POLYTECHNIQUE MONTRÉAL
UNIVERSITÉ D'INGÉNIERIE

LOG1810

STRUCTURES DISCRÈTES

TD 7 : THÉORIE DES NOMBRES

E2025

SOLUTIONNAIRE

Exercice 1 :

a) En utilisant l'algorithme d'Euclide étendu, trouvez pgcd(1180, 482) ainsi que les entiers x et y tels que $1180x + 482y = \text{pgcd}(1180, 482)$. Présentez toutes les étapes de votre calcul.

On applique l'algorithme d'Euclide *étendu* sous sa forme par soustractions successives. Chaque ligne donne les deux vecteurs

$$A_k = [a_k,\ s_k,\ t_k], \qquad B_k = [b_k,\ u_k,\ v_k],$$

tels que $a_k = 1180s_k + 482t_k$ et $b_k = 1180u_k + 482v_k$.

Étape	A_k	B_k
0	$[1180,\ 1,\ 0]$	$[482,\ 0,\ 1]$
1	$[698,\ 1,\ -1]$	$[482,\ 0,\ 1]$
2	$[216,\ 1,\ -2]$	$[482,\ 0,\ 1]$
3	$[216,\ 1,\ -2]$	$[266,\ -1,\ 3]$
4	$[216,\ 1,\ -2]$	$[50,\ -2,\ 5]$
5	$[166,\ 3,\ -7]$	$[50,\ -2,\ 5]$
6	$[116,\ 5,\ -12]$	$[50,\ -2,\ 5]$
7	$[66,\ 7,\ -17]$	$[50,\ -2,\ 5]$
8	$[16,\ 9,\ -22]$	$[50,\ -2,\ 5]$
9	$[16,\ 9,\ -22]$	$[34,\ -11,\ 27]$
10	$[16,\ 9,\ -22]$	$[18,\ -20,\ 49]$
11	$[16,\ 9,\ -22]$	$[2,\ -29,\ 71]$
12	$[14,\ 38,\ -93]$	$[2,\ -29,\ 71]$
13	$[12,\ 67,\ -164]$	$[2,\ -29,\ 71]$
14	$[10,\ 96,\ -235]$	$[2,\ -29,\ 71]$
15	$[8,\ 125,\ -306]$	$[2,\ -29,\ 71]$
16	$[6,\ 154,\ -377]$	$[2,\ -29,\ 71]$
17	$[4,\ 183,\ -448]$	$[2,\ -29,\ 71]$
18	$[2,\ 212,\ -519]$	$[2,\ -29,\ 71]$

Arrêt. À l'étape 18, les composantes a_{18} et b_{18} sont égales :

$$a_{18} = b_{18} = 2 = pgcd(1180,\ 482).$$

Deux couples (x, y) conviennent :

$$\boxed{(x,\ y) = (212,\ -519)} \quad \text{ou} \quad \boxed{(x,\ y) = (-29,\ 71)}.$$

En effet

$$1180 \times 212 + 482 \times (-519) = 2, \qquad 1180 \times (-29) + 482 \times 71 = 2.$$

b) Soit $d = \text{pgcd}(a, b)$. L'équation suivante $ax + by = c$ a des solutions entières (x, y) si et seulement si d divise c.
Considérez l'équation $1180x+482y = 90$. A-t-elle des solutions entières ? Si oui, donnez une solution particulière (x_p, y_p) et la forme générale de toutes les solutions. Si non, expliquez pourquoi.

L'équation $1180x + 482y = 90$.
Nous avons trouvé $d = \text{pgcd}(1180, 482) = 2$.
Pour que l'équation ait des solutions entières, d doit diviser c. Ici $c = 90$.
Est-ce que 2 divise 90 ? Oui, $90 = 45 \cdot 2$.
Donc, l'équation a des solutions entières.
Nous avons :

$$1180(-29) + 482(71) = 2$$

Multiplions par 45 (car $90/2 = 45$) pour obtenir 90 du côté droit :

$$1180(-29 \cdot 45) + 482(71 \cdot 45) = 2 \cdot 45 = 90$$

$$x_p = -29 \cdot 45 = -1305$$
$$y_p = 71 \cdot 45 = 3195$$

Une solution particulière est $(x_p, y_p) = (-1305, 3195)$.
La forme générale des solutions est :

$$x = x_p + t \cdot \left(\frac{b}{d}\right) = -1305 + t \cdot \left(\frac{482}{2}\right) = -1305 + 241t$$
$$y = y_p - t \cdot \left(\frac{a}{d}\right) = 3195 - t \cdot \left(\frac{1180}{2}\right) = 3195 - 590t, \quad \text{où } t \in \mathbb{Z}$$

c) Trouvez toutes les solutions entières de la congruence $482k \equiv \text{pgcd}(1180, 482) \pmod{1180}$.

Congruence $482k \equiv \text{pgcd}(1180, 482) \pmod{1180}$.

$$482k \equiv 2 \pmod{1180}$$

Cela équivaut à trouver les solutions entières de l'équation :

$$482k - 1180m = 2$$

Ou encore :

$$482k + 1180(-m) = 2$$

Soit $j = -m$, on obtient :

$$482k + 1180j = 2$$

De la partie a), nous avons :

$$1180(-29) + 482(71) = 2$$

Donc, une solution particulière est :

$$j_0 = -29 \quad \text{et} \quad k_0 = 71$$

Le nombre de solutions incongrues modulo 1180 est :

$$\text{pgcd}(482, 1180) = 2$$

Les solutions générales pour k sont données par :

$$k = k_0 + \frac{1180}{d}t = 71 + \frac{1180}{2}t = 71 + 590t, \quad \text{où } t \in \mathbb{Z}$$

Exercice 2 :

a) Soit $S_n = \sum_{k=1}^{n}(k^2 - k + 1)$.

i) Simplifiez l'expression de S_n.

Simplification de S_n : $S_n = \sum_{k=1}^{n} k^2 - \sum_{k=1}^{n} k + \sum_{k=1}^{n} 1$. Nous utilisons les formules connues : $\sum_{k=1}^{n} k^2 = \frac{n(n+1)(2n+1)}{6}$. $\sum_{k=1}^{n} k = \frac{n(n+1)}{2}$. $\sum_{k=1}^{n} 1 = n$. Donc,

$$\begin{aligned}
S_n &= \frac{n(n+1)(2n+1)}{6} - \frac{n(n+1)}{2} + n \\
&= \frac{n(n+1)(2n+1) - 3n(n+1) + 6n}{6} \\
&= \frac{n}{6}[(n+1)(2n+1) - 3(n+1) + 6] \\
&= \frac{n}{6}[(2n^2 + n + 2n + 1) - (3n + 3) + 6] \\
&= \frac{n}{6}[2n^2 + 3n + 1 - 3n - 3 + 6] \\
&= \frac{n}{6}[2n^2 + 4] \\
&= \frac{n \cdot 2(n^2 + 2)}{6} \\
&= \frac{n(n^2 + 2)}{3}
\end{aligned}$$

La formule simplifiée pour S_n est $\frac{n(n^2+2)}{3}$.

i) Pour quelles valeurs de $n \pmod 3$ la somme S_n est-elle divisible par 3 ?

Divisibilité de S_n par 3 :
Nous voulons savoir quand $S_n \equiv 0 \pmod 3$.
Puisque $S_n = \dfrac{n(n^2+2)}{3}$, S_n est divisible par 3 si $\dfrac{n(n^2+2)}{3}$ est un multiple de 3, ce qui signifie que $n(n^2+2)$ doit être un multiple de 9.
Nous devons donc analyser $n(n^2+2) \pmod 9$.
Considérons les cas pour $n \pmod 3$:

— **Cas 1 :** $n \equiv 0 \pmod 3$
Soit $n = 3k$ pour un entier k.

$$n(n^2+2) = 3k((3k)^2 + 2) = 3k(9k^2 + 2) = 27k^3 + 6k$$

$$27k^3 + 6k \equiv 6k \pmod 9$$

Pour que $n(n^2+2) \equiv 0 \pmod 9$, il faut $6k \equiv 0 \pmod 9$, donc $9 \mid 6k \Rightarrow 3 \mid 2k$.
Comme $pgcd(3,2) = 1$, il faut $3 \mid k \Rightarrow k = 3j$.
Ainsi, $n = 3(3j) = 9j$.
Donc, si $n \equiv 0 \pmod 3$, alors S_n est divisible par 3 si et seulement si $n \equiv 0 \pmod 9$.

— **Cas 2 :** $n \equiv 1 \pmod 3$

$$n^2 \equiv 1 \pmod 3 \Rightarrow n^2 + 2 \equiv 0 \pmod 3$$

Donc $n^2 + 2 = 3m$, alors :

$$n(n^2+2) = n \cdot 3m = 3nm$$

Pour que $3nm \equiv 0 \pmod 9$, il faut $nm \equiv 0 \pmod 3$.
Comme $n \not\equiv 0 \pmod 3$, il faut $m \equiv 0 \pmod 3$.
Or $m = \dfrac{n^2+2}{3}$, donc :

$$\frac{n^2+2}{3} \equiv 0 \pmod 3 \Rightarrow n^2 + 2 \equiv 0 \pmod 9$$

Testons les valeurs possibles :

$$\begin{aligned} n \equiv 1 \pmod 9 &\Rightarrow n^2 + 2 = 1^2 + 2 = 3 \not\equiv 0 \pmod 9 \\ n \equiv 4 \pmod 9 &\Rightarrow 4^2 + 2 = 16 + 2 = 18 \equiv 0 \pmod 9 \\ n \equiv 7 \pmod 9 &\Rightarrow 7^2 + 2 = 49 + 2 = 51 \equiv 6 \not\equiv 0 \pmod 9 \end{aligned}$$

Donc si $n \equiv 1 \pmod 3$, alors S_n est divisible par 3 si et seulement si $n \equiv 4 \pmod 9$.

— **Cas 3 :** $n \equiv 2 \pmod 3$

$$n^2 \equiv 4 \equiv 1 \pmod 3 \Rightarrow n^2 + 2 \equiv 0 \pmod 3$$

Soit $n^2 + 2 = 3m'$, donc :

$$n(n^2+2) = n \cdot 3m' = 3nm'$$

Pour que $3nm' \equiv 0 \pmod 9$, il faut $nm' \equiv 0 \pmod 3$.
Comme $n \not\equiv 0 \pmod 3$, il faut $m' \equiv 0 \pmod 3$.

$$m' = \frac{n^2+2}{3} \Rightarrow n^2 + 2 \equiv 0 \pmod 9$$

Testons les cas :

$$\begin{aligned} n \equiv 2 \pmod 9 &\Rightarrow n^2 + 2 = 4 + 2 = 6 \not\equiv 0 \pmod 9 \\ n \equiv 5 \pmod 9 &\Rightarrow 25 + 2 = 27 \equiv 0 \pmod 9 \\ n \equiv 8 \pmod 9 &\Rightarrow 64 + 2 = 66 \equiv 3 \not\equiv 0 \pmod 9 \end{aligned}$$

Donc si $n \equiv 2 \pmod 3$, alors S_n est divisible par 3 si et seulement si $n \equiv 5 \pmod 9$.

Conclusion : S_n est divisible par 3 si et seulement si :

$$n \equiv 0,\ 4 \text{ ou } 5 \pmod 9$$

Exercice 3 :

a) En utilisant le petit théorème de Fermat, calculez le reste de la division de 29^{203} par 19. Montrez toutes les étapes de réduction.

Calcul de $29^{203} \pmod{19}$

19 est un nombre premier.

Réduisons la base modulo 19 :

$$29 = 1 \cdot 19 + 10 \Rightarrow 29 \equiv 10 \pmod{19}$$

Donc :

$$29^{203} \equiv 10^{203} \pmod{19}$$

Par le petit théorème de Fermat : Si $a^{p-1} \equiv 1 \pmod{p}$ pour p premier et $p \nmid a$, alors ici :

$$a = 10,\ p = 19,\ \Rightarrow 10^{18} \equiv 1 \pmod{19}$$

Nous devons maintenant réduire l'exposant 203 modulo 18 :

$$203 = 18 \cdot 11 + 5 \Rightarrow 203 \equiv 5 \pmod{18}$$

Ainsi :

$$10^{203} \equiv 10^{18 \cdot 11 + 5} \equiv (10^{18})^{11} \cdot 10^5 \pmod{19}$$

Puisque $10^{18} \equiv 1 \pmod{19}$, on obtient :

$$(10^{18})^{11} \cdot 10^5 \equiv 1^{11} \cdot 10^5 \equiv 10^5 \pmod{19}$$

Calcul de $10^5 \mod 19$:

$$\begin{aligned}
&10^1 \equiv 10 \pmod{19} \\
&10^2 = 100 \Rightarrow 100 = 5 \cdot 19 + 5 \Rightarrow 10^2 \equiv 5 \pmod{19} \\
&10^3 = 10 \cdot 10^2 = 10 \cdot 5 = 50 \Rightarrow 50 = 2 \cdot 19 + 12 \Rightarrow 10^3 \equiv 12 \equiv -7 \pmod{19} \\
&10^4 = (10^2)^2 = 5^2 = 25 \Rightarrow 25 = 1 \cdot 19 + 6 \Rightarrow 10^4 \equiv 6 \pmod{19} \\
&10^5 = 10 \cdot 10^4 = 10 \cdot 6 = 60 \Rightarrow 60 = 3 \cdot 19 + 3 \Rightarrow 10^5 \equiv 3 \pmod{19}
\end{aligned}$$

Conclusion :

$$29^{203} \equiv 3 \pmod{19}$$

b) Soit $\phi(n)$ l'indicatrice d'Euler et $\lambda(n)$ la fonction de Carmichael. Calculez $\phi(100)$ et $\lambda(100)$.

Calcul de $\phi(100)$ et $\lambda(100)$.

On a :

$$100 = 10^2 = (2 \cdot 5)^2 = 2^2 \cdot 5^2$$

$$\phi(100) = \phi(2^2 \cdot 5^2) = \phi(2^2) \cdot \phi(5^2) \quad \text{car } pgcd(2^2, 5^2) = 1$$

$$\phi(2^2) = 2^2 - 2^1 = 4 - 2 = 2$$
$$\phi(5^2) = 5^2 - 5^1 = 25 - 5 = 20$$
$$\phi(100) = 2 \cdot 20 = 40$$

$$\lambda(100) = \text{ppcm}(\lambda(2^2), \lambda(5^2))$$
$$\lambda(2^2) = \lambda(4) = 2 \quad (\text{car } a^2 \equiv 1 \pmod 4 \text{ pour } a \text{ impair : } 1^2 = 1,\ 3^2 = 9 \equiv 1)$$
$$\lambda(5^2) = \phi(5^2) = 20$$
$$\lambda(100) = \text{ppcm}(2, 20) = 20$$

$\lambda(100) = 20, \quad \phi(100) = 40$

c) Calculez $23^{643} \pmod{100}$.

Calcul de $23^{643} \pmod{100}$
Vérifions d'abord :

$$pgcd(23, 100)$$

Les facteurs de 100 sont 2 et 5, et 23 n'est divisible ni par 2 ni par 5. Donc :

$$pgcd(23, 100) = 1$$

On peut utiliser le théorème d'Euler ou de Carmichael. Carmichael donne un exposant plus petit, donc utilisons :

$$\lambda(100) = 20 \Rightarrow 23^{20} \equiv 1 \pmod{100}$$

Réduisons l'exposant modulo 20 :

$$643 = 20 \cdot 32 + 3 \Rightarrow 643 \equiv 3 \pmod{20}$$

Donc :

$$23^{643} \equiv 23^{20\cdot 32+3} \equiv (23^{20})^{32} \cdot 23^3 \equiv 1^{32} \cdot 23^3 \equiv 23^3 \pmod{100}$$

Calculons $23^3 \mod 100$:

$$23^1 \equiv 23 \pmod{100}$$
$$23^2 = 529 \Rightarrow 529 \equiv 29 \pmod{100}$$
$$23^3 = 23 \cdot 29 = 667 \Rightarrow 667 \equiv 67 \pmod{100}$$

Conclusion :

$$23^{643} \equiv 67 \pmod{100}$$

Exercice 4 :

Alice souhaite envoyer un message secret à Bob en utilisant le cryptosystème RSA. Bob choisit deux nombres premiers $p = 11$ et $q = 13$.

a) Calculez n et $\lambda(n)$.

Données :

$$p = 11, \quad q = 13$$

Calcul de n :

$$n = p \cdot q = 11 \cdot 13 = 143$$

Calcul de $\lambda(n)$ (fonction de Carmichael) :

$$\lambda(n) = \mathrm{ppcm}(p-1, q-1) = \mathrm{ppcm}(11-1,\ 13-1) = \mathrm{ppcm}(10,\ 12)$$

Décompositions en facteurs premiers :

$$10 = 2 \cdot 5, \quad 12 = 2^2 \cdot 3$$

Donc :

$$\mathrm{ppcm}(10, 12) = 2^2 \cdot 3 \cdot 5 = 4 \cdot 15 = 60$$

Conclusion :

$$n = 143, \quad \lambda(n) = 60$$

b) Bob choisit $e = 7$. Vérifiez que e est un choix valide.

Pour le chiffrement RSA, l'entier e doit vérifier les conditions suivantes :

$$1 < e < \lambda(n) \quad \text{et} \quad pgcd(e, \lambda(n)) = 1$$

Prenons $\lambda(n) = 60$.
Vérifions que $e = 7$ est un choix valide :

— $1 < 7 < 60$, donc la première condition est satisfaite.
— Calculons $pgcd(7, 60)$ à l'aide de l'algorithme d'Euclide :

$$\begin{aligned} 60 &= 8 \times 7 + 4 \\ 7 &= 1 \times 4 + 3 \\ 4 &= 1 \times 3 + 1 \\ 3 &= 3 \times 1 + 0 \end{aligned}$$

— On obtient donc $pgcd(7, 60) = 1$.

Ainsi, $e = 7$ est un choix valide pour la clé de chiffrement RSA.

c) Calculez la clé privée d de Bob. Montrez les étapes de l'algorithme d'Euclide étendu.

Nous cherchons d tel que :

$$ed \equiv 1 \pmod{\lambda(n)} \quad \text{soit} \quad 7d \equiv 1 \pmod{60}$$

Cela revient à résoudre l'équation diophantienne :

$$7d - 60k = 1 \quad \text{pour des entiers } d, k$$

Utilisons l'algorithme d'Euclide étendu (en partant du calcul du pgcd vu précédemment) :

$$\begin{aligned}
1 &= 4 - 1 \cdot 3 \\
&= 4 - 1 \cdot (7 - 1 \cdot 4) = 2 \cdot 4 - 1 \cdot 7 \\
&= 2 \cdot (60 - 8 \cdot 7) - 1 \cdot 7 \\
&= 2 \cdot 60 - 16 \cdot 7 - 1 \cdot 7 \\
&= 2 \cdot 60 - 17 \cdot 7
\end{aligned}$$

Donc :

$$1 = (-17) \cdot 7 + 2 \cdot 60$$

Ce qui signifie que :

$$7d + 60k = 1 \quad \text{avec } d_0 = -17$$

On veut une solution positive pour d, donc on ajoute un multiple de 60 :

$$d = -17 + 60 = 43$$

Vérification :

$$7 \cdot 43 = 301, \quad \text{et} \quad 301 \equiv 1 \pmod{60}$$

Conclusion : la clé privée est :

$$d = 43$$

d) Alice veut envoyer le message $M = 140$. Chiffrez le message pour Bob. Soit C le message chiffré.

Alice souhaite chiffrer le message $M = 140$ en utilisant la clé publique $(n = 143, e = 7)$.
Comme $0 \leq 140 < 143$, le message est dans l'intervalle valide.

On calcule :

$$C = M^e \bmod n = 140^7 \bmod 143$$

Remarquons que :

$$140 \equiv -3 \pmod{143} \Rightarrow C \equiv (-3)^7 \pmod{143}$$

Calculons les puissances successives de -3 modulo 143 :

$$
\begin{aligned}
&(-3)^1 = -3 \equiv 140 \pmod{143} \\
&(-3)^2 = 9 \\
&(-3)^3 = -27 \equiv 116 \pmod{143} \\
&(-3)^4 = (-3) \cdot 116 = -348 \equiv -348 + 3 \cdot 143 = 81 \pmod{143} \\
&(-3)^5 = (-3) \cdot 81 = -243 \equiv -243 + 2 \cdot 143 = 43 \pmod{143} \\
&(-3)^6 = ((-3)^3)^2 = 116^2 = 13456 \\
&\qquad \Rightarrow 13456 \div 143 = 94 \text{ reste } 14 \Rightarrow 116^2 \equiv 14 \pmod{143} \\
&(-3)^7 = (-3) \cdot 14 = -42 \equiv -42 + 143 = 101 \pmod{143}
\end{aligned}
$$

Ainsi, le message chiffré est :

$$C = 101$$

e) Montrez comment Bob déchiffre C pour retrouver M.

Bob utilise sa clé privée $d = 43$ avec $n = 143$ pour déchiffrer le message reçu.

Le message chiffré est $C = 101$, et on calcule :

$$M = C^d \bmod n = 101^{43} \bmod 143$$

Grâce à la propriété de RSA :

$$e \cdot d \equiv 1 \pmod{\lambda(n)} \Rightarrow M^{ed} \equiv M \pmod{n}$$

Comme $C = M^e$, on a :

$$C^d = (M^e)^d = M^{ed} \equiv M \pmod{n}$$

Donc :

$$101^{43} \equiv 140 \pmod{143}$$

Le message déchiffré est donc :

$$M = 140$$

f) Supposons qu'Ève intercepte $C = 10$, $n = 55$ et $e = 7$. Ève ne connaît pas p, q ni d. Comment Ève pourrait-elle essayer de casser le code ? Trouvez M.

Ève intercepte $n = 55$. Comme ce nombre est petit, elle peut facilement le factoriser :

$$55 = 5 \cdot 11 \Rightarrow p = 5, \quad q = 11$$

Elle calcule ensuite l'indicatrice de Carmichael :

$$\lambda(n) = \mathrm{ppcm}(p-1, q-1) = \mathrm{ppcm}(4, 10) = \mathrm{ppcm}(2^2, 2 \cdot 5) = 2^2 \cdot 5 = 20$$

Sachant que la clé publique est $e = 7$, Ève cherche d tel que :

$$ed \equiv 1 \pmod{20} \quad \Rightarrow \quad 7d \equiv 1 \pmod{20}$$

Elle résout l'équation diophantienne $7d - 20k = 1$ à l'aide de l'algorithme d'Euclide étendu :

$$\begin{aligned}
20 &= 2 \cdot 7 + 6 \\
7 &= 1 \cdot 6 + 1 \\
1 &= 7 - 1 \cdot 6 \\
&= 7 - 1 \cdot (20 - 2 \cdot 7) = 3 \cdot 7 - 1 \cdot 20
\end{aligned}$$

Ainsi,

$$1 = 3 \cdot 7 + (-1) \cdot 20 \Rightarrow d = 3$$

Ève peut maintenant déchiffrer le message intercepté $C = 10$:

$$M = C^d \bmod n = 10^3 \bmod 55$$

Calcul des puissances :

$$\begin{aligned}
&10^1 = 10 \\
&10^2 = 100 \equiv 45 \pmod{55} \\
&10^3 = 10 \cdot 45 = 450 \equiv 10 \pmod{55}
\end{aligned}$$

Donc, le message original était :

$$M = 10$$

Exercice 5 (facultatif) :

a) Trouvez toutes les solutions entières (s'il en existe) de la congruence linéaire $55x \equiv 30 \pmod{125}$.

Résolvons la congruence suivante :

$$55x \equiv 30 \pmod{125}$$

Cela revient à résoudre l'équation diophantienne :

$$55x - 125y = 30$$

Calculons le plus grand commun diviseur :

$$\begin{aligned}
125 &= 2 \cdot 55 + 15 \\
55 &= 3 \cdot 15 + 10 \\
15 &= 1 \cdot 10 + 5 \\
10 &= 2 \cdot 5 + 0
\end{aligned}$$

Donc :

$$pgcd(55, 125) = 5$$

Comme 5 divise 30 ($30 = 6 \cdot 5$), l'équation admet des solutions.
Il y aura 5 solutions incongrues modulo 125.
Divisons la congruence initiale par 5 :

$$11x \equiv 6 \pmod{25}$$

Cherchons l'inverse de 11 modulo 25 à l'aide de l'algorithme d'Euclide étendu :

$$\begin{aligned}
25 &= 2 \cdot 11 + 3 \\
11 &= 3 \cdot 3 + 2 \\
3 &= 1 \cdot 2 + 1 \\
1 &= 3 - 1 \cdot 2 \\
&= 3 - 1 \cdot (11 - 3 \cdot 3) = 4 \cdot 3 - 11 \\
&= 4 \cdot (25 - 2 \cdot 11) - 11 = 4 \cdot 25 - 9 \cdot 11
\end{aligned}$$

On a :

$$1 = 4 \cdot 25 - 9 \cdot 11 \Rightarrow 1 \equiv -9 \cdot 11 \pmod{25}$$

Donc l'inverse de 11 modulo 25 est :

$$-9 \equiv 16 \pmod{25}$$

Vérification :

$$11 \cdot 16 = 176 \Rightarrow 176 \equiv 1 \pmod{25}$$

Multiplions la congruence par l'inverse :

$$16 \cdot 11x \equiv 16 \cdot 6 \pmod{25} \Rightarrow x \equiv 96 \pmod{25}$$

Puisque $96 \div 25 = 3$ reste 21, alors :

$$x \equiv 21 \pmod{25}$$

Les solutions générales sont :

$$x = 21 + 25k, \quad \text{où } k \in \mathbb{Z}$$

Les 5 solutions incongrues modulo 125 (pour $k = 0, 1, 2, 3, 4$) sont :

$$\begin{aligned}
x_0 &= 21 \pmod{125} \\
x_1 &= 46 \pmod{125} \\
x_2 &= 71 \pmod{125} \\
x_3 &= 96 \pmod{125} \\
x_4 &= 121 \pmod{125}
\end{aligned}$$

b) Un système de congruences est donné : $N \equiv 2 \pmod 3$ $N \equiv 3 \pmod 5$ $N \equiv 2 \pmod 7$ Quel est le plus petit entier positif N qui satisfait ces conditions ?

Résolvons le système de congruences :

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

Étape 1 : Première congruence

$$N \equiv 2 \pmod{3} \Rightarrow N = 3k_1 + 2$$

Étape 2 : Substituer dans la deuxième

$$3k_1 + 2 \equiv 3 \pmod{5} \Rightarrow 3k_1 \equiv 1 \pmod{5}$$

Trouvons l'inverse de 3 modulo 5 :

$$3 \cdot 1 = 3, \quad 3 \cdot 2 = 6 \equiv 1 \pmod{5} \Rightarrow \text{inverse} = 2$$

$$2 \cdot 3k_1 \equiv 2 \cdot 1 \Rightarrow 6k_1 \equiv 2 \pmod{5} \Rightarrow k_1 \equiv 2 \pmod{5} \Rightarrow k_1 = 5j + 2$$

Étape 3 : Substituer dans l'expression de N

$$N = 3k_1 + 2 = 3(5j + 2) + 2 = 15j + 6 + 2 = 15j + 8$$

Étape 4 : Substituer dans la troisième congruence

$$15j + 8 \equiv 2 \pmod{7}$$

$$15 \equiv 1 \pmod{7}, \quad 8 \equiv 1 \pmod{7} \Rightarrow j + 1 \equiv 2 \pmod{7} \Rightarrow j \equiv 1 \pmod{7} \Rightarrow j = 7m + 1$$

Étape 5 : Calcul final de N

$$N = 15j + 8 = 15(7m + 1) + 8 = 105m + 15 + 8 = 105m + 23$$

Le plus petit entier positif solution est obtenu pour $m = 0$:

$$N = 23$$

Vérification :

$$\begin{aligned} 23 \div 3 &= 7 \text{ reste } 2 \quad &\Rightarrow N \equiv 2 \pmod 3 \\ 23 \div 5 &= 4 \text{ reste } 3 \quad &\Rightarrow N \equiv 3 \pmod 5 \\ 23 \div 7 &= 3 \text{ reste } 2 \quad &\Rightarrow N \equiv 2 \pmod 7 \end{aligned}$$

Donc $N = \boxed{23}$ est la plus petite solution du système.

c) Soient $m, n \in \mathbb{N}_{>0}$ et $a, b \in \mathbb{Z}$. Considérez le système de congruences :

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

i) **Existence** – Montrer que le système admet une solution x si et seulement si $\text{pgcd}(m, n) \mid (a - b)$.

Considérons le système :

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

Cela signifie qu'il existe des entiers $k_1, k_2 \in \mathbb{Z}$ tels que :

$$x = a + k_1 m = b + k_2 n \Rightarrow a + k_1 m = b + k_2 n \Rightarrow k_1 m - k_2 n = b - a$$

Nous obtenons une équation diophantienne linéaire de la forme :

$$mX + nY = C$$

avec $X = k_1$, $Y = -k_2$ et $C = b - a$.
Il est bien connu qu'une telle équation admet des solutions entières si et seulement si :

$$pgcd(m, n) \mid C \Rightarrow pgcd(m, n) \mid (b - a)$$

Comme $pgcd(m, n)$ divise $(b - a)$ si et seulement s'il divise $-(a - b)$, on conclut que :

$$pgcd(m, n) \mid (a - b)$$

Donc, le système a une solution x si et seulement si $pgcd(m, n) \mid (a - b)$. □

ii) **Unicité modulo** – Lorsqu'une solution existe, démontrer qu'elle est unique modulo $\text{ppcm}(m, n)$.

Supposons qu'une solution x_0 existe. Alors :

$$x_0 \equiv a \pmod m \quad \text{et} \quad x_0 \equiv b \pmod n$$

Soit x_1 une autre solution du même système :

$$x_1 \equiv a \pmod{m} \quad \text{et} \quad x_1 \equiv b \pmod{n}$$

Alors, par transitivité des congruences :

$$x_1 \equiv x_0 \pmod{m} \Rightarrow m \mid (x_1 - x_0)$$

$$x_1 \equiv x_0 \pmod{n} \Rightarrow n \mid (x_1 - x_0)$$

Ainsi, $(x_1 - x_0)$ est divisible à la fois par m et par n, donc :

$$\text{ppcm}(m, n) \mid (x_1 - x_0)$$

Ce qui signifie :

$$x_1 \equiv x_0 \pmod{\text{ppcm}(m, n)}$$

Donc toutes les solutions du système sont congrues entre elles modulo $\text{ppcm}(m, n)$. Cela implique que la solution est **unique modulo** $\text{ppcm}(m, n)$. □

iii) **Construction explicite** – Fournir une formule pour une solution particulière en termes des coefficients u, v tels que $mu + nv = \text{pgcd}(m, n)$ (obtenus par l'algorithme d'Euclide étendu), en supposant que la condition d'existence est satisfaite.

Considérons le système :

$$\begin{cases} x \equiv a \pmod{m} & (1) \\ x \equiv b \pmod{n} & (2) \end{cases}$$

Étape 1 : Substitution

De la première congruence :

$$x = a + km \quad \text{pour un certain } k \in \mathbb{Z}$$

Substituons dans (2) :

$$a + km \equiv b \pmod{n} \Rightarrow km \equiv b - a \pmod{n}$$

Étape 2 : Utiliser l'algorithme d'Euclide étendu

Soit $d = pgcd(m, n)$. Par l'algorithme d'Euclide étendu, il existe des entiers u, v tels que :

$$mu + nv = d$$

Puisque nous supposons qu'une solution existe, on a $d \mid (b - a)$, donc il existe un entier q tel que :

$$b - a = qd$$

Étape 3 : Résolution

Multiplions $mu + nv = d$ par q :

$$m(uq) + n(vq) = qd = b - a$$

Cela donne :

$$m(uq) \equiv b - a \pmod{n}$$

Donc une solution particulière pour k est :

$$k_0 = u \cdot \frac{b-a}{d}$$

Étape 4 : Substitution dans l'expression de x

En substituant k_0 dans $x = a + km$, on obtient une solution particulière :

$$x_0 = a + m \cdot \left(u \cdot \frac{b-a}{d} \right)$$

Conclusion : cette expression donne une solution particulière x_0 au système. $\square$

Feuille supplémentaire