PGCD PPCM ET APPLICATIONS

1. LE PGCD

a. Définition

Remarque préliminaire : l'ensemble des diviseurs $\mathcal{D}(a)$ d'un nombre entier naturel a est un ensemble fini non vide, puisqu'il contient 1, et admettant un élément maximal, qui est a. De même, l'ensemble des diviseurs $\mathcal{D}(a, b)$ communs à deux entiers naturels a et b est un ensemble fini non vide, puisqu'il contient 1, et admettant un élément maximal, qui est inférieur ou égal au minimum de a et de b.

Définition : le plus grand commun diviseur de deux entiers naturels non nuls est le plus grand élément de l'ensemble des diviseurs $\mathcal{D}(a, b)$ communs à a et b. On note $\text{pgcd}(a,b)$ ou $a \wedge b$[1].

Propriété immédiate : $\text{pgcd}(a,b) = \text{pgcd}(b,a)$

Généralisation : cette notion se généralise à deux entiers relatifs non nuls.

Exemples :

- $\text{pgcd}(a,a) =$
- $\text{pgcd}(a,1) =$
- $\text{pgcd}(a,ka) =$ $\quad k \in \mathbb{Z}^*$
- Si $b \mid a$ alors $\text{pgcd}(a,b) =$

définition : a et b sont dits premiers entre eux si leur pcgd vaut 1.

b. Méthodes de calcul du pgcd

i. Ensembles des diviseurs.

Exemple : on veut déterminer le pgcd de 378 et 525.

$\mathcal{D}(378)$ = {1, 2, 3, 6, 7, 9, 14, 18, 21, 27, 42, 54, 63, 126, 189, 378}

$\mathcal{D}(525)$ = {1, 3, 5, 7, 15, 21, 25, 35, 75, 105, 175, 525}

$\mathcal{D}(378) \cap \mathcal{D}(525)$ = {1, 3, 7, 21} donc $\text{pgcd}(a,b) = 21$

On remarque que $\mathcal{D}(378) \cap \mathcal{D}(525) = \mathcal{D}(21)$: l'ensemble des diviseurs communs est l'ensemble des diviseurs du pgcd.

ii. Soustractions successives d'Euclide.

Théorème : si $a > b$, alors $\text{pgcd}(a,b) = \text{pgcd}(a-b,b)$.

Démonstration : on utilise les propriétés de la divisibilité.

$d \mid a$ et $d \mid b \Leftrightarrow d \mid a-b$ et $d \mid b$, donc l'ensemble des diviseurs communs à a et à b est égal à l'ensemble des diviseurs communs à $a-b$ et à b. En particulier le plus grand élément de cet ensemble est le $\text{pgcd}(a,b)$ et également celui de $\text{pgcd}(a-b,b)$.

Méthode : en se basant sur la propriété précédente, on ramène le calcul du pgcd de deux nombres au calcul du pgcd de deux nombres dont l'un des deux est strictement plus petit.

Comme la suite des calculs de $a-b$ est strictement décroissante dans $\mathbb{N}$, elle admet un plus petit élément et s'arrête.

Exemple : calcul de $357 \wedge 153$.

[1] Cette dernière notation est moins utilisée, elle utilise la notation du « et » en logique.

$357-153=204$

$204-153=51$

$153-51=102$

$102-51=51$

$\text{pgcd}(51,51)=51$

Remarque : essayez le calcul de $456 \wedge 183$ avec cette méthode, c'est très long et peu efficace.

iii. Algorithme d'Euclide

C'est la méthode la plus rapide en général.

On effectue une suite de divisions euclidiennes pour calculer $\text{pgcd}(a,b)$:

On divise *a* par *b* : $a=bq_0+r_0$

Puis *b* par r_0 : $b=r_0q_1+r_1$

Puis r_0 par r_1 : $r_0=r_1q_2+r_2$

…

Puis r_{n-1} par r_n : $r_{n-1}=r_nq_{n+1}+r_{n+1}$

Jusqu'à ce que l'on obtienne un reste nul. Le pgcd est le dernier reste non nul.

Démonstration :

- Par définition de la division euclidienne, $b>r_0>r_1>\ldots>r_n>\ldots\geq 0$. La suite (r_n) des restes est une suite d'entiers naturels strictement décroissante, elle est donc finie. Donc l'algorithme s'arrête.
- Si *d* est un diviseur de *a* et de *b*, alors *d* divise toute combinaison linéaire de *a* et *b*. En particulier *d* divise $a-bq_0$, c'est-à-dire que $d \mid r_0$ et $d \mid b$.

  Réciproquement si $d \mid r_0$ et $d \mid b$, alors $d \mid r_0+bq_0$, c'est à dire que *d* divise *a*.

  Donc $\mathcal{D}(a, b) = \mathcal{D}(b, r_0)$.
- Finalement, soit r_i le dernier reste non nul

  On a $\mathcal{D}(a, b) = \mathcal{D}(b, r_0) = \mathcal{D}(r_0, r_1) = \ldots = \mathcal{D}(r_{i-1}, r_i)$ d'après ce qui précède.

  Et par définition de r_i : $r_{i-1}=r_iq_{i+1}+0$, soit r_i divise r_{i-1}.

  Donc $\text{pgcd}(a,b)=\text{pgcd}(r_{i-1},r_i)=r_i$ ■

Remarque : cet algorithme est très rapide, voir l'exercice XXXV sur la page http://www.maths-info-lycee.fr/exos_arithmetique.html

Exemple : calcul de pgcd(5525, 1989)

$5525=1989\times 2+1547$

$1989=1547\times 1+442$

$1547=442\times 3+221$

$442=221\times 2$

Le pgcd vaut 221

c. Propriétés du pgcd

Propriétés : soient *a*, *b* et *k* trois entiers naturels non nuls. Alors :

- $\text{pgcd}(ka,kb)=k\times\text{pgcd}(a,b)$
- Si $k \mid a$ et $k \mid b$ alors $\text{pgcd}\left(\frac{a}{k},\frac{b}{k}\right)=\frac{1}{k}\times\text{pgcd}(a,b)$
- $\text{pgcd}(a,b)=\text{pgcd}(a+kb,b)=\text{pgcd}(a,b+ka)$

Démonstrations :

- Pour $\text{pgcd}(ka,kb) = k \times \text{pgcd}(a,b)$.
  - 1ère méthode : on reprend la suite des divisions euclidiennes et on les multiplie par k :

$$\begin{array}{ll} a = bq_0 + r_0 & ka = kbq_0 + kr_0 \\ b = r_0q_1 + r_1 & kb = kr_0q_1 + kr_1 \\ r_0 = r_1q_2 + r_2 & kr_0 = kr_1q_2 + kr_2 \\ \ldots \quad \Rightarrow & \ldots \\ r_{i-1} = r_iq_{i+1} + 0 & kr_{i-1} = kr_iq_{i+1} + 0 \end{array}$$

d'où $\text{pgcd}(a,b) = \text{pgcd}(r_{i-1},r_i) = r_i$

d'où $\text{pgcd}(ka,kb) = \text{pgcd}(kr_{i-1},kr_i) = kr_i$

CQFD

  - 2ème méthode : on utilise les propriétés de la divisibilité

Soit $\delta = \text{pgcd}(a,b)$. Alors $\begin{cases} \delta \mid a \\ \delta \mid b \end{cases} \Rightarrow \begin{cases} k\delta \mid ka \\ k\delta \mid kb \end{cases} \Rightarrow \delta \mid \text{pgcd}(a,b)$

Réciproquement, soit q tel que $q(k\delta) = \text{pgcd}(ka,kb)$

$\begin{cases} qk\delta \mid ka \\ qk\delta \mid kb \end{cases} \Rightarrow \begin{cases} q\delta \mid a \\ q\delta \mid b \end{cases} \Rightarrow q\delta \mid \text{pgcd}(a,b) \Rightarrow q\delta \mid 1 \Rightarrow q \mid 1 \Rightarrow q = 1$ CQFD

- Pour : Si $k \mid a$ et $k \mid b$ alors $\text{pgcd}\left(\frac{a}{k},\frac{b}{k}\right) = \frac{1}{k} \times \text{pgcd}(a,b)$

  Immédiat d'après la propriété précédente. Presque immédiat… pas si simple à rédiger, poser $a = ka'$ et $b = kb'$ et conclure :

- Pour $\text{pgcd}(a,b) = \text{pgcd}(a+kb,b) = \text{pgcd}(a,b+ka)$

$\begin{cases} d \mid a \\ d \mid b \end{cases} \Rightarrow \begin{cases} d \mid a+kb \\ d \mid b \end{cases} \Rightarrow \text{pgcd}(a,b) = \text{pgcd}(a+kb,b)$

Contre-exemple : la propriété précédente est fausse avec $\text{pgcd}(a,a+kb)$.

$\text{pgcd}(18,12) =$ et $\text{pgcd}(18,18+3\times12) =$

Corollaire important :

Si $\delta = \text{pgcd}(a,b)$ alors $\text{pgcd}\left(\frac{a}{\delta},\frac{b}{\delta}\right) = 1$, c'est à dire que $\frac{a}{\delta}$ et $\frac{b}{\delta}$ sont premiers entre eux.

2. LE PPCM

De même que l'on a défini l'ensemble des diviseurs communs à deux entiers naturels non nuls, on peut définir l'ensemble des multiples communs non nuls à deux entiers naturels non nuls a et b. Cet ensemble est non vide, puisqu'il contient ab, et c'est un ensemble d'entiers naturels : il admet donc un plus petit élément.

Définition : soient a et b deux entiers naturels non nuls. Le plus petit commun multiple de a et b est le plus petit élément non nul de l'ensemble des multiples communs à a et b.

Cette notion se généralise à deux entiers relatifs non nuls, le ppcm étant positif par définition.

On le note $\text{ppcm}(a,b)$ ou plus rarement $a \vee b$[2].

Exemple : $\text{ppcm}(378,525) = 9450$

Théorème : l'ensemble des multiples communs à *a* et à *b* est l'ensemble des multiples de $\text{ppcm}(a,b)$.

Démonstration :

- Soit $\mu = \text{ppcm}(a,b)$

  Si *m* est multple de μ, comme μ est multiple de *a*, alors *m* est multiple de *a*.
  De même *m* est un multiple de *b*.
  Donc tout multiple de *m* est un multiple commun à *a* et *b*.
- Réciproquement, si *m* est un multiple commun à *a* et *b*, effectuons la division euclidienne de *m* par μ : $m = \mu q + r$ avec $0 \le r < \mu$.

  m et μ sont des multiples de *a* donc $m - \mu q$ est un multiple de *a*, donc *r* est un multiple de *a*.

  De même, *r* est un multiple commun à *a* et *b* avec $r < \mu$. Comme μ est le plus petit multiple commun non nul de *a* et *b*, alors *r* = 0 et $m = \mu q$: *m* est un multiple de μ.

CQFD

Corollaire :

$$\begin{cases} a \mid m \\ b \mid m \end{cases} \Leftrightarrow \text{ppcm}(a,b) \mid m$$

Lemme : Soit $\mu = \text{ppcm}(a,b)$, soient α et β tels que $\mu = \alpha a = \beta b$. Alors $\text{pcgd}(\alpha,\beta) = 1$

Démonstration :

Soit *d* un diviseur commun à α et β.

$d \mid \alpha$ donc $\alpha = kd$, or $\mu = \alpha a$, donc $\mu = kda$.

Donc $\frac{\mu}{d}$ est entier, et $a \mid \frac{\mu}{d}$.

De même $b \mid \frac{\mu}{d}$.

Donc $\frac{\mu}{d}$ est un multiple commun à *a* et *b*, donc un multiple de leur ppcm. Par ailleurs $d \ge 1$, donc $\frac{\mu}{d} \le \mu$. Comme μ est le plus petit des multiples communs, on a forcément *d* = 1. CQFD

Théorème : Soient *a* et *b* deux entiers naturels non nuls. Alors $\text{ppcm}(a,b) \times \text{pgcd}(a,b) = ab$.

Démonstration : on utilise les notations et le résultat du lemme précédent.

On part de $\text{pcgd}(\alpha,\beta) = \text{pgcd}\left(\frac{\mu}{a}, \frac{\mu}{b}\right)$

On multiplie les deux membres par *ab* :

$$ab \cdot \underbrace{\text{pcgd}(\alpha,\beta)}_{1} = \text{pgcd}\left(ab\frac{\mu}{a}, ab\frac{\mu}{b}\right) = \text{pgcd}(\mu b, \mu a) = \underbrace{\mu}_{\text{ppcm}(a,b)} \cdot \text{pgcd}(b,a)$$ CQFD

Propriétés : soient *a*, *b* et *k* trois entiers naturels non nuls.

- $\text{ppcm}(ka,kb) = k \cdot \text{ppcm}(a,b)$
- Si $k \mid a$ et $k \mid b$ alors $\text{ppcm}\left(\frac{a}{k}, \frac{b}{k}\right) = \frac{1}{k} \times \text{ppcm}(a,b)$

[2] Comme ci-dessus pour le pgcd, cette notation est celle du « ou » en logique.

Démonstration : pour $\text{ppcm}(ka,kb) = k \cdot \text{ppcm}(a,b)$

On utilise le théorème précédent, $\text{ppcm}(a,b) \times \text{pgcd}(a,b) = ab$, en remplaçant *a* par *ka* et *b* par *kb*.

$$\text{ppcm}(ka,kb) \times \text{pgcd}(ka,kb) = kakb \Rightarrow \text{ppcm}(ka,kb) \times k \times \text{pgcd}(a,b) = k^2 ab$$

$$\text{ppcm}(ka,kb) = k\frac{ab}{\text{pgcd}(a,b)} \Rightarrow \text{ppcm}(ka,kb) = k\frac{\text{ppcm}(a,b) \times \cancel{\text{pgcd}(a,b)}}{\cancel{\text{pgcd}(a,b)}}$$

■

Remarques :

- La démonstration de la deuxième propriété ci-dessus peut se faire sur le modèle de la preuve de la propriété similaire pour le pgcd.
- Si $\delta = \text{pgcd}(a,b)$, $a = \delta a'$, $b = \delta b'$, alors $\text{ppcm}(a,b) = ab' = a'b = \delta a' b'$
- Propriétés similaires avec $\mu = \text{ppcm}(a,b)$.

3. THÉORÈME DE BEZOUT

Théorème : soient *a* et *b* deux entiers naturels non nuls, et soit δ leur pgcd. Alors il existe deux entiers relatifs *u* et *v* tels que $au + bv = \delta$.

Démonstration :

- Si $b \mid a$ alors $\text{pgcd}(a,b) =$, d'où $u =$ et $v =$ donnent $a \times \quad + b \times \quad = \quad$.
- De même si $a \mid b$.
- Sinon, on reprend les divisions successives de l'algorithme d'Euclide pour l'obtention du pgcd :

$a = bq_0 + r_0$

$b = r_0 q_1 + r_1$

$r_0 = r_1 q_2 + r_2$

…

$r_{i-3} = r_{i-2} q_{i-1} + r_{i-1}$ ligne ③

$r_{i-2} = r_{i-1} q_i + r_i$ ligne ②

$r_{i-1} = r_i q_{i+1} + 0$ ligne ①

avec $\text{pgcd}(a,b) = \text{pgcd}(r_{i-1}, r_i) = r_i = \delta$

On parcourt le calcul à l'envers, de l'avant-dernière à la première ligne, en exprimant r_i en fonction des restes et quotients successifs :

$r_{i-2} = r_{i-1} q_i + r_i$ donne $r_i = r_{i-2} - r_{i-1} q_i$

En substituant r_{i-1} obtenu dans la ligne ③ : $r_{i-3} = r_{i-2} q_{i-1} + r_{i-1} \Leftrightarrow r_{i-1} = r_{i-3} - r_{i-2} q_{i-1}$ on obtient

$r_i = r_{i-2} - (r_{i-3} - r_{i-2} q_{i-1}) q_i = u_2 r_{i-2} + v_3 r_{i-3}$

On remplace ensuite r_{i-1} à l'aide de la ligne précédente, etc. jusqu'à la ligne de départ, où l'on obtient alors $r_i = au + bv$ ■

Remarques :

- le couple (u,v) n'est pas unique. En effet, si $au + bv = \delta$ alors $\forall k \in \mathbb{Z} \quad a(u + kb) + b(v - ka) = \delta$
- Ce théorème est une implication, pas une équivalence. *Contre-exemple* :

$\underbrace{7}_{a} \times \underbrace{4}_{u} + \underbrace{3}_{b} \times \underbrace{(-8)}_{v} = 4$ et $\text{pgcd}(7,3) = 1$

Exemple : On a vu que pgcd(5525, 1989) = 221

$$\begin{aligned} 5525 &= 1989\times 2+1547 \\ 1989 &= 1547\times 1+442 \\ 1547 &= 442\times 3+221 \\ 442 &= 221\times 2 \end{aligned}$$

d' où

$$\begin{aligned} 221 &= \left(5525-1989\times 2\right)\times 4-1989\times 3 = 5525\times 4-1989\times 11 \\ 221 &= 1547-\left(1989-1547\times 1\right)\times 3 = 1547\times 4-1989\times 3 \\ 221 &= 1547-442\times 3 \end{aligned}$$

Théorème : deux entiers naturels non nuls a et b sont premiers entre eux si et seulement si il existe deux entiers relatifs u et v tels que $au+bv=1$.

Démonstration :

- Implication : d'après le théorème de Bézout, a et b sont premiers entre eux implique qu'il existe deux entiers relatifs u et v tels que $au+bv=1$.
- Réciproque : Soit $\delta=\text{pgcd}\left(a,b\right)$, et soient u et v tels que $au+bv=1$. Comme δdivise a et b, δ divise $au+bv$, donc δ divise 1, d'où $\delta=1$. ■

Remarques :

- On en déduit que a et v sont premiers entre eux, de même que u et b, ainsi que u et v.
- Important : on déduit du théorème de Bézout que l'équation $au+bv=D$ admet des solutions si et seulement si $\text{pcd}\left(a,b\right)\left|D\right.$.
  - Faire la preuve en exercice.
  - Comme précédemment, le couple $\left(u,v\right)$ n'est pas unique.

4. THEOREME DE GAUSS

Théorème : Soient a, b et c trois entiers relatifs non nuls. Si a divise bc et si a et b sont premiers entre eux, alors a divise c.

Démonstration :

- a divise bc donc il existe k entier relatif tel que $bc=ka$.
- par ailleurs, comme $\text{pgcd}\left(a,b\right)=1$, il existe u et v entiers relatifs tels que $au+bv=1$ d'après le théorème de Bezout.
  D'où $acu+bcv=c$
  $\Rightarrow acu+kav=c$
  $\Rightarrow a\left(cu+kv\right)=c$
  Donc a divise c.

■

Corollaires : Soient a, b et c trois entiers relatifs non nuls.

- Si a divise b, a divise c et si a et b sont premiers entre eux, alors ab divise c ;
- Si un nombre p premier divise le produit ab alors p divise a ou p divise b ;
- Si a est premier avec le produit bc, alors a est premier avec b et a est premier avec c ;
- Si a est premier avec c, alors PGCD(a , b) = PGCD(a, bc)

5. APPLICATION AUX EQUATIONS DIOPHANTIENNES

Une équations diophantienne est une équations dont la ou les inconnues sont des entiers.

a. Résolution dans $\mathbb{Z}^2$ d'équations du type $ax+by=c$, où a, b, c sont des entiers relatifs fixés.

Il y a trois cas à envisager

- Si c n'est pas un multiple de $\text{pgcd}\left(a,b\right)$:
  Alors il n'y a pas de solution d'après le théorème de Bezout.
  Exemple : $77x-21y=18$ $\quad S=\varnothing$
- Si $c=\text{pgcd}\left(a,b\right)$:
  Il y a une infinité de solutions d'après le théorème de Bezout.

Exemple : $77x-21y=7$

- On simplifie par le pgcd pour avoir un des nombres plus petits et des calculs plus simples : $77x-21y=7 \Leftrightarrow 11x-3y=1$.
- On cherche une solution particulière grâce à l'algorithme d'Euclide :

$$\begin{array}{l} 11=3\times 3+2 \\ 3=2\times 1+1 \end{array} \quad \text{donc} \quad \begin{array}{l} \boxed{1=-11-3\times(-4)} \\ 1=3-(11-3\times 3) \\ 1=3-2 \end{array}$$

Une solution particulière est $(-1,-4)$

On peut également trouver une solution évidente, par exemple ici $(2,7)$ *convient.*

- On trouve ensuite les solutions potentielles en utilisant à la fois la solution particulière et l'équation générale. *Les solutions sont potentielles car il s'agît ici d'une condition nécessaire et non d'une condition « nécessaire et suffisante ».*

$$\begin{cases} 11x-3y=1 \\ 11\times(-1)-3\times(-4)=1 \end{cases} \Rightarrow 11(x+1)-3(y+4)=0 \Rightarrow 11(x+1)=3(y+4) \quad ①$$

On applique le théorème de Gauss :

11 divise $3(y+4)$, et 11 et 3 sont premiers entre aux, donc 11 divise $y+4$.

D'où $\exists k \in \mathbb{Z} \quad y+4=11k$, puis en reportant dans ① :

$11(x+1)=3\times 11k \Leftrightarrow x+1=3k$.

On a donc $x=3k-1$ et $y=11k-4$, $k \in \mathbb{Z}$

- On vérifie que ces solutions conviennent (condition suffisante) :
  On remplace x et y dans l'équation initiale
  $11x-3y=11(3k-1)-3(11k-4)=1$ donc les valeurs trouvées conviennent.
- Conclusion $S=\{(3k-1,11k-4), k \in \mathbb{Z}\}$

- Si c est un multiple de $\text{pgcd}(a,b)$:

La méthode ressemble beaucoup au cas précédent, il y a également une infinité de solutions.

Exemple : $49x-21y=14$

$\text{pgcd}(49,21)=7$, 14 est un multiple de 7 donc il y a une infinité de solutions et $49x-21y=14 \Leftrightarrow 7x-3y=2$.

Dans un premier temps, on raisonne comme pour le cas précédent et l'on cherche une solution particulière à $7x-3y=1$, grâce à l'algorithme d'Euclide ou par intuition.

Ici $(1,2)$ convient.

On multiplie ces solutions par 2 pour avoir une solution particulière de $7x-3y=2$:

$7\times 2-3\times 4=2$

On trouve les solutions potentielles (condition nécessaire) :

$$\begin{cases} 7x-3y=2 \\ 7\times 2-3\times 4=2 \end{cases} \Rightarrow 7(x-2)-3(y-4)=0 \Rightarrow 7(x-2)=3(y-4) \quad ①$$

Puis, par le théorème de Gauss : 7 divise $3(y-4)$, et 7 et 3 sont premiers entre aux, donc 7 divise $y-4$.

D'où $\exists k \in \mathbb{Z} \quad y-4=7k$, puis en reportant dans ① :

$7(x-2)=3\times 7k \Leftrightarrow x-2=3k$.

D'où $x=3k+2$ et $y=7k+4$, $k \in \mathbb{Z}$

On vérifie que ces solutions conviennent (condition suffisante), en remplace x et y dans l'équation initiale

$7x-3y=7(3k+2)-3(7k+4)=2$ donc les valeurs trouvées conviennent.

Conclusion $S=\{(3k+2,7k+4), k\in\mathbb{Z}\}$

b. Résolution dans $\mathbb{Z}$ d'équations du type $ax\equiv b[c]$.

On remarque que $ax\equiv b[c]\Leftrightarrow ax+cv=b$, ce qui rappelle le théorème de Bézout.

Il y a de même trois cas à envisager

- Si b n'est pas un multiple de $\text{pgcd}(a,c)$:

  Il n'y a pas de solution d'après le théorème de Bézout.
- Si a et c sont premiers entre eux :

  Il y a une infinité de solution d'après le théorème de Bézout.

  Exemple : résoudre dans $\mathbb{Z}$ l'équation $28x\equiv 3[41]$.

  D'après le théorème de Bézout, il existe au moins un couple d'entiers $(u,v)\in\mathbb{Z}^2$ tel que :

  $28u-41v=1$.

  On applique l'algorithme d'Euclide :

  $41=1\times 28+13$ $\qquad 1=13-6\times 2$

  $28=2\times 13+2$ d'où $1=13-6\times(28-2\times 13)=13\times 13-6\times 28$

  $13=6\times 2+1$ $\qquad 1=13\times(41-28)-6\times 28=13\times 41-19\times 28$

  De $-19\times 28+13\times 41\equiv 1[41]$ on déduit $-19\times 28\equiv 1[41]$

  On multiplie alors les deux membres de $28x\equiv 3[41]$ par –19 :

  $-19\times 28x\equiv -19\times 3[41]\overset{(1)}{\Leftrightarrow} x\equiv -57[41]\Leftrightarrow x\equiv 25[41]$

  (1) on rappelle que $28\times(-19)\equiv 1[41]$

  Les solutions sont $S=\{41k+25, k\in\mathbb{Z}\}$
- Si a et c sont ne sont pas premiers entre eux, et si b est un multiple de $\delta=\text{pgcd}(a,c)$:

  On pose $a'=\frac{a}{\delta}$, $b'=\frac{b}{\delta}$ et $c'=\frac{c}{\delta}$; on est alors ramené au cas précédent, l'équation devenant $a'x\equiv b'[c']$ avec $\text{pgcd}(a',c')=1$.

Remarque : un cas particulier est la recherche d'un inverse de a modulo c, c'est-à-dire d'un nombre x tel que $ax\equiv 1[c]$. On constate que ce n'est pas toujours possible ; étudiez les cas suivants :

- $5x\equiv 1[7]$
- $4x\equiv 1[12]$