

c'est-à-dire : $10^{x+1} \equiv 20[19]$

Et puisque : $20 \equiv 1[19]$

alors : $10^{x+1} \equiv 1[19]$

b- On a : $10 \wedge 19 = 1$ et 19 est un nombre premier

Donc d'après le théorème de Fermat on a : $10^{19-1} \equiv 1[19]$

par suite, $10^{18} \equiv 1[19]$

2) a- On a : $(x+1) \wedge 18 = d$

Donc : $(\exists(u,v) \in \mathbb{Z}^2) \quad (x+1)u + 18v = d$

Et puisque les nombres $(x+1)$ et 18 sont positifs

et d est leur plus grand diviseur commun

alors u et v ont des signes contraires

1er cas : $u \geq 0$ et $v \leq 0$ c'est-à-dire $u \geqslant 0$ et $-v \geqslant 0$

On a : $10^{(x+1)u} = 10^{d-18v} = 10^d \times (10^{18})^{-v}$

Donc : $10^{(x+1)u} \equiv 10^d \times 1[19]$

Et puisque : $10^{(x+1)u} \equiv 1[19]$

alors : $10^d \equiv 1[19]$

2ème cas : $u \leq 0$ et $v \geq 0$

En utilisant la même méthode, on montre que : $10^d \equiv 1[19]$

b- On a : $10^d \equiv 1[19]$ et d est un diviseur de 18

donc : $d = 1$ ou $d = 2$ ou $d = 3$ ou $d = 6$ ou $d = 9$ ou $d = 18$

et on a :

$10^1 \equiv 10[19]$ et $10^2 \equiv 5[19]$ et $10^3 \equiv 12[19]$ et $10^6 \equiv 11[19]$ et $10^9 \equiv 18[19]$

donc : $d = 18$

c- On a : 18 divise $(x+1)$

Donc : $x + 1 \equiv 0[18]$ c'est-à-dire : $x \equiv -1[18]$

Et puisque : $-1 \equiv 17[18]$

alors : $x \equiv 17[18]$

Exercice 7 Juin 2011

Soit N le nombre entier naturel dont l'écriture dans le système décimal est :

$N = \underbrace{111\cdots11}_{2010\ uns}$

1) Montrer que le nombre N est divisible par 11

2) a- Vérifier que le nombre 2011 est premier et que: $10^{2010} - 1 = 9N$

b- Montrer que le nombre 2011 divise le nombre $9N$

c- En déduire que le nombre 2011 divise le nombre N

3) Montrer que le nombre N est divisible par 22121

Solution

1) On a : $N = \underbrace{111\cdots11}_{2010\ uns}$

$$= 11 + 11 \times 10^2 + 11 \times 10^4 + \cdots + 11 \times 10^{2008}$$

$$= 11 \times (1 + 10^2 + 10^4 + \cdots + 10^{2006} + 10^{2008})$$

Donc le nombre N est divisible par 11

Autre méthode : Utiliser le critère de divisibilité par 11

On a : $\underbrace{(1-1)+(1-1)+\cdots+(1-1)}_{1005 \text{ fois } (1-1)} = 0$

donc le nombre N est divisible par 11

2) a- • On a : $\sqrt{2011} \simeq 44,8$ et les nombres premiers positifs inférieurs à $\sqrt{2011}$ sont $2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41$ et 43

Et puisque 2011 n'est divisible par aucun de ces nombres

Alors le nombre 2011 est premier

• On a : $N = 1 + 10 + 10^2 + \cdots + 10^{2009}$ (somme des termes consécutifs d'une suite géométrique de raison 10)

$$= 1 \times \frac{10^{2010}-1}{10-1}$$

$$= \frac{10^{2010}-1}{9}$$

Donc : $9N = 10^{2010} - 1$

b- On a : 2011 est premier et $2011 \wedge 10 = 1$

Donc : $10^{2010} \equiv 1[2011]$ (d'après le théorème de Fermat)

par suite, $10^{2010} - 1 \equiv 0[2011]$

D'où : 2011 divise $(10^{2010} - 1)$

c'est-à-dire 2011 divise $9N$

c- On a : $2011 | 9N$ et $2011 \wedge 9 = 1$ (car 2011 est premier)

Donc : 2011 divise N (d'après le théorème de Gauss)

3) On remarque que $22121 = 2011 \times 11$

On a : $11 | N$ et $2011 | N$ et $2011 \wedge 11 = 1$

Donc : $11 \times 2011 | N$

par suite, 22121 divise N

Exercice 8

On considère dans $\mathbb{Z}^2$ l'équation $(E) : 3x^2 + 3x + 7 = y^3$

1) Montrer que l'équation $x^2 + x + \overline{2} = \overline{0}$ n'admet pas de solution dans $\mathbb{Z}/3\mathbb{Z}$

2) Soit (a, b) une solution de l'équation (E)

Montrer qu'il existe un entier k tel que : $b = 3k + 1$ et que : $a^2 + a + 2 \equiv 0[3]$

3) Résoudre dans $\mathbb{Z}^2$ l'équation (E)

Solution

1) Le tableau suivant donne la valeur de $x^2 + x + \overline{2}$ dans $\mathbb{Z}/3\mathbb{Z}$:

x	$\overline{0}$	$\overline{1}$	$\overline{2}$
x^2	$\overline{0}$	$\overline{1}$	$\overline{1}$
$x^2 + x + \overline{2}$	$\overline{2}$	$\overline{1}$	$\overline{2}$

donc : $\left(\forall x \in \mathbb{Z}/3\mathbb{Z}\right) \quad x^2 + x + \overline{2} \neq \overline{0}$

par suite, l'équation $x^2 + x + \overline{2} = \overline{0}$ n'admet pas de solution dans $\mathbb{Z}/3\mathbb{Z}$

2) • Soit (a,b) une solution de l'équation (E)

donc: $3a^2 + 3a + 7 = b^3$

par suite, $b^3 \equiv 1[3]$ c'est-à-dire $3\,|\,(b-1)(b^2+b+1)$

et comme 3 est un nombre premier, donc: $3\,|\,b-1$ ou $3\,|\,b^2+b+1$

c'est-à-dire : $b-1 \equiv 0[3]$ ou $b^2+b+1 \equiv 0[3]$

c'est-à-dire : $b \equiv 1[3]$ ou $b^2+b-2 \equiv 0[3]$

c'est-à-dire : $b \equiv 1[3]$ ou $(b-1)(b+2) \equiv 0[3]$

donc: $b \equiv 1[3]$ ou $b-1 \equiv 0[3]$ ou $b+2 \equiv 0[3]$ (car 3 est un nombre premier)

c'est-à-dire : $b \equiv 1[3]$

d'où : $(\exists k \in \mathbb{Z}) \quad b = 3k+1$

• On a : $3a^2 + 3a + 7 = b^3$, c'est-à-dire : $3a^2 + 3a + 6 = (b-1)(b^2+b+1)$

donc : $3(a^2+a+2) = 3k(b^2+b+1)$

par suite, $a^2+a+2 = k(b^2+b+1)$

or : $b \equiv 1[3]$, donc: $b^2+b+1 \equiv 0[3]$

par suite, $a^2+a+2 \equiv 0[3]$

3) D'après le résultat de la question 2), si (a,b) est une solution de l'équation (E)

alors : $a^2+a+2 \equiv 0[3]$

or d'après le résultat de la question 1), l'équation $x^2+x+2 \equiv 0[3]$ n'admet pas de solution

donc l'équation (E) n'admet pas de solution dans $\mathbb{Z}^2$

Exercice 9

1) Soit $n \in \mathbb{N}^*$, montrer que : $(2n+1) \wedge n^2 = 1$

2) Déterminer l'ensemble des entiers n de $\mathbb{N}^*$ tels que $(2n+1) \wedge 5 = 5$

3) Soient a, b, c et d des entiers relatifs non nuls

a- Montrer que : si $a \wedge c = 1$ et $d\,|\,c$ alors $a \wedge d = 1$

b- Montrer que : si $a \wedge c = 1$ alors $ab \wedge c = b \wedge c$

4) a- Montrer que : $(\forall n \in \mathbb{N}^*) \quad n^2(n^2+1) \wedge (2n+1) = (2n+1) \wedge 5$

b- En déduire l'ensemble des entiers naturels non nuls n pour lesquels le nombre $\dfrac{n^2(n^2+1)}{2n+1}$ est irréductible.

Solution

1) Soit $n \in \mathbb{N}^*$, posons $d = (2n+1) \wedge n^2$

On a : $d\,|\,(2n+1)$ et $d\,|\,n^2$

donc : $d\,|\,n(2n+1) - 2n^2$ c'est-à-dire : $d\,|\,n$

par suite, $d|(2n+1)-2n$ c'est-à-dire : $d|1$

donc : $d=1$

c'est-à-dire : $(2n+1)\wedge n^2=1$

Autre méthode :

On a : $4n^2-(2n+1)(2n-1)=1$

Donc d'après le théorème de Bezout : $n^2\wedge(2n+1)=1$

2) Soit $n\in\mathbb{N}^*$, on a :

$$(2n+1)\wedge 5=5 \Leftrightarrow 5|(2n+1)$$
$$\Leftrightarrow 2n+1\equiv 0[5]$$
$$\Leftrightarrow 2n\equiv 4[5]$$
$$\Leftrightarrow n\equiv 2[5] \text{ (car } 2\wedge 5=1)$$

Donc l'ensemble des entiers n de $\mathbb{N}^*$ pour lesquels $(2n+1)\wedge 5=5$ est $E=\{5k+2/k\in\mathbb{N}\}$

3) a- Supposons que : $a\wedge c=1$ et $d|c$

On a : $a\wedge c=1$, donc : $(\exists(u,v)\in\mathbb{Z}^2)\quad au+cv=1$

et puisque $d|c$, alors $(\exists k\in\mathbb{Z}^*)\quad c=kd$

donc : $au+d(kv)=1$

par suite, d'après le théorème de Bezout : $a\wedge d=1$

b- Supposons que : $a\wedge c=1$

posons : $d=ab\wedge c$ et $d'=b\wedge c$

• On a : $d|ab$ et $d|c$

or : $a\wedge c=1$ et $d|c$

Donc : $a\wedge d=1$ (d'après **3) a-**)

et puisque $d|ab$ alors : $d|b$ (d'après le théorème de Gauss)

On a : $d|b$ et $d|c$, donc : $d|(b\wedge c)$ c'est-à-dire $d|d'$

• On a : $d'|b$ et $d'|c$

donc : $d'|ab$ et $d'|c$

et par suite, $d'|(ab\wedge c)$ c'est-à-dire : $d'|d$

• On a : $d|d'$ et $d'|d$, donc $d=d'$

Conclusion : si $a\wedge c=1$ alors $ab\wedge c=b\wedge c$

4) a- Soit $n\in\mathbb{N}^*$

Ona: $n^2(n^2+1)\wedge(2n+1)=(n^2+1)\wedge(2n+1)$ (d'après **3) b-**) car $(2n+1)\wedge n^2=1$)

Et en posant : $\alpha=(n^2+1)\wedge(2n+1)$ et $\beta=(2n+1)\wedge 5$, montrer que : $\alpha|\beta$ et $\beta|\alpha$, donc : $\alpha=\beta$

D'où : $(n^2+1)\wedge(2n+1)=(2n+1)\wedge 5$

et par suite, $n^2(n^2+1)\wedge(2n+1)=(2n+1)\wedge 5$

b- Soit $n\in\mathbb{N}^*$, on a :

$\left(\dfrac{n^2(n^2+1)}{2n+1}\right.$ irréductible) $\Leftrightarrow n^2(n^2+1)\wedge(2n+1)=1$

$\Leftrightarrow (2n+1)\wedge 5 = 1$

$\Leftrightarrow (2n+1)\wedge 5 \neq 5$

$\Leftrightarrow n \not\equiv 2[5]$ $\quad (2n+1\equiv 0[5] \Leftrightarrow n\equiv 2[5])$

$\Leftrightarrow n \notin E$ $\quad (E=\{5k+2/k\in\mathbb{N}\})$

Exercice 10

Soient a et b deux nombres entiers naturels non nuls vérifiant $a^2 = 2b^2+1$

1) Montrer que : $a\wedge b = 1$

2) Montrer que : $(a-1)\wedge(a+1)=2$

3) En déduire que l'un des deux nombres $(a-1)$ ou $(a+1)$ n'est pas divisible par 4

4) On suppose que $(a-1)$ n'est pas divisible par 4

a- Montrer que les nombres $\left(\dfrac{a-1}{2}\right)$ et $(a+1)$ sont premiers entre eux

b- En déduire que $\sqrt{\dfrac{a-1}{2}}$ et $\sqrt{a+1}$ sont des nombres entiers qui divisent le nombre b

Solution

1) On a : $a^2 = 2b^2+1$, Donc : $a\times a + (-2b)\times b = 1$

Et d'après le théorème de Bezout, on a : $a\wedge b = 1$

2) On a : $a^2 = 2b^2+1$, Donc : $a^2-1 = 2b^2$

c'est-à-dire : $(a-1)(a+1) = 2b^2$

On pose : $d=(a-1)\wedge(a+1)$

D'où : $d\,|\,(a+1)-(a-1)$ c'est-à-dire : $d\,|\,2$

par suite, $d=1$ ou $d=2$

Et puisque : $(a-1)(a+1)=2b^2$, alors $(a-1)(a+1)$ est un nombre pair

par suite, $(a-1)$ et $(a+1)$ sont tous les deux pairs ou l'un d'eux est pair et l'autre est impair

Et puisque : $(a-1)+(a+1)=2a$

alors : $(a-1)$ et $(a+1)$ ont la même parité

par suite, $(a-1)$ et $(a+1)$ sont pairs

D'où : $d=2$ c'est-à-dire : $(a-1)\wedge(a+1)=2$

3) Si les deux nombres $(a-1)$ et $(a+1)$ sont divisibles par 4

alors : $(a-1)\wedge(a+1)\geq 4$, Et ceci contredit le fait que $(a-1)\wedge(a+1)=2$

Donc l'un des deux nombres $(a-1)$ ou $(a+1)$ n'est pas divisible par 4

4) On suppose que $(a-1)$ n'est pas divisible par 4

a- Le nombre $(a-1)$ est pair et n'est pas divisible par 4

Donc : $(\exists k \in \mathbb{N}) \quad a-1=2(2k+1)$
par suite : $a+1=2(2k+1)+2=4(k+1)$
D'où : $\left(\frac{a-1}{2}\right)\wedge(a+1)=(2k+1)\wedge 4(k+1)$
Et puisque : $(2k+1)\wedge 4=1$ (car $2k+1$ est un nombre impair)
et : $(2k+1)\wedge(k+1)=1$ (car $2(k+1)-(2k+1)=1$)
alors : $(2k+1)\wedge 4(k+1)=1$ c'est-à-dire : $\left(\frac{a-1}{2}\right)\wedge(a+1)=1$

b- On a : $\left(\frac{a-1}{2}\right)(a+1)=b^2$
On pose : $x=\frac{a-1}{2}$ et $y=a+1$
On a : $xy=b^2$ et $x\wedge y=1$
On pose : $x\wedge b=\alpha$
Donc il existe x' et b' de $\mathbb{N}$ tels que : $x=\alpha x'$ et $b=\alpha b'$ et $x'\wedge b'=1$
On a : $\alpha x'y=(\alpha b')^2$ c'est-à-dire : $x'y=\alpha b'^2$
Donc : $\alpha \mid x'y$ et $x' \mid \alpha b'^2$
Et puisque : $\alpha\wedge y=1$ (car $\alpha \mid x$ et $x\wedge y=1$) et $x'\wedge b'^2=1$
alors : $\alpha \mid x'$ et $x' \mid \alpha$
D'où : $\alpha=x'$
Donc : $\alpha y=\alpha b'^2$, D'où : $y=b'^2$ et $x=\alpha x'=\alpha^2$
par suite, x et y sont deux carrés parfaits
Et puisque : $xy=b^2$ alors : $\sqrt{x}.\sqrt{y}=b$
c'est-à-dire : $\sqrt{\frac{a-1}{2}}.\sqrt{a+1}=b$
Donc $\sqrt{\frac{a-1}{2}}$ et $\sqrt{a+1}$ sont deux nombres entiers qui divisent b

Exercice 11

Soient p et q deux nombres premiers positifs et distincts
1) Montrer que : $q^{p-1}\equiv 1[p]$ et $p^{q-1}\equiv 1[q]$
2) Montrer que : $p^{q-1}+q^{p-1}\equiv 1[pq]$
3) Résoudre dans $\mathbb{Z}^2$ l'équation: $(71^{60}+61^{70})x+4330y\equiv x+y[4331]$

Solution

1) Les nombres p et q sont deux nombres premiers positifs distincts, donc $p\wedge q=1$
Et d'après le théorème de Fermat on a : $p^{q-1}\equiv 1[q]$ et $q^{p-1}\equiv 1[p]$
2) On a : $q^{p-1}\equiv 1[p]$ et $p^{q-1}\equiv 0[p]$
Donc : $p^{q-1}+q^{p-1}\equiv 1[p]$
et on a : $p^{q-1}\equiv 1[q]$ et $q^{p-1}\equiv 0[q]$

Donc : $p^{q-1}+q^{p-1}\equiv 1[q]$

par suite, $p|(p^{q-1}+q^{p-1}-1)$ et $q|(p^{q-1}+q^{p-1}-1)$

Et puisque : $p\wedge q=1$ alors : $pq|(p^{q-1}+q^{p-1}-1)$

par suite : $p^{q-1}+q^{p-1}\equiv 1[pq]$

3) On considère les deux nombres premiers distincts 61 et 71

D'après le résultat de la question précèdente on a : $71^{60}+61^{70}\equiv 1[71\times 61]$

c'est-à-dire : $71^{60}+61^{70}\equiv 1[4331]$

par suite, $(71^{60}+61^{70})x+4330y\equiv x+y[4331]\Leftrightarrow x+4330y\equiv x+y[4331]$

$$\Leftrightarrow 4329y\equiv 0[4331]$$

Et puisque : $4331\wedge 4329=1$

(car $4331=71\times 61$ et 71 et 61 ne divisent pas 4329)

alors l'équation proposée est équivalente à l'équation $y\equiv 0[4331]$

c'est-à-dire : $y=4331k$ où $k\in\mathbb{Z}$

Conclusion : l'ensemble de solutions de l'équation est donc:

$$S=\{(x,4331k)/(x,k)\in\mathbb{Z}^2\}$$

Exercice 12

Pour tout entier naturel n, on pose $A_n=6n^2-3n-2$ et $B_n=2n+1$ et on considère dans $\mathbb{Z}^2$ l'équation $(E_n): A_nx+B_ny=1$

1) a- Montrer que l'équation (E_n) admet au moins une solution dans $\mathbb{Z}^2$

b- Résoudre dans $\mathbb{Z}^2$ l'équation (E_n)

2) Montrer que 113 est un nombre premier

3) a- Montrer que : $A_n-B_n\equiv 113[n+4]$

b- Déterminer les entiers naturels n tels que $(n+4)$ divise (A_n-B_n)

Solution

1) a- Soit $n\in\mathbb{N}$

On a : $6n^2-3n-2=(2n+1)(3n-3)+1$

Donc : $A_n-(3n-3)B_n=1$

par suite, d'après le théorème de Bezout : $A_n\wedge B_n=1$

Donc l'équation (E_n) admet au moins une solution dans $\mathbb{Z}^2$ (une solution particulière de (E_n) est $(1,3-3n)$)

b- Soit $n\in\mathbb{N}$

On a : $(E_n) \Leftrightarrow A_n x + B_n y = A_n - (3n-3)B_n$

$$\Leftrightarrow A_n(x-1) = (3-3n-y)B_n$$

$$\Leftrightarrow \begin{cases} A_n(x-1) = (3-3n-y)B_n \\ B_n | A_n(x-1) \end{cases}$$

$$\Leftrightarrow \begin{cases} A_n(x-1) = (3-3n-y)B_n \\ B_n | (x-1) \qquad (car\ A_n \wedge B_n = 1) \end{cases}$$

$$\Leftrightarrow \begin{cases} A_n k B_n = (3-3n-y)B_n \\ x-1 = kB_n \ \ (k \in \mathbb{Z}) \end{cases}$$

$$\Leftrightarrow \begin{cases} x = 1 + kB_n \\ y = 3 - 3n - kA_n \end{cases} \quad (k \in \mathbb{Z})$$

Donc : $S = \{(1+kB_n, 3-3n-kA_n) / k \in \mathbb{Z}\}$

2) On a : $\sqrt{113} \simeq 10,63$

Les nombres premiers positifs inférieurs à $\sqrt{113}$ sont 2; 3; 5 et 7

Aucun de ces nombres ne divise 113

Donc 113 est un nombre premier

3) a- Soit $n \in \mathbb{N}$

On a : $A_n - B_n - 113 = (6n^2 - 3n - 2) - (2n+1) - 113$

$$= 6n^2 - 5n - 116$$

$$= (n+4)(6n-29)$$

donc : $(n+4)$ divise $(A_n - B_n - 113)$

par suite, $A_n - B_n \equiv 113[n+4]$

b- Soit $n \in \mathbb{N}$

On a : $(n+4)|(A_n - B_n) \Leftrightarrow A_n - B_n \equiv 0[n+4]$

$$\Leftrightarrow 113 \equiv 0[n+4]$$

$$\Leftrightarrow (n+4)|113$$

$$\Leftrightarrow n+4 = 1 \text{ ou } n+4 = 113$$

$$\Leftrightarrow n = 109$$

Exercice 13 juillet 2005

1) On considère dans $\mathbb{Z}^2$ l'équation $(E):(x+1)^2 = 9 + 5y$

a- Soit (x,y) une solution de l'équation (E)

Montrer que : $x \equiv 1[5]$ ou $x \equiv 2[5]$

b- Résoudre dans $\mathbb{Z}^2$ l'équation (E)

2) Montrer que : $(\forall k \in \mathbb{Z}) \ \ (5k^2 + 4k - 1) \wedge (5k+1) = (k-3) \wedge 8$

3) Résoudre dans $\mathbb{N}^2$ le système : $\begin{cases} \overline{121}^{(x)} = \overline{59}^{(y)} \\ x \wedge y = 8 \\ x \equiv 1[5] \end{cases}$

Solution

1) a- Soit (x,y) une solution de l'équation (E) dans $\mathbb{Z}^2$

On a : $(x+1)^2 = 9+5y$

Donc : $(x+1)^2 - 9 = 5y$ c'est-à-dire : $(x+1-3)(x+1+3) = 5y$

c'est-à-dire : $(x-2)(x+4) = 5y$, Donc 5 divise $(x-2)(x+4)$

et puisque 5 est un nombre premier alors: $5|(x-2)$ ou $5|(x+4)$

par suite, $x-2 \equiv 0[5]$ ou $x+4 \equiv 0[5]$

c'est-à-dire : $x \equiv 2[5]$ ou $x \equiv -4[5]$

c'est-à-dire : $x \equiv 2[5]$ ou $x \equiv 1[5]$

b- Soit (x,y) une solution de l'équation (E)

Donc : $x \equiv 1[5]$ ou $x \equiv 2[5]$ (d'après le résultat de la question précèdente)

• Si $x \equiv 1[5]$ alors $x = 5k+1 \quad (k \in \mathbb{Z})$

par suite, $9+5y = (5k+2)^2$

D'où : $y = 5k^2+4k-1$

• Si $x \equiv 2[5]$ alors $x = 5k+2 \quad (k \in \mathbb{Z})$

par suite, $9+5y = (5k+3)^2$

D'où : $y = 5k^2+6k$

• Réciproquement, vérifier que pour tout k de $\mathbb{Z}$, les couples $(5k+1, 5k^2+4k-1)$ et $(5k+2, 5k^2+6k)$ sont des solutions de l'équation (E)

Conclusion : L'ensemble de solutions de l'équation (E) est :

$S = \{(5k+1, 5k^2+4k-1)/k \in \mathbb{Z}\} \cup \{(5k+2, 5k^2+6k)/k \in \mathbb{Z}\}$

2) On a : $(\forall k \in \mathbb{Z}) \quad 5k^2+4k-1 = k(5k+1)+(3k-1)$

D'où : $(5k^2+4k-1) \wedge (5k+1) = (5k+1) \wedge (3k-1)$

et on a : $5k+1 = 2(3k-1)-(k-3)$

D'où : $(5k+1) \wedge (3k-1) = (3k-1) \wedge (k-3)$

et on a : $3k-1 = 3(k-3)+8$

D'où : $(3k-1) \wedge (k-3) = (k-3) \wedge 8$

Conclusion : $(\forall k \in \mathbb{Z}) \quad (5k^2+4k-1) \wedge (5k+1) = (k-3) \wedge 8$

Remarque :

On a utilisé le résultat suivant :

Pour tout (a,b,q,α) de $\mathbb{Z}^4$, si $a = bq+\alpha$ alors : $a \wedge b = b \wedge \alpha$

Montrer ce résultat en posant $d = a \wedge b$ et $d' = b \wedge \alpha$

3) Le système $\begin{cases} \overline{121}^{(x)} = \overline{59}^{(y)} \\ x \wedge y = 8 \\ x \equiv 1[5] \end{cases}$ est équivalent au système $\begin{cases} x^2+2x+1 = 5y+9 \\ x \wedge y = 8 \\ x \equiv 1[5] \end{cases}$

On a vu que si $x \equiv 1[5]$ alors les solutions de l'équation $x^2+2x+1 = 5y+9$ sont $(5k+1, 5k^2+4k-1)$ où $k \in \mathbb{Z}$

Et on a vu aussi que : $(5k^2+4k-1) \wedge (5k+1) = (k-3) \wedge 8$

Donc : $x \wedge y = 8 \Leftrightarrow (k-3) \wedge 8 = 8$

$$\Leftrightarrow 8 | (k-3)$$

$$\Leftrightarrow k = 3 + 8\alpha \qquad (\alpha \in \mathbb{N})$$

$$\Leftrightarrow \begin{cases} x = 40\alpha + 16 \\ y = 320\alpha^2 + 272\alpha + 56 \end{cases} \qquad (\alpha \in \mathbb{N})$$

Conclusion :

L'ensemble de solutions du système proposé est:

$$\{(40\alpha + 16, 320\alpha^2 + 272\alpha + 56) / \alpha \in \mathbb{N}\}$$

Exercice 14

Soit n un élément de $\mathbb{N}^*$

On pose: $b_n = 2.10^n + 1$ et $c_n = 2.10^n - 1$

1) Montrer que: $b_n \wedge c_n = c_n \wedge 2$

2) En déduire que $b_n \wedge c_n = 1$

3) Trouver un couple (x_n, y_n) de $\mathbb{Z}^2$ vérifiant: $b_n x_n + c_n y_n = 1$

Solution

1) • On pose: $d = b_n \wedge c_n$ et $d' = c_n \wedge 2$

On a: $d | b_n$ et $d | c_n$

Donc: $d | b_n - c_n$ c'est-à-dire: $d | 2$

par suite: $d | c_n \wedge 2$ c'est-à-dire: $d | d'$

• On a: $d' | c_n$ et $d' | 2$

Donc: $d' | (b_n - c_n) + c_n$ (car $b_n - c_n = 2$), c'est-à-dire: $d' | b_n$

D'où: $d' | b_n \wedge c_n$ c'est-à-dire: $d' | d$

Conclusion: On a: $d | d'$ et $d' | d$ donc: $d = d'$ (d et d' sont deux entiers naturels)

D'où: $b_n \wedge c_n = c_n \wedge 2$

2ème méthode:

On a: $b_n = c_n + 2$ et 2 est le reste de la division euclidienne de b_n par c_n

(car $0 \leq 2 < c_n$)

Donc: $b_n \wedge c_n = c_n \wedge 2$

2) On a: $c_n = 2.10^n - 1$, Donc c_n est un nombre impair

D'où: $c_n \wedge 2 = 1$

Et puisque: $c_n \wedge 2 = b_n \wedge c_n$ (d'après le résultat de la question précèdente)

alors: $b_n \wedge c_n = 1$

3) On a: $c_n = 2(10^n - 1) + 1$

Donc: $c_n = (b_n - c_n)(10^n - 1) + 1$ (car $2 = b_n - c_n$)

c'est-à-dire: $c_n - b_n(10^n - 1) + c_n(10^n - 1) = 1$

D'où: $b_n(1-10^n)+c_n.10^n=1$
par suite, le couple $(x_n, y_n)=(1-10^n, 10^n)$ vérifie $b_nx_n+c_ny_n=1$

Exercice 15 juillet 2007

On considère dans $\mathbb{Z}$ le système (S) suivant: $\begin{cases} x\equiv a[p] \\ x\equiv b[q] \end{cases}$

où a,b,p et q sont des entiers relatifs et $p\wedge q=1$

1) a- Montrer qu'il existe un couple (u_0,v_0) de $\mathbb{Z}^2$ tel que: $pu_0+qv_0=1$

b- Montrer que le nombre $x_0=bpu_0+aqv_0$ est une solution du système (S)

2) Soit x une solution du système (S) , montrer que le nombre pq divise le nombre $(x-x_0)$

3) Soit x un nombre entier relatif tel que pq divise $(x-x_0)$

Montrer que x est une solution du système (S)

4) En déduire l'ensemble de solutions du système (S)

5) Résoudre dans $\mathbb{Z}$ le système $\begin{cases} x\equiv 1[8] \\ x\equiv 3[13] \end{cases}$

Solution

1) a- On a: $p\wedge q=1$

Donc, d'après le théorème de Bezout, il existe un couple (u_0,v_0) de $\mathbb{Z}^2$ tel que: $pu_0+qv_0=1$

b- • On a: $x_0-a=bpu_0+aqv_0-a$

$$=bpu_0+a(qv_o-1)$$
$$=bpu_o-apu_o$$
$$=p(bu_o-au_o)$$

Donc: $p|(x_0-a)$, et par suite $x_0\equiv a[p]$

• on a: $x_0-b=bpu_0+aqv_0-b$

$$=b(pu_0-1)+aqv_o$$
$$=-bqv_o+aqv_o$$
$$=q(av_o-bv_o)$$

Donc: $q|(x_0-b)$, et par suite: $x_0\equiv b[q]$

De ce qui précède, on déduit que x_0 est une solution du système (S)

2) Soit x une solution du système (S)

Donc: $\begin{cases} x\equiv a[p] \\ x\equiv b[q] \end{cases}$

Et puisque x_0 est une solution du système (S) alors: $\begin{cases} x_0 \equiv a\,[p] \\ x_0 \equiv b\,[q] \end{cases}$

par suite: $\begin{cases} x \equiv x_0\,[p] \\ x \equiv x_0\,[q] \end{cases}$

D'où: $p|(x - x_0)$ et $q|(x - x_0)$

Et puisque: $p \wedge q = 1$ alors : $pq|(x - x_0)$

Conclusion: Si x est une solution de (S) alors: $pq|(x - x_0)$

3) On suppose que $pq|(x - x_0)$, donc: $(\exists k \in \mathbb{Z})\ x - x_0 = k\,pq$

D'où: $x = x_0 + kpq$

Et puisque: $pqk \equiv 0[p]$ et $pqk \equiv 0\,[q]$

alors: $x \equiv x_0\,[p]$ et $x \equiv x_0\,[q]$

Et puisque : $x_0 \equiv a[p]$ et $x_0 \equiv b\,[q]$

alors: $x \equiv a[p]$ et $x \equiv b\,[q]$

par suite, x est une solution du système (S)

Conclusion: Si $pq|(x - x_0)$ alors x est une solution de (S)

4) Soit S' l'ensemble de solutions du système (S)

D'après les résultats des questions (2) et (3) on a:

$$x \in S' \Leftrightarrow pq|(x - x_0)$$
$$\Leftrightarrow (\exists k \in \mathbb{Z})\ x = x_0 + kpq$$

Donc: $S' = \{x_0 + kpq \,/\, k \in \mathbb{Z}\}$

5) Puisque $8 \wedge 13 = 1$, alors d'après le résultat de la dernière question, l'ensemble de solutions du système $\begin{cases} x \equiv 1\,[8] \\ x \equiv 3\ [13] \end{cases}$ est $S' = \{x_0 + 104k/k \in \mathbb{Z}\}$

Et puisque: $5 \times 8 - 3 \times 13 = 1$ alors on peut prendre : $u_0 = 5$ et $v_0 = -3$

Par suite: $x_0 = bpu_0 + aqv_0$

$$= 3 \times 8 \times 5 + 1 \times 13 \times (-3) = 81$$

Conclusion: $S' = \{81 + 104k \,/\, k \in \mathbb{Z}\}$

Exercice 16 juin 2014

Soit $n \in \mathbb{N}^*$, on pose: $a_n = \underbrace{333...3}_{n\ fois}1$ (n fois le chiffre 3)

1) Vérifier que les deux nombres a_1 et a_2 sont premiers.

2) Montrer que pour tout n de $\mathbb{N}^*$: $3a_n + 7 = 10^{n+1}$

3) Montrer que pour tout k de $\mathbb{N}$: $10^{30k+2} \equiv 7[31]$

4) Montrer que pour tout k de $\mathbb{N}$: $3a_{30k+1} \equiv 0\,[31]$, puis en déduire que 31 divise a_{30k+1}

5) Montrer que pour tout n de $\mathbb{N}$, si $n \equiv 1\ [30]$ alors l'équation $a_n x + 31y = 1$ n'admet pas de solutions dans $\mathbb{N}^2$

Solution

1) • On a: $a_1 = 31$ et 31 est un nombre premier

• On a: $a_2 = 331$ et $\sqrt{331} \simeq 18,2$

Les nombres premiers positifs inférieurs à $\sqrt{331}$ sont $2, 3, 5, 7, 11, 13$ et 17

Et puisque chacun de ces nombres ne divise pas 331

alors 331 est un nombre premier.

Conclusion: a_1 et a_2 sont des nombres premiers

2) Soit n un élément de $\mathbb{N}^*$

On a: $3a_n + 7 = \underbrace{999...9}_{n \text{ fois neuf}}3 + 7$

$= 1\underbrace{00...00}_{(n+1) \text{ fois zéros}}$

Donc: $3a_n + 7 = 10^{n+1}$

3) • On a: 31 est un nombre premier et 31 ne divise pas 10

Donc: $10^{30} \equiv 1\ [31]$ (d'après le théorème de Fermat)

• Soit $k \in \mathbb{N}$

on a : $10^{30k} \equiv 1\ [31]$, donc $10^{30k} \times 10^2 \equiv 10^2 [31]$

et puisque $10^2 \equiv 7[31]$, alors: $(\forall k \in \mathbb{N})\ 10^{30k+2} \equiv 7\ [31]$

4) Soit k un élément de $\mathbb{N}$

• On a: $3a_{30k+1} + 7 = 10^{30k+2}$ (d'après le résultat de la question 2)

et on a : $10^{30k+2} \equiv 7\ [31]$ (d'après le résultat de la question 3)

Donc: $3a_{30k+1} + 7 \equiv 7\ \ [31]$

par suite: $3a_{30k+1} \equiv 0\ \ [31]$

• On a: 31 divise $3a_{30k+1}$ et $31 \wedge 3 = 1$

Donc : 31 divise a_{30k+1} (d'après le théorème de Gauss)

5) Soit n un élément de $\mathbb{N}$ tel que: $n \equiv 1\ [30]$

Donc: $(\exists k \in \mathbb{N}) n = 30k + 1$, par suite : $a_n \equiv 0\ [31]$

(d'après le résultat de la question précèdente)

si $a_n x + 31y = 1$ admet une solution (x, y) alors $31 | a_n$ et donc $31 | a_n x$

Et puisque : $31 | 31y$ alors: $31 | a_n x + 31y$

par suite: $31 | 1$, ce qui est faux

Donc pour tout n de $\mathbb{N}$, si $n \equiv 1[30]$ alors l'équation $a_n x + 31y = 1$ n'admet pas de solution dans $\mathbb{N}^2$

Exercice 17

1) Montrer que le nombre 2017 est premier

2) Soit a un nombre entier relatif tel que $a^5 \equiv -1[2017]$

a- Montrer que $a^{2016} \equiv 1[2017]$

b- Montrer que $a^{2015} \equiv -1[2017]$ puis en déduire que $a \equiv 2016[2017]$

3) Résoudre dans $\mathbb{Z}$ l'équation : $x^5 \equiv -1[2017]$

Solution

1) On a: $\sqrt{2017} \simeq 44,91$

Les nombres premiers positifs inférieurs à $\sqrt{2017}$ sont :

$2;3;5;7;11;13;17;19;23;29;31;37;41$ et 43

Aucun de ces nombres ne divise 2017

Donc 2017 est un nombre premier.

2) a- On a: $a^5 \equiv -1[2017]$

donc 2017 ne divise pas a

et puisque 2017 est un nombre premier

alors , d'après le théorème de Fermat: $a^{2017-1} \equiv 1[2017]$

C'est-à-dire: $a^{2016} \equiv 1[2017]$

b- • On a: $a^5 \equiv -1[2017]$

donc: $(a^5)^{403} \equiv (-1)^{403}[2017]$ c'est-à-dire: $a^{2015} \equiv -1[2017]$

• On a: $a^{2016} \equiv 1[2017]$ c'est-à-dire: $a^{2015} \times a \equiv 1[2017]$

Or: $a^{2015} \equiv -1[2017]$, donc : $-a \equiv 1[2017]$

D'où: $a \equiv -1[2017]$, donc: $a \equiv -1+2017[2017]$

c'est-à-dire: $a \equiv 2016[2017]$

3) D'après ce qui précède: $x^5 \equiv -1[2017] \Longrightarrow x \equiv 2016[2017]$

Réciproquement , si $x \equiv 2016[2017]$

alors: $x \equiv -1[2017]$, donc: $x^5 \equiv -1[2017]$

et par suite on a l'équivalence : $x^5 \equiv -1[2017] \Longleftrightarrow x \equiv 2016[2017]$

Donc: $S = \{2016 + 2017k \,/\, k \in \mathbb{Z}\}$

Exercice 18 juin 2017

On admet que le nombre 2017 est premier et que: $2016 = 2^5 \times 3^2 \times 7$

Soit p un nombre premier tel que $p \geq 5$

1) Soit le couple (x,y) de $\mathbb{N}^* \times \mathbb{N}^*$ tel que: $px + y^{p-1} = 2017$

a- Vérifier que: $p < 2017$

b- Montrer que p ne divise pas y

c- Montrer que $y^{p-1} \equiv 1[p]$ et en déduire que p divise 2016

d- Montrer que: $p = 7$

2) Déterminer, suivant les valeurs de p , les couples (x,y) de $\mathbb{N}^* \times \mathbb{N}^*$ vérifiant: $px + y^{p-1} = 2017$

Solution

1) a- Soit (x,y) un élément de $(\mathbb{N}^*)^2$ tel que: $px+y^{p-1}=2017$

On a : $px-2017=-y^{p-1}$ et $-y^{p-1}<0$

Donc: $px<2017$

et puisque $x\geqslant 1$ alors : $p\leqslant px$

par suite: $p<2017$

b- Montrons que p ne divise pas y

Supposons que: $p|y$

et puisque: $p|px$ alors: $p|px+y^{p-1}$

par suite: $p|2017$, ce qui est faux car 2017 est un nombre premier

Donc p ne divise pas y

c- • On a: p est premier et p ne divise pas y

Donc d'après le théorème de Fermat on a: $y^{p-1}\equiv 1[p]$

• On a: $px+y^{p-1}=2017$

Donc: $px+y^{p-1}\equiv 2017[p]$

par suite: $0+1\equiv 2017[p]$

D'où: $2016\equiv 0[p]$

Ce qui signifie que : p divise 2016

d- On a: p est premier et divise 2016 et $2016=2^5\times 3^2\times 7$

Donc: $p=2$ ou $p=3$ ou $p=7$

Et comme: $p\geq 5$ alors: $p=7$

2) Considèrons dans $(\mathbb{N}^*)^2$ l'équation (E): $px+y^{p-1}=2017$

où p est un nombre premier supérieur ou égal à 5

et soit S son ensemble de solutions.

D'après ce qui précède:

• Si $p\neq 7$ alors $S=\phi$

• Si $p=7$ alors: $(E)\Longleftrightarrow 7x+y^6=2017$

$$\Longleftrightarrow \begin{cases} y=1 \\ 7x=2016 \end{cases} \text{ ou } \begin{cases} y=2 \\ 7x=1953 \end{cases} \text{ ou } \begin{cases} y=3 \\ 7x=1288 \end{cases}$$

$$\Longleftrightarrow \begin{cases} y=1 \\ x=288 \end{cases} \text{ ou } \begin{cases} y=2 \\ x=279 \end{cases} \text{ ou } \begin{cases} y=3 \\ x=184 \end{cases}$$

Remarquons que : $3^6<2017$ et $4^6>2017$

Donc si $p=7$ alors: $S=\{(288,1),(279,2),(184,3)\}$

Exercice 19 Juin 2009

Pour tout $n\in\mathbb{N}^*$, on pose: $a_n=2^n+3^n+6^n-1$

1) a- Vérifier que a_n est pair pour tout $n\in\mathbb{N}^*$

b- Déterminer les valeurs de n pour lesquelles $a_n \equiv 0[3]$

2) Soit p un nombre premier tel que $p \geq 5$

a- Montrer que: $2^{p-1} \equiv 1[p]$, $3^{p-1} \equiv 1[p]$ et $6^{p-1} \equiv 1[p]$

b- Montrer que p divise a_{p-2}

3) Montrer que pour tout entier naturel premier q, il existe un entier naturel non nul n tel que: $a_n \wedge q = q$

Solution

1) a- Soit $n \in \mathbb{N}^*$, on a:

$2^n \equiv 0[2]$ et $6^n \equiv 0[2]$ et $3^n \equiv 1[2]$

donc : $a_n \equiv 0 + 1 + 0 - 1[2]$

C'est-à-dire: $a_n \equiv 0[2]$, donc: 2 divise a_n

par suite, a_n est un nombre pair pour tout $n \in \mathbb{N}^*$

b- Soit $n \in \mathbb{N}^*$, on a:

$$\begin{aligned} a_n \equiv 0[3] &\iff 2^n + 3^n + 6^n - 1 \equiv 0[3] \\ &\iff (-1)^n + 0 + 0 - 1 \equiv 0[3] \\ &\iff (-1)^n \equiv 1[3] \\ &\iff n \text{ est pair} \end{aligned}$$

Donc : $a_n \equiv 0[3]$ si et seulement si n est pair

2) a- p est un nombre premier positif différent de 2 et de 3

donc : $p \wedge 2 = 1$ et $p \wedge 3 = 1$

Alors, d'après le théorème de Fermat, $2^{p-1} \equiv 1[p]$ et $3^{p-1} \equiv 1[p]$

et comme : $6 = 2 \times 3$ donc $p \wedge 6 = 1$

par suite, on a aussi: $6^{p-1} \equiv 1[p]$

b- On a: $a_{p-2} = 2^{p-2} + 3^{p-2} + 6^{p-2} - 1$

donc: $6a_{p-2} = 3.2^{p-1} + 2.3^{p-1} + 6^{p-1} - 6$

et comme: $2^{p-1} \equiv 1[p]$ et $3^{p-1} \equiv 1[p]$ et $6^{p-1} \equiv 1[p]$

donc: $$\begin{aligned} 6a_{p-2} &\equiv 3 \times 1 + 2 \times 1 + 1 - 6[p] \\ &\equiv 0[p] \end{aligned}$$

par suite, p divise $6a_{p-2}$

et comme $p \wedge 6 = 1$ donc p divise a_{p-2}

3) Soit q un entier naturel premier

- Si $q = 2$, alors: $(\forall n \in \mathbb{N}^*)$ $a_n \wedge 2 = 2$

car tous les nombres a_n sont pairs (d'après **1) a-**)

- Si $q = 3$, alors $(\forall n \in 2\mathbb{N}^*)$ $a_n \wedge 3 = 3$

car tous les nombres a_n où n est pair sont des multiples de 3 (d'après **1) b-**)

- Si $q \geq 5$, alors $a_{q-2} \wedge q = q$ car q divise a_{q-2} (d'après **2) b-**)

Donc pour tout entier naturel premier q, il existe un entier naturel non nul n tel que $a_n \wedge q = q$

Exercice 20

On considère le nombre: $A = 101^{101} - 1$

1) Vérifier que 101 est un nombre premier et que 2 et 5 divisent A

2) Soit p un diviseur premier de A tel que $p \geq 7$ et soit a le plus petit entier naturel non nul qui vérifie: $101^a \equiv 1[p]$

a- Montrer que: $a \neq 1$

b- Montrer que si un nombre n de $\mathbb{N}$ vérifie $101^n \equiv 1[p]$ alors a divise n (on pourra considérer la division euclidienne de n par a)

c- Vérifier que: $101^{101} \equiv 1[p]$ et en déduire que: $a = 101$

d- Montrer que: $101^{p-1} \equiv 1[p]$ puis: $p \equiv 1[101]$

3) Vérifier que 811 est un nombre premier , est-il un diviseur de A ?

Solution

1) • Les nombres premiers positifs inférieurs à $\sqrt{101}$ sont: 2 ; 3 ; 5 et 7, et aucun de ces nombres ne divise 101

donc 101 est un nombre premier

• On a: $101 \equiv 1[2]$ et $101 \equiv 1[5]$, donc: $101^{101} \equiv 1[2]$ et $101^{101} \equiv 1[5]$

par suite, 2 et 5 divisent $A = 101^{101} - 1$,

2) a- Si $a = 1$ alors: $101 \equiv 1[p]$, donc: $p|100$

et puisque p est premier, alors $p = 2$ ou $p = 5$, ce qui est faux car $p \geq 7$

donc: $a \neq 1$

b- Soit $n \in \mathbb{N}$ tel que $101^n \equiv 1[p]$

On a, dans la division euclidienne de n par a : $n = qa + r$ où $q \in \mathbb{N}$

et $0 \leqslant r < a$

donc: $101^{qa+r} \equiv 1[p]$, c'est-à-dire: $(101^a)^q.101^r \equiv 1[p]$, donc: $101^r \equiv 1[p]$

car: $101^a \equiv 1[p]$

Si $r \neq 0$, alors: $101^r \equiv 1[p]$ et $r < a$

Cela contredit le fait que a est le plus petit entier naturel non nul tel que: $101^a \equiv 1[p]$

et par suite $r = 0$, donc: $n = qa$, d'où: a divise n

c- • Le nombre p divise A

donc: $101^{101} - 1 \equiv 0[p]$

d'où: $101^{101} \equiv 1[p]$

• Puisque: $101^{101} \equiv 1[p]$

donc d'après **2) b-** on a: a divise 101

et puisque 101 est premier et $a \neq 1$

Alors $a = 101$

d- • On a: $101^{101} \equiv 1[p]$

donc p ne divise pas 101

et comme p est premier, alors: $101^{p-1} \equiv 1[p]$ (d'après le théorème de Fermat)

• On a: $101^{p-1} \equiv 1[p]$

donc d'après 2) b): $a|(p-1)$

et puisque $a = 101$, alors: $p \equiv 1[101]$

3) • On a: $\sqrt{811} \simeq 28,48$

Les nombres premiers positifs inférieurs à $\sqrt{811}$ sont:

$2;3;5;7;11;13;17;19$ et 23, et aucun de ces nombres ne divise 811

Donc 811 est un nombre premier.

• Si 811 divise A

Alors , d'après le résultat de la question 2) : $811 \equiv 1[101]$

or: $811 \equiv 3[101]$, donc: $3 \equiv 1[101]$ ce qui est faux

par suite le nombre premier 811 n'est pas un diviseur de A

Exercice 21

1) Résoudre dans $\mathbb{Z}^2$ l'équation (E): $51x - 11y = 1$

2) Résoudre dans $\mathbb{Z}$ le système: $\begin{cases} 5x \equiv 7[11] \\ 2x \equiv 1[7] \end{cases}$

Solution

1) Déterminons une solution particulière de l'équation (E)

D'après l'algorithme d'Euclide on a:

$$51 = 4 \times 11 + 7$$
$$11 = 7 + 4$$
$$7 = 4 + 3$$
$$4 = 3 + 1$$

D'où: $1 = 4 - 3$

$$= 4 - (7 - 4)$$
$$= 2 \times 4 - 7$$
$$= 2 \times (11 - 7) - 7$$
$$= 2 \times 11 - 3 \times 7$$
$$= 2 \times 11 - 3 \times (51 - 4 \times 11)$$
$$= -3 \times 51 + 14 \times 11$$

par suite, $51 \times (-3) - 11 \times (-14) = 1$

Donc: $(E) \Leftrightarrow 51x - 11y = -3 \times 51 + 14 \times 11$

$\Leftrightarrow 51(x+3) = 11(y+14)$

$\Leftrightarrow \begin{cases} 51(x+3) = 11(y+14) \\ 11 | 51(x+3) \end{cases}$

$\Leftrightarrow 51(x+3) = 11(y+14)$ *et* $11 | (x+3)$ (*car* $51 \wedge 11 = 1$)

$\Leftrightarrow 51(x+3) = 11(y+14)$ *et* $x + 3 = 11k$ $(k \in \mathbb{Z})$

$\Leftrightarrow x = 11k - 3$ *et* $y = 51k - 14$ $(k \in \mathbb{Z})$

Conclusion:

L'ensemble de solutions de l'équation (E) est: $S = \{(11k - 3, 51k - 14) / k \in \mathbb{Z}\}$

2) On a:

$\begin{cases} 5x \equiv 7[11] \\ 2x \equiv 1[7] \end{cases} \Leftrightarrow \begin{cases} 5x \equiv 7[11] \\ 2x \equiv 8[7] \end{cases}$

$\Leftrightarrow \begin{cases} 5x \equiv 7[11] \\ x \equiv 4[7] \end{cases}$ (car $2 \wedge 7 = 1$)

$\Leftrightarrow \begin{cases} 5(7k+4) \equiv 7[11] \\ x = 7k + 4 \end{cases}$ $(k \in \mathbb{Z})$

$\Leftrightarrow \begin{cases} 2k \equiv 9[11] \\ x = 7k + 4 \end{cases}$ $(k \in \mathbb{Z})$

$\Leftrightarrow \begin{cases} 2k \equiv 20[11] \\ x = 7k + 4 \end{cases}$ $(k \in \mathbb{Z})$

$\Leftrightarrow \begin{cases} x = 7k + 4 \\ k \equiv 10[11] \end{cases}$ $(k \in \mathbb{Z})$ (car : $2 \wedge 11 = 1$)

$\Leftrightarrow \begin{cases} x = 7k + 4 \\ k \equiv 11\alpha + 10 \end{cases}$ $(\alpha \in \mathbb{Z})$

$\Leftrightarrow x = 77\alpha + 74 (\alpha \in \mathbb{Z})$

Donc l'ensemble de solutions du système $\begin{cases} 5x \equiv 7[11] \\ 2x \equiv 1[7] \end{cases}$ est $S = \{77\alpha + 74 / \alpha \in \mathbb{Z}\}$

Exercice 22

Soit p un nombre premier tel que $p \geq 3$

On pose: $A_p = \{1, 2, ..., p-1\}$

1) Soit a un élément de A_p

a- Montrer que a^{p-2} est une solution de l'équation $ax \equiv 1[p]$

b- Soit r le reste de la division euclidienne de a^{p-2} par p

Montrer que r est la solution unique de l'équation $ax \equiv 1[p]$ dans A_p

2) a- Résoudre dans A_{71} l'équation $3x \equiv 1[71]$ et en déduire que: $3^{69} \equiv 24[71]$

b- Montrer que le nombre: $(3^{69}+4^{69}+6^{69}+8^{69}+9^{69})$ est un multiple de 71

Solution

1) a- Puisque $a\in A_p$, alors: $a\wedge p=1$ (car p est premier)
donc, d'après le théorème de Fermat: $a^{p-1}\equiv 1[p]$
C'est-à-dire: $a\times a^{p-2}\equiv 1[p]$
Donc, a^{p-2} est en effet une solution de l'équation $ax\equiv 1[p]$
b- On a: $a^{p-2}\equiv r[p]$
donc: $a^{p-1}\equiv ar[p]$, or: $a^{p-1}\equiv 1[p]$, donc: $ar\equiv 1[p]$
et par suite, r est une solution de l'équation $ax\equiv 1[p]$
et $r\in A$ car: $1\leq r\leq p-1$
Supposons qu'il existe r' de A_p tel que: $ar'\equiv 1[p]$
donc: $a(r-r')\equiv 0[p]$, d'où: $p|a(r-r')$
or: $p\wedge a=1$ donc: $p|(r-r')$
et puisque: $-p<r-r'<p$ car $1\leqslant r\leqslant p-1$ et $1\leqslant r'\leqslant p-1$
alors: $r-r'=0$, par suite: $r=r'$
(0 est le seul multiple de p compris strictement entre $-p$ et p)
Donc r est l'unique solution de l'équation $ax\equiv 1[p]$ dans A_p
2) a- On a: $3x\equiv 1[71]\Longleftrightarrow 3x\equiv 72[71]$
$\Longleftrightarrow x\equiv 24[71]$ (car $3\wedge 71=1$)
et puisque $24\in A_{71}$ alors 24 est la solution de l'équation $3x\equiv 1[71]$ dans A_{71}
et d'après le résultat de la question précèdente, 24 est le reste de la division euclidienne de 3^{69} par 71
c'est-à-dire: $3^{69}\equiv 24[71]$
b- On obtient de même (dans le contexte de l'exercice):
$4^{69}\equiv 18[71]$, $6^{69}\equiv 12[71]$; $8^{69}\equiv 9[71]$ et $9^{69}\equiv 8[71]$
Donc: $3^{69}+4^{69}+6^{69}+8^{69}+9^{69}\equiv 71[71]$
$\equiv 0[71]$
par suite, le nombre $(3^{69}+4^{69}+6^{69}+8^{69}+9^{69})$ est un multiple de 71

Exercice 23

1- Soient n un nombre entier naturel non nul et x un nombre entier naturel tels que: $(x+1)^n-x^n=n$
Soit p le plus petit diviseur premier positif de n
a- Vérifier que : $(x+1)^n\equiv x^n[p]$
b- Montrer que : $p\wedge x=1$ et $p\wedge(x+1)=1$
c- En déduire que: $x^{p-1}\equiv 1[p]$ et $(x+1)^{p-1}\equiv 1[p]$
d- Montrer qu'il existe un couple (u,v) de $\mathbb{N}^2$ tel que $nu-(p-1)v=1$

e- En déduire que $x+1 \equiv x[p]$
2) En déduire de ce qui précède que l'équation $(x+1)^n - x^n = n$ n'admet pas de solution dans $\mathbb{N}$

Solution

1) a- On a : $p|n$, donc : $p|((x+1)^n - x^n)$ car $n=(x+1)^n - x^n$
par suite : $(x+1)^n \equiv x^n[p]$
b- Supposons que: $p \wedge x \neq 1$
donc : $p|x$ car p est premier
par suite, $p|x^n$
et on a: $p|n$, donc $p|n+x^n$ et par suite : $p|(x+1)^n$
d'où : $p|(x+1)$ car p est premier
Or : $p|x$ donc : $p|(x+1)-x$
C'est-à-dire $p|1$ ce qui est faux (p est premier)
Donc $p \wedge x = 1$
Or : $(x+1)^n \equiv x^n[p]$, donc : $(x+1)^n \not\equiv 0[p]$ car $x^n \not\equiv 0[p]$
C'est-à-dire p ne divise pas $(x+1)^n$
donc p ne divise pas $(x+1)$ et par suite $p \wedge (x+1) = 1$ car p est premier
c- Le nombre p est premier et ne divise ni x ni $(x+1)$
donc d'après le théorème de Fermat: $x^{p-1} \equiv 1[p]$ et $(x+1)^{p-1} \equiv 1[p]$
d- Si $n \wedge (p-1) \neq 1$
alors il existe un nombre premier q positif divisant n et $(p-1)$
On a: $q \leq p-1$, donc: $q < p$ et $q|n$
Ce qui contredit le fait que p est le plus petit diviseur premier positif de n
Donc : $n \wedge (p-1) = 1$
et par suite : $(\exists(\alpha,\beta) \in \mathbb{Z}^2) \quad \alpha n + \beta(p-1) = 1$
α et β ne sont pas de même signe car n et $p-1$ sont strictement positifs
donc : $(\exists(u,v) \in \mathbb{N}^2) \quad nu - (p-1)v = 1$
e- On a $nu = 1 + (p-1)v$ où $(u,v) \in \mathbb{N}^2$
Or : $(x+1)^n \equiv x^n[p]$
donc : $(x+1)^{nu} \equiv x^{nu}[p] \quad (u \in \mathbb{N})$
C'est-à-dire: $(x+1)^{1+(p-1)v} \equiv x^{1+(p-1)v}[p]$
donc: $((x+1)^{p-1})^v \cdot (x+1) \equiv x \cdot (x^{p-1})^v[p] \quad (v \in \mathbb{N})$
Or: $(x+1)^{p-1} \equiv 1[p]$ et $x^{p-1} \equiv 1[p]$
donc : $x+1 \equiv x[p]$
2) On considère l'équation $(E):(x \in \mathbb{N}) \quad (x+1)^n - x^n = n$
Si l'équation (E) admet une solution x dans $\mathbb{N}$
alors : $x+1 \equiv x[p]$ où p est le plus petit diviseur positif premier de n
(d'après ce qui précède)

par suite, $p|(x+1)-x$ c'est-à-dire : $p|1$
Ce qui est faux car p est premier
Donc l'équation (E) n'admet pas de solution dans $\mathbb{N}$

Exercice 24

Soit n un nombre entier naturel non nul
On pose $a = 11n+3$ et $b = 13n-1$
1) Montrer que $a \wedge b$ divise 50
2) a- Déterminer une solution particulière de l'équation $50x-11y=1$ dans $\mathbb{Z}^2$
b- Résoudre dans $\mathbb{Z}^2$ l'équation $(E): 50x-11y=3$
c- En déduire les valeurs de n pour lesquelles $a \wedge b = 50$
3) a- Montrer que: $b^{11} \equiv b[11]$ et $a^{10} \equiv 1[11]$
b- Déterminer les valeurs de n pour lesquelles $b \equiv 0[11]$
c- En déduire que si $n \not\equiv 6[11]$ alors $((13n-1)(11n+3))^{2010} \equiv 1[11]$

Solution

1) Soit $n \in \mathbb{N}^*$, on pose $d = a \wedge b$
On a: $d|a$ et $d|b$
C'est-à-dire: $d|(11n+3)$ et $d|(13n-1)$
donc: $d|13(11n+3)-11(13n-1)$
C'est-à-dire : $d|50$
2) a- On pose : $50=\alpha$ et $11=\beta$
On a: $\alpha = 4\beta+6$ et $\beta = 6+5$ et $6=5+1$
donc : $6=\alpha-4\beta$ et $5=\beta-6=5\beta-\alpha$
et : $1=6-5=(\alpha-4\beta)-(5\beta-\alpha)$
et par suite : $2\alpha-9\beta=1$
C'est-à-dire : $50\times 2-11\times 9=1$
Donc le couple $(2;9)$ est une solution de l'équation $50x-11y=1$
b- On a: $50\times 2-11\times 9=1$, donc: $50\times 6-11\times 27=3$
par suite, $(E) \Longleftrightarrow 50x-11y = 50\times 6-11\times 27$

$$\Longleftrightarrow 50(x-6)=11(y-27)$$

$$\Longleftrightarrow \begin{cases} 50(x-6)=11(y-27) \\ 11|50(x-6) \end{cases}$$

$$\Longleftrightarrow \begin{cases} 50(x-6)=11(y-27) \\ 11|x-6 \;\; (car\, 11\wedge 50 = 1) \end{cases}$$

$$\Longleftrightarrow \begin{cases} x-6=11k\,(k\in\mathbb{Z}) \\ 50(x-6)=11(y-27) \end{cases}$$

$$\Leftrightarrow \begin{cases} x-6=11k \\ y-27=50k \end{cases} \quad (k \in \mathbb{Z})$$

$$\Leftrightarrow \begin{cases} x=6+11k \\ y=27+50k \end{cases} \quad (k \in \mathbb{Z})$$

Donc l'ensemble de solutions dans $\mathbb{Z}^2$ de l'équation $50x-11y=3$ est $S=\{(6+11k, 27+50k)/k \in \mathbb{Z}\}$

c- On a: $(a \wedge b)|50$ d'après 1)

Donc : $a \wedge b = 50 \Leftrightarrow 50|a$ et $50|b$

et on a: $50|a \Leftrightarrow (\exists x \in \mathbb{N})\ a = 50x$

$\Leftrightarrow (\exists x \in \mathbb{N})\ 11n+3 = 50x$

$\Leftrightarrow (\exists x \in \mathbb{N})\ 50x - 11n = 3$

$\Rightarrow (\exists k \in \mathbb{N})\ n = 27 + 50k$ (d'après le résultat de la question précèdente)

et si $n = 27 + 50k$ où $k \in \mathbb{N}$

alors: $a = 11(27+50k)+3 = 50(6+11k)$

et $b = 13(27+50k)-1 = 50(7+13k)$

donc: $50|a$ et $50|b$

Les valeurs de n pour lesquelles $a \wedge b = 50$ sont $27+50k$ où $k \in \mathbb{N}$

3) a- Le nombre 11 est premier

donc d'après le théorème de Fermat: $b^{11} \equiv b[11]$ et $a^{11} \equiv a[11]$

On a: $a = 11n+3$, donc $a \equiv 3[11]$

et par suite 11 ne divise pas a

Donc: $a^{10} \equiv 1[11]$

b- On a: $b \equiv 0[11] \Leftrightarrow 13n-1 \equiv 0[11]$

$\Leftrightarrow 2n \equiv 1[11]$

$\Leftrightarrow 2n \equiv 12[11]$

$\Leftrightarrow n \equiv 6[11] \quad (car\ 2 \wedge 11 = 1)$

$\Leftrightarrow n = 11k + 6\ (k \in \mathbb{N})$

c- Soit $n \in \mathbb{N}$ tel que $n \not\equiv 6[11]$

donc: $b \not\equiv 0[11]$ c'est-à-dire 11 ne divise pas b

Or 11 est premier, donc: $b^{10} \equiv 1[11]$

On a aussi: $a^{10} \equiv 1[11]$

donc: $(ab)^{10} \equiv 1[11]$ et par suite: $(ab)^{2010} \equiv 1[11]$

C'est-à-dire: $((13n-1)(11n+3))^{2010} \equiv 1[11]$

Exercice 25 juin 2007

1) On considère dans $\mathbb{Z}^2$ l'équation $(E): 195x - 232y = 1$

a- Déterminer $232 \wedge 195$

b- Montrer que l'ensemble de solutions de l'équation (E) est:

$S = \{(163 + 232k, 137 + 195k) / k \in \mathbb{Z}\}$

c- Déterminer l'unique entier naturel d qui vérifie:

$0 \leq d \leq 232$ et $195d \equiv 1[232]$

2) Montrer que 233 est un nombre premier.

3) Soit A l'ensemble des entiers naturels compris entre 0 et 232

On considère l'application f de A vers A définie par: pour tout a de A, l'entier $f(a)$ est le reste de la division euclidienne de a^{195} par 233

a- Montrer que: $(\forall a \in A - \{0\}) \quad a^{232} \equiv 1[233]$

b- Montrer que pour tout (a,b) de A^2, si $f(a) = f(b)$ alors $a = b$

c- Soit $(a,b) \in A^2$ tel que $f(a) = b$, Déterminer a en fonction de b

d- En déduire que f est bijective et déterminer sa bijection réciproque f^{-1}

Solution

1) a- Décomposons les nombres 232 et 195 en produit de facteur premiers:

On a: $232 = 2^3 \times 29$ et $195 = 3 \times 5 \times 13$

par suite: $232 \wedge 195 = 1$

b- • On a: $195 \times 163 - 232 \times 137 = 31785 - 31784 = 1$

Donc le couple $(163, 137)$ est une solution de l'équation (E)

• On a: $(E) \Leftrightarrow 195x - 232y = 195 \times 163 - 232 \times 137$

$$\Leftrightarrow 195(x-163) = 232(y-137)$$

$$\Leftrightarrow \begin{cases} 195(x-163) = 232(y-137) \\ 195 | 232(y-137) \end{cases}$$

$$\Leftrightarrow \begin{cases} 195(x-163) = 232(y-137) \\ 195 | (y-137) \quad (car\ 195 \wedge 232 = 1) \end{cases}$$

$$\Leftrightarrow \begin{cases} x - 163 = 232k \\ y - 137 = 195k \end{cases} (k \in \mathbb{Z})$$

$$\Leftrightarrow \begin{cases} x = 163 + 232k \\ y = 137 + 195k \end{cases} (k \in \mathbb{Z})$$

Donc l'ensemble de solutions de l'équation (E) est:

$S = \{(163 + 232k, 137 + 195k) / k \in \mathbb{Z}\}$

c- On a: $195d \equiv 1[232] \Leftrightarrow (\exists d' \in \mathbb{Z}) 195d - 232d' = 1$

Et d'après le résultat de la question précèdente on a: $d = 163 + 232k \quad (k \in \mathbb{Z})$

Et puisque: $0 \leq d \leq 232$ alors: $0 \leq 163 + 232k \leq 232$

par suite: $\frac{-163}{232} \leq k \leq \frac{69}{232}$

et puisque $k \in \mathbb{Z}$ alors: $k = 0$

par suite: $d = 163$

2) On a: $\sqrt{233} \simeq 15,26$

et les nombres premiers positifs inférieurs à $\sqrt{233}$ sont $2, 3, 5, 7, 11$ et 13

Et puisque aucun de ces nombres ne divise 233

alors 233 est un nombre premier.

3) a- Soit a un élément de $A - \{0\}$

On a: 233 est un nombre premier et a n'est pas divisible par 233

Donc: $a^{232} \equiv 1[233]$ (d'après le théorème de Fermat)

b- Soient a et b deux éléments de A tels que $f(a) = f(b)$

On a: $a^{195} \equiv f(a)[233]$ et $b^{195} \equiv f(b)[233]$

Donc: $a^{195} \equiv b^{195}[233]$ $(*)$

Et puisque le couple $(163, 137)$ est une solution de l'équation (E)

alors: $195 \times 163 = 1 + 232 \times 137$

par suite: $a^{195\times163} \equiv b^{195\times163}[233]$ (d'après $(*)$)

C'est-à-dire: $a \times (a^{232})^{137} \equiv b \times (b^{232})^{137}[233]$

Et puisque: $a^{232} \equiv 1[233]$ et $b^{232} \equiv 1\ [233]$

alors: $a \equiv b\ [233]$

C'est-à-dire: $a - b \equiv 0\ [233]$ c'est-à-dire: $233 \mid (a - b)$

et puisque : $0 \leq a \leq 232$ et $0 \leq b \leq 232$

alors: $-232 \leq a - b \leq 232$

Par suite: $a - b = 0$ d'où: $a = b$

(0 est le seul multiple de 233 compris entre -232 et 232)

Conclusion: $(\forall (a,b) \in A^2) \quad f(a) = f(b) \Longrightarrow a = b$

c- Soient a et b deux éléments de A tels que $f(a) = b$

Donc: $a^{195} \equiv b[233]$

Et puisque: $195 \times 163 = 1 + 232 \times 137$

alors: $(a^{195})^{163} \equiv b^{163}\ [233]$

par suite: $a \times (a^{232})^{137} \equiv b^{163}\ [233]$

Et puisque: $a^{232} \equiv 1[233]$

alors: $a \equiv b^{163}\ [233]$

Donc a est le reste de la division euclidienne de b^{163} par 233

d- D'après le résultat de la question **(3) b-**), on déduit que f est injective

et d'après le résultat de la question **(3) c-**), on déduit que f est surjective

Par suite, f est bijective de A vers A et sa bijection réciproque f^{-1} est définie de A vers A par:

pour tout b de A , l'entier $f^{-1}(b)$ est le reste de la division euclidienne de b^{163} par 233

Exercice 26 juin 2008

I. On considère dans $\mathbb{Z}^2$ l'équation $(E): 35u - 96v = 1$

1) Vérifier que le couple $(11;4)$ est une solution de l'équation (E)

2) En déduire l'ensemble de solutions de l'équation (E)

II. On considère dans $\mathbb{N}$ l'équation $(F): x^{35} \equiv 2[97]$

1) Soit x une solution de l'équation (F)

a- Montrer que 97 est un nombre premier et que : $x \wedge 97 = 1$

b- Montrer que : $x^{96} \equiv 1[97]$

c- Montrer que: $x \equiv 2^{11}[97]$

2) Montrer que si un entier naturel x vérifie $x \equiv 2^{11}[97]$ alors x est une solution de l'équation (F)

3) Montrer que l'ensemble de solutions de l'équation (F) est $\{11 + 97k / k \in \mathbb{N}\}$

Solution

I. 1) Vérifier que: $35 \times 11 - 96 \times 4 = 1$

Remarquer alors que: $35 \wedge 96 = 1$ (d'après le théorème de Bezout)

2) On a: $(E) \Longleftrightarrow 35u - 96v = 35 \times 11 - 96 \times 4$

$$\Longleftrightarrow 35(u-11) = 96(v-4)$$

$$\Longleftrightarrow \begin{cases} 35(u-11) = 96(v-4) \\ 35 | 96(v-4) \end{cases}$$

$$\Longleftrightarrow \begin{cases} 35(u-11) = 96(v-4) \\ 35 | v-4 \qquad (car:\ 35 \wedge 96 = 1) \end{cases}$$

$$\Longleftrightarrow \begin{cases} u - 11 = 96k \\ v - 4 = 35k \end{cases} \quad (k \in \mathbb{Z})$$

$$\Longleftrightarrow \begin{cases} u = 11 + 96k \\ v = 4 + 35k \end{cases} \quad (k \in \mathbb{Z})$$

Donc l'ensemble de solutions de l'équation (E) est:

$S = \{(11 + 96k, 4 + 35k) | k \in \mathbb{Z}\}$

II. 1) a- • On a: $\sqrt{97} \simeq 9,8$

et les nombres premiers positifs inférieurs à $\sqrt{97}$ sont $2, 3, 5$ et 7

Et puisque aucun de ces nombres ne divise 97

alors 97 est un nombre premier.

• Soit x une solution de l'équation (F)

On a: $x^{35} \equiv 2[97]$

Donc 97 ne divise pas x (car 97 ne divise pas x^{35})

Et puisque 97 est premier alors: $x \wedge 97 = 1$

b- On a: 97 est un nombre premier et 97 ne divise pas x

Donc : $x^{96} \equiv 1[97]$ (d'après le théorème de Fermat) c- On a: $x^{96} \equiv 1[97]$, donc: $(x^{96})^4 \equiv 1[97]$ c'est-à-dire: $x^{96\times 4} \equiv 1[97]$

donc: $x^{96\times 4}x \equiv x[97]$, c'est-à-dire: $x^{96\times 4+1} \equiv x[97]$

Or: $35 \times 11 - 96 \times 4 = 1$

Donc: $x^{35\times 11} \equiv x[97]$

C'est-à-dire: $x \equiv (x^{35})^{11}[97]$

Par suite: $x \equiv 2^{11}[97]$ $(car\ x^{35} \equiv 2[97])$

2) Soit x un élément de $\mathbb{N}$ qui vérifie $x \equiv 2^{11}\ [97]$

Donc: $x^{35} \equiv 2^{11\times 35}[97]$

C'est-à-dire: $x^{35} \equiv 2^{1+96\times 4}[97]$

par suite: $x^{35} \equiv (2^{96})^4 \times 2[97]$

et puisque 97 est un nombre premier et $2 \wedge 97 = 1$

Alors: $2^{96} \equiv 1[97]$

Par suite: $x^{35} \equiv 2[97]$

Donc, x est bien une solution de l'équation (F)

3) Soit S l'ensemble de solutions de l'équation (F)

D'après ce qui précède, on a :

$$\begin{aligned} x \in (F) &\Leftrightarrow x \equiv 2^{11}\quad [97] \\ &\Leftrightarrow x \equiv 2048[97] \\ &\Leftrightarrow x \equiv 11\quad [97]\ (car\ 2048 = 21 \times 97 + 11) \\ &\Leftrightarrow x = 11 + 97k\ (k \in \mathbb{N}) \end{aligned}$$

Donc: $S = \{11 + 97k \ / \ k \in \mathbb{N}\}$

Exercice 27 juin 2016

Première partie:

Soit (a,b) un élément de $\mathbb{N}^* \times \mathbb{N}^*$ tel que le nombre premier 173 divise $a^3 + b^3$

1) Montrer que: $a^{171} \equiv -b^{171}[173]$ (Remarquer que: $171 = 3 \times 57$)

2) Montrer que: 173 divise a si et seulement si 173 divise b

3) On suppose que 173 divise a, montrer que 173 divise $(a+b)$

4) On suppose que 173 ne divise pas a

a- En utilisant le théorème de Fermat, montrer que: $a^{172} \equiv b^{172}[173]$

b- Montrer que: $a^{171}(a+b) \equiv 0[173]$

c- En déduire que 173 divise $(a+b)$

Deuxième partie:

On considère dans $\mathbb{N}^* \times \mathbb{N}^*$ l'équation suivante: (E): $x^3 + y^3 = 173(xy+1)$

Soit (x,y) un élément de $\mathbb{N}^* \times \mathbb{N}^*$ solution de (E), on pose: $x + y = 173k$ avec $k \in \mathbb{N}^*$

1) Vérifier que: $k(x-y)^2 + (k-1)xy = 1$

2) Montrer que $k = 1$ puis résoudre l'équation (E)

Solution

Première partie:

1) On a: $173|(a^3+b^3)$, donc: $a^3 \equiv -b^3[173]$

Par suite: $(a^3)^{57} \equiv (-b^3)^{57}[173]$

C'est - à - dire: $a^{171} \equiv -b^{171}[173]$

2) On a:

$173|a \Leftrightarrow a \equiv 0[173]$

$\Leftrightarrow a^{171} \equiv 0[173]$ ($a^{171} \equiv 0[173] \Rightarrow a \equiv 0[173]$, car 173 est un nombre premier)

$\Leftrightarrow -b^{171} \equiv 0[173]$ (car $a^{171} \equiv -b^{171}[173]$)

$\Leftrightarrow b^{171} \equiv 0[173]$

$\Leftrightarrow 173|b^{171}$

$\Leftrightarrow 173|b$ (car 173 est un nombre premier)

3) On suppose que: $173|a$

Donc: $173|b$ (d'après le résultat de la question précèdente)

par suite: $173|a+b$

4) a- On suppose que 173 ne divise pas a

et puisque 173 est un nombre premier

alors : $a^{172} \equiv 1[173]$ (d'après le théorème de Fermat)

Et puisque 173 ne divise pas a alors 173 ne divise pas b

(d'après le résultat de la question **2**)

par suite, $b^{172} \equiv 1[173]$ (d'après le théorème de Fermat)

Donc: $a^{172} \equiv b^{172}[173]$

b- On a: $a^{171}(a+b) = a^{172} + a^{171}b$

Et puisque: $a^{172} \equiv b^{172}[173]$

alors: $a^{172} + a^{171}b \equiv b^{172} + a^{171}b[173]$

$\equiv b(b^{171} + a^{171})[173]$

$\equiv b \times 0[173]$ (d'après le résultat de la question 1)

$\equiv 0[173]$

par suite: $a^{171}(a+b) \equiv 0[173]$

c- On a: $173|a^{171}(a+b)$ (d'après le résultat de la question précèdente)

et on a: 173 est un nombre premier et 173 ne divise pas a

Donc: $173 \wedge a = 1$, par suite : $173 \wedge a^{171} = 1$

D'où: $173|a+b$ (d'après le théorème de Gauss)

Deuxième partie:

1) • Remarquons tout d'abord que:

$x^3 + y^3 = (x+y)(x^2 - xy + y^2) = 173k(x^2 - xy + y^2)$

• On a: $k(x-y)^2+(k-1)xy = k(x-y)^2+kxy-xy$

$$= k(x^2-2xy+y^2+xy)-xy = k(x^2-xy+y^2)-xy$$

$$= \frac{x^3+y^3}{173}-xy = \frac{173(xy+1)}{173}-xy = xy+1-xy$$

Donc: $k(x-y)^2+(k-1)xy=1$

2) On a: $k(x-y)^2+(k-1)xy=1$

Donc: $\begin{cases} k(x-y)^2=0 \\ (k-1)xy=1 \end{cases}$ ou $\begin{cases} k(x-y)^2=1 \\ (k-1)xy=0 \end{cases}$ (car $k(x-y)^2 \in \mathbb{N}$ et $(k-1)xy \in \mathbb{N}$)

par suite: $\begin{cases} k=0 \text{ ou } x=y \\ k-1=1 \text{ et } x=1 \text{ et } y=1 \end{cases}$ ou $\begin{cases} k=1 \text{ et } (x-y)^2=1 \\ k-1=0 \end{cases}$

Et puisque le système $\begin{cases} k=0 \text{ ou } x=y \\ k-1=1 \text{ et } x=1 \text{ et } y=1 \end{cases}$ n'a pas de solution car $x+y=173k$

alors: $\begin{cases} k=1 \text{ et } (x-y)^2=1 \\ k-1=0 \end{cases}$, donc: $\begin{cases} k=1 \\ (x-y)^2=1 \end{cases}$

par suite: $\begin{cases} x+y=173 \\ x-y=1 \end{cases}$ ou $\begin{cases} x+y=173 \\ x-y=-1 \end{cases}$

D'où: $\begin{cases} x=87 \\ y=86 \end{cases}$ ou $\begin{cases} x=86 \\ y=87 \end{cases}$

Et réciproquement, vérifier que les couples $(87,86)$ et $(86,87)$ sont des solutions de l'équation (E)

Conclusion:

L'ensemble de solutions de l'équation (E) est: $S=\{(87;86),(86;87)\}$

Exercice 28 juin 2015

Soit x un nombre entier relatif tel que : $x^{1439} \equiv 1436[2015]$

1) Sachant que : $1436 \times 1051 - 2015 \times 749 = 1$, montrer que 1436 et 2015 sont premiers entre eux.

2) Soit d un diviseur commun de x et 2015

a- Montrer que d divise 1436

b- En déduire que : $x \wedge 2015 = 1$

3) a- En utilisant le théorème de Fermat, montrer que : $x^{1440} \equiv 1[5]$, $x^{1440} \equiv 1[13]$ et $x^{1440} \equiv 1[31]$ (Remarquer que: $2015 = 5 \times 13 \times 31$)

b- Montrer que : $x^{1440} \equiv 1[65]$ puis que : $x^{1440} \equiv 1[2015]$

4) Montrer que : $x \equiv 1051[2015]$

Solution

1) Comme : $1436 \times 1051 - 2015 \times 749 = 1$

Alors, d'après le théorème de Bezout : $1436 \wedge 2015 = 1$

2) a- Soit d un diviseur commun de x et 2015

puisque : $x^{1439} \equiv 1436[2015]$

alors : $(\exists k \in \mathbb{Z})\ x^{1439} = 2015k + 1436$

et comme : $d|x$ et $d|2015$

alors : $d|x^{1439} - 2015k$

C'est-à-dire : $d|1436$

b- On pose : $\alpha = x \wedge 2015$

α est un diviseur commun de x et 2015

Donc d'après la question précèdente : α divise 1436

par suite, $\alpha|2015$ et $\alpha|1436$

D'où : $\alpha|(2015 \wedge 1436)$

C'est-à-dire : $\alpha|1$

Donc : $\alpha = 1$ et par suite : $x \wedge 2015 = 1$

3) a- • Le nombre 5 est premier et ne divise pas x

car $x \wedge 2015 = 1$ et 5 divise 2015

Donc, d'après le théorème de Fermat : $x^4 \equiv 1[5]$

par suite, $(x^4)^{380} \equiv 1[5]$ c'est-à-dire : $x^{1440} \equiv 1[5]$

• Montrer de même que : $x^{1440} \equiv 1[13]$ et $x^{1440} \equiv 1[31]$

b- • On a : $x^{1440} \equiv 1[5]$ et $x^{1440} \equiv 1[13]$

donc : $5|(x^{1440} - 1)$ et $13|(x^{1440} - 1)$

et comme : $5 \wedge 13 = 1$ alors : $5 \times 13|(x^{1440} - 1)$

c'est-à-dire : $65|(x^{1440} - 1)$

d'où : $x^{1440} \equiv 1[65]$

• On a : $65|(x^{1440} - 1)$ et $31|(x^{1440} - 1)$ et $65 \wedge 31 = 1$

Donc : $65 \times 31|(x^{1440} - 1)$

c'est-à-dire : $2015|(x^{1440} - 1)$, d'où : $x^{1440} \equiv 1[2015]$

4) On a : $x^{1439} \equiv 1436[2015]$

Donc : $1051.x^{1439} \equiv 1051 \times 1436[2015]$

C'est-à-dire : $1051.x^{1439} \equiv 1 + 2015 \times 749[2015]$ (car $1436 \times 1051 - 2015 \times 749 = 1$)

Donc : $1051.x^{1439} \equiv 1[2015]$, d'où : $1051x^{1440} \equiv x[2015]$

Or : $x^{1440} \equiv 1[2015]$, donc : $1051 \equiv x[2015]$

Exercice 29 juillet 2012

1) a- Vérifier que 503 est un nombre premier.

b- Montrer que $7^{502} \equiv 1[503]$ et en déduire que : $7^{2008} \equiv 1[503]$

2) On considère dans $\mathbb{Z}^2$ l'équation (E): $49x - 6y = 1$
Sachant que $(1;8)$ est une solution de (E), résoudre dans $\mathbb{Z}^2$ l'équation (E)
3) On pose : $N = 1 + 7 + 7^2 + \cdots + 7^{2007}$
a- Montrer que le couple $(7^{2006}, N)$ est une solution de l'équation (E)
b- Montrer que : $N \equiv 0\,[4]$ et $N \equiv 0\,[503]$
c- En déduire que N est divisible par 2012

Solution

1) a- On a : $\sqrt{503} \simeq 22,43$
Les nombres premiers positifs inférieurs à $\sqrt{503}$ sont $2, 3, 5, 7, 11, 13, 17$ et 19,
et aucun de ces nombres ne divise 503
Donc 503 est un nombre premier.
b- • Le nombre 503 est premier et ne divise pas 7
Donc, d'après le théorème de Fermat : $7^{502} \equiv 1\,[503]$
• On a : $7^{502} \equiv 1\,[503]$
Donc : $(7^{502})^4 \equiv 1\,[503]$
C'est-à-dire: $7^{2008} \equiv 1\,[503]$
2) Soit $(x, y) \in \mathbb{Z}^2$
On a : $49x - 6y = 1 \Leftrightarrow 49x - 6y = 49 \times 1 - 6 \times 8$

$$\Leftrightarrow 49(x-1) = 6(y-8)$$

$$\Leftrightarrow \begin{cases} 49(x-1) = 6(y-8) \\ 6 \mid 49(x-1) \end{cases}$$

$$\Leftrightarrow \begin{cases} 49(x-1) = 6(y-8) \\ 6 \mid (x-1) \end{cases} \quad (\text{car } 6 \wedge 49 = 1)$$

$$\Leftrightarrow \begin{cases} 49 \times 6k = 6(y-8) \\ x - 1 = 6k \quad (k \in \mathbb{Z}) \end{cases}$$

$$\Leftrightarrow \begin{cases} x = 1 + 6k \\ y = 8 + 49k \end{cases} \quad (k \in \mathbb{Z})$$

Donc : $S = \{(1 + 6k, 8 + 49k) / k \in \mathbb{Z}\}$
3) a- On a : $49 \times 7^{2006} - 6N = 7^{2008} - 6N$
Or : $N = 1 \times \dfrac{7^{2008} - 1}{7 - 1} = \dfrac{7^{2008} - 1}{6}$
Donc : $6N = 7^{2008} - 1$
Par suite, $49 \times 7^{2006} - 6N = 1$
D'où : $(7^{2006}, N)$ est une solution de l'équation (E)
b- • On a : $N \equiv (1 + 7) + (7^2 + 7^3) + \cdots + (7^{2006} + 7^{2007})\,[4]$ (car $7 \equiv -1\,[4]$)
$\equiv (1 - 1) + (1 - 1) + \cdots + (1 - 1)\,[4]$

Donc : $N \equiv 0[4]$

Autre méthode :

On a : $6N = 7^{2008} - 1$ et $7 \equiv -1[8]$

Donc : $6N \equiv 0[8]$

Par suite, $3N \equiv 0[4]$ (si $pa \equiv pb[pn]$ alors $a \equiv b[n]$)

et puisque : $3 \wedge 4 = 1$

Alors : $N \equiv 0[4]$

• On a: $6N = 7^{2008} - 1$

et comme : $7^{2008} \equiv 1[503]$ alors : $6N \equiv 0[503]$

C'est-à-dire : $503 | 6N$

et comme : $503 \wedge 6 = 1$, donc d'après le théorème de Gauss : $503 | N$

Par suite : $N \equiv 0[503]$

c- On a : $N \equiv 0[4]$ et $N \equiv 0[503]$

Donc : $4 | N$ et $503 | N$

et comme : $4 \wedge 503 = 1$, alors : $4 \times 503 | N$ c'est-à-dire : $2012 | N$

Exercice 30

1) Soit p un nombre premier tel que : $p \geq 3$ et soit x un nombre entier relatif.
Montrer que si $x \equiv 1[p]$ alors : $x^p \equiv 1[p^2]$

2) Soit $a \in \mathbb{Z}$ tel que : $a \wedge 4225 = 1$

a- Montrer que : $a^4 \equiv 1[5]$ et $a^{12} \equiv 1[13]$

b- Déterminer : $20 \vee 156$ puis en déduire que : $a^{780} \equiv 1[4225]$

Solution

1) On a : $x^p - 1 = (x-1)(x^{p-1} + x^{p-2} + \cdots + x^2 + x + 1)$

Or : $x \equiv 1[p]$, donc : $(\exists k \in \mathbb{Z})\ x - 1 = kp$ et $(\forall i \in \{1, \ldots, p-1\})\ x^i \equiv 1[p]$

Donc : $(x^{p-1} + x^{p-2} + \cdots + x^2 + x + 1) \equiv p[p]$,

par suite, $(x^{p-1} + x^{p-2} + \cdots + x^2 + x + 1) \equiv 0[p]$

D'où : $(\exists k' \in \mathbb{Z})\ x^{p-1} + \cdots + x + 1 = k'p$

Donc : $x^p - 1 = kp.k'p = kk'p^2$

Par suite : $x^p \equiv 1[p^2]$

2) a- On a : $a \wedge 4225 = 1$

et comme : $4225 = 5^2 \times 13^2$

Alors : $a \wedge 5 = 1$ et $a \wedge 13 = 1$

et puisque : 5 et 13 sont des nombres premiers

alors, d'après le théorème de Fermat : $a^4 \equiv 1[5]$ et $a^{12} \equiv 1[13]$

b- • On a : $20 = 2^2 \times 5$ et $156 = 2^2 \times 3 \times 13$

Donc : $20 \vee 156 = 2^2 \times 3 \times 5 \times 13 = 780$

• On a : $a^4 \equiv 1[5]$, donc : $(a^4)^5 \equiv 1[25]$ (d'après 1) c'est-à-dire : $a^{20} \equiv 1[25]$
et $a^{12} \equiv 1[13]$, donc : $(a^{12})^{13} \equiv 1[169]$ c'est-à-dire : $a^{156} \equiv 1[169]$
Donc : $a^{780} \equiv 1[25]$ et $a^{780} \equiv 1[169]$ (on a : $20 \times 39 = 780$ et $156 \times 5 = 780$)
C'est-à-dire : $25 \mid (a^{780} - 1)$ et $169 \mid (a^{780} - 1)$
et puisque : $25 \wedge 169 = 1$, alors : $(25 \times 169) \mid (a^{780} - 1)$
c'est-à-dire : $4225 \mid (a^{780} - 1)$ et par suite : $a^{780} \equiv 1[4225]$

Exercice 31 juin 2013

Le but de l'exercice est de déterminer les entiers naturels n supérieurs à 1 qui vérifient la propriété: (R): $3^n - 2^n \equiv 0[n]$

1) Soit $n \in \mathbb{N}^* - \{1\}$ tel que n vérifie la propriété (R) et soit p le plus petit diviseur premier positif de n

a- Montrer que : $3^n - 2^n \equiv 0[p]$ et en déduire que $p \geq 5$

b- Montrer que : $2^{p-1} \equiv 1[p]$ et $3^{p-1} \equiv 1[p]$

c- Montrer qu'il existe un couple (a,b) de $\mathbb{Z}^2$ tel que : $an - b(p-1) = 1$

d- Soient r et q le reste et le quotient de la division euclidienne de a par $(p-1)$ $(q \in \mathbb{Z}, 0 \leq r < p-1$ et $a = q(p-1) + r)$

Montrer qu'il existe un entier naturel k tel que : $rn = 1 + k(p-1)$

2) Déduire de ce qui précède qu'il n'existe aucun entier naturel n supérieur à 1 qui vérifie la propriété (R)

Solution

1) a- * On a : $3^n - 2^n \equiv 0[n]$

Donc : n divise $(3^n - 2^n)$

et comme p divise n, donc p divise $(3^n - 2^n)$, par suite, $3^n - 2^n \equiv 0[p]$

* Si $p = 2$

Alors : $3^n \equiv 0[2]$ car : $3^n - 2^n \equiv 0[2]$ et $2^n \equiv 0[2]$

C'est-à-dire : $1 \equiv 0[2]$, ce qui est faux, donc : $p \neq 2$

* Si $p = 3$

alors : $-2^n \equiv 0[3]$ car : $3^n - 2^n \equiv 0[3]$ et $3^n \equiv 0[3]$

C'est-à-dire : $3 \mid 2^n$, donc : $3 \mid 2$ car 3 est premier, ce qui est faux, donc : $p \neq 3$

* p est un nombre premier positif tel que : $p \neq 2$ et $p \neq 3$

Donc : $p \geq 5$

b- p est un nombre premier ne divise ni 2 ni 3 (car $p \geq 5$)

Donc d'après le théorème de Fermat : $2^{p-1} \equiv 1[p]$ et $3^{p-1} \equiv 1[p]$

c- Montrons que : $n \wedge (p-1) = 1$

Si n et $(p-1)$ ne sont pas premiers entre eux

Alors n et $(p-1)$ admettent un diviseur premier positif commun α

Donc n admet un diviseur premier positif α vérifiant $\alpha \leq p-1 < p$

(car $\alpha | (p-1)$)

Ce qui contredit le fait que p est le plus petit diviseur premier positif de n

et par suite : $n \wedge (p-1) = 1$

Donc, d'après le théorème de Bezout : $(\exists(a,b) \in \mathbb{Z}^2)$ $an - b(p-1) = 1$

d- On a : $a = q(p-1) + r$ où $0 \leq r < p-1$

Donc : $an = nq(p-1) + nr$

Or : $an = 1 + b(p-1)$, donc : $nr = (b-nq)(p-1)+1$

Le nombre $(b-nq)$ est entier, montrons qu'il est positif.

Si : $b-nq < 0$ alors : $b-nq \leq -1$, par suite, $(b-nq)(p-1) \leq 1-p$

D'où : $(b-nq)(p-1)+1 \leq 2-p$ c'est-à-dire : $nr \leq 2-p$

Or : $p \geq 5$, donc : $2-p < 0$, par suite $nr < 0$ ce qui est faux (car $r \geq 0$ et $n \geq 2$)

Donc le nombre $k = b - nq$ est un entier naturel, et on a : $rn = 1 + k(p-1)$

2) Supposons qu'il existe un entier n supérieur à 1 tel que : $3^n \equiv 2^n [n]$

Donc il existe (r,k) de $\mathbb{N}^2$ tel que : $rn = 1 + k(p-1)$ où p est le plus petit diviseur premier positif de n et $p \geq 5$

Par suite, $3^{rn} \equiv 2^{rn} [p]$

C'est-à-dire : $3^{1+k(p-1)} \equiv 2^{1+k(p-1)} [p]$

C'est-à-dire : $3 \times (3^{p-1})^k \equiv 2 \times (2^{p-1})^k [p]$

Or : $3^{p-1} \equiv 1 [p]$ et $2^{p-1} \equiv 1 [p]$

Donc : $3 \equiv 2 [p]$

D'où : p divise 1, ce qui est faux

Donc : il n'existe pas de tel entier n

Exercice 32 Juin 2012

On considère dans $\mathbb{Z}^2$ l'équation (E) : $143x - 195y = 52$

1) a- Déterminer $143 \wedge 195$ et en déduire que l'équation (E) admet des solutions dans $\mathbb{Z}^2$

b- Sachant que $(-1;-1)$ est une solution de (E), résoudre dans $\mathbb{Z}^2$ l'équation (E)

2) Soit $n \in \mathbb{N}^*$ tel que : $n \wedge 5 = 1$

Montrer que : $(\forall k \in \mathbb{N})$ $n^{4k} \equiv 1 [5]$

3) Soit $(x,y) \in (\mathbb{N}^*)^2$ tel que : $x \equiv y [4]$

a- Montrer que : $(\forall n \in \mathbb{N}^*)$ $n^x \equiv n^y [5]$

b- En déduire que : $(\forall n \in \mathbb{N}^*)$ $n^x \equiv n^y [10]$

4) Soient x et y deux entiers naturels tels que le couple (x,y) est une solution de l'équation (E)

Montrer que pour tout entier naturel non nul n, les deux nombres n^x et n^y ont le même chiffre des unités dans le système de numération décimale.

Solution

1) a- • $195 = 143 + 52$

$143 = 2 \times 52 + 39$

$52 = 39 + 13$

$39 = 3 \times 13 + 0$

Le dernier reste non nul est 13

Donc : $195 \wedge 143 = 13$

Autrement, on a : $195 = 13 \times 5 \times 3$ et $143 = 13 \times 11$

Donc : $195 \wedge 143 = 13$

• L'équation (E) est : $143x - 195y = 52$

et on a : $143 \wedge 195 = 13$ et 13 divise 52

Donc l'équation (E) admet des solutions dans $\mathbb{Z}^2$

b- On a : $(E) \Leftrightarrow 11x - 15y = 4$

$$\Leftrightarrow 11x - 15y = 11 \times (-1) - 15 \times (-1)$$

$$\Leftrightarrow 11(x+1) = 15(y-1)$$

$$\Leftrightarrow \begin{cases} 11(x+1) = 15(y-1) \\ 11 \mid (y-1) \end{cases} \quad \text{(car } 11 \wedge 15 = 1\text{)}$$

$$\Leftrightarrow \begin{cases} 11(x+1) = 15 \times 11k \\ y - 1 = 11k \end{cases} (k \in \mathbb{Z})$$

$$\Leftrightarrow \begin{cases} x = 15k - 1 \\ y = 11k + 1 \end{cases} (k \in \mathbb{Z})$$

Donc : $S = \{(15k - 1, 11k + 1) / k \in \mathbb{Z}\}$

2) Soit $n \in \mathbb{N}^*$ tel que : $n \wedge 5 = 1$

Le nombre 5 est premier et $n \wedge 5 = 1$

Donc, d'après le théorème de Fermat : $n^4 \equiv 1 [5]$

par suite, $(\forall k \in \mathbb{N}) \ (n^4)^k \equiv 1 [5]$

C'est-à-dire : $(\forall k \in \mathbb{N}) \ n^{4k} \equiv 1 [5]$

3) a- Soit $(x, y) \in (\mathbb{N}^*)^2$ tel que : $x \equiv y [4]$

• Soit $n \in \mathbb{N}^*$ tel que : $n \wedge 5 = 1$

- Si : $x \geq y$ alors : $x = y + 4k$ où $k \in \mathbb{N}$

par suite, $n^x = n^{y+4k} = n^y \times n^{4k}$

et puisque : $n^{4k} \equiv 1 [5]$

Alors : $n^x \equiv n^y [5]$

- Si : $x \leq y$ alors : $y = x + 4k$ où $k \in \mathbb{N}$

Par suite, $n^y = n^{x+4k} = n^x \times n^{4k}$

D'où : $n^y \equiv n^x[5]$

• Soit $n \in \mathbb{N}^*$ tel que : $n \wedge 5 \neq 1$

Donc : 5 divise n

Par suite, $n^x \equiv 0[5]$ et $n^y \equiv 0[5]$

D'où : $n^x \equiv n^y[5]$

b- Soit $(x,y) \in (\mathbb{N}^*)^2$ et soit $n \in \mathbb{N}^*$

Les deux nombres n^x et n^y ont la même parité, donc : $n^x \equiv n^y[2]$

et on a : $n^x \equiv n^y[5]$ (d'après la question précèdente)

Donc : $2 \mid (n^x - n^y)$ et $5 \mid (n^x - n^y)$

et comme : $2 \wedge 5 = 1$, alors : $2 \times 5 \mid (n^x - n^y)$ c'est-à-dire : $10 \mid (n^x - n^y)$

D'où : $n^x \equiv n^y[10]$

4) • Remarquons tout d'abord que le chiffre des unités d'un nombre entier naturel est, dans le système de numération décimale, le reste de la division de ce nombre par 10

C'est-à-dire, si $n \equiv u[10]$ et $0 \leq u \leq 9$, alors u est le chiffre des unités du nombre entier naturel n

• Soit (x,y) une solution de l'équation (E) tel que : $(x,y) \in \mathbb{N}^2$ et soit $n \in \mathbb{N}^*$

Donc : $11x - 15y = 4$, par suite : $11x - 15y \equiv 0[4]$

Et puisque $11 \equiv -1[4]$ et $-15 \equiv 1[4]$

Alors : $-x + y \equiv 0[4]$ c'est-à-dire : $x \equiv y[4]$

Donc d'après le résultat de la question **3) b-** : $n^x \equiv n^y[10]$

Par suite, les deux nombres n^x et n^y ont le même chiffre des unités dans le système de numération décimale.

Exercice 33

1) Soit n un entier naturel premier.

Montrer que si n divise $(5^n - 2^n)$ alors : $n = 3$

2) Soient p et q deux nombres entiers naturels premiers tels que : $3 < q < p$ et pq divise $(5^p - 2^p)(5^q - 2^q)$

a- Montrer que q divise $(5^p - 2^p)$

b- Soit a un entier naturel tel que : $2a \equiv 5[q]$

Montrer que q ne divise pas a et $a^p \equiv 1[q]$ et $a^{q-1} \equiv 1[q]$

c- En déduire que $a \equiv 1[q]$ (Remaquer que: $p \wedge (q-1) = 1$)

3) En déduire de tout ce qui précède que si p et q sont des entiers naturels premiers tels que : $q < p$ et pq divise $(5^p - 2^p)(5^q - 2^q)$, alors : $(p,q) = (13;3)$

Solution

1) Soit n un entier naturel premier tel que : n divise $(5^n - 2^n)$

D'après le théorème de Fermat : $5^n \equiv 5[n]$ et $2^n \equiv 2[n]$ (car n est premier)

Donc : $5^n - 2^n \equiv 3[n]$

et puisque : $n|(5^n - 2^n)$, alors : $n|3$, d'où : $n = 3$ (car n est premier)

2) a- On a : $q|pq$ et $pq|(5^p - 2^p)(5^q - 2^q)$

Donc : $q|(5^p - 2^p)(5^q - 2^q)$

Or $q \neq 3$ donc : q ne divise pas $(5^q - 2^q)$ (d'après la question 1)

et puisque q est premier

alors : $q \wedge (5^q - 2^q) = 1$

Donc d'après le théorème de Gauss : $q|(5^p - 2^p)$

b- • Si q divise a, alors : $2a \equiv 0[q]$, donc : $5 \equiv 0[q]$ c'est-à-dire : $q|5$

et par suite : $q = 5$

Or : $5^p - 2^p \equiv 0[q]$ (d'après la question précèdente)

Donc : $5^p - 2^p \equiv 0[5]$

par suite, $2^p \equiv 0[5]$ c'est-à-dire : $5|2^p$, donc : $5|2$ car 5 est premier, ce qui est faux et par suite : q ne divise pas a

• On a : $2a \equiv 5[q]$, donc : $(2a)^p \equiv 5^p[q]$

par suite, $2^p(a^p - 1) \equiv 5^p - 2^p[q]$

c'est-à-dire : $2^p(a^p - 1) \equiv 0[q]$ car q divise $(5^p - 2^p)$

Or : $q \wedge 2^p = 1$ donc : $a^p - 1 \equiv 0[q]$

par suite, $a^p \equiv 1[q]$

• Le nombre q est premier et ne divise pas a (car $a^p \equiv 1[q]$)

Donc, d'après le théorème de Fermat : $a^{q-1} \equiv 1[q]$

c- • On a : $q - 1 < q$, donc : $q - 1 < p$

et comme p est premier, alors : $p \wedge (q-1) = 1$

Donc, d'après le théorème de Bezout : $(\exists (u,v) \in \mathbb{N}^2)(q-1)u - pv = 1$

• On a : $a^{q-1} \equiv 1[q]$, donc : $(a^{q-1})^u \equiv 1[q]$

et par suite : $a^{1+pv} \equiv 1[q]$, c'est-à-dire : $a(a^p)^v \equiv 1[q]$

Or : $a^p \equiv 1[q]$, donc : $(a^p)^v \equiv 1[q]$

Par suite, $a \equiv 1[q]$

3) Soient p et q deux entiers naturels premiers tels que : $q < p$

et $pq|(5^p - 2^p)(5^q - 2^q)$

• Si : $3 < q < p$ et a un entier naturel tel que : $2a \equiv 5[q]$ (un tel nombre existe, il suffit par exemple de prendre $a = \dfrac{q+5}{2}$)

Alors (d'après 2)c) : $a \equiv 1[q]$

Donc : $2 \equiv 5[q]$, c'est-à-dire : $3 \equiv 0[q]$

et par suite q divise 3, donc : $q = 3$ ce qui contredit le fait que : $q > 3$

• Si $q = 2$ on aurait : $5^p - 2^p \equiv 0[2]$ car $q|(5^p - 2^p)$ d'après 2)a)

c'est-à-dire : $1 \equiv 0[2]$ ce qui est faux.

Donc : $q \neq 2$

- Alors nécessairement : $q = 3$

On a donc : $p > 3$ et $3p|117(5^p - 2^p)$

Par suite, $p|39(5^p - 2^p)$

et comme $p \neq 3$ (car $p > 3$) alors p ne divise pas $(5^p - 2^p)$ (d'après 1)

et puisque p est premier alors : $p \wedge (5^p - 2^p) = 1$

Donc, d'après le théorème de Gauss : $p|39$

Par suite, $p = 13$ (car p premier et $p > 3$)

Donc : $(p,q) = (13;3)$

Exercice 34

Soient a et b deux éléments de $\mathbb{N}^* - \{1\}$ tels que : $a \wedge b = 1$

1) Montrer que : $(a^2 + ab + b^2) \wedge (a^2 + b^2) = 1$

2) Soit p un nombre premier tel que : $p \geq 5$ et $p|(a^2 + ab + b^2)$

a- Montrer que : $p \wedge a = 1$ et $p \wedge b = 1$

b- Montrer que : $a^3 \equiv b^3 [p]$

c- Montrer que si $p = 5 + 6k$ où $k \in \mathbb{N}$, alors : $a \equiv b[p]$, puis que : $p|3ab$

d- En déduire que : $p \equiv 1[6]$

3) Résoudre dans $(\mathbb{N}^*)^2$ l'équation : $x^2 + xy + y^2 = 34(x \wedge y)^2$

Solution

1) On pose : $(a^2 + ab + b^2) \wedge (a^2 + b^2) = d$

- On a : $d|a^2 + ab + b^2$ et $d|a^2 + b^2$

Donc : $d|ab$ (car : $(a^2 + ab + b^2) - (a^2 + b^2) = ab$)

D'où : $d|ab^2$ et $d|a^3 + ab^2$ (car : $a(a^2 + b^2) = a^3 + ab^2$)

et par suite : $d|a^3$

- de même on obtient : $d|b^3$
- On a donc : $d|a^3$ et $d|b^3$

D'où : $d|a^3 \wedge b^3$

Or : $a \wedge b = 1$ donc : $a^3 \wedge b^3 = 1$

et par suite : $d|1$, d'où : $d = 1$

Donc, $(a^2 + ab + b^2) \wedge (a^2 + b^2) = 1$

2) a- • Supposons que : $p \wedge a \neq 1$

Donc : $p \wedge a = p$ (car p est premier), par suite, $p|a$

Donc : $p|a^2 + ab$ (car : $a^2 + ab = a(a + b)$)

Or : $p|a^2 + ab + b^2$, donc : $p|b^2$ (car : $(a^2 + ab + b^2) - (a^2 + ab) = b^2$)

On a : $p|a$ et $p|b^2$, donc : $p|a \wedge b^2$

Or : $a \wedge b = 1$, donc : $a \wedge b^2 = 1$

par suite, $p|1$, d'où : $p=1$ ce qui est faux
Donc : $p \wedge a = 1$
• Montrer de même que : $p \wedge b = 1$
b- On a : $a^3 - b^3 = (a-b)(a^2+ab+b^2)$
et puisque : $p|a^2+ab+b^2$
alors : $p|a^3-b^3$, d'où : $a^3 \equiv b^3[p]$
c- • Supposons que : $p = 5+6k \ (k \in \mathbb{N})$
Le nombre p est premier et : $p \wedge a = 1$ et $p \wedge b = 1$
Donc, d'après le théorème de Fermat : $a^{p-1} \equiv 1[p]$ et $b^{p-1} \equiv 1[p]$
C'est-à-dire : $a^{4+6k} \equiv 1[p]$ et $b^{4+6k} \equiv 1[p]$
Donc : $a^{4+6k} \equiv b^{4+6k}[p]$
C'est-à-dire : $a.(a^3)^{1+2k} \equiv b.(b^3)^{1+2k}[p]$
Or : $a^3 \equiv b^3[p]$, donc : $(a^3)^{1+2k} \equiv (b^3)^{1+2k}[p]$
et par suite : $a.(a^3)^{1+2k} \equiv b(a^3)^{1+2k}[p]$
et comme : $p \wedge a = 1$ alors : $p \wedge (a^3)^{1+2k} = 1$
Donc : $a \equiv b[p]$
• On a : $a \equiv b[p]$, donc : $p|a-b$ et par suite : $p|(a-b)^2$
Or : $p|a^2+ab+b^2$, donc : $p|(a^2+ab+b^2)-(a-b)^2$
C'est-à-dire : $p|3ab$
d- Un nombre premier est soit de la forme $6k+1$ ou de la forme $6k+5 \ (k \in \mathbb{N})$
Si $p = 6k+5$, alors d'après le résultat de la question précèdente : $p|3ab$
Or : $p \wedge a = 1$ et $p \wedge b = 1$, donc : $p \wedge ab = 1$
par suite $p|3$, donc : $p = 3$ ce qui contredit le fait que $p \geq 5$
Donc : $p = 6k+1 \ (k \in \mathbb{N})$ et par suite : $p \equiv 1[6]$
3) Soit $(x,y) \in (\mathbb{N}^*)^2$ tel que : $x^2+xy+y^2 = 34(x \wedge y)^2$
On pose : $d = x \wedge y$
Donc : $(\exists (a,b) \in (\mathbb{N}^*)^2) \ x = da$ et $y = db$ et $a \wedge b = 1$
par suite, $d^2(a^2+ab+b^2) = 34d^2$
C'est-à-dire : $a^2+ab+b^2 = 2 \times 17$
et par suite : $17|(a^2+ab+b^2)$
Donc, d'après ce qui précède : $17 \equiv 1[6]$
Ce dernier résultat est fausse.
Donc l'équation : $x^2+xy+y^2 = 34(x \wedge y)^2$ n'admet pas de solution dans $(\mathbb{N}^*)^2$

Exercice 35

On considère dans l'ensemble $\mathbb{N}^3$ l'équation : $(E): (\overline{xyz}^{(10)})^{143} \equiv 2\,[899]$
1) a- Résoudre dans $\mathbb{Z}^2$ l'équation : $143u - 840v = 1$
b- En déduire le plus petit nombre entier naturel d qui vérifie : $143d \equiv 1[840]$
2) Soit n un nombre entier naturel premier avec 899

a- Montrer que n est premier avec 29 et avec 31
b- En déduire que : $n^{840} \equiv 1[899]$
c- Montrer que si $n^{143} \equiv 2[899]$ alors : $n \equiv 2^{d}[899]$
3) Résoudre dans $\mathbb{N}^3$ l'équation (E)

Solution

1) a- • Il faut d'abord trouver une solution particulière de cette équation, on utilise l'algorithme d'Euclide :

$840 = 5 \times 143 + 125$ (1)
$143 = 125 + 18$ (2)
$125 = 6 \times 18 + 17$ (3)
$18 = 17 + 1$ (4)

On a : $1 = 18 - 17$ d'après (4)
$1 = 18 - (125 - 6 \times 18)$ d'après (3)
$1 = 7 \times 18 - 125$
$1 = 7 \times (143 - 125) - 125$ d'après (2)
$1 = 7 \times 143 - 8 \times 125$
$1 = 7 \times 143 - 8 \times (840 - 5 \times 143)$ d'après (1)
Donc : $143 \times 47 - 840 \times 8 = 1$

• On a : $143u - 840v = 1 \iff 143u - 840v = 143 \times 47 - 840 \times 8$

$$\iff 143(u-47) = 840(v-8)$$

$$\iff \begin{cases} 143(u-47) = 840(v-8) \\ 143 \mid 840(v-8) \end{cases}$$

$$\iff \begin{cases} 143(u-47) = 840(v-8) \\ 143 \mid v-8 \end{cases} \quad (\text{car } 143 \wedge 840 = 1)$$

$$\iff \begin{cases} 143(u-47) = 840 \times 143k \\ v - 8 = 143k \end{cases} (k \in \mathbb{Z})$$

$$\iff \begin{cases} u = 840k + 47 \\ v = 143k + 8 \end{cases} (k \in \mathbb{Z})$$

Donc l'ensemble de solutions de l'équation : $143u - 840v = 1$ est :
$S = \{(840k + 47, 143k + 8) / k \in \mathbb{Z}\}$

b- D'après ce qui précède, on a : $(\forall k \in \mathbb{Z})\ 143(840k + 47) - 840(143k + 8) = 1$
Donc : $143(840k + 47) \equiv 1[840]$ (*)
Par suite, le plus petit nombre entier naturel d qui vérifie $143d \equiv 1[840]$ est égal à 47 obtenu en remplaçant k par 0 dans la relation (*)

2) a- On a : $899 = 29 \times 31$
Et puisque : $n \wedge 899 = 1$ alors les nombres 29 et 31 ne sont pas des diviseurs de n
Et puisque les nombres 29 et 31 sont premiers

Alors : $n \wedge 29 = 1$ et $n \wedge 31 = 1$

b- On a : $n \wedge 29 = 1$ et 29 est un nombre premier

Donc : $n^{28} \equiv 1[29]$ (d'après le théorème de Fermat)

Par suite : $(n^{28})^{30} \equiv 1[29]$

C'est-à-dire : $n^{840} \equiv 1[29]$

et on a : $n \wedge 31 = 1$ et 31 est un nombre premier

Donc : $n^{30} \equiv 1[31]$ (d'après le théorème de Fermat)

Par suite : $(n^{30})^{28} \equiv 1[31]$

C'est-à-dire : $n^{840} \equiv 1[31]$

Donc : $29 | (n^{840} - 1)$ et $31 | (n^{840} - 1)$

Et puisque : $29 \wedge 31 = 1$

Alors : $29 \times 31 | (n^{840} - 1)$ c'est-à-dire : $899 | (n^{840} - 1)$

Par suite : $n^{840} \equiv 1[899]$

c- On suppose que : $n^{143} \equiv 2[899]$

et comme : $143d - 840 \times 8 = 1$ (on a vu que : $d = 47$)

Donc : $143d = 840 \times 8 + 1$

Et puisque : $n^{143} \equiv 2[899]$

Alors : $(n^{143})^d \equiv 2^d [899]$

C'est-à-dire : $n^{840 \times 8 + 1} \equiv 2^d [899]$

C'est-à-dire : $(n^{840})^8 . n \equiv 2^d [899]$

Et puisque : $n^{840} \equiv 1[899]$ alors : $(n^{840})^8 \equiv 1[899]$

Par suite : $n \equiv 2^d [899]$

3) Résolvons dans $\mathbb{N}^3$ l'équation (E): $(\overline{xyz}^{(10)})^{143} \equiv 2[899]$

On pose : $n = \overline{xyz}^{(10)}$

On peut appliquer les résultats précèdents car le nombre $\overline{xyz}^{(10)}$ est écrit dans le système décimal.

On a : $n \not\equiv 0[899]$, donc 899 ne divise pas n

Par suite, les nombres 29 et 31 ne divisent pas n (car $899 = 29 \times 31$)

D'où : $29 \wedge n = 1$ et $31 \wedge n = 1$ (car les nombres 29 et 31 sont premiers).

Donc : $(29 \times 31) \wedge n = 1$ c'est-à-dire : $899 \wedge n = 1$

Et puisque : $n^{143} \equiv 2[899]$

Alors : $n \equiv 2^{47} [899]$ (d'après **2) c-**)

C'est-à-dire : $n \equiv 345[899]$ (montrer que : $2^{47} \equiv 345[899]$)

Par suite : $n = 345 + 899k$ où $k \in \mathbb{Z}$

Et puisque : $100 \leq n \leq 999$

Alors : $k = 0$

Par suite : $n = 345$

Donc : $x = 3$ et $y = 4$ et $z = 5$

Conclusion : L'ensemble de solutions de l'équation (E) est : $S = \{(3;4;5)\}$

Exercice 36 Juin 2019

On admet que 2969 est un nombre premier.

Soient n et m deux entiers naturels vérifiant : $n^8 + m^8 \equiv 0[2969]$

1) On suppose dans cette question que 2969 ne divise pas n

a- En utilisant le théorème de BEZOUT, montrer que : $(\exists u \in \mathbb{Z})\ u.n \equiv 1[2969]$

b- En déduire que : $(n.m)^8 \equiv -1[2969]$ et que : $(u.m)^{2968} \equiv -1[2969]$

(On remarque que : $2968 = 8 \times 371$)

c- Montrer que 2969 ne divise pas $u \times m$

d- En déduire qu'on a aussi $(u \times m)^{2968} \equiv 1[2969]$

2) a- En utilisant les résultats précèdents, montrer que 2969 divise n

b- Montrer que : $n^8 + m^8 \equiv 0[2969] \Longleftrightarrow n \equiv 0[2969]$ et $m \equiv 0[2969]$

Solution

1) a- On suppose que 2969 ne divise pas n

et puisque 2969 est un nombre premier

alors : $2969 \wedge n = 1$

Par suite, d'après le théorème de Bezout : $(\exists(u,v) \in \mathbb{Z}^2)\ nu + 2969v = 1$

Donc : $(\exists(u,v) \in \mathbb{Z}^2)\ n.u + 2969v \equiv 1[2969]$

et par suite : $(\exists u \in \mathbb{Z})\ n.u \equiv 1[2969]$

b- • On a : $n^8 + m^8 \equiv 0[2969]$

donc : $u^8 n^8 + u^8 m^8 \equiv 0[2969]$

c'est-à-dire : $(u \times n)^8 + (m \times u)^8 \equiv 0[2969]$

et puisque : $(u \times n)^8 \equiv 1[2969]$ car $u \times n \equiv 1[2969]$

alors : $1 + (m \times u)^8 \equiv 0[2969]$

Donc : $(m \times u)^8 \equiv -1[2969]$

• On a : $(m \times u)^8 \equiv -1[2969]$

donc : $((m \times u)^8)^{371} \equiv (-1)^{371}[2969]$

c'est-à-dire : $(m \times u)^{2968} \equiv -1[2969]$

c- Si 2969 divise $u \times m$ alors : $u \times m \equiv 0[2969]$

par suite, $(u \times m)^{2968} \equiv 0[2969]$ ce qui contredit le résultat de la question précédente

Donc : 2969 ne divise pas $u \times m$

d- Puisque 2969 est un nombre premier et ne divise pas $u \times m$, alors d'après le théorème de Fermat, on a :

$(u \times m)^{2969-1} \equiv 1[2969]$, c'est-à-dire: $(u \times m)^{2968} \equiv 1[2969]$

2) a- Si 2969 ne divise pas n

Alors, d'après les résultats de la première question; on a : $(u \times m)^{2968} \equiv 1[2969]$ et $(u \times m)^{2968} \equiv -1[2969]$

Donc : $1 \equiv -1[2969]$
c'est-à-dire: 2969 divise 2, ce qui est faux
Donc : 2969 divise n
b- • Supposons que : $m \equiv 0[2969]$ et $n \equiv 0[2969]$
Donc : $m^8 + n^8 \equiv 0^8 + 0^8[2969]$
c'est-à-dire : $m^8 + n^8 \equiv 0[2969]$
• Supposons que : $n^8 + m^8 \equiv 0[2969]$
Donc d'après le résultat de la question 2)a), le nombre 2969 divise n
Par suite, $n \equiv 0[2969]$, d'où : $n^8 \equiv 0[2969]$
Donc : $m^8 \equiv 0[2969]$, d'où 2969 divise m^8
et puisque : 2969 est premier
alors : 2969 divise m, par suite : $m \equiv 0[2969]$

Exercice 37

I. Soit p un nombre premier tel que : $p \geq 7$

1) a- Vérifier que le nombre $\frac{p-1}{2}$ est un entier pair et que : $2 < \frac{p-1}{2} < p-2$

b- En déduire que $(p-1)^2$ divise $(p-1)!$

2) On suppose qu'il existe un entier naturel non nul n tel que : $(p-1)! = p^n - 1$

et on pose : $S = \sum_{k=0}^{n-1} p^k$

a- Montrer que : $S \equiv n[p-1]$ et en déduire que $(p-1)$ divise n

b- Montrer que $(p-1)$ divise S et en déduire que $(p-1)$ divise n — b- Montrer que $(p-1)$ divise S

c- Montrer que : $(p-1)^p < p^n$ (on admet que : $((\forall m \in \mathbb{N}^* - \{1\})\ m^m > 1 + m!)$

et en déduire que :$(p-1)! < p^n - 1$

II. Déterminer les nombres premiers positifs p pour lesquels il existe un entier non nul n tels que : $(p-1)! = p^n - 1$

III. Résoudre dans $\mathbb{N}$ l'équation : $1 + 11 + 11^2 + ... + 11^{n-1} = 362880$
$(10! = 3628800)$

Solution

I. 1) a- • Comme p est un nombre premier supérieur ou égal à 7
alors : $(\exists k \in \mathbb{N}^*)\ p = 4k + 1$ ou $p = 4k + 3$

par suite, $\frac{p-1}{2} = 2k$ ou $\frac{p-1}{2} = 2(k+1)$

Donc le nombre $\frac{p-1}{2}$ est un entier pair.

• On a : $p \geq 7$, donc : $\frac{p-1}{2} \geq 3$, d'où : $2 < \frac{p-1}{2}$

et on a : $(p-2)-\frac{p-1}{2}=\frac{p-3}{2}$

donc : $(p-2)-\frac{p-1}{2}>0$ car $p\geq 7$

par suite, $\frac{p-1}{2}<p-2$

d'où : $2<\frac{p-1}{2}<p-2$

b- • Si $p\geq 11$, on a :

$$\begin{aligned}(p-1)! &= 1\times 2\times 3\times\cdots\times(p-1)\\ &= 2\times 3\times\cdots\times\frac{p-3}{2}\times\frac{p-1}{2}\times\frac{p+1}{2}\times\cdots\times(p-2)\times(p-1)\\ &= 3\times\cdots\times\frac{p-3}{2}\times(p-1)\times\frac{p+1}{2}\times\cdots\times(p-2)\times(p-1)\\ &= (p-1)^2\times\left(3\times\cdots\times\frac{p-3}{2}\times\frac{p+1}{2}\times\cdots\times(p-2)\right)\end{aligned}$$

Donc : $(p-1)^2$ divise $(p-1)!$

• Si $p=7$, on a : $(7-1)!=6!=720$ et $(7-1)^2=36$ et 36 divise 720

• Par suite, si p est un nombre premier tel que : $p\geq 7$

alors $(p-1)^2$ divise $(p-1)!$

2) a- On a : $S=1+p+p^2+\cdots+p^{n-1}$

et on a : $1\equiv 1[p-1]$ et $p\equiv 1[p-1]$

Donc : $S\equiv\underbrace{1+1+\cdots+1}_{n\ fois}[p-1]$

C'est-à-dire : $S\equiv n[p-1]$

b- • On a : $S=\sum_{k=0}^{n-1}p^k=1\times\frac{1-p^n}{1-p}=\frac{p^n-1}{p-1}$

donc : $(p-1)S=p^n-1$

et puisqu'on a supposé que : $p^n-1=(p-1)!$ alors : $(p-1)S=(p-1)!$

et comme $(p-1)^2$ divise $(p-1)!$, donc : $(p-1)!=\alpha(p-1)^2$ où α est un nombre entier naturel non nul

par suite, $(p-1)S=\alpha(p-1)^2$, d'où $S=\alpha(p-1)$

Donc : $(p-1)$ divise S

• On a : $S\equiv 0[p-1]$ car : $(p-1)$ divise S

Or $S\equiv n[p-1]$, donc : $n\equiv 0[p-1]$, par suite, $(p-1)$ divise n

c- On a : $(p-1)|n$, donc : $p-1\leq n$

• Si : $p-1=n$ alors : $n!=(n+1)^n-1$ car $(p-1)!=p^n-1$

par suite, $(n+1)^n=n!+1$

Or : $(n+1)^n>n^n>1+n!$

Ce qui contredit l'égalité : $(n+1)^n=n!+1$

Donc : $p-1<n$ c'est-à-dire : $p \leq n$

par suite, $(p-1)^p < p^p$ et $p^p \leq p^n$, donc: $(p-1)^p < p^n$

• Pour tout $k \in \{1,2,...,p-2\}$ on a : $k < p-1$

donc : $(p-2)! < (p-1)^{p-2}$

par suite, $(p-1)\times(p-2)! < (p-1)^{p-1}$ c'est-à-dire : $(p-1)! < (p-1)^{p-1}$

Or : $(p-1)^{p-1} < (p-1)^p$ et $(p-1)^p < p^n$

donc : $(p-1)! < (p-1)^{p-1} < p^n$

Par suite, $(p-1)!+1 < p^n$, d'où $(p-1)! < p^n - 1$

II. Soit p un nombre premier positif.

• Si $p \geq 7$ et s'il existe un entier non nul n tel que : $(p-1)! = p^n - 1$

Alors : $(p-1)! < p^n - 1$ d'après ce qui précède, ce qui est impossible.

Donc pour les nombres premiers p tels que : $p \geq 7$, il n'existe pas d'entier n tel que $(p-1)! = p^n - 1$

• Si $p = 5$, on a : $(p-1)! = 24$ et $p^2 - 1 = 24$

Donc : $(5-1)! = 5^2 - 1$

• Si $p = 3$, on a : $(p-1)! = 2$ et $p^1 - 1 = 2$

Donc : $(3-1)! = 3^1 - 1$

• Si $p = 2$, on a : $(p-1)! = 1$ et $p^1 - 1 = 1$

Donc : $(2-1)! = 2^1 - 1$

Conclusion :

Les nombres premiers positifs p pour lesquels il existe un entier naturel non nul n tels que : $(p-1)! = p^n - 1$ sont 2 , 3 et 5

III. Soit $n \in \mathbb{N}$, on a :

$$\begin{aligned} 1 + 11 + 11^2 + \cdots + 11^{n-1} = 362880 &\Leftrightarrow \frac{11^n - 1}{11 - 1} = 362880 \\ &\Leftrightarrow 11^n - 1 = 3628800 \\ &\Leftrightarrow 11^n - 1 = 10! \\ &\Leftrightarrow (11-1)! = 11^n - 1 \end{aligned}$$

et comme 11 est premier et $11 \geq 7$, alors d'après le résultat de la partie **II** l'égalité $1 + 11 + 11^2 + \cdots + 11^{n-1} = 362880$ ne peut pas exister.