Maths 4 : TD 2 Congruences

04.03.2021

Exercice 1

1) Rappelons que si $a_0 \equiv a_1 \mod 4$ et $b_0 \equiv b_1 \mod 4$ alors $a_0 b_0 \equiv a_1 b_1 \mod 4$ et $a_0 + b_0 \equiv a_1 + b_1 \mod 4$

En outre $x \equiv r \mod 4$ ou $0 \leq r \leq 3$ ssi r est le reste de la division euclidienne de x par 4.

Si $x \in \mathbb{Z}$, les restes possibles de $x \mod 4$ sont 0, 1, 2 ou 3

Donc on a $x \equiv 0\ [4]$ ou $x \equiv 1\ [4]$ ou $x \equiv 2\ [4]$ ou $x \equiv 3\ [4]$

par la règle de multiplication $\Rightarrow$ $x^2 \equiv 0^2\ [4]$ $\quad x^2 \equiv 1^2\ [4]$ $\quad x^2 \equiv 4 \equiv 0\ [4]$ $\quad x^2 \equiv 9 \equiv 1\ [4]$

$\boxed{\text{Donc } x^2 \equiv 0\ [4] \text{ ou } x^2 \equiv 1\ [4]}$

2) Si $x \in \mathbb{Z}$ $\quad x \equiv 0\ (3)$ ou $x \equiv 1\ [3]$ ou $x \equiv 2\ [3]$ $\Rightarrow$ $x^2 \equiv 0\ [3]$ ou $x^2 \equiv 1\ [3]$

Donc $X = x^2$ a pour reste 0 ou 1 dans la division euclidienne par 3.

Exercice 2

$n \mod 4$	$n^2 \mod 4$	$n^2+1 \mod 4$
0	0	1
1	1	2
2	0	1
3	1	2

tous $\neq 0$

Donc n^2+1 n'est jamais divisible par 4.

Exercice 3

n	$7^n \mod 8$	$7^n + 1 \mod 8$
0	1	2
1	$-1 \equiv 7$	0
2	$1 = (-1)^2$	2
3	$-1 = (-1)^3$	0
4	$1 = (-1)^4$	2
⋮	⋮	⋮

Résumons : $7 \equiv -1 \mod 8$

donc $7^n \equiv (-1)^n \mod 8$

$$\equiv \begin{cases} 1 \mod 8 & \text{si } n \text{ pair} \\ -1 \mod 8 & \text{si } n \text{ impair} \end{cases}$$

donc $7^n + 1 \equiv \begin{cases} 2 \mod 8 & \text{si } n \text{ pair} \\ 0 \mod 8 & \text{si } n \text{ impair} \end{cases}$

Exercice 4 09.03.2021

On suit la méthode de la page 48 du poly.

$d = PGCD(m, n) = PGCD(6, 9) = 3$

a) On sait que si $x \equiv r \mod n$, alors on a aussi $x \equiv r \mod d$ pour tout diviseur d de n. Donc ici on a

$$x \equiv 4 \mod 6 \Rightarrow x \equiv 4 \mod 3 \quad (1)$$
$$\text{et } x \equiv 7 \mod 9 \Rightarrow x \equiv 7 \mod 3 \quad (2)$$

La différence de (1) et (2) nous donne $0 \equiv 7-4 \mod 3$ ce qui est vrai.

b) Déterminons une solution $(u,v) \in \mathbb{Z}^2$ de l'équation de Bézout

$$9u + 6v = 3$$
$$\Leftrightarrow \quad 3u + 2v = 1$$

On a la solution $u = 1$ et $v = -1$.

c) Posons $m' = m/d = 9/3 = 3$

et $n' = n/d = 6/3 = 2$

On a $\begin{cases} x \equiv \overset{a}{7} \mod \overset{m}{9} \\ x \equiv \underset{b}{4} \mod \underset{n}{6} \end{cases}$

Alors $x_0 = b u m' + a v n' = 4 . 1 . 3 + 7 . (-1) . 2 = \boxed{-2}$ est bien une solution.

⚠ on "échange" a et b

d) La solution générale du système sera de la forme $x_0 + x_h$

où x_h est la solution du système homogène

$$S_h : \begin{cases} x_h \equiv 0 \mod 9 \\ x_h \equiv 0 \mod 6 \end{cases}$$

Donc x_h est à la fois multiple de 6 et de 9, donc multiple de $PPCM(6,9) = 6 \cdot 9 / PGCD(6,9) = 6 \cdot 9/3 = 18$

Donc la solut° générale de (S_h) est $x_h = 18k, k \in \mathbb{Z}$

et la solution générale du système de départ est $\boxed{x = x_0 + x_h = -2 + 18k, k \in \mathbb{Z}}$

Exercice 5

0) exercice général : mq si p est un nb premier, alors on a $ab \equiv 0 \mod p \Rightarrow a \equiv 0 \mod p$ ou $b \equiv 0 \mod p$

$ab \equiv 0 \mod p$

$\Leftrightarrow p$ divise $ab \Rightarrow$ par le lemme d'Euclide et car p premier : $p \mid a$ ou $p \mid b$

$\Rightarrow a \equiv 0 \mod p$ ou $b \equiv 0 \mod p$

1) Mq $x^2 \equiv 1 \mod p \Leftrightarrow x \equiv 1 \mod p$ ou $x \equiv -1 \mod p$
si p est premier.

$x^2 \equiv 1 \mod p \iff x^2 - 1 \equiv 0 \mod p \iff (x-1)(x+1) \equiv 0 \mod p$

$\underset{\text{par c)}}{\Rightarrow}$ $x-1 \equiv 0 \mod p$ ou $x+1 \equiv 0 \mod p$

$\iff x \equiv 1 \mod p$ ou $x \equiv -1 \mod p$

2) $\begin{cases} 2x \equiv 3 \mod 5 \\ 4x \equiv 3 \mod 7 \end{cases}$

Dans un premier temps, on va remplacer $2x \equiv 3 \mod 5$ par une congruence équivalente de la forme $x \equiv a \mod 5$

↳ on multiplie par 3 des deux côtés :

$\iff 3 \times 2x \equiv 3 \times 3 \mod 5$

$\iff 6x \equiv 9 \mod 5$

$\iff x \equiv 4 \mod 5$

ça marche parce que $2.3 \equiv 1 \mod 5$

↳ donc 2 et 3 sont inverses l'un de l'autre mod 5.

Si on a une congruence $ux \equiv v \mod 5$, alors elle est équivalente à $2ux \equiv 2v \mod 5$ car on peut passer de $2ux \equiv 2v \mod 5$ à $ux \equiv v \mod 5$ en multipliant par 3.

De même $4x \equiv 3 \mod 7$ car $4 \times 2 \equiv 1 \mod 7$

$\iff x \equiv 6 \mod 7$

On a donc $(*) \begin{cases} x \equiv 4 \mod 5 \\ x \equiv 6 \mod 7 \end{cases}$

Dans ce nouveau système $(*)$, les modules 5 et 7 sont 1ers entre eux.

Pour trouver une solution, on commence par déterminer une solution de l'équation de Bézout :

$5u + 7v = 1 = PGCD(5,7)$

$(u,v) = (3,-2)$ est solution. Cette solution donne $15 + (-14) = 1$

On a : $(1) \begin{cases} 15 \equiv 0 \mod 5 \\ 15 \equiv 1 \mod 7 \end{cases}$ $\left.\begin{matrix} -14 \equiv 1 \mod 5 \\ -14 \equiv 0 \mod 7 \end{matrix}\right\} (2)$

On en déduit une solution de $(3) \begin{cases} x \equiv a \mod 5 \\ x \equiv b \mod 7 \end{cases}$

à savoir $a.(-14) + b.15$ car $-14a + 15b \equiv 0 + 1 \mod 5$

et $\equiv 1 + 0 \mod 7$

Ici on a $a = 9$ et $b = 6$

donc $x = 9 \times (-14) + 6 \times 15 = -126 + 90 = \boxed{-36}$

Vérification : $-36 \equiv -1 \mod 5 \equiv 9 \mod 5$

$-36 \equiv -1 \mod 7 \equiv 6 \mod 7$

La solution générale du système homogène $\left.\begin{matrix} 2x \equiv 0 \mod 5 \overset{\times 3}{\iff} x \equiv 0 \mod 5 \\ 4x \equiv 0 \mod 7 \iff x \equiv 0 \mod 7 \end{matrix}\right\} \Rightarrow x$ multiple de $PPCM(5,7) = \boxed{35}$

La sol générale du système est $\boxed{x = -36 + 35k, k \in \mathbb{Z}}$.

Exercice 6

1) $PGCD(9n+15, 4n+7)$

On sait que $PGCD(a,b) = PGCD(a, b+ka), \forall k \in \mathbb{Z}$
$= PGCD(a+kb, b), \forall k \in \mathbb{Z}$

$$PGCD(\overbrace{9n+15}^{a}, \overbrace{4n+7}^{b}) = PGCD(a-2b, b)$$
$$= PGCD(\underbrace{n+1}_{a}, \underbrace{4n+7}_{b}) = PGCD(a, b-4a)$$
$$= PGCD(n+1, 3)$$
$$= PGCD(r, 3)$$ où r est le reste de la division eucl. de $n+1$ par 3.
$n+1 = 3q + r$

Si $r = 0$ alors $PGCD = 3$
Si $r = 1$ alors $PGCD = 1$
Si $r = 2$ alors $PGCD = 1$

Conclusion :

Si $n \equiv 2 \mod 3$ alors $PGCD = 3$
Sinon $PGCD = 1$.