Divisibilité

La divisibilite dans Z pour 4è annee

Divisibilité :

Dans ce module d'introduction à l'arithmétique, retour sur les notions connues depuis le collège que sont la division euclidienne, les nombres premiers et la décomposition d'un nombre en produit de facteurs premiers.

Avertissement :

L'arithmétique concerne le raisonnement sur les entiers qu'ils soient naturels ou relatifs.

Cependant, certaines propriétés et certaines notions ne sont valables que pour des entiers naturels,

c'est pourquoi il faudra être toujours très vigilant tout au long de ce chapitre et bien regarder quel est l'ensemble dans lequel on travaille.

La divisibilite da

1/ Divisibilité : *définition(s)*

Divisibilité dans $\mathbb{N}$:

Soient a et b deux entiers *naturels.*

* On dit que *a divise b* s'il existe un entier naturel k tel que : b = a x k. On note a \ b

* On dit également que *b est un multiple de a* ou que *a est un diviseur de b.*

Propriété : *ordre et **divisibilité**.*

Soient a et b deux entiers *naturels* : si a divise b et b $\neq$ 0 alors a $\leq$ b

Les diviseurs d'un nombre entier non nul lui sont inférieurs.
Propriété qui servira très souvent dans les démonstrations.

De même, on définit :

Divisibilité dans $\mathbb{Z}$:

Soient a et b deux entiers *relatifs.*

* On dit que *a divise b* s'il existe un *entier relatif* k tel que : ***b = a x k .*** On note a \ b

* On dit également que *b est un multiple de a* ou que *a est un **diviseur** de b.*
Remarque : si b n'est pas un multiple de a alors a ne divise pas b.

Exemples :

► 6 = 2 x 3
Donc : 2 \6 et 3 \ 6 6 = (-1) x (-6)
Donc (-1) \ 6 et (-6) \ 6

Si on note D_6 l'ensemble des **diviseurs entiers** de 6 :

Attention à ne pas oublier :
le nombre lui même, son opposé,
1 et (-1)

D_6 = *-6 ; -3 ; -2 ; -1 ; 1 ; 2 ; 3 ; 6*

► -5 = (-1) x 5 Donc : 5 \ (-5) et pourtant attention : 5 > -5.

1/ Divisibilité : *division euclidienne dans* $\mathbb{N}$

Division euclidienne dans $\mathbb{N}$:

Soient a $\in \mathbb{N}$ et b $\in \mathbb{N}^*$

Il existe un unique couple (q , r) d'entiers naturels tels que :

$a = b \times q + r$ avec $0 \leq r < b$

q est le quotient, *r* le reste, *b* le **diviseur** et *a* le **dividende**.

Propriété :

« b divise a » si et seulement si « le reste de la **division euclidienne** de a par b est nul ».

Remarque :

Nous n'abordons pas dans ce module le cas de la division euclidienne dans $\mathbb{Z}$.
Cette notion sera travaillée en détail et sera le sujet d'exercices dans le module sur le pgcd.
Dans ce module-ci, nous nous contenterons d'utiliser la propriété pour montrer qu'un nombre n'en divise pas un autre.

1/ Divisibilité : *rappel des critères*

Divisibilité dans $\mathbb{N}$:

Soit n $\in \mathbb{N}$

► n est divisible par 2 si et seulement si : *son dernier chiffre est 0, 2, 4, 6 ou 8*

On dit alors que n est pair.
Dans le cas contraire, il est dit impair.

► n est divisible par 3 si et seulement si : *la somme de ses chiffres est divisible par 3.*

Remarque :
Ne pas hésiter à répéter l'application de ce critère à la somme trouvée s'il est difficile de savoir si cette somme est elle-même divisible par 3.

Exemple :
9876977 est-il divisible par 3 ?

9+8+7+6+9+7+7 = 53
5+3=8 qui n'est pas divisible par 3

Donc : 9876977 n'est pas divisible par 3.

► n est **divisible** par 4 si et seulement si : *le nombre formé par ses deux derniers chiffres est divisible par 4.*

► n est **divisible** par 5 si et seulement si : *son dernier chiffre est 0 ou 5.*

► n est **divisible** par 9 si et seulement si : *la somme de ses chiffres est divisible par 9.*
La technique des sommes successives vue avec 3 pouvant être utilisée également pour 9.

► n est **divisible** par 10 si et seulement si : *son dernier chiffre est 0.*

► n est **divisible** par 11 si et seulement si : *il s'agit d'un nombre à deux chiffres dont les deux chiffres sont égaux.*
Ou s'il s'agit d'un nombre à trois chiffres dont le chiffre des dizaines est égal à la somme du chiffre

des centaines et du chiffre des unités. (à condition que cette somme ne dépasse pas 9)

A ces critères, se rajoute évidemment la connaissance des tables de multiplication.

2/ Divisibilité : *résultats de référence*

Divisibilité dans $\mathbb{N}$	Divisibilité dans $\mathbb{Z}$
1° Quel que soit $a \in \mathbb{N}$: a \ a .	1° Quel que soit $a \in \mathbb{Z}$: a \ a et (-a) \ a .
2° 1 divise tout entier naturel.	2° 1 et (-1) divisent tout entier relatif.
3° Tout entier divise 0.	
4° 0 ne divise que 0.	
	5° a et (-a) ont les mêmes diviseurs.
6° 1 a pour seul diviseur naturel 1.	6° Les seuls diviseurs de 1 sont 1 et (-1).

Démonstration du 6° :
Soit a entier naturel tel que a \ 1.
D'après la propriété sur l'ordre : $a \leq 1$ donc $a = 0$ ou $a = 1$.

Or 0 ne divise pas 1 donc $a = 1$.
Soit a entier relatif tel que a \ 1. Alors, il existe k entier relatif tel que : $\boldsymbol{a = 1 \times k}$

D'où : $|a| = 1 \times |k|$ avec $|k| \in \mathbb{N}$

donc $|a| \backslash 1$ au sens de la **divisibilité** dans $\mathbb{N}$.

Par conséquent : $|a| = 1$ et donc a = 1 ou a = -1.

3/ Divisibilité : *propriétés*

Transitivité :
Si a \ b et b \ c alors a \ c.

Divisibilité dans $\mathbb{N}$	Divisibilité dans $\mathbb{Z}$
Soient a et b deux entiers naturels :	Soient a et b deux entiers relatifs :
Si a \ b et b \ a alors : a = b	Si a \ b et b \ a alors : a = b ou a = -b
Si a \ b alors quel que soit k entier naturel : $a \backslash k \times b$	Si a \ b alors quel que soit k entier relatif : $a \backslash k \times b$

Cette propriété nous servira à montrer l'égalité de deux PGCD.

Si a divise b alors a divise tout multiple de b.

Si c\a et c\b alors $c \backslash u \times a + v \times b$ quels que soient u et v *entiers relatifs.*
On dit que c divise toute combinaison linéaire de a et de b à coeficients entiers.

En particulier : c\a + b et c\a - b
Cette propriété peut évidemment être adaptée aux entiers naturels et à la **division** dans $\mathbb{N}$

4/ Nombres premiers : *définition*

Définition :
Soit p $\in \mathbb{N}$

On dit que p est un nombre premier ou plus simplement qu'il est premier si :
il admet exactement 2 diviseurs entiers naturels distincts.

Diviseurs qui sont 1 et lui-même.
(puisque 1 divise tout nombre et tout nombre est diviseur de lui-même.)

Remarques :
1) La notion de nombre premier ne concerne que les entiers naturels.
Il est donc ici question de **divisibilité** dans $\mathbb{N}$.
2) 0 a une infinité de diviseurs donc il n'est pas premier.
3) 1 n'a qu'un seul diviseur, qui est lui-même donc 1 n'est pas premier.
4) 2 a exactement 2 diviseurs : 1 et 2 donc 2 est le plus petit des nombres premiers.
5) L'ensemble des nombres premiers est noté : $\mathbb{P}$
6) Si n ≠ 1 n'est pas premier alors il possède au moins un diviseur autre que 1 et lui-même.

5/ Nombres premiers : *théorèmes*

Les nombres premiers constituent un des grands domaines de recherche en mathématiques.

A ce jour, il n'existe toujours pas de critère ou de formule qui permette instantanément de dire si un nombre quelconque est premier.

Prenons un entier naturel n différent de 1,et cherchons s'il est premier.

Si nous trouvons un entier naturel p, différent de 1 et de n, qui divise n alors par définition,
n *n'est pas premier.*

Or si (p divise n) et (p différent de n), *alors (p*

Il suffit donc de partir de 2 et de tester tous les entiers jusqu'à (n -1)

Mais, prenons par exemple n = 247,
est-il vraiment nécessaire de tester tous les entiers de 2 à 246
jusqu'à ce que l'on trouve ou non un diviseur de 247 ?

Un premier théorème va nous aider à affiner notre stratégie :
Théorème n°1 : Soit n $\in \mathbb{N}$
Si n ≠ 1 alors n admet au moins un diviseur premier.

Démonstration :

Cas n°1 : n = 0
2 divise 0 donc 0 admet au moins un diviseur premier.

Cas n°2 : n ≠ 0
a) si n est premier, ce diviseur est lui-même et la propriété est démontrée.
b) si n n'est pas premier, n possède au moins un diviseur différent de 1 et de lui-même.

D, ensemble des diviseurs de n autres que 1 et n n'est donc pas vide.

D étant un sous ensemble non vide de $\mathbb{N}$, il possède un plus petit élément que nous noterons p.

p n'est pas nul car 0 ne divise que 0 et n est différent de 0.

Montrons par l'absurde que p est premier :

Si p n'est pas premier, en tenant le même raisonnement que pour n, nous pouvons affirmer qu'il possède un diviseur k autre que 1 et lui-même.

Or k \ p et p ≠ 0 donc k ≤ p
mais k ≠ p donc k < p

De plus : p \ n non nul et p ≠ n donc p < n
D'où : k < n et donc : k ≠ n

Or : k \ p et p \ n donc k \ n.
Par conséquent : k ∈ D.
Donc D possède un élément strictement inférieur à p.

Ce qui est incompatible avec la définition de p. Donc p ne peut pas « ne pas être premier ».

Conclusion : n admet dans tous les cas un diviseur premier.

Conséquence de ce théorème au niveau de notre stratégie :
De 2 à (n -1) inclus nous n'allons donc tester que les nombres premiers.

en effet :

* Si on trouve que l'un de ces nombres premiers divise n alors n n'est pas premier.
* Si aucun de ces nombres ne divise n, n peut-il ne pas être premier ?
Autrement dit, est-il possible qu'il existe entre 2 et (n -1) un diviseur non premier de n ?

Supposons qu'un tel nombre existe et appelons-le d.
Comme d > 1, d possède au moins un diviseur premier : p

p \ d et d \ n donc p \ n.
De plus : p \ d et d est non nul et non premier donc : p < d.
Et d \ n avec n non nul donc d < n.

D'où : 1< p

Il existerait alors un nombre premier entre 2 et (n – 1) qui divise n.
Ce qui est contraire à l'hypothèse, donc n est premier.

Nous en sommes donc à la stratégie suivante :

Tester tous les nombres premiers de 2 à (n-1) inclus.

Avec comme méthode de discrimination :
♦ Si un de ces nombres divise n alors n n'est pas premier.
♦ Sinon n est premier.

Mais, tester tous les nombres premiers de 2 à (n-1) reste fastidieux.
Heureusement, un autre théorème va alléger nos efforts :

Théorème n°2 : Soit n ∈ ℕ avec **n > 2**

Si n n'est pas premier alors n admet au moins un diviseur premier p tel que : $p \leq \sqrt{n}$

Il nous suffit donc maintenant de tester les nombres premiers inférieurs ou égaux à $\sqrt{n}$
En effet :

* Si on trouve que l'un de ces nombres premiers divise n alors n n'est pas premier.

→ Si aucun de ces nombres ne divise n, n peut-il ne pas être premier ?
- Non car d'après le théorème n° 2, il admettrait alors au moins un diviseur premier inférieur ou égal à $\sqrt{n}$, ce qui est contraire à l'hypothèse.
Donc n est premier

D'où la version finale de la méthode de discrimination d'un nombre premier :

Tester dans l'ordre croissant les nombres premiers inférieurs ou égaux $\sqrt{n}$
Si l'un d'eux divise n alors n n'est pas premier.
Sinon, n est premier.

Cette méthode étant souvent énoncée comme un théorème :

Théorème n°3 (contraposée du théorème n° 2) :

Si n n'est divisible par aucun nombre premier inférieur ou égal à $\sqrt{n}$ alors n est premier.

Cependant, il demeure un problème de taille :
Pour appliquer cette méthode, nous avons besoin de la liste des nombres premiers inférieurs ou égaux à $\sqrt{n}$
Cette liste peut être obtenue entre autre grâce à la méthode du crible d'Eratosthène.

Quant à la liste complète des nombres premiers, c'est l'objet de notre quatrième théorème :

Théorème n°4 :

L'ensemble $\mathbb{P}$ des nombres premiers est infini.
En voici la démonstration par l'absurde :

Supposons que $\mathbb{P}$ est fini et donc égal à $p_1 ; p_2 ; ... ; p_n$
* Soit a le nombre défini par : $a = p_1 \times p_2 \times ... \times p_n + 1$
$a \neq 1$ donc a admet au moins un diviseur premier, appelons-le p_k

$p_k \backslash a$ et $p_k \backslash p_1 \times p_2 \times ... \times p_n$ donc $pk \backslash a - p_1 \times p_2 \times ... \times p_n$
d'où $p_k \backslash 1$ Or le seul diviseur entier naturel de 1 est 1 donc $p_k = 1$
Ce qui est impossible car 1 n'est pas un nombre premier.

Conclusion : l'ensemble des nombres premiers est infini.

6/ Application de la méthode de discrimination

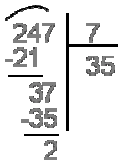
Si nous reprenons notre exemple : « 247 est-il premier ? » ,

Nous avons besoin de la liste des nombres premier inférieurs ou égaux à $\sqrt{247}$

Or : $\sqrt{247} \approx 15,7$ donc il nous faut la liste des nombres premiers inférieurs ou égaux à 15.
Qui est : 2, 3, 5, 7, 11, 13.

On utilise alors les critères de **divisibilité** :

247 ne se termine pas par 0, 2, 4, 6 ou 8 donc 2 ne le divise pas.
2+4+7=11 et 3 ne divise pas 11 donc 3 ne divise pas 247.
247 ne se termine pas par 0 ou 5 donc



247=35x7+2 et $0 \leq 2 < 7$

Donc 2 est le reste de la division euclidienne de 247 par 7.

2≠0 donc 7 ne divise pas 247.

5 ne le divise pas.

2 + 7= 9 ≠ 4 donc 11 ne divise pas 247

247 / 13 = 19 d'où 247 = 13 x 19 ; 13 divise 247
donc 247 n'est pas premier

7/ Décomposition d'un entier en produit de facteurs premiers

Nous avons vu que si n ≥ 2 alors il possède au moins un diviseur premier p_1

Il existe alors q_1 entier naturel non nul tel que : $n = p_1 \times q_1$
Et q_1 divisant n non nul, $q_1 < n$ car $p_1 \neq 1$
Si $q_1 \neq 1$ alors il possède à son tour au moins un diviseur premier p_2 (qui peut être égal à p_1).

Il existe alors q_2 entier naturel non nul tel que : $q_1 = p_2 \times q_2$
Et q_2 divisant q_1 non nul, $q_2 < q_1$ car $p_2 \neq 1$
On construit ainsi une suite (q_n) qui est strictement décroissante et minorée par 1.
Cette suite s'arrête donc « forcément » or elle ne peut s'arrêter que si l'un de ses termes vaut 1.

D'où : $n = p_1 \times q_1 = p_1 \times (p_2 \times q_2) = \ldots = p_1 \times p_2 \times p_3 \ldots \times (p_k \times 1)$

Et en écrivant les produits de nombres premiers égaux entre eux sous forme de puissance, on obtient donc le théorème suivant :

Théorème n° 5 :
Tout entier **n > 2** se décompose de façon unique sous la forme :

$$n = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \ldots \times p_m^{\alpha_m}$$

Où : $p_1, p_2, \ldots p_m$ sont des nombres premiers tels que : $p_1 < p_2 < \ldots < p_m$
et $\alpha_1, \alpha_2, \ldots, \alpha_m$ sont des entiers naturels non nuls.
L'écriture de n sous cette forme est appelée *décomposition de n en produit de facteurs premiers.*

Remarques :
1) Ce théorème peut être montré de façon rigoureuse à l'aide d'un raisonnement par récurrence.
2) L'ordre strict imposé sur les facteurs sert à garantir l'unicité de la décomposition.
3) Quel que soit i : $\alpha_i \neq 0$ donc quel que soit i : $p_i \setminus n$

De plus, il ne peut exister de nombre premier p différent des p_i qui divise n
car sinon la décomposition ne serait pas unique.

Conclusion : l'ensemble des diviseurs premiers de n est $p_1, p_2, \ldots p_m$

Exemple de décomposition : *technique et présentation.*
Décomposons n = 72.

Méthode :
Il faut appliquer à 72 la même méthode que si l'on cherchait à savoir s'il est premier.
C'est à dire qu'il faut tester si les nombres premiers inférieurs ou égaux à sa racine, le divisent.
* Si on lui trouve un diviseur, il faut alors continuer à appliquer cette méthode au quotient de 72 par ce diviseur. Et ainsi de suite, jusqu'à obtention d'un quotient égal à 1.

Présentation :

72	2
36	2
18	2
9	3
3	3
1	

2 divise 72 et 72/2 = 36.
Attention à bien repartir de 2 ! 2 divise 36 et 36/2 = 18

2 divise 18 et 18/2 = 9

2 ne divise pas 9
* Il ne sera donc plus nécessaire de tester 2 à l'avenir.
* Car par transitivité, si 2 ne divise pas un nombre,
* il ne peut pas non plus diviser ses diviseurs.

Passons au nombre premier suivant : 3 divise 9 et 9/3 = 3
3 divise 3 et 3/3 = 1.
Fin de la décomposition.

Conclusion : $72 \times 2^3 \times 3^2$

8/ Recherche des diviseurs d'un entier naturel

Soit n dont la décomposition en facteurs premiers est : $n = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \ldots \times p_m^{\alpha_m}$
Si a ≠ 1 et a divise n, montrons que sa décomposition ne peut contenir de nombre premier autre que les p_i

Démonstration :
Supposons qu'il existe p premier différent des p_i qui divise a.
p\a donc p\n
Et p fait alors partie de l'ensemble des diviseurs premiers de n.
Ce qui est impossible car l'ensemble des diviseurs premiers de n se limite aux p_i

La décomposition de tout diviseur de n ne peut donc contenir que des nombres premiers égaux aux p_i

De plus, β_i l'exposant de p_i dans la décomposition de a ne peut être strictement supérieur à α_i car par transitivité $p_i^{\beta_i}$ diviserait n, qui possèderait alors une décomposition en facteurs premiers dans laquelle l'exposant de p_i serait différent de α_i

Ce qui est impossible par unicité de la décomposition de n.

D'où le théorème suivant :

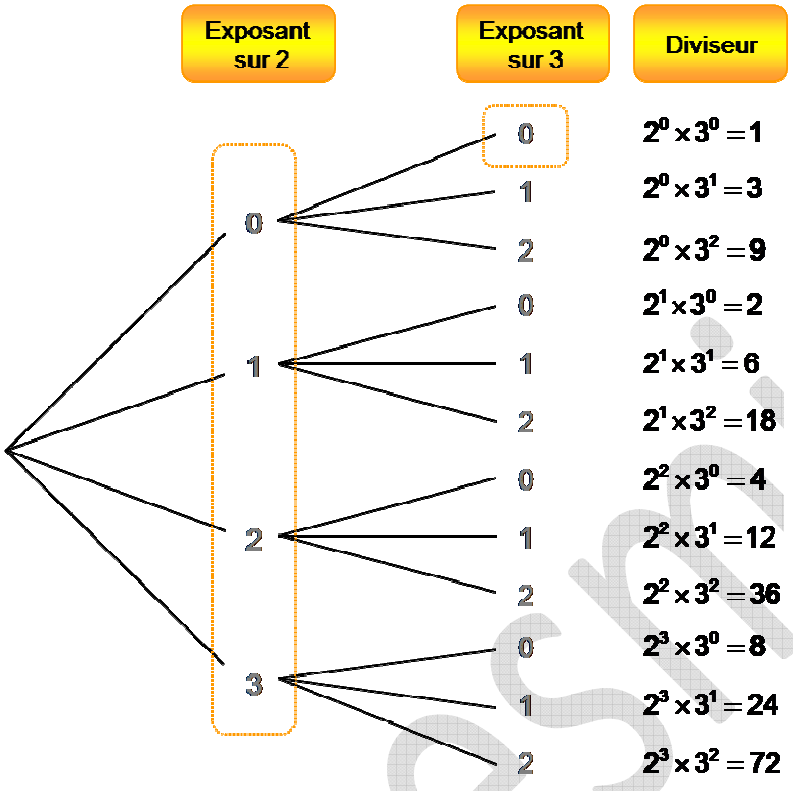
Si la décomposition en facteurs premiers de n est : $n = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \ldots \times p_m^{\alpha_m}$
Alors, tout diviseur a de n s'écrit : $a = p_1^{\beta_1} \times p_2^{\beta_2} \times \ldots \times p_m^{\beta_m}$
avec pour tout i compris entre 1 et m : $0 \leq \beta_i \leq \alpha_i$

Remarques :
1) si $\beta_{i=0}$ alors p_i n'est pas un diviseur premier de a.
2) si tous les β_i sont nuls alors a = 1 et si pour tout i : $\beta_{i=} \alpha_i$ alors **a = n**

3) par multiplication des choix possibles de puissances pour chaque diviseur premier, on obtient que :

Le nombre de diviseurs de n est : (α_1 +1) x (α_2 + 1) x ... x (α_m +1)

Exemple : reprenons 72. $72 = 2^3 \times 3^2$
Le plus simple et le plus clair au niveau présentation pour trouver tous les diviseurs de 72 est de faire un arbre de choix comme en probabilités.



3+1
=
4 choix
pour l'exposant de 2
multipliés par
2+1
=
3 choix
pour l'exposant de 3

Il y a donc
12 choix possibles

72 a donc 12 diviseurs
dont la liste est ci-contre.

Pgcd

Pgcd :
Le cours commence par la révision de la division euclidienne dans $\mathbb{N}$, puis étend la définition de cette division à $\mathbb{Z}$. La notion de PGCD de deux nombres entiers est abordée ainsi que les méthodes pour le calculer. Il finit avec le théorème de Gauss.

1/ Division euclidienne

Division euclidienne dans $\mathbb{N}$:

Soient $a \in \mathbb{N}$ et $b \in \mathbb{N}^*$
Il existe un unique couple (q , r) d'entiers *naturels* tels que :
$a = b \times q + r$ avec $0 \leq r < b$

q est le quotient, r le reste, b le diviseur et a le dividende.

Propriété :
« b divise a » si et seulement si « le reste de la division euclidienne de a par b est nul ».

Division euclidienne dans $\mathbb{Z}$:

Soient a $\in \mathbb{Z}$ et b $\in \mathbb{Z}^*$
Il existe un unique couple (q , r) d'entiers *realtifs* tels que :

$a = b \times q + r$ avec $0 \leq r < |b|$

Remarques :
1) si a et b sont des naturels, le couple obtenu dans les deux divisions est le même
2) dans tous les cas, r est un entier naturel

2/ PGCD

Soient a et b deux entiers naturels non nuls.
Notons *D*(a) l'ensemble des diviseurs de a et *D*(b) celui des diviseurs de b.

L'ensemble de leurs diviseurs communs est noté : *D*(a,b) , *D*(a,b) = *D*(a) $\cap$ *D*(b)
1 divise a et b donc *D*(a,b) n'est pas vide.

De plus, a et b admettant un nombre fini de diviseurs,leurs diviseurs communs sont en nombre fini.
D(a,b) étant un sous ensemble fini et non vide de $\mathbb{N}$, il admet donc un plus grand élément d.

Définition du ***PGCD*** *de deux entiers naturels non nuls :*

Si a et b sont deux entiers naturels non nuls,
alors ils possèdent un plus grand diviseur commun, d, aussi appelé **plus grand commun diviseur**
et donc noté :

d = pgcd (a,b) ou d = a $\wedge$ b

Remarques :
1) pgcd (a,b) = pgcd (b,a)
2) si a et b sont des entiers relatifs non nuls : pgcd (a,b) = pgcd ($|a|$,$|b|$)

3/ Recherche du PGCD : *diviseurs communs*

Chercher le pgcd de deux entiers c'est par définition, chercher le plus grand de leurs diviseurs communs.

D'où la première méthode de recherche du pgcd :

Méthode n° 1 :

- trouver l'ensemble des diviseurs de chaque nombre.
- lister les diviseurs communs dans l'ordre croissant et prendre le plus grand.

Remarque :
il existe plusieurs façons de trouver les diviseurs d'un nombre.

Exemple : recherchons le pgcd de 150 et 120.
Utilisons la technique vue au collège, qui consiste à écrire le nombre comme le produit de deux facteurs.

150	1
75	2
50	3
30	5
25	6
15	10

120	1
60	2
40	3
30	4
24	5
20	6
15	8
12	10

Les diviseurs communs à 150 et 120 sont donc :
1, 2, 3, 5, 6, 10, 15, 30.
D'où : pgcd (120 , 150) = 30

3/ Recherche du PGCD : *décomposition en facteurs premiers*

Une autre façon de trouver l'ensemble des diviseurs d'un nombre est d'utiliser sa décomposition en produit de facteurs premiers.

Rappels :

Si la décomposition en facteurs premiers de a est : $n = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \ldots \times p_m^{\alpha_m}$

Alors, tout diviseur d de a s'écrit : $d = p_1^{\gamma_1} \times p_2^{\gamma_2} \times \ldots \times p_m^{\gamma_m}$

avec pour tout i compris entre 1 et m : $0 < \gamma_i < \alpha_i$

Mais si l'on possède les décompositions de a et de b, il est alors inutile de rechercher l'ensemble des diviseurs communs pour n'en garder que le plus grand.

En effet, si on appelle p_1, p_2, ... , p_n les facteurs premiers figurant soit dans la décomposition de a soit dans celle de b alors a et b s'écrivent :

$$a = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \ldots \times p_n^{\alpha_n} \qquad b = p_1^{\beta_1} \times p_2^{\beta_2} \times \ldots \times p_n^{\beta_n}$$

Avec pour tout i compris entre 1 et n : $\alpha_i \geq 0$ et $\beta_i \geq 0$
Alors, si d\a et d\b la décomposition de d ne peut comporter que des p_i

d'où si d diviseur commun à a et b : $d = p_1^{\gamma_1} \times p_2^{\gamma_2} \times \ldots \times p_m^{\gamma_m}$

Avec pour tout i compris entre 1 et n : $0 \leq \gamma_i \leq \min(\alpha_i ; \beta_i)$
Remarque :

si p_i n'apparaît pas dans une des décompositions alors $\min(\alpha_i ; \beta_i)$

D'où : $\gamma_i = 0$, et ce facteur n'apparaît alors pas dans la décomposition de d.

Le plus grand diviseur étant celui qui a les puissances les plus grandes :

$$pgcd\ (a,b) = p_1^{\gamma_1} \times p_2^{\gamma_2} \times \ldots \times p_n^{\gamma_n}$$

Avec pour tout i compris entre 1 et n : $\gamma_i = \min(\alpha_i ; \beta_i)$

D'où :
Méthode n° 2 :
- décomposer chaque nombre en produit de facteurs premiers.
- affecter aux facteurs premiers communs l'exposant le plus petit.

Application : reprenons l'exemple de a = 150 et b = 120.

150	2
75	3
25	5
5	5
1	

$150 = 2^1 \times 3^1 \times 5^2$

120	2
60	2
30	2
15	3
5	5
1	

$120 = 2^3 \times 3^1 \times 5^1$

D'où pgcd (120 , 150) = $2^1 \times 3^1 \times 5^1 = 30$

3/ Recherche du PGCD : *algorithme d'Euclide*

Il existe enfin une troisième méthode qui consiste à réaliser une suite de divisions euclidiennes jusqu'à obtention d'un reste nul.

Montrons tout d'abord deux résultats intermédiaires
Soient a et b deux entiers naturels non nuls.

① Si a = b x q + r avec q et r entiers naturels non nuls alors **pgcd** (a,b) = **pgcd** (b,r)

Si d\a et d\b alors d\a-b x q donc d\r d'où : $D(a,b) \subset D(b,r)$

Si d\r et d\b alors d\b x q + r donc d \ a d'où : $D(b,r) \subset D(a,b)$

$\Big\} \; D(b,r) = D(a,b)$

Ayant les mêmes diviseurs communs, les deux couples ont donc le même plus grand diviseur commun.

Plus généralement, si l'on travaille avec des entiers relatifs :
$pgcd\,(a,b) = |b|$

② si b \ a alors **pgcd** (a,b) = b

Si d est un diviseur commun à a et b alors d divise b. Or b non nul, d'où d ≤ b
De plus, b est un diviseur commun à a et b.
b est donc le plus grand diviseur commun à a et b.

La division euclidienne de a par b s'écrit : $a = b \times q_1 + r_1$ avec $0 \leq r_1 < b$

Soit $r_1 = 0$ auquel cas b \ a et alors **pgcd** (a,b) = b

soit $r_1 \neq 0$ On a alors : **pgcd** (a,b) = **pgcd** (b,r_1)
et la division euclidienne de b par $\mathbf{r_1}$ s'écrit : $b = r_1 \times q_2 + r_2$ avec $0 \leq r_2 < r_1$

Soit $r_2 = 0$ auquel cas r_1 \b et alors **pgcd** (b,r_1) = r_1 d'où **pgcd** (a,b) = r_1

Soit $r_2 \neq 0$ On a alors : **pgcd** (b,r_1) = **pgcd** (r_1, r_2)
et la division euclidienne de r_1 par r_2 s'écrit : $r_1 = r_2 \times q_3 + r_3$ avec $0 \leq r_3 < r_2$

On construit ainsi une suite (r_n) d'entiers naturels.
Avec pour tout n : $r_{n+1} + r_n$, donc cette suite est strictement décroissante.
Or une suite strictement décroissante d'entiers naturels est obligatoirement finie.

Par conséquent, la suite s'arrête à un rang p, rang pour lequel on a donc : $r_p = 0$
D'où rp-1 \ rp-2 et donc pgdc $(r_{p-2}, r_{p-1}) = r_{p-1}$

Par cette suite de divisions euclidiennes on obtient donc le pgcd qui est le dernier reste non nul.
Cette procédure de recherche du pgcd est appelée algorithme d'Euclide.

D'où :

Théorème de l'algorithme d'Euclide : Soient a et b deux entiers naturels non nuls.

Si b divise a alors **pgcd** (a,b) = b
Sinon **pgcd** (a,b) est le dernier reste non nul
dans les divisons euclidiennes successives du diviseur par le reste.

D'où :

Méthode n° 3 :

- effectuer les divisions successives de l'algorithme d'Euclide.
- le dernier reste non nul est le pgcd de a et de b.

Remarques :
1) Que l'on divise a par b ou b par a n'a aucune importance.
En effet, si a < b alors a = b x 0 + a est la division euclidienne de a par b car 0 ≤ a < b
Et donc dans l'algorithme d'Euclide la division suivante est : b divisé par a.
Autant donc toujours diviser dès le départ le plus grand nombre par le plus petit, étant donné de plus que :**pgcd** (a,b) = **pgcd** (b,a)

2) Si une des divisions a un reste égal à 1 alors **pgcd** (a,b) = 1 car le reste suivant strictement inférieur à 1 ne peut être que nul.

Application : reprenons l'exemple de a = 150 et b = 120.

150 = 120 x 1 + 30
120 = 30 x 4 + 0
Donc : **pgcd (150 , 120) = 30**

4/ Nombres premiers entre eux

Définition : *Soient a et b deux entiers relatifs non nuls.*

a et b sont dits premiers entre eux si **pgcd (a,b) = 1**
Remarques :
1) deux nombres premiers entre eux ont donc 1 pour seul diviseur commun.
2) si a est un nombre premier et que a ne divise pas b alors a et b sont premiers entre eux.

Théorème de Bézout :
a et b sont premiers entre eux
si et seulement si
il existe u et v entiers relatifs tels que : $a \times u + b \times v = 1$
Remarques :
1) Le couple (u,v) n'est pas unique.

2) Ce couple peut être trouvé en « remontant » les divisons de l'algorithme d'Euclide.
Cette technique sera vue dans le module sur les équations diophantiennes.

3) Selon les livres, les professeurs et les moments de la scolarité, le théorème de Bézout peut comporter un contenu différent. La version qui en est donnée ici suffit pour la terminale.

Démonstration du théorème de Bézout :

Sens direct : supposons a et b premiers entre eux.
E l'ensemble des nombres *naturels non nuls* s'écrivant $a \times u + b \times v$ avec u et v entiers relatifs n'est pas vide donc il admet un plus petit élément n. $n = a \times u' + b \times v'$
La division euclidienne de a par n s'écrit : $a = b \times q + r$ avec : $0 \leq r < n$
Donc : $a = (a \times u' + b \times v') \times q + r$ d'où $r = a(1 - u' \times q) + b(-v' \times q)$

r est donc un entier naturel de la forme $a \times u + b \times v$

Or $r < n$ donc si r est n'est pas nul, E possède un élément plus petit que n ce qui est absurde.
Par conséquent r = 0 et n divise donc a.

De même on peut démontrer que n divise b.

n est donc un diviseur commun à a et b, or 1 étant le seul : n = 1

Et donc 1 peut s'écrire : $1 = a \times u' + b \times v'$
avec u' et v' entiers relatifs.

Sens réciproque : supposons que 1 s'écrive : $1 = a \times u + b \times v$
* Si d entier naturel, diviseur commun à a et b,
d divise alors toute combinaison linéaire de a et de b
donc : $d \backslash a \times u + b \times v$
D'où $d \backslash 1$ or le seul diviseur entier naturel de 1 est 1
donc d = 1.
a et b possèdent donc un seul diviseur commun qui est 1, ils sont premiers entre eux.

Soient a et b deux entiers relatifs non nuls.

Propriété n° 1
Quel que soit k, entier naturel non nul : si pgcd (a,b) = 1 alors pgcd (ka,kb) = k

si k est un relatif non nul : $(ka,kb) = |k|$

Démonstration :
k divise ka et kb donc k est un diviseur commun à ka et kb.

D'après le théorème de Bézout : il existe u et v entiers relatifs tels que : $a \times u + b \times v = 1$

Donc : $ka \times u + kb \times v = k$
Si d est un entier naturel diviseur commun à ka et kb, d divise donc k.
d divise k avec k non nul donc $d \leq k$

k est donc le plus grand diviseur commun à ka et kb.

Propriété n° 2
pgcd (a,b) = d
⇔
il existe a' et b' entiers relatifs tels que : a = da' et b = db' avec pgcd (a',b') = 1

Démonstration :
Sens direct : soit d = pgcd (a,b)
$d \backslash a$ donc il existe a' entier relatif tel que : a = da'
De même, b peut s'écrire b = db'

Soit d diviseur commun à a' et b'
Alors : a' = d'a'' et b' = d'b''

Donc a = (dd')a'' et b = (dd')b''et dd' est donc un diviseur commun à a et b.
Si d' > 1 alors dd' > d ce qui est absurde car d est le plus grand diviseur commun à a et b.

Donc *d'* ≤ 1 d'où d' = 1
Le seul diviseur commun à a' et b' est 1 donc ils sont premiers entre eux.

Sens réciproque :
pgcd (a,b) = pgcd (da',db') = d
D'après la propriété n°1.

Remarques :
1) Cette propriété est très utile pour ramener la résolution de problèmes au cas plus simple de nombres premiers entre eux.

2) Elle peut également être utilisée pour trouver le PGCD de deux nombres écrits sous la forme d'un produit de deux facteurs.

Exemple : 55 = 5 x 11 et 65 = 5 x 13.
11 et 13 sont premiers entre eux donc d'après la réciproque le PGCD de 55 et 65 est 5.

Propriété n° 1 (étendue)
Quel que soit k, entier naturel non nul : pgcd (ka,kb) = kpgcd (a,b)

si k est un relatif non nul : pgcd (ka,kb) = |k|pgcd (a,b)

Cette propriété est particulièrement utile pour simplifier la recherche du pgcd de deux grands nombres ayant un diviseur commun évident.

Démonstration :
D'après la propriété n°2 :
* Si d = pgcd (a,b) alors a et b peuvent s'écrire : a = da' et b = db' avec **pgcd** (a',b') = 1

D'où : pgcd (ka,kb) = pgcd ((kd)a' , (kd)b') = kd d'après la propriété n°1.

Par conséquent : pgcd (ka , kb) = kpgcd (a,b)

Propriété n° 3 : (extension du sens direct du Théorème de Bézout)

Si pgcd (a,b) = d alors il existe u et v entiers relatifs tels que : $a \times u + b \times v = d$

Démonstration :
D'après la propriété n° 2 :
d = pgcd (a,b) donc a et b peuvent s'écrire : a = da' et b = db' avec pgcd (a',b') = 1

D'où d'après le théorème de Bézout : il existe u et v entiers relatifs tels que : $a' \times u + b' \times v = 1$
donc $da' \times u + db' \times v = d$ Par conséquent d s'écrit : $d = a \times u + b \times v$
Peut-on étendre la réciproque du Théorème de Bézout ?
Soit d entier relatif non nul et différent de 1 tel que : $a \times u + b \times v = d$, d est-il le pgcd de a et de b ?

Prenons par exemple : a = 6 et a = 4. pgcd (4, 6) = 2

On peut écrire : 6 x 2 + 4 x (-2) = 4 alors que 4 n'est pas le pgcd de 4 et 6.
La réciproque est donc fausse, mais…

Propriété n° 4 :
Si d entier non nul peut s'écrire $d = a \times u + b \times v$ avec u et v entiers relatifs alors :pgcd (a,b) divise d.

La démonstration en est évidente.
La contraposée sera utile pour la résolution des équations diophantiennes, à savoir :
« si pgcd (a,b) ne divise pas d alors d ne peut s'écrire sous la forme : $d = a \times u + b \times v$ »
Nous y reviendrons dans le module concerné.

Propriété n° 5 :
Tout diviseur commun à a et b divise le pgcd de a et b.
Démonstration :
D'après Bézout direct étendu , il existe u et v entiers relatifs tels que : pgcd (a,b) = $a \times u + b \times v$

Or, si d est un diviseur commun à a et b, il divise toute combinaison linéaire de a et de b.

Donc d divise pgcd (a,b)
Et comme réciproquement, tout diviseur de d divise a et b, on en déduit donc que :
Les diviseurs communs à a et b sont les diviseurs du pgcd de a et b.

Théorème de Gauss **:** soient a, b et c trois entiers relatifs non nuls.
Si a divise bc et a et b premiers entre eux alors a divise c.
Intuitivement ce théorème se comprend assez facilement :
Si a divise bc c'est qu'il peut être vu comme le produit de deux facteurs : l'un divisant b et l'autre divisant c.

Le premier facteur étant donc *un diviseur commun à a et b* et le second, *un facteur commun à a et c.*

Si a et b sont premiers entre eux, leur seul facteur commun est 1 et donc le second facteur vaut a.
a divise alors c.

Démonstration rigoureuse :

pgcd (ac , bc) = |c| pgcd (a,b) = |c|

Or a \ bc et a \ ac donc a est un diviseur commun à ac et bc.

Il divise donc leur pgcd qui est |c|

D'où : a \ c.

Remarque :
ce théorème sera en particulier très utile pour résoudre les équations diophantiennes.

Congruences
(4ème maths)

Congruences :
Dans ce module, étude de la notion de congruence.
La congruence modulo n de deux entiers relatifs est tout d'abord définie, ensuite la notion de classe et de représentant d'une classe, modulo n. Le cours de termine

par le petit théorème de Fermat et son corollaire.

1/ Division euclidienne

Division euclidienne dans $\mathbb{N}$:

Soient a $\in \mathbb{N}$ et b $\in \mathbb{N}^*$
Il existe un unique couple (q , r) d'entiers *naturels* tels que :
$a = b \times q + r$ avec $0 \leq r < b$

q est le quotient, *r* le reste, *b* le diviseur et *a* le dividende.

Propriété :

« b divise a » si et seulement si « le reste de la division euclidienne de a par b est nul ».

Division euclidienne dans $\mathbb{Z}$ **:**

Soient a $\in \mathbb{Z}$ et b $\in \mathbb{Z}^*$
Il existe un unique couple (q , r) d'entiers *realtifs* tels que :
$a = b \times q + r$ avec $0 \leq r < |b|$

Remarques :
1) si a et b sont des naturels, le couple obtenu dans les deux divisions est le même
2) dans tous les cas, r est un entier naturel

2/ Congruence : *définition*

Définition :
soient a et b deux entiers relatifs et n entier naturel, $n \geq 2$

On dit que « a est congru à b modulo n » ou que « a et b sont congrus modulo n » si :
a et b ont le même reste dans la division euclidienne par n.

On note $a \equiv b\ [n]$ ou $a \equiv b\ (n)$

Remarques :
1) On dit aussi que a et b sont égaux modulo n.

2) La **congruence modulo** 1 ne présente aucun intérêt car dans la division e0uclidienne par 1, tout nombre a pour reste 0. Et donc deux nombres quelconques sont égaux modulo 1.

3) Cette notion de **congruence** a déjà été rencontrée en trigonométrie, où l'on parle d'angles égaux modulo 2π

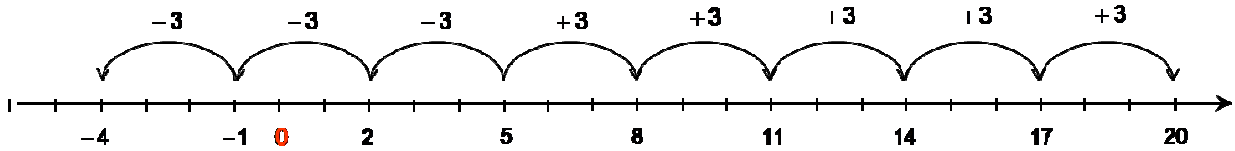
De part sa définition, la relation de **congruence** présente trois propriétés évidentes :

a $\equiv$ a[n] (*réflexivité*)
Si a $\equiv$ b[n] alors b $\equiv$ a[n] (*symétrie*)
Si a $\equiv$ b[n] et b $\equiv$ c[n] (*transivité*)

Toute relation ayant ces 3 propriétés est qualifiée de relation d'équivalence.

Exemple :
5 et 14 sont-ils congrus modulo 3 ?

Leurs divisions euclidiennes par 3 sont : $5 = 3 \times 1 + 2$ $14 = 3 \times 4 + 2$
5 et 14 ont le même reste dans la division euclidienne par 3 donc : $5 \equiv 14\ [3]$



Si on ajoute 3 à 5 alors la division euclidienne devient :

$$5 + 3 = 3 \times 1 + 2 + 3$$
$$8 = 3 \times (1+1) + 2$$

Le reste de la division est inchangé donc $8 \equiv 5[3]$
Et l'on peut faire pareil avec le nombre trouvé.

Le résultat est également le même si au lieu d'ajouter 3, on enlève 3.
Comme tous ces nombres sont congrus à 5 modulo 3, par tansitivité,
ils sont congrus deux à deux modulo 3.

On peut remarquer que la différence entre deux de ces nombres est un multiple de 3.

Etendons cette remarque au cas général :

3/ Congruence : *équivalence*

Propriété :
soient a et b deux entiers relatifs et n entier naturel, $n \geq 2$

$a \equiv b\ [n] \Leftrightarrow$ n divise (a-b)

Démonstration :
Sens direct :
Soient a et b congrus modulo n.
Il existe q et r entiers relatifs tels que : $a = n \times q + r$ avec $0 \leq r < n$
b ayant le même reste, il existe q' entier relatif tel que : $b = n \times q' + r$

D'où $a - b = n \times q - nq' = n \times (q - q')$
Donc n divise (a-b)
Sens réciproque :
Supposons que n divise (a-b). Alors il existe k entier relatif tel que : a-b = nk.

Soit r le reste dans la division euclidienne de a par n :
$a = n \times q + r$ avec $0 \leq r < n$

Alors : b = a - nk = n x (q - k) + r
Avec $0 \leq r < n$ et q-k entier relatif
donc r est le reste dans la division euclidienne de b par n.

a et b ont le même reste donc : $a \equiv b[n]$

Remarque :
Pour montrer que deux nombres sont congrus modulo n, il suffira donc de montrer que leur différence est un multiple de n.

Conséquences :

$a \equiv 0[n] \Leftrightarrow$ n divise a

Remarque :
en particulier, n divise n et n divise 0 donc : $n \equiv 0[n]$ et $0 \equiv 0[n]$

$$a \equiv b[n] \Leftrightarrow \text{n divise } (a-b) \Leftrightarrow a - b \equiv 0[n]$$

Quel que soit d entier naturel supérieur ou égal à 2 :

Si $a \equiv b[n]$ et d divise n alors $a \equiv b[d]$

Démonstration :

donc n divise (a-b) Or par transitivité : si d divise n alors d divise (a-b).
Par conséquent : $a \equiv b[d]$

4/ Congruence : *restes et classes*

En trigonométrie où il est question d'angles égaux modulo 2π, on parle de mesure principale, comprise par exemple entre 0 et 2π exclu.
Cette idée de choisir un représentant pour un ensemble de nombres égaux modulo 2π est transposable au cas modulo n.

Propriété :
soient a entier relatif et n entier naturel, $n \geq 2$

Si r est le reste dans la division euclidienne de a par n alors $a \equiv r[n]$

Démonstration :
En effet, si r est le reste dans la division euclidienne de a par n alors
il existe q entier relatif tel que : $a = n \times q + r$ avec $0 \leq r < n$
Donc n divise (a-r) et par conséquent a est congru à r modulo n.

Propriété réciproque :
soient a entier relatif et n entier naturel, .
Si $a \equiv r[n]$ et $0 \leq r < n$ alors r est le reste dans la division euclidienne de a par n.
Démonstration :
Si a et r sont congrus modulo n alors n divise (a-r) et il existe donc k entier relatif tel que : $a - r = n \times k$
D'où $a = n \times k + r$
Or $0 \leq r < n$
Donc il s'agit de la division euclidienne de a par n et r en est le reste.

Si $a \equiv r[n]$ et $0 \leq r < n$ alors r est le reste dans la division euclidienne de a par n.
Donc par unicité de la division euclidienne, chaque entier *a* ne peut être congru qu'à un seul entier compris entre 0 et n exclu.

Cet entier étant le reste dans la division euclidienne de *a* par *n*.

Chacun des restes possibles dans la division euclidienne par *n* peut donc être considéré comme le représentant d'un ensemble de nombres qui lui sont congrus modulo *n*.
Les restes possibles étant : 0, 1, …, n-1 ; $\mathbb{Z}$ peut donc être découpé en n classes, modulo n.
Ces classes forment une partition de $\mathbb{Z}$.
C'est à dire que leur union est égale à $\mathbb{Z}$, et que leurs intersections, deux à deux, sont vides.
Exemple :
Considérons l'ensemble $\mathbb{Z}$ modulo 2.
Les restes possibles dans la division euclidienne par 2 sont 0 et 1.
Donc quel que soit a entier relatif :

* Soit $a \equiv 0[2]$, ce qui est équivalent à 2 divise a (a pair)

* Soit $a \equiv 1[2]$, ce qui est équivalent à 2 ne divise pas a. (a impair)

Le terme de « classe » n'est pas explicitement au programme de la terminale mais voir les choses de cette façon permet d'avoir une vision plus claire de la **congruence**.

Forts de ce découpage en classes, on pourra ramener la résolution de certains exercices à une simple étude de n cas,
correspondants aux différents restes possibles dans la division euclidienne par n.

5/ Congruence et opérations

Les démonstrations des propriétés qui suivent peuvent faire l'objet d'un R.O.C.
Soient a, b, a' et b' quatre entiers relatifs et n entier naturel, **n ≥ 2**

1. Si $a \equiv b\ [n]$ et $a' \equiv b'\ [n]$ alors : $a + a' \equiv b + b'\ [n]$.

*La **congruence** est compatible avec l'addition.*

Conséquence :

2. Quel que soit $c \in \mathbb{Z}$: si $a \equiv b\ [n]$ alors : $a + c \equiv b + c\ [n]$.

Conséquences :

3. Si $a \equiv b\ [n]$ et $a' \equiv b'\ [n]$ alors : $a \times a' \equiv b \times b'\ [n]$.

*La **congruence** est compatible avec la multiplication.*

Conséquences :

4. Quel que soit k entier naturel non nul : si $a \equiv b\ [n]$ alors : $a^k \equiv b^k\ [n]$.

5. Quel que soit $c \in \mathbb{Z}$: si $a \equiv b\ [n]$ alors : $a \times c \equiv b \times c\ [n]$.

   En particulier : si $a \equiv b\ [n]$ alors : $(-a) \equiv (-b)\ [n]$.

Conséquence de 1 et 4 :

6. Si $a \equiv b\ [n]$ et $a' \equiv b'\ [n]$ alors : $a - a' \equiv b - b'\ [n]$.

Les démonstrations des propriétés 1 et 3 s'appuient sur l'équivalence a $\equiv$ b[n] ⇔ n divise (a-b).

*La propriété 4 peut être montrée par récurrence et les déductions 2 et 5 utilisent le fait que : **c $\equiv$ c[n]***

Grâce à ces propriétés nous allons pouvoir manipuler la congruence de façon assez intuitive mais attention :

La congruence n'est pas compatible avec la division !

~~Si $a \equiv b\ [n]$ et $a' \equiv b'\ [n]$ alors : $\frac{a}{a'} \equiv \frac{b}{b'}\ [n]$.~~

En particulier parce que la **congruence** est une notion qui s'applique à des nombres relatifs et que le rapport de deux relatifs n'est pas toujours un relatif.

Et même si les rapports sont des entiers, il faudra se méfier des simplifications abusives en particulier lors de la résolution d'équations modulo n.

$$ka \equiv kb\ [n] \Rightarrow a \equiv b\ [n]$$

En effet, par exemple :

45 et 63, multiples de 3 sont congrus à 0 modulo 3 donc : $63 \equiv 45[3]$.

En simplifiant par 9, on obtiendrait :7 $\equiv$ 5[3]

Or : 7-5 = 2 qui n'est pas un multiple de 3 et donc : 7 $\not\equiv$ 5[3]

Exemples de manipulations de la congruence :

Exercice n° 1 :

Montrer que le produit de deux nombres impairs est un nombre impair.

Soit n et m deux nombres impairs.

n impair ⇔ n $\equiv$ 1[2] et m impair ⇔ m $\equiv$ 1[2]

Comme la **congruence** est compatible avec la multiplication : $n \times m \equiv 1 \times 1[2]$

$n \times m \equiv 1[2]$ donc nxm est impair.

Conclusion : le produit de nombres impairs est un nombre impair.

Exercice n° 2 : Déterminer le reste dans la division euclidienne de :

a) 54^{16} par 3
b) 21^{17} par 4
c) 23^2 par 4
d) $(-39)^3$ par 7
e) 120^{13}par 11

L'idée est ici de trouver un représentant plus simple du nombre puis d'appliquer la puissance. Dans la plupart des cas, on pourra se contenter de prendre comme représentant le reste dans la division euclidienne.

a) 54^{16} par 3

Ce cas est extrêmement simple : 5+4 = 9 donc 3 divise 54.

D'où 54 $\equiv$ 0[3]

Et comme la **congruence** est compatible avec la puissance : $54^{16} \equiv 0^{16}[3]$

D'où : $54^{16} \equiv 0^{16}[3]$, le reste dans la division euclidienne de $54^{16} \equiv$ par 3 est donc 0.

b) 21^{17} par 4

21 = 4 x 5 + 1 Donc : 21 $\equiv$ 1[4]

D'où : $27^{17} \equiv 1^{17}[4]$

D'où : $27^{17} \equiv 1^{17}[4]$, le reste dans la division euclidienne de 27^{17} par 4 est donc 1.

c) 23^2 par 4

23 = 4 x 5 + 3

Donc 23 $\equiv$ 3[4]

D'où : $23^2 \equiv 3^2[4]$

Soit : $23^2 \equiv 9[4]$

Or : $9 \equiv 4 \times 2 + 1$

Donc : $9 \equiv 1[4]$

$23^2 \equiv 1[4]$Le reste dans la division euclidienne de 23^2 par 4 est donc 1.

d) $(-39)^3$ par 7

La division euclidienne est plus difficile à manipuler dans $\mathbb{Z}$ que dans $\mathbb{N}$.
Cherchons donc plutôt un multiple de 7 proche de (-39).

-39 = -42 + 3

-42 est un multiple de 7 donc : $-39 \equiv 3[7]$

Remarque :
une façon simple de travailler, par exemple modulo 7, est de se dire que :
• tout multiple de 7 compte pour 0,
• de la même façon que nous éliminons tout multiple de 2π dans la recherche de la mesure principale d'un angle.

D'où : $(-39)^3 \equiv 27[7]$
Or : $27 = 3 \times 7 + 6$

Donc : $(-39)^3 \equiv 6[7]$
Le reste dans la division euclidienne de $(-39)^3$ par 7 est donc 6.
e) 120^{13} par 11
120 = 11 x 10 + 10

Donc : $120 \equiv 10[11]$
Mais mettre 10 à la puissance 13 ne va pas faciliter la résolution du problème.
Il est donc ici plus judicieux d'utiliser un autre représentant de la classe :

en enlevant 11 à 10, on obtient que : $10 \equiv -1[11]$

D'où : $120^{13} \equiv (-1)^{13}[11]$

Soit $120^{13} \equiv -1[11]$

Le reste dans la division euclidienne de 120^{13} par 11 est donc 10.

6/ Petit théorème de Fermat

Petit théorème de Fermat :

Soient p un *nombre premier* et a un entier naturel *non nul.*

Si *pgcd (a ; p) = 1* alors $a^{p-1} \equiv 1[p]$

Remarques :
1) La démonstration de ce théorème, assez technique, est ici admise.

2) Ce théorème, quand il est nécessaire à la résolution d'un exercice de BAC, est souvent rappelé dans l'énoncé.
Mais pas systématiquement donc …

3) Rappel : si p est premier alors « a est premier avec p » si et seulement si « p ne divise pas a ».

Corollaire du petit théorème de Fermat :

Soient p un *nombre premier*,

quel que soit a entier naturel : $ap \equiv a[p]$

Démonstration :
* *Si a est un entier naturel non nul et si p ne divise pas a* alors a et p sont premiers entre eux et d'après le petit théorème de Fermat :

$a^{p-1} \equiv 1[p]$ D'où : $a \times a^{p-1} \equiv a \times 1[p]$ Et donc : $a^p \equiv a[p]$

* *Si a est un entier naturel non nul et si p divise a* alors : $a \equiv 0[p]$

Donc : $a^p \equiv 0[p]$ D'où $a^p \equiv a[p]$

* *Si a vaut 0* , $0 \equiv 0[p]$ donc $a \equiv 0[p]$
On retombe alors sur le cas précédent.

Quel que soit a, on a donc bien : $a^p \equiv a[p]$

Exemple d 'utilisation :
Montrer que 3 divise *n3 - n* quel que soit n entier naturel.
3 est un nombre premier donc d'après le corollaire du petit théorème de Fermat :

quel que soit n entier naturel : $n^3 \equiv n[3]$

D'où : $n^3 - n \equiv 0[3]$
Par conséquent : 3 divise *n3 - n* , pour tout n entier naturel.

Avis au lecteur.
La notion de congruence est en général traitée à la fin du chapitre d'arithmétique.
C'est pourquoi il n'est pas rare que les exercices sur la congruence fassent intervenir la résolution d'équations diophantiennes.
Cependant certains professeurs traitent la congruence avant les équations diophantiennes, c'est pourquoi par souci d'équité, les exercices dans votre espace membre n'abordent pas cette notion.

Equations diophantiennes

(4ème annee maths système Tunisien)

Equations diophantiennes :

Dans ce module, étude des équations diophantiennes. Après un bref rappel des résultats d'arithmétique utiles à la résolution de telles équations, la notion d'équation diophantienne est définie.

1/ Résultats utiles

Dans les démonstrations à venir, nous aurons besoin de certains résultats vus et démontrés dans le module sur le PGCD.

rappel : Soient a et b deux entiers relatifs non nuls.
a et b sont dits premiers entre eux si *pgcd (a,b) = 1*

Théorème de Bézout : soient a et b deux entiers relatifs non nuls.
a et b sont premiers entre eux
si et seulement si
il existe u et v entiers relatifs tels que : $a \times u + b \times v = 1$

De ce théorème découlent les résultats suivants :

Propriété n° 1

pgcd (a,b) = d
⇔
il existe a' et b' entiers relatifs tels que : a = da' et b = db' avec *pgcd (a',b') = 1*

Théorème de Gauss : soient a, b et c trois entiers relatifs non nuls.
Si a divise bc et a et b premiers entre eux alors a divise c.

Il est à noter que le théorème de Gauss peut être déduit de celui de Bézout et que cette démonstration est un des R.O.C les plus fréquents au BAC.

2/ Equations diophantiennes : *définition*

Définition :

Toute équation (E) du type : *ax +by = c*
où a, b et c sont trois entiers relatifs et où les inconnues x et y sont des relatifs
est appelée ***équation diophantienne***.

Remarque :
dans la suite du cours, nous aurons besoin de parler du PGCD de a et de b, donc seul le cas où a et b sont non nuls sera étudié dans ce module.

2/ Equations diophantiennes : *le cas c = 0*

Si c = 0 alors x et y solutions de (E) ⇔ *ax + by = 0* ⇔ *ax = b(-y)*

Donc si x et y sont solutions de (E) alors a divise b(-y)

Attention,
ce n'est qu'une implication,
nous avons perdu l'équivalence.
Il faudra donc faire l'étude d'une réciproque par la suite.

Sous cas n° 1 : a et b sont premiers entre eux.
a divise b(-y) et a est premier avec b donc d'après le théorème de Gauss :
a divise (–y) et par conséquent, il existe k entier relatif tel que : -y = ka.

d'où ax = b (-y) ⇔ ax = bka
⇔ = kb car a est nul

Si x et y solutions de (E), il existe alors k entier relatif tel que : $\begin{cases} x = kb \\ y = -ka \end{cases}$

Réciproque :
Soient x et y s'écrivant x = kb et y = -ka.

alors : ax = akb et b(-y) = bka.
donc ***ax = -by***
d'où ***ax + by = 0***

x et y sont solutions de (E)
Conclusion : les couples solutions de (E) sont les couples (kb, -ka) avec k entier relatif.

Sous cas n° 2 : a et b ne sont pas premiers entre eux.
Soit ***d = pgdc (a,b)***

Il existe a' et b' premiers entre eux tels que : a = da' et b = db'

Et alors : ax = b (-y) ⇔ da' x = db' (-y)
⇔ a'x = b'(-y) car d non nul
On retombe alors sur le sous cas n°1

Et donc : les couples solutions de (E) sont les couples (kb', -ka') avec k entier relatif.
Il est à retenir de l'étude de ce cas c = 0 :
- la technique pour se ramener au sous cas n°1.
- la technique d'utilisation du théorème de Gauss.
- la nécessité de montrer la réciproque pour pouvoir conclure sur l'ensemble des solutions.
- l'existence d'une infinité de solutions

2/ Equations diophantiennes : *existence de solutions*

La suite du cours va être gérée comme l'étude générale d'une équation diophantienne.

A savoir : l'équation a-t-elle des solutions ? Si oui, combien et comment les trouver ?

Étape n° 1 : A quelle condition (E) admet-elle au moins une solution ?
Si (E) admet au moins une solution alors il existe u et v entiers relatifs tels que : ***au + bv = c***

Soit ***d = pgcd (a,b)***
d divise a et b donc d divise tout combinaison linéaire de a et de b.
Par conséquent d divise c.

Une condition nécessaire à l'existence d'au moins une solution est donc :
que le PGCD de a et de b divise c.
Cette condition est-elle suffisante ?

Supposons que d divise c.

Il existe alors k entier relatif tel que c = kd
d = pgcd (a,b) donc il existe a' et b' premiers entre eux tels que : a = da' et b = db'.

Et d'après le sens direct du théorème de Bézout, alors il existe u et v tels que : *a'u' + b'v' = 1*
d'où : *kda'u' + kdb'v' = kd* Soit : *aku' + bkv' = c*

En posant : *u = ku'* et *v = kv'* qui sont tous deux des relatifs,
nous obtenons que l'équation admet alors au moins une solution.

La condition est donc suffisante.

Conclusion : condition nécessaire et suffisante d'existence s'une solution :

L' équation (E) :*ax + by = c* admet au moins une solution
si et seulement si
le PGCD de a et de b divise c.

Remarques :
1) La première chose à faire est évidemment de calculer le PGCD de a et de b.

2) Si a et b sont premiers entre eux, (E) admet des solutions quel que soit c.

3) Si c = 0, tout nombre divisant 0, (E) admet des solutions, comme vu précédemment.

2/ Equations diophantiennes : *solution particulière*

En supposant que l'équation admette au moins une solution,
essayons maintenant d'en trouver au moins une.

Étape n° 2 : Recherche d'une solution particulière.
Deux cas de figure sont possibles :

* *Soit* la solution particulière est donnée par le texte
et il ne reste qu'à vérifier qu'elle est bien solution de (E).

* *Soit* il faut la trouver par soi-même.

- Soit il y a alors une solution particulière évidente.
- Soit il faut trouver cette solution par le calcul et ce « en remontant » l'algorithme d'Euclide.

Prenons un exemple concret : (E) : 616x + 585y = 12

616 = 585 x 1 + 31 Le dernier reste non nul est 1 donc ***pgcd (616,585) = 1***

585 = 31 x 18
+27
31 = 27 x 1 + 4

1 divise 12 donc ce qui est certain
c'est que l'équation a des solutions.

27 = 4 x 6 + 3
4 = 3 x 1 + 1

Voici maintenant la technique à adopter
pour remonter la suite de divisions.

(E) : $616x+585y=12$

$616=585\times1+31$ ←
$585=31\times18+27$
$31=27\times1+4$
$27=4\times6+3$
$4=3\times1+1$

Exprimer le PGCD :	$1=4-3\times1$
Remplacer le reste précédent :	$1=4-(27-4\times6)\times1$
Factoriser :	$1=4\times7-27\times1$
Remplacer le reste précédent :	$1=(31-27\times1)\times7-27\times1$
Factoriser :	$1=31\times7-27\times8$
Remplacer le reste précédent :	$1=31\times7-(585-31\times18)\times8$
Factoriser :	$1=31\times151-585\times8$
Remplacer le reste précédent :	$1=(616-585\times1)\times151-585\times8$
Factoriser :	$1=616\times151+585\times(-159)$
Multiplier par 12 :	$12=616\times1812+585\times(-1908)$

Et vue la probabilité de se tromper dans ce genre de manipulation,
il est conseillé de vérifier le résultat trouvé :

En effet, la calculatrice confirme que : 616 x 1812 + 585 x (-1908) =12

Une solution particulière de (E) est donc le couple (1812 ; -1908)

2/ Equations diophantiennes : *solution générale*

Étape n° 3 : Recherche de l'ensemble des solutions.
Supposons que nous ayons trouvé le couple (u ; v) comme solution particulière de (E).
Le couple (u, v), vérifie donc : $au + bv = c$

on a alors : x et y solutions de (E)
⇔ ax + by = au + bv
⇔ a(x - u) + b(y - v) = 0
⇔aX + bY = 0 avec X = x - u et Y = y - v

Et l'on retombe donc sur le cas c = 0 étudié plus haut, genre d'équation que l'on sait résoudre.
Et d'après l'étude qui en a été faite, on peut affirmer que si l'équation (E) possède au moins une solution dans $\mathbb{Z}$, alors elle en possède une infinité dans $\mathbb{Z}$.

Voyons cependant sur notre exemple comment rédiger la fin de la résolution.

(E) 616x + 585y = 12 a pour solution particulière le couple (1812 ; -1908).

Donc 616x + 585y = 12 ⇔ 616x + 585y = 616 x 1812 + 585 x (-1908)
⇔ 616(x - 1812) = 585x (-y - 1908)

Donc si x et y solutions de (E) alors 616 divise 585x (-y - 1908)
Or 616 est premier avec 585
donc d'après le théorème de Gauss : 616 divise (-y -1908)

Il existe donc un entier relatif k tel que : -y -1908 = 616k

D'où : 616(x - 1812) = 585 x 616k
Et donc : x - 1812 = 585k

si x et y sont solutions de (E), il existe donc un entier relatif k tel que : $\begin{cases} x = 1812 + 585k \\ y = -1908 - 616k \end{cases}$

Réciproque :
Soient x et y s'écrivant 1812 + 585k et y = -1908 - 616k avec k entier relatif.

616x + 585 x y = 616 x (1812 + 585k) + 585 (- 1908 - 616k)
= 616 x 1812 + 585 x (-1908) + 616 x 585k - 585 x 616k = 12

Conclusion : les couples solutions de (E) sont les couples avec k entier relatif.

2/ Equations diophantiennes : *nombre de solutions*

Étape n° 4 : Recherche de solutions spécifiques.
Même si (E) a une infinité de solutions dans $\mathbb{Z}$, le contexte de l'exercice peut obliger à en éliminer certaines.

Il se peut donc parfois qu'il faille faire une étape de plus qui consiste à sélectionner les solutions respectant des contraintes imposées.

Ce sera le cas en particulier si la résolution d'une équation diophantienne doit apporter une réponse à un problème concret.

Si par exemple dans l'équation : **(E) : 616x + 585y = 12**
x et y sont des entiers naturels représentant des nombres de tours de piste.
Alors x ≥ 0 et k doit donc vérifier : 1812 + 585k ≥ 0

Soit : $k \geq \frac{-1812}{585}$ Or : $\frac{-1812}{585} \approx -3{,}09$

k étant entier, il doit donc vérifier : k ≥ -3

De même avec la contrainte y ≥ 0 , on obtient : -1908 - 616k ≥ 0 Soit : $k \leq \frac{-1908}{616}$

Or $\frac{-1908}{616} \approx -3{,}09$ Il faut donc également : k ≥ -4
Aucun k ne pouvant respecter ces deux contraintes, le problème n'a pas de solution.

3/ Bilan pratique

Nous allons maintenant à partir d'un exemple, essayer de faire le tour des stratégies à adopter en fonction des situations et des questions qui peuvent être posées dans un exercice.

Pour ce faire prenons l'exemple de (E) : 1462x - 408y =136

* Quelles que soient les questions à venir, commencer par regarder si l'équation peut être simplifiée de façon évidente.
Ici, c'est la cas, on peut simplifier l'équation par 2.
(x ; y) solution de (E) ⇔ (x ; y) solution de (E') : 731x - 204y = 68
1° Si la question est : « L'équation admet-elle des solutions ? »
► Il faut alors trouver le pgcd de 731 et (-204), autrement dit le pgcd de 731 et 204.

► *Il y a au moins 3 façons de trouver ce pgcd.*

Si cette question n'a pas de suite, comme par exemple dans un QCM, les 3 méthodes de recherche du pgcd se valent.
Sinon, il est conseillé d'utiliser l'algorithme d'Euclide.

►Une fois le pgcd trouvé, soit il divise 68 et (E) a des solutions soit il ne divise pas 68 et (E) n'a pas de solution.

Rappel de (E') : 731x - 204y = 68

Utilisons l'algorithme d'Euclide :

$$731 = 204 \times 3 + 119$$
$$204 = 119 \times 1 + 85$$
$$119 = 85 \times 1 + 34$$
$$85 = 34 \times 2 + 17$$
$$34 = 17 \times 2 + 0$$

Le pgcd de 731 et 204 est donc 17.

68 = 4 x 17
17 divise 68, l'équation a donc des solutions.

2° Si la question à suivre est : « Donner une solution particulière de (E) » ou encore « Résoudre (E) ».

La première question que l'on se pose souvent est :
« A-t-on intérêt à simplifier l'équation par le pgcd ? »

Auquel cas elle deviendrait (E'') : 43x -12y = 4

Cette opération comporte des avantages et un inconvénient.

Son premier avantage est que 43 et 12 sont premiers entre eux,
ce qui pourra éviter des erreurs dans la résolution à suivre
Son deuxième avantage est que l'équation étant plus simple,
il est alors plus facile de trouver une solution particulière évidente.

Son troisième avantage est que si le pgcd a été trouvé autrement qu'avec l'algorithme d'Euclide, l'algorithme d'Euclide qu'il faut maintenant faire en cas d'absence de solution évidente, est plus court à remonter.

Enfin *le seul inconvénient*, c'est que s'il n'y a pas de solution évidente et que l'on a déjà fait une première fois l'algorithme d'Euclide, cela oblige à le refaire.

Rappel de (E'') : 43x - 12y = 4

Il n' y a pas de solution évidente, revenons donc à (E') : 731x - 204y = 68
et remontons notre algorithme :

$731 - 204 \times 3 + 119$
$204 = 119 \times 1 + 85$
$119 = 85 \times 1 + 34$
$85 = 34 \times 2 \mid 17$ ←

Exprimer le reste	

$731 = 204 \times 3 + 119$
$204 - 119 \times 1 + 85$
$119 - 85 \times 1 + 34$ ←
$85 = 34 \times 2 + 17$

Exprimer le reste	
$17 - 85 - 34 \times 2$	

$731 = 204 \times 3 + 119$
$204 = 119 \times 1 + 85$
$119 - 85 \times 1 + 34$ ←
$85 - 34 \times 2 + 17$

Exprimer le reste	Factoriser
$17 = 85 \quad 34 \times 2$	
$17 - 85 - (119 - 85 \times 1) \times 2$	

$731 = 204 \times 3 + 119$
$204 = 119 \times 1 \mid 85$ ←
$119 = 85 \times 1 + 34$
$85 = 34 \times 2 + 17$

Exprimer le reste	Factoriser
$17 = 85 \quad 34 \times 2$	
$17 - 85 - (119 - 85 \times 1) \times 2$	$- 85 \times 3 - 119 \times 2$

$731 = 204 \times 3 + 119$
$204 - 119 \times 1 + 85$ ←
$119 = 85 \times 1 + 34$
$85 = 34 \times 2 \mid 17$

Exprimer le reste	Factoriser
$17 - 85 - 34 \times 2$	
$17 = 85 \quad (119 \quad 85 \times 1) \times 2$	$= 85 \times 3 \quad 119 \times 2$
$17 = (204 - 119 \times 1) \times 3 - 119 \times 2$	

$731 = 204 \times 3 \mid 119$ ←
$204 - 119 \times 1 + 85$
$119 - 85 \times 1 + 34$
$85 = 34 \times 2 + 17$

Exprimer le reste	Factoriser
$17 = 85 - 34 \times 2$	
$17 = 85 - (119 - 85 \times 1) \times 2$	$= 85 \times 3 - 119 \times 2$
$17 = (204 - 119 \times 1) \times 3 - 119 \times 2$	$= 204 \times 3 - 119 \times 5$

$731 = 204 \times 3 \mid 119$ ←
$204 = 119 \times 1 + 85$
$119 - 85 \times 1 + 34$
$85 = 34 \times 2 + 17$

Exprimer le reste	Factoriser
$17 = 85 - 34 \times 2$	
$17 = 85 - (119 - 85 \times 1) \times 2$	$= 85 \times 3 - 119 \times 2$
$17 - (204 - 119 \times 1) \times 3 - 119 \times 2$	$- 204 \times 3 - 119 \times 5$
$17 - 204 \times 3 - (731 - 204 \times 3) \times 5$	

$731 = 204 \times 3 + 119$ ←

$204 - 119 \times 1 + 85$

$119 = 85 \times 1 + 34$

$85 = 34 \times 2 + 17$

Exprimer le reste	Factoriser
$17 = 85 - 34 \times 2$	
$17 = 85 - (119 - 85 \times 1) \times 2$	$= 85 \times 3 - 119 \times 2$
$17 = (204 - 119 \times 1) \times 3 - 119 \times 2$	$= 204 \times 3 - 119 \times 5$
$17 = 204 \times 3 - (731 - 204 \times 3) \times 5$	$= 204 \times 18 - 731 \times 5$

Attention !
Arrangez vous pour que cette égalité respecte bien les mêmes signes que dans l'équation (E').

D'où 731 x (-5) - 204 x (-18) = 17
Il reste alors à multiplier l'équation par 68/17, c'est à dire 4 : 731 x(-20) - 204 x (-72) = 68
attention : avant conclure regardez si cette égalité est vraie

Le couple (-20 ; -72) est donc une solution particulière de (E).

Rappel de (E) : 1492x - 408y = 136
1° et 2° bis
Si la première question posée est : « Monter que le couple (-20 ; -72) est solution de (E). »
On vérifie simplement que : 1462x (-20) + 408x (-72) = 136
Nous en sommes alors au même point qu'avec les questions précédentes, à ceci près que nous n'avons calculé aucun pgcd.

3° Quel qu'ait été notre cheminement jusqu'à une solution particulière, arrive alors la question finale : « Résoudre (E) ».

Dans tous les cas :
il faut remplacer le membre de droite par la combinaison
que représente la solution particulière puis manipuler l'équation,
en ne laissant aucun signe sur les coefficients,
afin de faciliter la résolution.

Exemple : 1462x - 408y = 1462x (-20) - 408x (-72) ⇔ 1462 (x + 20) = 408x (y +72)
Situation n° 1 : les coefficients sont premiers entre eux,
soit parce que nous avions simplifié l'équation en divisant par le pgcd,
soit en raison des données initiales de l'exercice.

Situation n° 2 : les coefficients ne sont pas premiers entre eux.
Il faut alors simplifier l'équation par leur pgcd
sinon on ne peut pas appliquer le théorème de Gauss.

Appliquer le théorème de Gauss à des nombres non premiers entre eux est l'erreur n° 1 chez les élèves.

Dans le cas d'une solution donnée par le texte, il faut donc tout de même trouver le pgcd.

Revenons au cas où nous avions nous-même trouvé une solution particulière.
Reprenons par exemple (E') : 731x - 204y = 68

⇔ 731x - 204y = 731x (-20) - 204x (-72)
⇔ 731(x + 20) = 204(y + 72)

On simplifie par 17 :
⇔ 43(x + 20) = 12(y + 72)

- 17 étant le pgcd de 731 et 204, on est certain que 43 et 12 sont premiers entre eux.
- 43 divise 12(y+72) et 43 premier avec 12 donc d'après le théorème de Gauss,
- 43 divise y+72.

D'où, il existe k entier relatif tel que : y+72 = 43k.
Inutile alors, comme font certains livres, de réutiliser Gauss avec 12.

Rappel : (E) ⇔43 (x + 20) = 12(y + 72)
y + 72 = 43k
donc 43 (x+20) = 12x 43k et par conséquent : x + 20 = 12k.

Les couples solutions sont donc du type (-20+12k ; -72 + 43k).

Ne pas oublier de vérifier la réciproque et conclure.

Enfin, un dernier conseil, prendre une valeur simple pour k, et tester si le couple correspondant est bien solution de (E).

BONNE CHANCE (Guesmi.B)