

*Feuille 2 : Congruences***Exercice 1.** Soit $X = x^2$ le carré d'un entier.

1. Quels sont les restes possibles de X dans la division par 4 ?
2. Quels sont les restes possibles de X dans la division par 3 ?

Exercice 2. Montrer que 4 ne peut diviser aucun nombre de la forme $n^2 + 1$.**Exercice 3.** Démontrer que le nombre $7^n + 1$ est divisible par 8 si n est un entier naturel impair ; dans le cas n pair, donner le reste de sa division par 8.**Exercice 4.** Résoudre dans \mathbb{Z} le système suivant :

$$S : \begin{cases} x \equiv 4 \pmod{6} \\ x \equiv 7 \pmod{9} \end{cases}$$

Exercice 5.

1. Soit p un nombre premier. Justifier que

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

si et seulement si

$$x \equiv 1 \pmod{p} \text{ ou } x \equiv -1 \pmod{p} .$$

2. Résoudre le système de congruences

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

Exercice 6. Soit n un entier.

1. Déterminer le pgcd de $9n + 15$ et $4n + 7$ en fonction de n .
2. Montrer que n^2 et $2n + 1$ sont premiers entre eux.

Exercice 7. Soit n un entier naturel à 6 chiffres tel que lorsque l'on échange les trois premiers chiffres avec les trois derniers, le résultat obtenu est $6n + 21$. Déterminer n .**Exercice 8.** Pour tout $n \in \mathbb{N}$, on pose $P(n) = n^2 - n + 41$.

1. La quantité $P(n)$ est-elle un nombre premier pour tout $n \in \mathbb{N}$?
2. Montrer qu'il existe une infinité d'entiers $n \in \mathbb{N}$ tels que 43 divise $P(n)$.

Exercice 9.

1. Soit $a, b \in \mathbb{R}$. Montrer que pour tout entier $n \in \mathbb{N}^*$

$$a^n - b^n = (a - b) \sum_{k=0}^{n-1} a^k b^{n-1-k}.$$

2. Soient n et m deux entiers positifs et $a \in \mathbb{N}$. Montrer que $a^m - 1$ divise $a^n - 1$ si et seulement si m divise n .
3. Soit a un entier, $a > 2$. Montrer que pour $n > 1$, $a^n - 1$ n'est pas premier.
4. Montrer que si $2^n - 1$ est premier, alors n est premier.

Exercice 10. Déterminer :

1. Quel est le dernier chiffre de 77777777 ?
2. Quels sont les restes des divisions euclidiennes de 900^{2000} et de $101^{102^{103}}$ par 13 ?
3. Quel est le reste de la division euclidienne de $31^{32^{33}}$ par 7 ?
4. Quel est le reste de la division euclidienne de $100^{100^{100}}$ par 12 ?

Exercice 11. Montrer que $5^{6614} - 12^{857} \equiv 1 \pmod{7}$.**Exercice 12.** Résoudre les congruences suivantes :

- | | | | |
|--------------------------------|----------------------------|-----------------------------|------------------------------|
| a) $2x \equiv 1 \pmod{7}$ | b) $4x \equiv 6 \pmod{18}$ | c) $12x \equiv 9 \pmod{6}$ | d) $23x \equiv 41 \pmod{52}$ |
| e) $68x \equiv 100 \pmod{120}$ | f) $5x \equiv -1 \pmod{8}$ | g) $20x \equiv 4 \pmod{30}$ | g) $20x \equiv 30 \pmod{4}$ |

Exercice 13. Résoudre dans $\mathbb{Z}/212\mathbb{Z}$: $\overline{171}x = \overline{7}$.

$\text{Ex 1 : } X = n^2 \quad n \in \mathbb{Z}$

$\hookrightarrow X \equiv ? \pmod{4}$

si $n \equiv r \pmod{4}$

alors $X \equiv r^2 \pmod{4}$

x si $n \equiv 0 \pmod{4}$

alors $X \equiv 0^2 \equiv 0 \pmod{4}$

x si $n \equiv 1 \pmod{4}$

alors $X \equiv 1^2 \equiv 1 \pmod{4}$

x si $n \equiv 2 \pmod{4}$

alors $X \equiv 2^2 \equiv 4 \equiv 0 \pmod{4}$

x si $n \equiv 3 \pmod{4}$

alors $X \equiv 3^2 \equiv 9 \equiv 1 \pmod{4}$

Donc les restes possibles de la division de $X = n^2$ par 4 sont 1 ou 0

\hookrightarrow si $n \equiv 0 \pmod{3}$

alors $X \equiv 0^2 \equiv 0 \pmod{3}$

c si $n \equiv 1 \pmod{3}$

alors $X \equiv 1^2 \equiv 1 \pmod{3}$

c si $n \equiv 2 \pmod{3}$

alors $X \equiv 2^2 \equiv 4 \equiv 1 \pmod{3}$

Donc les restes possibles de la division de $X = n^2$ par 3 sont 0 ou 1

Ex 2 :

$$4 \mid n^2 + 1 \Leftrightarrow n^2 + 1 \equiv 0 \pmod{4}$$

$$\Leftrightarrow n^2 \equiv -1 \pmod{4}$$

$$\Leftrightarrow n^2 \not\equiv 3 \pmod{4}$$

$\forall n \in \mathbb{Z} \quad n^2 \equiv 0 \text{ ou } 1 \pmod{4}$

donc $4 \nmid n^2 + 1$

Amphi réservé !

Groupe :

- Ensemble : G

- une loi : $G \times G \xrightarrow{*} G$

+ Axiomes :

+ Associativité $(a \cdot b) \cdot c = a \cdot (b \cdot c)$

+ existence d'un inverse : $\forall g \in G, \exists g' \in G$ tq :

$$g \cdot g' = g' \cdot g = e$$

+ existence d'un neutre :

$$\exists ! e \in G \text{ tq } \forall g \in G$$

$$e \cdot g = g \cdot e = g$$

(Exo : Si g_1, g_2)

$$\text{Soit les } g, g_1, g_2 = e$$

\exists un inverse g' tq $g'g = e$

$$\text{alors } g' \cdot (g \cdot g_1) = g'(g \cdot g_2) = g'e$$

$$(g' \cdot g) \cdot g_1 = (g' \cdot g)g_2 = g' \leftarrow$$

$$e \cdot g_1 = e \cdot g_2 = g$$

$$g_1 = g_2 = g'$$

Théorème des restes chinois

$$\begin{cases} x \equiv a \pmod{n} \\ x \equiv b \pmod{m} \end{cases}$$

Si m, n premier entre eux alors $\exists!$ solution modulo mn

Cas général:

$$\begin{cases} x \equiv a \pmod{n} \\ x \equiv b \pmod{m} \end{cases}$$

$a \equiv b \pmod{\text{pgcd}(n, m)} \Rightarrow \exists!$ solution mod
 $\text{pgcd}(n, m)$

TD 2 :

Ex 3 :

$$7^n + 1 \mid 8$$

ou

$$\begin{cases} \text{si } n \in \mathbb{Z}(2k+1) \\ \text{si } n \in \mathbb{Z}(2k) \end{cases}$$

$$f \equiv -1 \pmod{8}$$

tg: $f^n + 1$ divisible par 8 quand n supérieur
dans le reste quand n pair

$$f \equiv -1 \pmod{8}$$

(car $f - (-1) = 8$ est un multiple de 8)

dans $f^n > 0 \quad f^n \equiv (-1)^n \pmod{8}$

Si n pair: $(-1)^n = 1$

$$\text{dans } (f^n) \equiv (-1)^n \equiv 1 \pmod{8}$$

$$\begin{aligned} \text{et dans } f^n + 1 &\equiv 1 + 1 \pmod{8} \\ &\equiv 2 \pmod{8} \end{aligned}$$

quand n est pair $f^n + 1$ dans un reste de 2
dans les div. par 8

quand n impair $(-1)^n = -1$

$$\text{dans } f^n \equiv (-1)^n \equiv -1 \pmod{8}$$

$$\text{dans } f^n + 1 \equiv -1 + 1 \equiv 0 \pmod{8}$$

dans $f^n + 1$ divisible par 8

$E \times 4$

$$(S) \begin{cases} x \equiv 4 \pmod{6} \\ x \equiv f \pmod{9} \end{cases}$$

$$\text{pgcd}(6, 9) = 3$$

$$f \equiv 4 \pmod{3}$$

donc $\exists!$ solution modulo $\text{lcm}(6, 9) = 18$

$$0, 1, 2, 3, 4, 5, 6, 7, 8, 10, 11, 12, 13, 14, 15 \\ 16, 17$$

On observe que $16 \equiv 4 \pmod{6}$

$$(\text{car } 16 = 2 \times 6 + 4)$$

$$\text{et } 16 \equiv f \pmod{9}$$

$$(\text{car } 16 = f + g)$$

donc 16 est solution de S

Car $\exists!$ solution modulo 18

les solutions générales sont de la forme

$$16 + 18k, k \in \mathbb{Z}$$

$$f \equiv 4 \pmod{9}$$

Cela veut dire :

$f - 4$ est un multiple de 3

f et 4 ont le même reste dans le division par 3

$4 - f$ est un multiple de 3

$$4 - f = 3k \quad \text{avec } k \in \mathbb{Z}$$

$$l = 3l + f \quad \text{avec } l \in \mathbb{Z}$$

Fx 4

$$(3) \left\{ \begin{array}{l} x \equiv 4 \pmod{6} \\ x \equiv 7 \pmod{9} \end{array} \right.$$

$$\text{pgcd}(6, 9) = 3 \rightarrow \text{lcm}(6, 9) = 18$$

On a $7 \equiv 4 \pmod{3}$ donc $\exists!$ solution

\Rightarrow on applique l'algorithme Euclidien à $(6, 9)$

$$\rightsquigarrow 6u + 9v = 3$$

(algo Euclidien)

$$6 \times (-1) + 9(1) = 3$$

$$m' = \frac{m}{\text{pgcd}(m, n)} = 2$$

$$n' = \frac{n}{\text{pgcd}(m, n)} = 3$$

Solution : $x = bu m' + av n'$

$$x = 7 \times (-1) \times 2 + 4 \times (1) \times 3$$

$$x = -2$$

Solution particulière

Solution générale : $x = -2 + 18k$, $k \in \mathbb{Z}$

Ex 5

$$(S) \begin{cases} 2x \equiv 3 \pmod{5} \\ 4x \equiv 3 \pmod{7} \end{cases}$$

Observation! Soit premier donc $\exists k \text{ tq } 2k \equiv 1 \pmod{5}$

$$2 \times 3 \equiv 1 \pmod{5}$$

$$a \equiv b \pmod{p} \Leftrightarrow ka \equiv kb \pmod{p}$$

Si k a un inverse mod p

4a : un inverse modulo 7

$$2 \times 4 \equiv 1 \pmod{7}$$

$$(S) \begin{cases} 2x \equiv 3 \pmod{5} \\ 4x \equiv 3 \pmod{7} \end{cases}$$

$$\Leftrightarrow \begin{cases} 3 \times 2x \equiv 3 \times 3 \pmod{5} \\ 2 \times 4x \equiv 2 \times 3 \pmod{7} \end{cases}$$

$$\Leftrightarrow \begin{cases} x \equiv 9 \pmod{5} \\ x \equiv 6 \pmod{7} \end{cases}$$

$$\Leftrightarrow \begin{cases} x \equiv 4 \pmod{5} \\ x \equiv 6 \pmod{7} \end{cases}$$

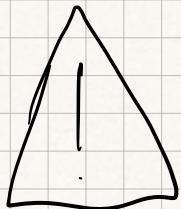
$$\Leftrightarrow \begin{cases} x \equiv -1 \pmod{5} \\ x \equiv -1 \pmod{7} \end{cases}$$

$x = -1$ est une solution

Par le théorème des restes chinois, elle est unique modulo 35

donc les solutions générales sont

$$x = -1 + 35k \quad k \in \mathbb{Z}$$



$$a \equiv b \pmod{4}$$

$$\Leftrightarrow 2a \equiv 2b \pmod{4}$$

$$\text{Ex} \quad a \equiv 2 \pmod{4}, \quad b \equiv 0 \pmod{4}$$

$$2a \equiv 2b \pmod{4}$$

Méthode 2:

$$\Rightarrow 2x = 5k + 3 \quad k \in \mathbb{Z}$$

$$4x = 10k + 6 = 7l + 3$$

$$\text{On résout } 10k + 6 = 7l + 3$$

$$\Leftrightarrow 10k - 7l = -3$$

$$\text{Algo d'Euler : } 10 \times (-2) + 7 \times (3) = 1$$

$$x - 3 ; \quad 10 \times (6) + 7 \times (-9) = -3 \\ k_0 = 6 , \quad l_0 = 9$$

$$(l = 10m + l_0, \quad k = 7m + k_0) \quad m \in \mathbb{Z}$$

$$2x = 5k + 3 = 5\left(\frac{7m}{3} + \frac{6}{3}\right) + 3 \\ = 35m + 34$$

Entrainement :

$$\begin{cases} 1) & x \equiv 5 \pmod{17} \\ (S) & x \equiv 6 \pmod{23} \end{cases}$$

$$S \Rightarrow x \equiv 17k + 5$$

$$x \equiv 17k + 5 = 23l + 6$$

$$\text{On résout } 17k + 5 = 23l + 6$$

$$\Leftrightarrow 17k - 23l = 1$$

Algo d'Euler :

$$17 \times (4) - 23 \times (3) = 1$$

Solution particulière pour $k_0 = 4$ et $l_0 = 3$

$$\text{Solution général } \left\{ \begin{array}{l} x = 4 + \\ \quad \quad \quad k \in \mathbb{Z} \\ x = 3 + \end{array} \right.$$

Correction :

$$\text{Calcul : pgcd}(14, 23) = 1$$

$$23 = 1 \times 14 + 6$$

$$14 = 2 \times 6 + 5$$

$$6 = 1 \times 5 + \textcircled{1} \leftarrow \text{pgcd}$$

$$1 = 6 - 5$$

$$= 6 - (14 - 2 \times 6)$$

$$= 3 \times 6 - 14$$

$$= 3 \times (23 - 14) - 14$$

$$1 = 3 \times 23 - 4 \times 14$$

$$x = aum + bon$$

dans $3 \times 23 \equiv 1 \pmod{14}$

dans $5 \times 3 \times 23 \equiv 5 \pmod{14}$

$$-4 \times 14 \equiv 1 \pmod{23}$$

$$6 \times (-4) \times 14 \equiv 6 \pmod{23}$$

$$x = 5 \times 3 \times 23 + 6 \times (-4) \times 14 \text{ est solution}$$

$$x_p = -63 \quad (\text{sol particulière})$$

On vérifie les solutions générales

$$\left\{ x = -63 + 39k \mid k \in \mathbb{Z} \right\}$$

$$\left| \begin{array}{l} -63 + 391 = 328 = 19 \times 17 + 5 \\ 328 = 19 \times 23 + 6 \end{array} \right.$$

$$2x \quad \begin{cases} x \equiv 1 \pmod{14} \\ x \equiv 6 \pmod{8} \end{cases}$$

On calcule $\text{pgcd}(14, 8) = 2$

$$\begin{aligned} 14 &= 1 \times 8 + 6 \\ 8 &= 1 \times 6 + 2 \\ 6 &= 3 \times 2 + 0 \end{aligned}$$

$$\text{ppcm}(14, 8) = 56$$

On applique l'algo Euclide à $(14, 8)$

$$14u + 8v = 2 \quad u = (-1) \quad v = 2$$

$$m' = \frac{m}{\text{pgcd}(m, n)} = 7$$

$$n' = \frac{n}{\text{pgcd}(m, n)} = 4$$

$$\begin{aligned} \text{Solutions} \quad x &= bum' + avn' \\ x &= 6 \times (-1) \times 7 + 1 \times (2) \times 4 \\ &= -42 + 8 = -34 \end{aligned}$$

Solution générale : $-34 + 56k, k \in \mathbb{Z}$

Correction

$$\text{pgcd}(8, 14) = 2 \neq 1$$

On vérifie si $2 \mid 5 - 1$?

$2 \nmid 5$ donc pas de solution

$$2x \quad \left\{ \begin{array}{l} x \equiv 1 \pmod{14} \\ x \equiv 5 \pmod{8} \end{array} \right.$$

$$\text{pgcd}(8, 14) = 2 \neq 1$$

$$2 \mid 5 - 1 = 4$$

donc on a une solution, unique modulo

56

On calcule $\text{pgcd}(14, 8) = 2$

$$14 = 1 \times 8 + 6$$

$$\text{dans } 2 = 8 - 6$$

$$8 = 1 \times 6 + 2$$

$$2 = 8 - (14 - 8)$$

$$6 = 3 \times 2 + 0$$

$$2 = 2 \times 8 - 14$$

$$1 = 2 \times 4 - *$$

$$\text{ppcm}(14, 8) = 56$$

On applique l'algo Euclide à (14, 8)

$$14u + 8v = 2 \quad u = (-1) \quad v = 2$$

$$m' = \frac{m}{\text{pgcd}(m, n)} = \frac{14}{2} = 7$$

$$n' = \frac{n}{\text{pgcd}(m, n)} = \frac{8}{2} = 4$$

Solution $x = bum' + avn'$
 $x = 5 \times (-1) \times 7 + 1 \times (2) \times 4$
 $= -35 + 8$
 $= -27$

Solution générale $-27 + 56k, k \in \mathbb{Z}$

$$\text{donc } 2 = 8 - 6$$

$$2 = 8 - (14 - 8) \Rightarrow x = (1) \times 2 \times 4 - (5) \times 7$$

$$2 = 2 \times 8 - 14$$

$$1 = 2 \times 4 - 7$$

$$x = -27$$

$$\begin{cases} d = um + vn \\ a \equiv b \pmod{d} \\ \Leftrightarrow a = b + kd \end{cases} \quad \begin{aligned} 1 &= u \frac{m}{d} + v \frac{n}{d} \end{aligned}$$

$$x = ac \frac{m}{d} + bv \frac{m}{d}$$

$$x = bu \frac{m}{a} + bv \frac{n}{q} + kf \frac{m}{d}$$

$$x = b \left(\underbrace{\frac{cu + vn}{d}}_1 \right) + km$$

les solutiuni generale: $\{x = 2f + 56k \mid k \in \mathbb{Z}\}$

3.

$$\begin{cases} 3x \equiv 1 \pmod{8} \\ 2x \equiv 5 \pmod{7} \end{cases} \Rightarrow \begin{cases} 9x \equiv 3 \pmod{8} \\ 8x \equiv 20 \pmod{7} \end{cases} \quad \begin{cases} 3x \equiv 1 \pmod{6} \\ 2x \equiv 5 \pmod{7} \end{cases}$$

$3 \times 3 = 9 \equiv 1 \pmod{8}$ $x \equiv 3 \pmod{8}$
 $x \equiv 6 \pmod{7}$ $\text{pgcd}(3, 6) = 3$

$\text{danc}(S) \Rightarrow \begin{cases} 3 \times 3x \equiv 3 \pmod{8} \text{ et } 3 \nmid 1 \\ 2x \equiv 5 \pmod{7} \text{ danc } \exists k \in \mathbb{Z} \end{cases}$

$$\Rightarrow \begin{cases} x \equiv 3 \pmod{8} \\ 2x \equiv 5 \pmod{7} \end{cases}$$

$$\text{pgcd}(2, f) = 1$$

$\text{danc } \exists k \in \mathbb{Z}$

$$\text{tq } 2u \equiv 1 \pmod{f}$$

0	0
1	3
2	0
3	3
4	0
5	5

Résout :

$$Ju, o, 2u + fo = 1$$

$$f = 3 \times 2 + 1$$

$$f + (-3) \times 2 = 1$$

dans $u = -3$

est tel que

$$(-3) \times 2 \equiv 1 \pmod{f}$$

et $(-3) \equiv 4 \pmod{f}$

dans

$$(S) \Rightarrow \begin{cases} x \equiv 3 \pmod{8} \\ x \equiv 6 \pmod{f} \end{cases}$$

20/02

Ex5 :

$$M_q \quad x^2 \equiv 1 \pmod{p} \Leftrightarrow x \equiv 1 \pmod{p}$$

ou

$$x \equiv -1 \pmod{p}$$

2 =

Si $x \equiv 1 \pmod{p}$ alors $x^2 \equiv 1^2 \equiv 1 \pmod{p}$

Si $x \equiv -1 \pmod{p}$ alors $x^2 \equiv (-1)^2 \equiv 1 \pmod{p}$

$\Rightarrow x^2 \equiv 1 \pmod{p} \Leftrightarrow \exists k \in \mathbb{Z} \text{ tel que } x^2 = kp + 1$

$$\Leftrightarrow x^2 - 1 = kp$$

$$\Leftrightarrow (x-1)(x+1) = kp$$

donc $p \mid (x-1)(x+1)$

donc $p \mid (x-1)$ ou $p \mid (x+1)$

donc $p \mid (x-1)$ et $p \mid (x+1)$

Si $p \mid (x-1)$

alors $x-1 \equiv 0 \pmod{p}$

$$\Leftrightarrow x \equiv 1 \pmod{p}$$

Ex 6

Calculer le pgcd de $3n+15$, $4n+7$

On peut écrire :

$$3n+15 = 2 \underbrace{(4n+7)}_{\square} + \boxed{n+1}$$

$$4n+7 = 4 \underbrace{(n+1)}_{\square} + \boxed{3}$$

$$n+1 = ? \quad \boxed{3} \quad + \quad ?$$

On a 3 cas :

• Si $n+1 \equiv 0 \pmod{3} \Leftrightarrow n \equiv 2 \pmod{3}$

$\Leftrightarrow \exists k \in \mathbb{Z}, n+1 = 3k$

Dans ce cas l'algorithme Euclide donne comme dernière ligne $n+1 = k \times 3 + 0$

Dans ce cas, $\text{pgcd}(3n+15, 4n+7) = 3$

• Si $n+1 \equiv 1 \pmod{3} \Leftrightarrow n \equiv 0 \pmod{3}$

alors $\exists k \in \mathbb{Z}, n+1 = k \times 3 + 1$

Dans la dernière ligne de l'algo d'Euclide donne :

$$n+1 = k \times 3 + \boxed{1}$$

Dans ce cas,

$$\text{pgcd}(3n+15, 4n+7) = 1$$

• Si $n+1 \equiv 2 \pmod{3} \Leftrightarrow n \equiv 1 \pmod{3}$

alors $\exists k \in \mathbb{Z} \text{ tq } n+1 = k \times 3 + 2$

d'algo Euclide donne :

$$n+1 = k \times 3 + 2$$

$$3 = 1 \times 2 + 1$$

Dans ce cas :

$$\text{pgcd}(3n+15, 4n+7) = 1$$

Conclusion

$$\text{pgcd}(3n+15, 4n+7) \left\{ \begin{array}{l} 3 \text{ si } n \equiv 2 \pmod{3} \\ 1 \text{ si } n \equiv 0 \text{ ou } 1 \pmod{3} \end{array} \right.$$

2x Soit p : premier qui divise n^2
 alors $p \mid n$ donc $p \mid 2n$
 donc $p \mid n^2 + 1$

$$\text{dans } \text{pgcd}(n^2, 2n+1) = 1$$

Ex 12

peut & une inverse

$$ax \equiv 1 \pmod{7} \leftarrow$$

x est nécessairement congru à $0, 1, 2, 3, 4, 5, 6$.

$$x \equiv 0 \pmod{7} \quad \text{alors } 2x \equiv 0 \pmod{7}$$

$$x \equiv 1 \pmod{7} \quad \text{alors } 2x \equiv 2 \equiv 2 \pmod{7}$$

$$x \equiv 2 \pmod{7} \quad \text{alors } 2x \equiv 4 \equiv 4 \pmod{7}$$

$$x \equiv 3 \pmod{7} \quad \text{alors } 2x \equiv 6 \equiv 6 \pmod{7}$$

$\mathbb{A} \equiv$	0	1	2	3	4	5	6
---------------------	---	---	---	---	---	---	---

$2\mathbb{A} \equiv$	0	2	4	6	1	3	5
----------------------	---	---	---	---	---	---	---

$$n \equiv 4 \pmod{7} \quad \text{mais } 2\mathbb{A} \equiv 8 \equiv 1 \pmod{7}$$

On multiplie l'équation par n

$$\Rightarrow 2xn \equiv n \pmod{7}$$

$$x \equiv 4 \pmod{7}$$

Réel 2

$$ax + 2x \equiv 1 \pmod{7}$$

$$t = 2 \times 3 + 1$$

$$1 = t - 3 \times 2$$

-3 est un inverse de 2 mod 7 (aussi)

Donc $2x \equiv 1 \pmod{7}$

$$\Leftrightarrow 4 \times 2x \equiv 4 \times 1 \pmod{7}$$

(car 4 est inversible mod 7)

$$\Leftrightarrow x \equiv 4 \pmod{7}$$

by $4x \equiv 6 \pmod{18}$

$$\text{pgcd}(4, 18) = 2 \neq 1$$

donc 4 pas inverse modulo 18

$$4x \equiv 6 \pmod{18}$$

$$\Leftrightarrow \exists k \in \mathbb{Z} \quad 4x = 18k + 6$$

$$\Leftrightarrow \exists k \in \mathbb{Z} \quad 2x = 9k + 3$$

$$\Leftrightarrow 2x \equiv 3 \pmod{9}$$

$$\text{pgcd}(2, 9) = 1$$

$$2 \times 5 \equiv 10 \equiv 1 \pmod{9}$$

5 est un inverse de 2 mod

donc $4x \equiv 6 \pmod{18}$

$$\Leftrightarrow x \equiv 15 \equiv 6 \pmod{9}$$

$$\Leftrightarrow x \equiv 6 \pmod{18} \text{ ou } x \equiv 15 \pmod{18}$$

$$x = 6 + kg, k \in \mathbb{Z}$$

Si k est pair, $k = 2n$

$$x = 6 + (2n)g = 6 + 18n$$

Si k impair, $k = 2n + 1$

$$x = 6 + (2n+1)g = 15 + 18n$$

donc $x \equiv 6 \pmod{9}$

$$\Leftrightarrow x \equiv 6 \pmod{18} \text{ ou } x \equiv 15 \pmod{18}$$

$$\text{Cp } 12x \equiv 9 \pmod{6}$$

$$\Leftrightarrow 0 \equiv 9 \pmod{6}$$

↑
Jamais vrai

donc pas de solution

à l'équation $12x \equiv 9 \pmod{6}$

$$\text{d) } 23x \equiv 41 \pmod{52}$$

$$52 = 2 \times 23 + 6$$

$$23 = 3 \times 6 + 5$$

$$6 = 1 \times 5 + 1$$

$$1 = 6 - (23 - 3 \times 6) = 4 \times 6 - 23$$

$$= 1 \times (52 - 2 \times 23) - 23$$

$$1 = 4 \times 52 - 9 \times 23$$

$$\text{donc } (-9) \times 23 \equiv 1 \pmod{52}$$

-9 est l'inverse de 23

$$23x \equiv 41 \pmod{52} \Leftrightarrow x = -9 \times 41 \pmod{52}$$

$$= -369 \pmod{52}$$

$$= -5 \pmod{52}$$

Ex 10

$$1. \quad (7777) \equiv 7777 \pmod{10}$$

$$7^2 \equiv 49 \equiv -1 \pmod{10}$$

$$7^4 \equiv (-1)^2 \equiv 1 \pmod{10}$$

$$7777 = 4 \times 1944 + 1$$

$$(7) = (7)^{4 \times 1944 + 1}$$

$$\equiv (7^4)^{1944} \times 7$$

$$\equiv (1)^{1944} \times 7$$

$$\equiv 7 \pmod{10}$$

$$2. \quad 900^{200} \pmod{13}$$

$$900 = 69 \times 13 + 3$$

$$\text{ donc } 900^{200} \equiv 3^{200} \pmod{13}$$

$$3^2 \equiv 9 \pmod{13}$$

$$3^3 \equiv 1 \pmod{13}$$

$$200 = 3 \times 66 + 2$$

$$(900)^{200} \equiv 3^{200} \equiv 3^{3 \times 66 + 2} \\ \equiv (3^3)^{66} \times 3^2 \\ \equiv 1^{66} \times 3^2$$

$$\equiv 9 \pmod{13}$$

$$(101)^{(102^{103})} \pmod{13}$$

$$101 = 2 \times 13 + 10$$

$$(101)^{(102^{103})} \equiv (10)^{(102^{103})} \pmod{13}$$