Exercice N°5

Soit a un entier naturel supérieur ou égal à 2 et soit

$A = 1 + a + a^2 + a^3 + a^4 + a^5 + a^6$

Soit p un nombre premier impair tel que p divise A

1/ a/ Montrer que $a^7 \equiv 1\ [p]$

En déduire que $\forall n \in IN,\ a^{7n} \equiv 1\ [p]$

b/ Montrer que a et p sont premier entre eux.

En déduire que $\forall m \in IN,\ a^{(p-1)m} \equiv 1\ [p]$

2/ On suppose que 7 ne divise pas $p - 1$

a/ Montrer que $a \equiv 1\ [p]$

b/ En déduire que $p = 7$

c/ Montrer que si p est un nombre premier impair tel que p divise A alors $p = 7$ ou $p \equiv 1\ [7]$

Exercice N°5

Soit a un entier naturel supérieur ou égal à 2 et soit

$A = 1 + a + a^2 + a^3 + a^4 + a^5 + a^6$

Soit p un nombre premier impair tel que p divise A

1/ a/ Montrer que $a^7 \equiv 1\ [p]$

En déduire que $\forall n \in IN,\ a^{7n} \equiv 1\ [p]$

b/ Montrer que a et p sont premier entre eux.

En déduire que $\forall m \in IN,\ a^{(p-1)m} \equiv 1 [p]$

2/On suppose que 7 ne divise pas p–1

a/ Montrer que $a \equiv 1\ [p]$

b/ En déduire que p = 7

c/ Montrer que si p est un nombre premier impair tel que p divise A alors p = 7 ou $p \equiv 1\ [7]$

1) a) $a^7 - 1 = (a-1)(a^6 + a^5 + \dots + 1) = (a-1)A$.

$p \mid A \rightarrow p \mid (a-1)A \rightarrow p \mid (a^7 - 1)$

$\rightarrow a^7 - 1 \equiv 0 [p] \rightarrow a^7 \equiv 1 [p]$

$a^7 \equiv 1 [p] \rightarrow (a^7)^n \equiv 1 [p] \rightarrow a^{7n} \equiv 1 [p]$

b) p premier $\rightarrow a \wedge p = 1$ ou $a \wedge p = p$.

si $a \wedge p = p$ alors $p \mid a \rightarrow a \equiv 0 [p] \rightarrow a^7 \equiv 0 [p]$

or $a^7 \equiv 1 [p]$ donc $1 \equiv 0 [p] \rightarrow p \mid 1 \rightarrow p = 1$

absurde car p premier.

d'où $a \wedge p = 1$

Exercice N°5

Soit a un entier naturel supérieur ou égal à 2 et soit

$A = 1 + a + a^2 + a^3 + a^4 + a^5 + a^6$

Soit p un nombre premier impair tel que p divise A

1/ a/ Montrer que $a^7 \equiv 1\ [p]$

En déduire que $\forall n \in \mathbb{N}$, $a^{7n} \equiv 1\ [p]$

b/ Montrer que a et p sont premier entre eux.

En déduire que $\forall m \in \mathbb{N}$, $a^{(p-1)m} \equiv 1 [p]$

2/On suppose que 7 ne divise pas p–1

a/ Montrer que $a \equiv 1\ [p]$

b/ En déduire que $p = 7$

c/ Montrer que si p est un nombre premier impair tel que p divise A alors $p = 7$ ou $p \equiv 1\ [7]$

$\left.\begin{array}{l} p \text{ premier} \\ p \nmid a \end{array}\right\} \xrightarrow{\text{Fermat}} a^{p-1} \equiv 1\ [p]$

$\longrightarrow (a^{p-1})^m \equiv 1\ [p]$

$\longrightarrow a^{(p-1)m} \equiv 1\ [p]$

2) a) $\left.\begin{array}{l} 7 \text{ premier} \\ 7 \nmid p-1 \end{array}\right\} \longrightarrow 7 \wedge (p-1) = 1$ donc, d'après (l'identité de Bézout, il existe

$(n,m) \in \mathbb{Z}^2$ tq : $7n + (p-1)m = 1$

1^er cas $m \geq 0$ et $n \geq 0$: $1 = 7n + (p-1)m \geq 7$ absurde.

2^e cas : $m < 0$ et $n < 0$: $1 = 7n + (p-1)m < 0$ absurde

3^e cas $m \leq 0$ et $n \geq 0$: $-m \in \mathbb{N}$ donc, d'après b), $a^{-(p-1)m} \equiv 1\ [p] \xrightarrow{\times a} a^{1-(p-1)m} \equiv a\ [p]$

$\longrightarrow a^{7n} \equiv a\ [p]$ or $a^{7n} \equiv 1\ [p]$ donc $a \equiv 1\ [p]$.

Exercice N°5

4ème cas : $m > 0$ et $n \leq 0$

$-n \in \mathbb{N}$ donc $a^{-7n} \equiv 1\ [p] \xrightarrow{\times a} a^{1-7n} \equiv a\ [p]$

$\longrightarrow a^{(p-1)m} \equiv a\ [p]$ or $a^{(p-1)m} \equiv 1\ [p]$

Alors $a \equiv 1\ [p]$.

cl : $a \equiv 1\ [p]$

b) $a \equiv 1\ [p] \longrightarrow a^{k} \equiv 1\ [p]\ ,\ \forall k \in \{0, 1, 2, \ldots, 6\}$

$\longrightarrow A \equiv 7\ [p]$ or $A \equiv 0\ [p]$

donc $7 \equiv 0\ [p] \longrightarrow p \mid 7 \xrightarrow{p \text{ premier}} p = 7$

Soit a un entier naturel supérieur ou égal à 2 et soit

$A = 1 + a + a^2 + a^3 + a^4 + a^5 + a^6$

Soit p un nombre premier impair tel que p divise A

1/ a/ Montrer que $a^7 \equiv 1\ [p]$

En déduire que $\forall n \in \mathbb{N}$, $a^{7n} \equiv 1\ [p]$

b/ Montrer que a et p sont premier entre eux.

En déduire que $\forall m \in \mathbb{N}$, $a^{(p-1)m} \equiv 1[p]$

2/On suppose que 7 ne divise pas p–1

a/ Montrer que $a \equiv 1\ [p]$

b/ En déduire que p = 7

c/ Montrer que si p est un nombre premier impair tel que p divise A alors p = 7 ou $p \equiv 1\ [7]$

Exercice N°5

c). si 7 divise $p-1$ alors $p-1=7k \rightarrow p=1+7k$

$\rightarrow p \equiv 1\,[7]$

• si 7 ne divise pas $p-1$ alors, d'après 2/b) $p=7$

cqfd

Soit a un entier naturel supérieur ou égal à 2 et soit

$A = 1 + a + a^2 + a^3 + a^4 + a^5 + a^6$

Soit p un nombre premier impair tel que p divise A

1/ a/ Montrer que $a^7 \equiv 1$ [p]

En déduire que $\forall n \in \mathbb{N}$, $a^{7n} \equiv 1$ [p]

b/ Montrer que a et p sont premier entre eux.

En déduire que $\forall m \in \mathbb{N}$, $a^{(p-1)m} \equiv 1$[p]

2/On suppose que 7 ne divise pas p–1

a/ Montrer que $a \equiv 1$ [p]

b/ En déduire que p = 7

c/ Montrer que si p est un nombre premier impair tel que p divise A alors p = 7 ou $p \equiv 1$ [7]

Exercice N°6

Soient p et q deux nombres premiers vérifiant :

$$p < q \text{ et } 9^{p+q-1} \equiv 1 \; [pq]$$

1/ a/ Montrer que p et 9 sont premiers entre eux.

b/ En déduire que : $9^{p-1} \equiv 1 \; [p]$ et $9^{q} \equiv 1 \; [p]$

2/ a/ Montrer que $p - 1$ et q sont premiers entre eux.

b/ En utilisant le théorème de Bézout, montrer que $p = 2$

3/ a/ Montrer que $9^{q-1} \equiv 1 \; [q]$

b/ En déduire que : $q = 5$.

Exercice N°6

Soient p et q deux nombres premiers vérifiant :

$p < q$ et $9^{p+q-1} \equiv 1\ [pq]$

1/ a/ Montrer que p et 9 sont premiers entre eux.

b/ En déduire que : $9^{p-1} \equiv 1\ [p]$ et $9^q \equiv 1\ [p]$

2/ a/ Montrer que $p - 1$ et q sont premiers entre eux.

b/ En utilisant le théorème de Bézout, montrer que $p = 2$

3/ a/ Montrer que $9^{q-1} \equiv 1\ [q]$

b/ En déduire que : $q = 5$.

1) a) $9^{p+q-1} \equiv 1\ [pq] \iff$ il existe $k \in \mathbb{N}$ tq :

$9^{p+q-1} = pqk + 1 \iff 9^{p+q-1} - pqk = 1$

posons $d = 9 \wedge p$.

$\left.\begin{array}{l} d \mid 9 \\ d \mid p \end{array}\right\} \Rightarrow d \mid 9^{p+q-1} - pqk = 1 \rightarrow d = 1$

$\Rightarrow 9 \wedge p = 1$

b) $\left.\begin{array}{l} p \text{ premier} \\ p \nmid 9 \end{array}\right\} \xrightarrow{\text{Fermat}} 9^{p-1} \equiv 1\ [p]$

$9^{p-1} \equiv 1\ [p] \rightarrow 9^q \times 9^{p-1} \equiv 9^q\ [p] \rightarrow 9^{p+q-1} \equiv 9^q\ [p]$

or $9^{p+q-1} \equiv 1\ [pq] \rightarrow pq \mid 9^{p+q-1} - 1 \rightarrow p \mid 9^{p+q-1} - 1 \Rightarrow 9^{p+q-1} \equiv 1\ [p]$

$\longrightarrow 9^q \equiv 1\ [p]$

Exercice N°6

Soient p et q deux nombres premiers vérifiant :

$p < q$ et $9^{p+q-1} \equiv 1\ [pq]$

1/ a/ Montrer que p et 9 sont premiers entre eux.

b/ En déduire que : $9^{p-1} \equiv 1\ [p]$ et $9^{q} \equiv 1\ [p]$

2/ a/ Montrer que $p - 1$ et q sont premiers entre eux.

b/ En utilisant le théorème de Bézout, montrer que $p = 2$

3/ a/ Montrer que $9^{q-1} \equiv 1\ [q]$

b/ En déduire que : $q = 5$.

2/ a) $\left.\begin{array}{l} p-1 < p < q \\ q \text{ premier} \end{array}\right\} \longrightarrow (p-1) \wedge q = 1$

b) $(p-1)\wedge q = 1 \xrightarrow{\text{Bézout}}$ il existe $(u,v) \in \mathbb{Z}^2$ tq :

$(p-1)u + qv = 1$

1er cas : $u \geq 0$ et $v > 0$: $1 = (p-1)u + qv > 1$ absurde.

2e cas : $u \leq 0$ et $v < 0$: $1 = (p-1)u + qv < 0$ absurde

3e cas : $u \geq 0$ et $v \leq 0$: $-v \geq 0$ $\quad 9^{q} \equiv 1\ [p] \longrightarrow 9^{-qv} \equiv 1\ [p]$

$\xrightarrow{\times 9} 9^{1-qv} \equiv 9\ [p] \longrightarrow (9^{p-1})^{u} \equiv 9\ [p]$

or $9^{p-1} \equiv 1\ [p]$ donc $9 \equiv 1\ [p] \longrightarrow p \mid 8 \xrightarrow{p \text{ premier}} \boxed{p = 2}$

4e cas : $u \leq 0$ et $v \geq 0$. $-u \geq 0$ $\quad 9^{p-1} \equiv 1\ [p] \longrightarrow 9^{-(p-1)u} \equiv 1\ [p]$

$\xrightarrow{\times 9} 9^{1-(p-1)u} \equiv 9\ [p] \longrightarrow (9^{q})^{v} \equiv 9\ [p] \longrightarrow 9 \equiv 1\ [p] \longrightarrow \boxed{p = 2}$

Exercice N°6

3/ a) $9^{q+1} \equiv 1 [2q] \longrightarrow 2q \mid (9^{q+1}-1)$

$\longrightarrow q \mid (9^{q+1}-1) \longrightarrow 9^{q+1} \equiv 1 [q]$

$\longrightarrow 9 \times 9^{q} - kq = 1 \xrightarrow{\text{Bézout}} 9 \wedge q = 1$

$\left.\begin{array}{l} q \text{ premier} \\ q \text{ ne divise pas } 9 \end{array}\right\} \xrightarrow{\text{Fermat}} 9^{q-1} \equiv 1 [q]$

b) $\begin{cases} 9^{q+1} \equiv 1 [q] \\ 9^{q-1} \equiv 1 [q] \end{cases} \longrightarrow \begin{cases} 9^{q+1} \equiv 1 [q] \\ 9^{q+1} \equiv 9^{2} [q] \quad (\times 9^{2}) \end{cases}$

$\longrightarrow 9^{2} \equiv 1 [q] \longrightarrow q \mid 9^{2}-1 = 80 = 2^{4} \times 5$

$\xrightarrow[q>2]{q \text{ premier}} q = 5$

Soient p et q deux nombres premiers vérifiant :

$p < q$ et $9^{p+q-1} \equiv 1 [pq]$

1/ a/ Montrer que p et 9 sont premiers entre eux.

b/ En déduire que : $9^{p-1} \equiv 1 [p]$ et $9^{q} \equiv 1 [p]$

2/ a/ Montrer que $p - 1$ et q sont premiers entre eux.

b/ En utilisant le théorème de Bézout, montrer que $p = 2$

3/ a/ Montrer que $9^{q-1} \equiv 1 [q]$

b/ En déduire que : $q = 5$.