TD

M22

Limites & Continuités

Limites M22 & Continuité

Vianney Combey

+

Congruences

1

Congruences

TD.

①

Ex 26 : Mq $\forall m \in \mathbb{N}, \exists n \in \mathbb{N}$,

/ $[\![n, n+m]\!]$ ne contienne aucun nbre premier

On pose l'intervalle d'entiers,

$$[\![(m+2)!+2, (m+2)!+2+m]\!],$$

si $m \leq (m+2)! \Rightarrow m \mid (m+2)!$ dc $m \mid (m+2)!+m$

Donc $(m+2)!+m$ n'est pas premier.

De m̂ pour $(m+2)!+m+2$.

Pour $m=0$, $(m+2)!+2$ n'est pas premier.

Dc $[\![(m+2)!+2, (m+2)!+2+m]\!]$ ne contient aucun nbre premier.

Ex 27 : Un nbr de Fermat est entier

$$F_n = 2^{2^n} + 1 \text{ où } n \in \mathbb{N}.$$

a) soit F_n, F_m 2 NDF tq $n > m$.

Mq si p est un nbre premier q divise F_m alors $2^{2^n} \equiv 1 \, [p]$.

On note $k = n - m \geq 1$, comme par hypothèse, $p \mid F_m$ alors $F_m \equiv 0 \, [p]$.

soit $2^{2^m} \equiv -1 \, [p]$ (on élève la puissance à la puissance paire)

② $\left(2^{2^m}\right)^{2^k} = 2^{2^{m+k}} \equiv 2^{2^n} \equiv 1 \, [p]$

b) En déd. 2 NDF distincts st PEE.

soit $n > m$, sibi A !! $(F_n \wedge F_m) \geq 2$

soit p : NP q divise $(F_n \wedge F_m)$. Alors $p \mid F_m$

et de $2^{2^n} \equiv 1 \, [p]$ d'après a).

Mais p divise aussi F_n, dc on a ici $2^{2^n} \equiv -1 \, [p]$

Par transitivité de congruence (mod p), on a

$-1 \equiv 1 \, [p]$, soit $2 \equiv 0 \, [p]$ & dc $p \mid 2$.

Puisque p & 2 : PEE, on obtient $p=2$, dc F_n est pair $\boxed{c?!c}$

c) on déd., preuve infinitude nbr premiers

$\forall n \in \mathbb{N}$, on note p_n un diviseur premier de F_n.

Les F_n étant PEE 2 à 2 d'après b), on en déduit que les p_n st distincts 2 à 2.

On a dc trouvé ∞té nbrs premiers, $p_0, p_1, p_2 \ldots$

Ex 22 : soit p : 𝒫. Mq $\forall x \in [\![1, p-1]\!]$ $\exists$ uniq entier $x' \in [\![1, p-1]\!]$, $xx' \equiv 1\ [p]$

soit $x \in [\![1, p-1]\!]$ alors $p \nmid x$, dc $(x \wedge p) = 1$, par TH, on en déduit $\exists$ uniq inverse de x (mod p), dc un uniq $x' \in [\![1, p-1]\!]$ tq $xx' \equiv 1\ [p]$.

b) p : 𝒫 Résoudre (mod p) $x^2 \equiv 1\ [p]$.

$$x^2 \equiv 1\ [p] \Leftrightarrow p \mid x^2 - 1 = (x-1)(x+1)$$

$$\Leftrightarrow p \mid x-1 \text{ ou } p \mid x+1 \quad \text{par lemme Euclide.}$$

$$\Leftrightarrow x - 1 \equiv 0\ [p] \Leftrightarrow x + 1 \equiv 0\ [p]$$

$$\Leftrightarrow x \equiv 1\ [p] \Leftrightarrow x \equiv -1 \equiv p-1\ [p].$$

ef 1 et $p-1$ st ss entiers de $[\![1, p-1]\!]$ q st lr propre inverse au sens a)

c) Edⁿ TH Wilson : mtre $p \geq 2$ est 𝒫 ssi $(p-1)! \equiv -1\ [p]$

sthi p 𝒫, mq $(p-1)! \equiv -1\ [p]$.

si $p = 2$, on a bien $(p-1)! \equiv 1 \equiv -1\ [2]$

sthi $p \geq 5$ alors $(p-1)! = 1 \times 2 \times \cdots (p-2)(p-1)$.

On regroupe les $\frac{p-3}{2}$ paires d'entiers $(x, x') \in [\![2, p-2]\!]^2$ + $x \neq x'$ tq $xx' \equiv 1\ [p]$.

$$2 \times 3 \times \cdots \times (p-2) \equiv 1 \times \cdots \times 1 \equiv 1\ [p]$$

Dc $(p-1)! \equiv 1 \times (p-1) \equiv p - 1 \equiv -1\ [p]$.

(Rec) soit $p \geq 2$, 𝒫 vérif $(p-1)! \equiv -1\ [p]$.

sthi (!!) p : ~~𝒫~~, notons d, divisⁿ de p : $2 \leq d \leq p-1$

ef $d \mid (p-1)!$ Dc+, $p \mid (p-1)! + 1$ par hypothèse.

Ex 23 : Mq $\exists$ ∞té 𝒫, $p \equiv 3\ [4]$.

sthi (?!) $\exists$ nbre fini nbp, $p \equiv 3\ [4]$.

on les note $p_1 < p_2 < \cdots < p_k$. soit $n = 4p_1p_2 \cdots p_k - 1$

Alors n est impair, $n \equiv -1 \equiv 3\ [4]$ &

$n \geq 11$ puisq $p_1 = 3$.

(Rq) $\forall 1 \leq i \leq k$, $p_i \nmid n$.

(DFP) $n = q_1^{\alpha_1} q_2^{\alpha_2} \cdots q_m^{\alpha_m}$, comme n est impair alors $\forall 1 \leq j \leq m$, on a $q_j \neq 2$. Comme $p_i \nmid n$ $\forall 1 \leq i \leq k$ alors $p_i \neq q_j$ $\forall 1 \leq i \leq k$ et tout $1 \leq j \leq m$. On en déduit que $\forall$ $1 \leq j \leq m$, on a $q_j \equiv 1\ [4]$, dc $n \equiv 1\ [4]$ par produit.

MS par construcⁿ, on a $n \equiv 3\ [4]$, d'où $\boxed{c?!c}$

Ex 22

Reste DE $\sum_{k=1}^{2002} k!$ par 15 ?

Rq $15 \mid k!$ pour $k \geq 5$ dc

$$\sum_{k=1}^{2002} k! \equiv 1! + 2! + 3! + 4! \equiv 1 + 2 + 6 + 24 \equiv 33 \equiv 3\ [15].$$

Ex 23 : soit $a^3 + 1 = (a+1)(a^2 - a + 1)$. si $a^3 + 1$ est 𝒫, $a \in \mathbb{N}$ alors

pq $a + 1 \geq 1 \Rightarrow a^3 + 1 \geq 1$, on nddt $a + 1 = 1$ ou $a^2 - a + 1 = 1$.

si $a + 1 = 1$ alors $a = 0$ ou $a^3 + 1 = 1$ q n'est ~~𝒫~~.

Ainsi $a^2 - a + 1 = 1$ soit $a(a-1) = 0 \Rightarrow$ ~~$a = 0$~~ ou $a = 1$. Dc $a = 1$.

Mq $2^n - 1$ 𝒫 alors n 𝒫. (!!) sthi n ~~𝒫~~. si $n = 0$ ou $n = 1$ alors $2^n - 1$ vaut 0 ou 1 q ~~𝒫~~. si $n \geq 4$, on a $n = rs$, $1 < r < n$, $1 < s < n$ Alors $X^s - 1 = (X-1)(1 + X + \cdots + X^{s-1})$, Dc

$2^n - 1 = (2^r)^s - 1 = (2^r - 1)(1 + 2^r + (2^r)^2 + \cdots + (2^r)^{s-1})$, $2^n -$

dc $2^r - 1 \mid 2^n - 1$ &, $1 < r < n$ alors $1 < 2^r - 1 < 2^n - 1$ n'est

Ex 24 : Trver entiers n tq

a) n est divisible par 4 & le reste de DE de n par 3 ou par 5 est 2.

$$\begin{cases} n \equiv 0\ [4] \\ n \equiv 2\ [3] \\ n \equiv 2\ [5] \end{cases}$$

soit n un entier soluⁿ de ce système, ef d'après 3° éqⁿ, $\exists k \in \mathbb{Z}$, $n = 2 + 5k$.

D'après 2° éq, $2 + 5k \equiv 2 - k \equiv 2\ [3]$

Dc $k \equiv 0\ [3]$, ainsi $\exists m \in \mathbb{Z}$, $k = 3m$,

dc $n = 2 + 5 \times 3m = 2 + 15m$.

Enfin d'ap 1° eq, on a $2 + 15m \equiv 2 - m \equiv 0\ [4]$

soit $m \equiv 2\ [4]$ dc $\exists l \in \mathbb{Z}$, $m = 2 + 4l$,

et $n = 2 + 15 \times (2 + 4l) = 32 + 60l$.

En vérifiant récipqt, $\forall n \in \mathbb{N}$, $n = 32 + 60l$ + $l \in \mathbb{Z}$, on en déduit que ens entiers n vérifiant (est $\{32 + 60l, l \in \mathbb{Z}\}$

b) Trouver reste DE de n par 11 est 4 ..., $\begin{cases} n \equiv 4\ [11] \\ n \equiv 3\ [17] \end{cases}$

soit n entier soluⁿ de ce système,

alors $n = 4 + 11a$, $a \in \mathbb{Z}$, $n = 3 + 17b$, $b \in \mathbb{Z}$.

ef $11a - 17b = -1$, & $(11 \wedge 17) = 1$: PEE.

Cette équaⁿ possède soluⁿs $\left(11 \wedge 17 \mid -1\right)$. Rq $(a_0, b_0) = (3, 2)$

On obtient dc $a = 3 + 17k$, $b = 2 + 11k$ + $k \in \mathbb{Z}$.

On en déduit $n = 4 + 11(3 + 17k) = 37 + 187k$.

On vérifie récipqt tt entier n, de la forme $37 + 187k$

$$\Rightarrow \mathcal{S} = \{37 + 187k, k \in \mathbb{Z}\}.$$

Ex 25 m, n : PEE, Mq $\forall y, z \in \mathbb{Z}$, $\exists x \in \mathbb{Z}$ tq $\begin{cases} x \equiv y\ [m] \\ x \equiv z\ [n] \end{cases}$

et que ttes ces soluⁿs st congrues (mod mn).

soit x un entier soluⁿ de ce système,

$\exists$ donc $a, b \in \mathbb{Z}$ tq $\begin{cases} x = y + am \\ x = z + bn. \end{cases}$

Il suffit de résoudre $am - bn = z - y$.

comme m & n : PEE, cette équaⁿ admt soluⁿs, (a_0, b_0) soluⁿs particulières.

On a $a = a_0 + kn$ & $b = b_0 + km$, $k \in \mathbb{Z}$

D'où $x = y + m(a_0 + kn) = y + m a_0 + kmn$

Donc $x = y + m \cdot a_0\ [mn]$

Ex 11 Résoudre $4x \equiv 8\ [16]$

$\forall$ entier x, on a $4x \equiv 8\ [16] \Leftrightarrow \exists k \in \mathbb{Z}, 4x - 8 = 16k$

$\Leftrightarrow \exists k \in \mathbb{Z}, x - 2 = 4k$

$\Leftrightarrow x \equiv 2\ [4]$.

Ex 17 : Trouvons inverse (mod 13) de 2 et 11. ⑦

⚠ comme $2 \wedge 13 = 1$, 2 est bien inversible (mod 13).
Trouver son inverse revient à trouver une sol° de Bézout entre 2 & 13 : Évident : $2 \times 7 - 13 \times 1 = 1$.
Dc l'inverse de 2 (mod 13) est 7.

Rq $11 \equiv -2$ [13], dc l'inverse de 11 (mod 13) est -7.

b) Mq si a' est l'inverse de a [m] & b' l'inverse de b [m] alors a'b' est l'inverse de ab [m]

comme $a'a \equiv 1$ [m] & $b'b \equiv 1$ [m] alors en multipliant les congruences : $(a'a)(b'b) = (a'b')(ab) \equiv 1$ [m]
$= ab \equiv 1$ [m].

Ex 18 Résoudre $\begin{cases} x \equiv 2 \ [5] \\ x \equiv 3 \ [7] \end{cases}$.

• ∃ $(k, l) \in \mathbb{Z}^2$ tq $\begin{cases} x = 2+5k \\ x = 3+7l \end{cases} \Rightarrow$ $5k+2 = 7l+3$
$5k - 7l = 1$.

Résolvons ds $\mathbb{Z}^2$, $5a - 7b = 1$,
Rq $(5 \wedge 7) = 1$, dc (E) admt solu°s.
De plus, le couple (3, 2) est solu° évidente. sinon cf AE ⑤.
$\mathcal{S} = \{ (3 + 7r, 2 + 5s), (r, s) \in \mathbb{Z}^2 \}$.

cf ∃ : $k' \in \mathbb{Z}$ tq $k = 3 + 7k'$, dc $x = 17 + 35k'$
$x \equiv 17$ [35]
(Resp) tt nbr congru à 17 (mod 35) est bien solu° du système.

Ens solu°s système $\mathcal{S} = \{ 17 + 35t, t \in \mathbb{Z} \}$.

⑧ Résoudre $\begin{cases} x \equiv 5 \ [6] \\ 7x \equiv 5 \ [12] \end{cases}$

• comme $7 \wedge 12 = 1$, le nombre 7 est inversible (mod 12).
Son inverse est 7 (mod 12).
En effet $7 \times 7 = 49 = 4 \times 12 + 1 \equiv 1$ [12]

comme $7 \times 5 = 35 \equiv 11$ [12] alors
$\begin{cases} x \equiv 5 \ [6] \\ 7x \equiv 5 \ [12] \end{cases} \iff \begin{cases} x \equiv 5 \ [6] \\ x \equiv 11 \ [12] \end{cases}$.

Comme $11 \equiv 5$ [6], système équivalent à $x \equiv 11$ [12]
$\mathcal{S} = \{ 11 + 12k, k \in \mathbb{Z} \}$.

Ex 19 : soit p : nb premier & a, nbr entier
Mq si $p \nmid a-1$ alors $p \mid a + a^2 + a^3 + \dots + a^{p-1}$

PTF affirme $a^p \equiv a$ [p] $\iff p \mid a^p - a$ on a
$a^p - a = (a-1)(a + a^2 + \dots + a^{p-1})$
Par lemme d'Euclide, & $p \nmid a-1$, il divise $a + a^2 + \dots + a^{p-1}$.

Ex : p & q nb premiers distincts, Mq $p^{q-1} + q^{p-1} \equiv 1$ [pq]
& p & q premiers entre eux alors $p \nmid q$ et $q \nmid p$ de cq coro PTF, on en déduit $q^{p-1} \equiv 1$ [p] et $p^{q-1} \equiv 1$ [q]. De plus, $p, q \geq 2$,
$q^{p-1} \equiv 0$ [q] et $p^{q-1} \equiv 0$ [p]. Ainsi $p^{q-1} + q^{p-1} \equiv 1$ [p]
et $p^{q-1} + q^{p-1} \equiv 1$ [q]. ie $p \& q \mid p^{q-1} + q^{p-1}$ & p & q PEE
on en déduit $pq \mid p^{q-1} + q^{p-1} - 1$ soit $p^{q-1} + q^{p-1} \equiv 1$ [pq]