Chapitre 4

Equations diophantiennes

4.1 Introduction

Les équations diophantiennes doivent leur nom au mathématicien grec Diophante d'Alexandrie (3ème siècle avant *J.C.*). Il s'agit d'une branche de la théorie des nombres qui cherche à résoudre des équations polynomiales, à coefficient entiers, ayant plusieurs inconnues. Une particularité de ce domaine est que les solutions sont cherchées parmi les nombres entiers.

Dans cette partie des mathématiques, les problèmes sont souvent simples à énoncer mais la mise en oeuvre de la résolution peut s'avérer complexe et difficile.

Par exemple, en Pierre de Fermat (17ème siècle) a affirmé dans une lettre qu'il était capable de résoudre, pour n'importe quel entier $n \geq 1$, l'équation

$$x^n + y^n = z^n \quad \text{avec} \quad (x, y, z) \in \mathbb{N}_*^3.$$

En particulier, il a énoncé, sans démonstration, le théorème suivant.

Théorème 24 (Fermat)**.** *Il n'existe pas de nombres entiers strictement positifs x, y et z tels que :*

$$x^n + y^n = z^n$$

dès que n est un entier strictement à 2.

Il fallut pourtant 357 ans pour qu'Andrew Wiles démontre, en 1944, de manière rigoureuse ce théorème. Pour cela, il a du inventer de nouveaux outils et de nouvelles méthodes dans ce domaine des mathématiques ; lesquels ont ouvert de nouveau champs d'investigations dans d'autres branches des mathématiques.

4.2 PGCD

Débutons ce nouveau chapitre en exposant, de manière formelle, des notions élémentaires déjà rencontrées dans votre scolarité.

4.2.1 Définition propriétés

Définition 4.2.1. *Soient $a, b \in \mathbb{Z}_*$. L'ensemble des diviseurs commun à a et b est une partie non vide de $\mathbb{Z}$ et majorée, cet ensemble admet un plus grand élément appelé* ***plus Grand Diviseur Commun*** *de a et b. Celui-ci sera noté $PGCD(a; b)$.*

Exemple 4.2.1. Déterminons le $PGCD$ de 30 et -12. Pour cela listons leurs diviseurs :

1. Pour 30, nous avons $-30, -15, -10, -6, -5, -3, -2, -1, 1, 2, 3, 5, 6, 10, 15, 30$?
2. Pour -12, nous avons $-12, -6, -4, -3, -2, -1, 1, 2, 3, 4, 6, 12$.

En conséquence, $PGCD(30; -12) = 6$.

Remarque. Observons en passant que les arguments précédents montrent également que $PGCD(30; 12) = PGCD(-30; 12) = PGCD(-30, -12) = 6$.

L'observation précédente montre que pour tout $a, b \in \mathbb{Z}_*$ alors

$$PGCD(a; b) = PGCD(|a|; |b|).$$

Nous pouvons donc restreindre nos calculs à ceux de $PGCD$ entres deux d'entiers naturels. Listons maintenant quelques propriétés du $PGCD$.

Proposition 25. *Soient $a, b \in \mathbb{N}$ avec $a \neq 0$.*

1. *$PGCD(a; b) \geq 1$; $PGCD(0; a) = a$ et $PGCD(1; a) = 1$.*
2. *$a|b$ si et seulement si $PGCD(a; b) = a$.*
3. *$PGCD(a; b) = PGCD(a - b; b)$.*

La dernière propriété est **importante** car elle va nous permettre de mettre en place un **algorithme** primordial. Voyons déjà comment l'utiliser sur un exemple.

Exemple 4.2.2. $PGCD(229; 225) = PGCD(229 - 225; 225) = PGCD(4; 225) = 1$ car 1 et le seul diviseur positif commun à 4 et 225.

Implicitement l'exemple précédent utilise une division euclidienne, nous allons approfondir cet aspect dans la section suivante.

Exercices à traiter : 21 et 30 page132.

4.2.2 Algorithme d'Euclide

Nous allons présenter un algorithme permettant de déterminer le $PGCD$ de deux nombres. Cet algorithme repose sur le Lemme suivant.

Lemme 26 (Euclide)**.** *Soient $a, b \in \mathbb{Z}_*$ alors*

$$PGCD(a; b) = PGCD(b; r)$$

où r est défini par la division euclidienne de a par b

$$i.e. \quad a = bq + r \quad avec \quad b \in \mathbb{Z} \quad et \quad 0 \leq r < b.$$

Démonstration. Pour démontrer ce résultat nous devons montrer l'égalité entre l'ensemble des diviseurs communs de a et b avec l'ensemble des diviseurs communs de b et r. Il suffit de procéder par **double inclusion**.

1. Soit d un diviseur commun de a et b, montrons qu'il s'agit aussi d'un diviseur commun de b et r. Nous savons que $a = bq + r$, autrement dit r s'exprime comme une combinaison linéaire de a et b :
$$r = a - bq$$
Puisque $d|a$ et $d|b$ (car d est un diviseur commun à a et b) alors d divise toute combinaison linéaire de a et b (cf. proposition 6 dans le chapitre 2). En particulier, $d|r$: il s'agit donc d'un diviseur commun de b et r.
2. Réciproquement, soit d' un diviseur commun de b et r. Nous savons que a s'exprime comme une combinaison linéaire de b et r :
$$a = bq + r.$$
En conséquence, d'après le même argument qu'auparavant, $d'|a$. Ainsi, d' est un diviseur commun à a et b.

Nous venons montrer que l'ensemble des diviseurs commun à a et b coïncide avec l'ensemble des diviseurs commun de b et r. En particulier, ils possèdent le même plus grand élément. Autrement dit,
$$PGCD(a; b) = PGCD(b; r).$$
□

Le lemme précédent est d'une **importance cruciale** car il permet de déterminer le PGCD de deux nombres de manière algorithmique. Voyons sur un exemple.

Exemple 4.2.3. Déterminons le $PGCD$ de 508 et 112. Chaque égalité entre deux $PGCD$ est obtenue via le Lemme 26.

1. Puisque $508 = 112 \times 4 + 60$,
$$PGCD(508; 112) = PGCD(112; 60).$$
2. Recommençons ce procédé : $112 = 60 \times 1 + 52$ donc
$$PGCD(112; 60) = PGCD(60; 52).$$
3. Une fois de plus : $60 = 52 \times 1 + 8$ donc
$$PGCD(60; 52) = PGCD(52; 8).$$
4. $52 = 8 \times 6 + 4$ donc
$$PGCD(52; 8) = PGCD(8; 4).$$
5. Enfin, $8 = 4 \times 2 + 0$ donc
$$PGCD(8; 4) = PGCD(4; 0) = 4.$$

En conclusion, le PGCD de 508 et 112 correspond au dernier reste non nul obtenu : 4

Remarque. Dans l'exemple précédent nous avons construit, de proche en proche, une suite de nombres (correspondant au reste des divisions euclidiennes successives)

$$r_1 = 60 \quad ; \quad r_2 = 52 \quad ; \quad r_3 = 8; \quad r_4 = 4 \quad ; \quad r_5 = 0.$$

Il se trouve qu'il est possible de formaliser ce procédé afin d'obtenir une suite **décroissante** $(r_n)_{n\geq 0}$ telle qu'au bout d'un certain rang la suite soit nulle (ce qui arrive à partir du rang 5 dans l'exemple précédent) et telle que le **dernier terme non nul** (r_4 dans ce qui précède) corresponde au **PGCD** de a et b.

Par analogie avec l'exemple 4.2.3, étant donnés $a, b \in \mathbb{N}_*$, nous définissons la suite $(r_n)_{n\geq 0}$ par récurrence de la manière suivante :

- $r_0 = b$ et r_1 est le reste de la division euclidienne de a par b ;
- Pour $n \geq 1$,
  1. si $r_n = 0$ alors $r_{n+1} = 0$;
  2. si $r_n \neq 0$ alors r_{n+1} est le reste de division euclidienne de r_{n-1} par r_n.

Le théorème suivant nous assure qu'un bout d'un moment la suite $(r_n)_{n\geq 0}$ permet d'obtenir le PGCD de a et b.

Théorème 27 (Algorithme d'Euclide)**.** *Soient $a, b \in \mathbb{N}_*$, $a > b$. Si $(r_n)_{n\geq 0}$ est la suite définie ci-dessus alors il existe un entier n_0 tel que $r_{n_0} \neq 0$ et $r_n = 0$ pour tout $n > n_0$. De plus,*

$$PGCD(a; b) = r_{n_0}.$$

Démonstration. Tout repose sur l'utilisation du lemme d'Euclide 26.

1. Par l'absurde, supposons que pour tout entier $n \in \mathbb{N}$, $r_n \neq 0$. Alors, par construction, nous savons que r_{n+1} est le reste de la division euclidienne de r_{n-1} par r_n. En outre, par définition du reste, pour tout $n \in \mathbb{N}$, nous avons

   $$0 \leq r_{n+1} < r_n$$

   En particulier, pour $n = 0$, cela implique que $0 < r_1 < r_0 = b$. Ceci s'exprimer de manière équivalente (en passant de l'inégalité stricte à l'inégalité large pour des entiers) en

   $$r_1 \leq b - 1.$$

   De même, pour $n = 1$, nous avons $0 < r_2 < r_1$ donc $0 < r_2 \leq r_1 - 1$ d'où

   $$r_2 \leq b - 2.$$

   En poursuivant ce raisonnement, il est possible de démontrer par récurrence sur n que, pour tout $n \in \mathbb{N}$, l'inégalité suivante est satisfaite :

   $$r_n \leq b - n.$$

En particulier, en choisissant $n = b + 1$, nous en déduisons que

$$r_{b+1} \leq b - (b+1) \quad \Longleftrightarrow \quad r_{b+1} \leq -1 < 0$$

ce qui est absurde puisque $r_{b+1} > 0$. Notre hypothèse de départ est donc fausse : il existe donc un entier n tel que $r_n = 0$.

2. L'ensemble des entiers n tels que $r_n = 0$ est une partie non vide de $\mathbb{N}$, il admet donc un plus petit élément n_1. Posons à présent $n_0 = n_1 - 1$ et montrons que ce rang est bien celui que nous recherchons

   - $n > n_0 \iff n \geq n_1$, nous avons donc, par construction, la propriété suivante $r_n = 0$ pour tout $n > n_0$.
   - Nous devons montrer que r_{n_0} correspond bien au PGCD de a et b. Puisque $n_0 < n_1$, le caractère minimal de n_1 nous assure alors que

     $$r_k \neq 0 \quad \text{pour tout} \quad k \leq n_0.$$

     Nous pouvons donc appliquer de manière successive le lemme d'Euclide 26 à ces éléments (tous non nuls) :

     $$\begin{aligned} PGCD(a;b) = PGCD(a;r_0) = PGCD(r_0;r_1) = \ldots &= PGCD(r_{n_0-1};r_{n_0}) \\ &= PGCD(r_{n_0};r_{n_1}) = PGCD(r_{n_0};0) \\ &= r_{n_0} \end{aligned}$$

     puisque $r_{n_0} + 1 = r_{n_1}$ est le premier terme nul de la suite.

□

Voyons une conséquence de ce résultat.

Corollaire 28. *Soient $a, b, k \in \mathbb{N}_*$ alors*

1. *$PGCD(ka; kb) = kPGCD(a; b)$.*
2. *d est un diviseur commun à a et b si et seulement si $d | PGCD(a; b)$.*

Exercices à traiter : 37, 38 (à la maison), 39 page 132.

4.3 Nombres premiers entre eux

4.3.1 Définition

Certains PGCD sont plus importants que d'autres, c'est l'intérêt de la définition suivante.

Définition 4.3.1. *Soient $a, b \in \mathbb{Z}_*$. Nous dirons que a et b sont **premiers entre eux** lorsque leurs seuls diviseurs communs sont 1 et -1. Autrement dit, a et b sont premiers entre eux lorsque*

$$PGCD(a; b) = 1.$$

Voyons un exemple.

Exemple 4.3.1. 18 et 35 sont premiers entres eux car 35 est un multiple de $1; 5; 7$ et 35 tandis que 18 n'est divisible par aucun de ces nombres sauf 1. D'où

$$PGCD(18; 35) = 1.$$

Cette nouvelle définition permet d'obtenir une nouvelle caractérisation du $PGCD$.

Proposition 29 (Caractérisation du $PGCD$)**.** *Soient $a, b \in \mathbb{Z}_*$.*

1. *Si $d = PGCD(a; b)$ alors il existe a' et b' deux entiers premiers entre eux tels que $a = da'$ et $b = db'$.*
2. *Réciproquement, s'il existe $d \in \mathbb{N}$, a' et b' deux entiers premiers entre eux tels que*

$$a = da' \quad et \quad b = db'$$

alors $d = PGCD(a; b)$.

Exemple 4.3.2. $36 = 12 \times 3$ et $60 = 12 \times 5$; 3 et 5 sont premiers entre eux alors, d'après la proposition 29, $PGCD(36; 60) = 12$.

Cette nouvelle caractérisation permet notamment de résoudre le problème suivant.

Exemple 4.3.3. Déterminons l'ensemble des couples $(a; b) \in \mathbb{N}^2$ tels que

$$\begin{cases} ab = 300 \\ PGCD(a; b) = 5. \end{cases}$$

1. **Analyse :** Puisque $PGCD(a; b) = 5$ nous savons (d'après la proposition 29) qu'il existe deux entiers premiers entre eux a' et b' tels que

$$\begin{cases} a = 5a' \\ b = 5b' \end{cases}$$

Ceci entraine que $ab = 25 \times a'b'$. Par suite, $25 \times a'b' = 300$ et ainsi $a'b' = 12$. Il ne reste plus qu'à énumérer les possibilités :

$$12 = 12 \times 1 = 6 \times 2 = 4 \times 3.$$

Comme a' et b' doivent être premiers entre eux, les couples envisageables sont

$$(1; 12), \quad (12; 1), \quad (3; 4), \quad (4; 3).$$

Ce qui donne pour a et b (en multipliant par 25) les couples

$$(5; 60), \quad (60; 5), \quad (15; 20), \quad (20; 15).$$

2. **Synthèse :** nous vérifions ensuite que chacun de ces couples est bien une solution du système.

Exercice à traiter : 33 page 132.

4.3.2 Théorème de Bézout et application

Dans cette section, nous allons exposer un résultat qui servira de pierre angulaire aux méthodes permettant de résoudre des équations diophantiennes.

Théorème 30 (Bézout)**.** *Soient $a, b \in \mathbb{Z}_*$. Les assertions suivantes sont alors équivalentes :*
- *a et b sont premiers entre eux.*
- *il existe deux entiers relatifs u et v tels que*

$$au + bv = 1.$$

Remarque. Attention les entiers u et v ne sont pas uniques.

Voyons un exemple d'application.

Exemple 4.3.4. Pour tout entier $n \in \mathbb{N}$, nous constatons que $(5n+7) \times 3 - (3n+4) \times 5 = 1$. D'après le théorème de Bézout $5n+7$ et $3n+4$ sont donc premiers entre eux pour tout $n \in \mathbb{N}$.

Remarque. Pour constater la force du théorème de Bézout 30, essayez d'imaginer une approche alternative.

Il serait utile de trouver une **méthode pratique** permettant de trouver les entiers u et v intervenant dans le théorème de Bézout 30. Nous expliquons cela ci-dessous.

Exemple 4.3.5. Il n'est pas difficile de vérifier que 29 et 12 sont premiers entre eux. Le théorème de Bézout 30 nous assure donc qu'il existe u et v tels que $29u + 12v = 1$. Comment déterminer ces entiers ?

Pour cela, nous allons utiliser l'algorithme d'Euclide 27.

$$(E_1) : \quad 29 = 12 \times 2 + 5 \quad ; \quad (E_2) : \quad 12 = 5 \times 2 + 2 \quad ; \quad (E_3) : \quad 5 = 2 \times 2 + 1.$$

Il ne reste plus qu'a exprimer (E_3) de manière alternative pour ensuite « remonter » l'algorithme.

$$(E_3) \quad \Longleftrightarrow \quad 1 = 5 - 2 \times 2.$$

Or, d'après (E_2), nous avons $2 = 12 - 5 \times 2$. D'où

$$1 = 5 - 2 \times (12 - 5 \times 2) \quad \Longleftrightarrow \quad 1 = 5 \times 5 - 2 \times 12.$$

en outre, d'après (E_1), nous avons $5 = 29 - 12 \times 2$. Par suite,

$$1 = 5 \times (29 - 12 \times 2) - 2 \times 12 \quad \Longleftrightarrow \quad 1 = 29 \times 5 + 12 \times (-12).$$

En choisissant $u = 5$ et $v = -12$, nous avons donc trouvé un couple de Bézout.

Exercice à traiter : 43 page 133.

Nous donnons ci-dessous, deux utilisations du théorème de Bézout 30.

Déterminer l'inverse d'un nombre modulo n

Exemple 4.3.6. Déterminons, après avoir justifier son existence, un entier a tel que $30a \equiv 1[23]$.

Puisque 30 et 23 sont premiers entre eux, le théorème de Bézout nous assure qu'il existe $u, v \in \mathbb{Z}$ tels que

$$30u + 23v = 1.$$

Modulo 23, cela s'écrit $30u \equiv 1[23]$. Il ne reste plus qu'à utiliser l'algorithme d'Euclide pour déterminer le couple u et v. Après quelques calculs, nous trouvons $1 = 30 \times 10 + 23(-13)$. Autrement dit, $u = 10$ et $v = -13$. Par suite, l'inverse de 30 modulo 23 vaut 10.

Remarque. Cette méthode de résolution est à comparer à ce que nous faisions dans le chapitre 2 avec les tableaux de congruences.

Exercice à traiter : 48 page 133.

Existence de solutions d'une équation diophantienne

.

Dans ce qui va suivre, nous débutons la résolution (en x, y) des équations (dites diophantiennes) de la forme

$$ax + by = c \quad \text{avec} \quad a, b, c \in \mathbb{Z}.$$

Cette résolution repose, en partie, sur l'utilisation de la proposition suivante.

Proposition 31 (Identité de Bézout)**.** *Pour tout couple $a, b \in \mathbb{Z}_*$, il existe $u, v \in \mathbb{Z}$ tels que*

$$au + bv = PGCD(a; b)$$

Démonstration. Soient $d = PGCD(a; b)$, nous savons qu'il existe deux entiers premiers entre eux a' et b' tels que

$$a = a'd \quad \text{et} \quad b = b'd.$$

De plus, nous pouvons appliquer le théorème de Bézout 30 au couple $(a'; b')$: il existe alors $u, v \in \mathbb{Z}$ tels que

$$a'u + b'v = 1.$$

Pour conclure, il ne reste plus qu'à multiplier chaque membre de l'égalité précédente par d. □

Exemple 4.3.7. Est-il possible de résoudre $84x + 18y = 6$? Cela revient à résoudre $14x + 3y = 1$. Puisque 14 et 3 sont premiers entre eux, le théorème de Bézout 30 nous assure qu'il existe au moins une solution.

En fait, nous avons un résultat plus général.

Corollaire 32 (Existence des solutions d'une équations diophantiennes)**.** *Soient* $a, b, c \in \mathbb{Z}_*$. *L'équation diophantienne*

$$ax + by = c$$

admet des solutions $(x; y) \in \mathbb{Z}^2$ *si et seulement si* $PGCD(a; b)|c$.

4.3.3 Théorème de Gauss

Pour continuer notre résolution des équations diophantiennes, nous avons besoin d'un résultat supplémentaire.

Théorème 33 (Gauss)**.** *Soient* $a, b, c \in \mathbb{Z}_*$. *Si* $a|bc$ *et si* a *et* b *sont premiers entre eux alors* $a|c$.

Démonstration. La démonstration repose de nouveau sur le théorème de Bézout 30. Puisque $PGCD(a; b) = 1$, il existe u et v des entiers tels que

$$au + bv = 1$$

D'où, $auc + buc = c$. Par hypothèse, $a|bc$ et, de manière évidente, $a|auc$ donc $a|(auc + buc)$ (d'après la proposition 6 du chapitre 2). Autrement dit, $a|c$. □

Voyons une application de ceci.

Exemple 4.3.8. Résolvons, dans $\mathbb{Z}^2$, l'équation

$$(E) \ : \ 65x = 91y.$$

1. **Analyse :** puisque $PGCD(65; 91) = 13$,

   $$(E) \quad \Longleftrightarrow \quad 5x = 7y.$$

   En outre, $7|7y$ alors $7|5x$. Comme 5 et 7 sont premiers entre eux, d'après le théorème de Gauss 33, cela signifie que $7|x$. Autrement dit, il existe $k \in \mathbb{Z}$ tel que $x = 7k$. D'où,

   $$5 \times 7k = 7y \quad \Longleftrightarrow \quad 5k = y.$$

2. **Synthèse :** nécessairement, un couple de solutions de (E) est de la forme $(7k; 5k)$ avec $k \in \mathbb{Z}$. Il suffit de vérifier ensuite qu'un tel couple est bien solution.
3. En conclusion, l'ensemble des solutions de (E) est

   $$\big\{(7k; 5k) \quad ; \quad k \in \mathbb{Z}\big\}.$$

Exercice à traiter : 52 page 133.

Ce genre d'approche est notamment efficace pour résoudre des équations diophantiennes.

Exemple 4.3.9. Résolvons $(E) \ : \ 7x - 11y = 3$ avec $(x; y) \in \mathbb{Z}^2$.

1. Tout d'abord, vérifions que $(x_0; y_0) = (13; 8)$ est une solution particulière de (E). Il est essentiel de trouver une solution particulière car cette dernière permet de se ramener à l'exemple 4.3.8. Ceci est visible dans l'étape suivante.

2. Ensuite, observons que $(x;y) \in \mathbb{Z}^2$ est solution de (E) si et seulement si Procéder à la différence des équations

$$7x - 11y = 3 \quad \Longleftrightarrow \quad 7x - 11y = 7x_0 - 11y_0 \quad \Longleftrightarrow \quad 7(x - x_0) = 11(y - y_0).$$

Dans cette étape, nous avons exprimé le membre de droite à l'aide d'une solution particulière pour ensuite rassembler dans le membre de gauche ou de droite les éléments de même nature (ici, les multiple de 7 ou de 11). En faisant ainsi, nous retrouvons face à une situation similaire à celle étudiée dans l'exemple 4.3.8.

Nous pouvons maintenant reprendre les arguments présntés plus tôt : puisque $7|11(y - y_0)$ et que 7 et 11 sont premiers entre eux, le théorème de Gauss 33 nous assure que $7|(y - y_0)$. Autrement dit, il existe $k \in \mathbb{Z}$ tel que

$$y - y_0 = 7k.$$

Par suite, $7(x - x_0) = 11(y - y_0) \quad \Longleftrightarrow \quad 7(x - x_0) = 11 \times 7k \quad \Longleftrightarrow \quad x - x_0 = 11k$. En résumé, nous avons montré que

$$y = y_0 + 7k \quad \text{et} \quad x = x_0 + 11k \quad \text{avec} \quad k \in \mathbb{Z}.$$

L'ensemble des solutions de (E) est précisément formé des couples de cette forme.

Exercice à traiter : Résoudre les équations diophantiennes du 50 page 133.

Voyons un dernier résultat lié au théorème de Gauss 33.

Corollaire 34. *Soient $a, b, c \in \mathbb{Z}_*$. Si b et c sont premiers entre eux et divisent tous les deux a alors $bc|a$.*

Remarque. Lorsque b et c ne sont pas premier entre eux la conclusion est fausse : $6|24$ et $12|24$ or 6 et 24 ne sont pas premiers entre eux et 6×12 ne divise pas 24.

Démonstration. Par hypothèse, il existe $k, l \in \mathbb{Z}$ tels que

$$a = bk \quad \text{et} \quad a = cl$$

En particulier, $bk = cl$ et $b|cl$. Puisque b et c sont premiers entre eux, le théorème de Gauss 33 nous assure que $b|l$. Il existe alors $K \in \mathbb{Z}$ tel que $l = bK$. Ainsi, $a = cl = cbK$ d'où $bc|a$. □

Voyons un exemple d'application.

Exemple 4.3.10. Soit $n \in \mathbb{N}$ et $a = n(2n + 1)(7n + 1)$. Montrons que a est divisible par 6.

Puisque $6 = 2 \times 3$ et que 2 et 3 sont premiers entre eux, le corollaire précédent (utilisé avec $b = 2$ et $c = 3$) nous assure que pour montrer que $6|a$ il suffit de montrer que $2|a$ et $3|a$.

Regardons a modulo 2.

$n \equiv \ldots [2]$	0	1
$2n+1 \equiv \ldots [2]$	1	1
$7n+1 \equiv \ldots [2]$	1	0
$a \equiv \ldots [2]$	0	0

donc a est divisible par 2. Regardons a modulo 3

$n \equiv \ldots [3]$	0	1	2
$2n+1 \equiv \ldots [3]$	1	0	2
$7n+1 \equiv \ldots [3]$	1	2	0
$a \equiv \ldots [3]$	0	0	0

donc a est divisible par 3. En conclusion a est bien divisible par 6

Remarque. Rappelons qu'il est essentiel que 2 et 3 soient premiers entre eux pour utiliser le corollaire précédent.

Exercice à traiter : 61 page 133.

4.4 Exercices bilan

Cette courte section propose plusieurs exercices bilan permettant de faire le point sur les notions présentées dans ce chapitre.

Exercices à traiter : 96 page 137 et 115 page 140

4.5 Pour aller plus loin

Comme il est exposé dans votre livre (page 166-169), il possible de généraliser ce que nous venons de voir avec des polynômes. Grossièrement, le point essentiel consiste à d'obtenir une notion division euclidienne entre deux polynômes.

4.5.1 Polynômes à coefficients dans $\mathbb{R}$

Pour définir un polynôme, il suffit de se donner une suite de nombre correspondant aux coefficients se trouvant devant les puissances successives de X. Cela est expliqué page 166.

Exercice à traiter : 3 page 166.

4.5.2 Division euclidienne dans $\mathbb{R}[X]$

Il est possible de généraliser la notion de divisibilité aux polynômes et de montrer qu'il existe une division euclidienne pour ce genre d'objets ; pas suite, il est également possible de définir la notion de $PGCD$, de polynômes premiers entre eux, etc .... Cela est exposé page 167 de votre livre.

Exemple 4.5.1. Effectuons la division euclidienne de $A(X) = X^2 + 3X - 2$ par $B(X) = X + 1$.

1. Observons qu'il est possible de retirer X fois $X + 1$ de $X^2 + 3X - 2$:
$$X^2 + 3X - 2 - X(X + 1) = X^2 + 3X - 2 - X^2 - X = 2X - 2.$$
2. Il faut maintenant retirer 2 fois $X + 1$ de $2X - 2$:
$$2X - 2 - 2 \times (X + 1) = -4.$$
3. En définitive, si $Q(X) = X + 2$ et $R(X) = -4$ nous avons montré que
$$A(X) = B(X)Q(X) + R(X) \quad \text{avec} \quad \deg(R) < \deg(B).$$
Autrement dit, $X^2 + 3X - 2 = (X + 1)(X + 2) - 4$.

Exercices à traiter : 6, 9 et 11 page 167.