UNIVERSITÉ DE RENNES 1

**ARA: Algèbre et Arithmétique**

*ARA-Partie 3 : Division euclidienne*

# 1 Divisibilité

### 1.1 Théorème

Soit $a$ et $d$ deux entiers relatifs, avec $d \neq 0$.

Il existe un unique couple $(q,\ r) \in \mathbb{Z}^2$ vériffiant :

- $a = dq + r$,
- $0 \leq r \leq |d| - 1$

L'entier $q$ est appelé quotient de la division euclidienne de a par $b$ ; l'entier $r$ est le reste.

---

*Démonstration:* Admis ■

### 1.3 Exemple.

- Lorsque $a$ et $d$ sont dans $\mathbb{N}$, la division euclidienne est simplement la division enseignée en primaire :
  La division de 43 par 5 s'écrit $43 = 5 \times 8 + 3$.
- La division de $-43$ par 5 s'écrit $-43 = 5 \times (-9) + 2$.

### 1.4 Définition

*Soient $a$ et $d$ deux entiers. On dit que $d$* divise *$a$ s'il existe $k \in \mathbb{Z}$ tels que $a = kd$.*

On dit aussi que $a$ est un multiple de $d$, et on note $d|a$.

---

### 1.5 Remarque

Dire que $d|a$ revient donc à dire que le reste dans la division euclidienne de $a$ par $d$ est 0.

### 1.6 Exemple.

- 1 et $-1$ divisent tous les entiers, mais ne sont divisibles que par 1 et $-1$.
- 0 est un multiple de tous les entiers mais ne divise que lui-même
- Les diviseurs de 6 sont
$$\{\pm 1,\ \pm 2,\ \pm 3,\ \pm 6\}.$$

### 1.7 Proposition

Soient $a,\ b,\ d \in \mathbb{Z}$

- Si $d|a$ *et* $d|b$, *alors* $\forall (u,\ v) \in \mathbb{Z}^2,\ d|au + bv$

- Si $a|b$ *et* $b|c$ *alors* $a|c$.
- Si $d|a$ *et* $a \neq 0$ alors $|d| \leq |a|$.
- Si $a|b$ *et* $b|a$ alors $a = \pm b$.
- Si $n \in \mathbb{Z}$ est non nul, alors
$$a|b \Leftrightarrow an|bn.$$

*Démonstration:* On démontre le premier point, le reste est laissé en exercice.

On a $d|a$ et $d|b$ : on écrit donc $a = kd$ et $b = k'd$ pour un certain couple $(k,\ k') \in \mathbb{Z}^2$. Soient $u,\ v \in \mathbb{Z}$, on termine en écrivant que
$$au\ + bv = d(ku + k'v).$$

# 2 Numérotation

## 2.1 Le système décimal

Les nombres que nous utilisons généralement sont écrits en base 10 : il y a dix symboles $(0,\ \ldots,9\ )$ appelés *chiffres* qui nous permettent d'écrire tous les nombres. Ainsi par exemple 2348 en base 10 (que l'on note $2348_{10}$) signifie $2 \times 10^3 + 3 \times 10^2 + 4 \times 10^1 + 8 \times 10^0$.

D'autres numérotations sont possibles, mais quelque soit la base, le chiffre de gauche est toujours celui de poids le plus élevé.

## 2.2 Un autre exemple : la numérotation binaire

Pour des raisons physiques, en automatisme, électronique ou informatique, c'est la base 2 qui est utilisée. Tous les nombres s'écrivent avec deux chiffres : 0 et 1 (on parle alors de *bit* pour *binary digit*). La présence d'une tension aux bornes d'un composant sera ainsi notée 1, et son absence 0.

2.1 EXEMPLE. $1011_2 = 1 \times 2^3 + 0 \times 2^2 + 1 \times 2^1 + 1 \times 2^0 = 11_{10}$.

2.2 Exercice Écriver les entiers de 1 à 8 en base 2.
Soit $N \in \mathbb{N}$. Comment s'écrivent $2^N$ et $2^N - 1$ en base 2?

L'addition en base 2 s'effectue comme en base 10 : bits par bits de la droite vers la gauche, en prenant garde de ne pas oublier les retenues.

2.3 EXEMPLE. $1_2 + 1_2 = 10_2$.

2.4 Exercice
- Poser et effectuer 1'addition $1011_2 + 101_2$.
- Nous avons vu comment passer de la base 2 à la base 10. Récipro- quement, essayer de comprendre comment passer de lécriture déci- male à lécriture binaire (essayer par exemple avec 172). Pouvez vous améliorer votre méthode ?
- En base 2, la multiplication par 2 est très facile : calculez par exemple
$$1011_2 + 1011_2,$$
puis
$$1011_2 + 1011_2 + 1011_2 + 1011_2.$$
Maintenant, trouvez et démontrez la règle pour multiplier un nombre en base 2 par $2^N$.

- En règle générale, il est facile de multiplier deux nombres en base 2, même s'ils sont très longs. Par exemple, poser et effectuer la multipli- cation

$$1101_2 \times 1110_2.$$

## 2.3 Ecriture en base $b$

2.5 PROPOSITION

Soit $b \geq 2$ *un entier. Pour tout entier* $n$*, il existe un entier* $k \geq 0$ *et des entiers* $c_0, \ldots, c_k \in \{0, \ldots, b-1\}$ *tels que*

$$n = c_k b^k + \cdots 1b + c_0.$$

*On impose les règles* $k = 0$ *si* $n = 0$ *et* $c_k \neq 0$ *si* $n \neq 0$*. Les entiers* $k, c_0, \ldots, c_k$ *sont alors uniques*.

*Démonstration:* On démontre d'abord l'existence par récurrence sur $n$.

Si $0 \leq n < b$, en posant $k = 0$ et $c_0 = b$, on obtient une écriture de $n$ en base $b$.

Soit $n \geq b$, on suppose que tout entier strictement inférieur à $n$ admette une écriture en base $b$. Soient $q$ et $r$ les quotient et reste de la division euclidienne de $n$ par $b$.

Comme $1 \leq b \leq n$, on a $0 < q < n$. Par hypothèse de récurrence, $q$ donc admet une écriture en base $b$ :

$$q = d_m b^m + \cdots + d_0,$$

avec les $d_i$ compris entre 0 et $b-1$ et $d_m \neq 0$.

On pose alors $c_0 = r$, $k = m+1$ et pour tout $1 \leq i \leq m+1 c_i = d_{i-1}$, et on a l'écriture de $n$ en base $b$ suivante :

$n = bq + r = b(d_m b^m + \cdots + b_0) + c_0 = c_{m+1} b^{m+1} + \cdots + c_1 b + c_0$.

On démontre maintenant l'unicité, par récurrence également.

Pour $n < b$ l'écriture est bien unique.

Soit $n \geq b$, on suppose que tout entier strictement inférieur à $n$ admette une unique écriture en base $b$.

On sait que $n$ admet une écriture en base $b$ sous la forme $c_k b^k + \cdots + c_0$. Supposons qu'on en ait une autre : $d_m b^m + \cdots + d_0$.

Comme $n \geq b$, on a $k \geq$ let $m \geq 1$. Alors, lécriture

$$n = b(c_k b^{k-1} + \cdots + c_1) + c_0 = b(d_m b^{m-1} + \cdots + d_1) + d_0$$

montre que le reste de la division euclidienne de $n$ par $b$ est égal à $c_0$ et à $d_0$. On a donc $c_0 = d_0$.

Soit $q$ le quotient de la division euclidienne de $n$ par $b$ :

$$q = c_k b^{k-1} + \cdots + c_1 = d_m b^{m-1} + \cdots + d_1.$$

Ce sont deux écritures en base $b$ de lentier $q < n$ : par hypothèse de récurrence elles coincident.

On voit ainsi que les chiffres du développement en base $b$ se détermine de droite à gauche par divisions euclidiennes successives par $b$.

**Notation :** Un chiffre $n = n = c_k b^k + \cdots + c_1 b + c_0$ est noté en base $b$ s'écrit

$$c_k \ldots c_{0b} \text{ ou } \overline{c_k \ldots c_0}^b$$

2.7 EXEMPLE. Ecrivons 1729 en base 7.

La division euclidienne de 1729 par 7 s'écrit $1729 = 247 \times 7 + 0$, puis on a $247 = 35 \times 7 + 2$, puis $35 = 5 \times 7$. Ainsi :
$1729 = 247 \times 7 + 0 = (35 \times 7 + 2) \times 7 + 0 = 5 \times 7^3 + 2 \times 7 + 0$,
et donc :

$$1729_{10} = 5020_7.$$

2.8 Exercice En base 16 (ou base *hexadécimale*), on a besoin de 16 chiffres : aux 10 chiffres de 0 à 9 on ajoute les 6 premières lettres de 1'alphabet. Ainsi, $10_{10} = A_{16}$, ..., $15_{10} = F_{16}$.
Effectuer les conversions suivantes :
$A3F_{16} = ???_{10}$
$1729_{10} = ???_{16}$

### 2.4 Arithmétique en base $b$

Dans toutes les bases, l'addition et la multiplication s'effectuent comme en base 10. Le point important est de prendre garde aux retenues.

2.9 Exercice Poser et effectuer les opérations suivantes : $A_{16} + B_{16}$ et $342_5 \times 43_5$.

## 3 Relation de congruence

Toutes les preuves de cette partie sont en exercice.

### 3.1 Définition, premières propriétés

3.1 DÉFINITION
Soit *$m$ un entier naturel. On* dit *que deux entiers relatifs $a$ et $b$ sont* congrus modulo $m$ *(et on note $a \equiv b \pmod m$* ou *$a \equiv b[m]$) si $b - a$ est un multiple de $m$.*

---

3.2 REMARQUE
- $a \equiv b \pmod 0$ si et seulement si $a = b$.
- Pour tout couple d'entiers $a$, $b \in \mathbb{Z}$, $a \equiv b \pmod 1$.
- $a \equiv 0 \pmod m$ si et seulement si $m|a$.
- $a \equiv b \pmod m$ si et seulement si $b \equiv a \pmod m$.

3.3 PROPOSITION
*Deux entiers sont congrus modulo $m$ si et seulement si leurs divisions euclidiennes par $m$ ont même reste.*

3.4 PROPOSITION
*Si $a \equiv b \pmod m$ et $b \equiv c \pmod m$ alors $a \equiv c \pmod m$.*

3.5 PROPOSITION
Soient $a$, $b$, $a'$ et $b'$ *des entiers relatifs*, $m$ *un entier naturel, avec* $a \equiv b \pmod{m}$ *et* $a' \equiv b' \pmod{m}$.
On a alors $a + a' \equiv b + b' \pmod{m}$ *et* $aa' \equiv bb' \pmod{m}$.

3.6 PROPOSITION
*Si* $a \equiv b \pmod{m}$ *alors pour tout entier naturel* $n$, $a^n \equiv b^n \pmod{m}$

**Application :** Si je veux calculer $a^n \bmod m$, j'ai intérêt à réduire le résultat au fur et à mesure. Ainsi, si je veux calculer $5^4 \bmod 11$ :
. $5^2 \equiv 25 \equiv 3 \pmod{11}$,
. $5^3 \equiv 5^2 \times 5 \equiv 3 \times 5 \equiv 15 \equiv 4 \pmod{11}$,
. $5^4 \equiv 5 \times 4 \equiv 20 \equiv 9 \pmod{11}$.

3.7 Exercice En remarquant que $3^2 \equiv 1 \pmod{8}$, montrer que
$$3^n \equiv \begin{cases} 3 \pmod 8 \text{ si } n \equiv 0 \pmod 2 \\ 1 \pmod 8 \text{ si } n \equiv 1 \pmod 2 \end{cases}$$

3.8 Exercice Calculer $2^{1025} \bmod 5$.

## 3.2 Critères de divisibilité

3.9 PROPOSITION
Soit $n$ un entier dont l'écriture *en base* 10 *est* $n_d n_{d-1} \dots n_0$, c' est-à-dire que

$$n = 10^d n_d + \cdots + n_0.$$

- $n$ *est un multiple de* 2 *si et seulement si* $n_0 \equiv 0 \pmod{2}$.
- $n$ *est un multiple de* 3 *si et seulement si* $n_d + \cdots + n_0 \equiv 0 \pmod{3}$.
- $n$ *est un multiple de* 5 *si et seulement si* $n_0 \equiv 0 \pmod{5}$.
- $n$ *est un multiple de* 9 *si et seulement si* $n_d + \cdots + n_0 \equiv 0 \pmod{9}$.
- $n$ *est un multiple de* 10 *si et seulement si* $n_0 \equiv 0 \pmod{10}$.

3.10 COROLLAIRE
- *Un entier est un multiple de* 2 *s'il se termine par* $0, 2, \dots, 8$.
- *Un entier est un multiple de* 5 *s'il se termine par* 0 *ou* 5.
- *Un entier est un multiple de* 10 *s'il se termine par* 0.

---

3.11 Exercice Énoncer (et démontrer) les critères de divisibilité par 4 et par 11 d'un nombre écrit en base 10.

# 4 PGCD et algorithme d'Euclide

**4.1 PROPOSITION**
*Soient* $(a,\ b) \neq (0,0) \in \mathbb{Z}^2$

- *Soit* $d \in \mathbb{Z}$. *Si* $d|a$ *et* $d|b$ *alors* $d \leq max(|a|,\ |b|)$.
- *Si de plus* $a \neq 0$ *et* $b \neq 0$, *alors* $d \leq \min(|a|,\ |b|)$.

*Démonstration:* Exercice ∎

**4.3 COROLLAIRE**
*Soient* $(a,\ b) \neq (0,\ 0) \in \mathbb{Z}^2$ . *L' ensemble des diviseurs communs à a et b est non vide* (*car contient* 1) et fini. En particulier il admet un plus grand élément.

---

**4.4 DÉFINITION**
Soient $(a,\ b) \in \mathbb{Z}^2$. *Le PGCD de a et b, noté* $a \wedge b$ *ou pgcd* $(a,\ b)$ *est* :
*le plus grand des diviseurs communs à a et b lorsque* $(a,\ b) \neq (0,\ 0)$
est égal à 0 *lorsque* $a = b = 0$.

---

**4.5 DÉFINITION**
*Deux entiers dont le pgcd vaut* 1 *sont dits* premiers entre eux.

---

**4.6 Exercice** Etant donnés deux entiers relatifs $a$ et $b$, montrer que $a \wedge b = |b| \wedge |b|$ et que $a \wedge 0 = |a|$.

On peut donc maintenant ne considérer que les cas où $a$ et $b$ sont des entiers naturels.

**4.7 PROPOSITION**
*Soit* $(a,\ b) \in \mathbb{N} \times \mathbb{N}^*$.
*Si r est le reste de la division euclidienne de a par b, alors on a* l'équivalence
$d|a$ *et* $d|b \Leftrightarrow d|b$ et $d|r$.
En particulier, $a \wedge b = b \wedge r$.

*Démonstration:* Si $d|a$ et $d|b$, on écrit la division euclidienne de $a$ par $b$ : $a = bq + r$.
Soit $k$ et $l$ les entiers tels que $a = dk$ et $b = dl$. Alors en remplaąant on obtient

$$r = a\ - bq = dk - qdl\ = d(k - ql).$$

Donc $d|r$.
Réciproquement, si $b = dk$ et $r = dl$, alors $a = bq + r = d(qk + rl)$.

Méthode : On veut calculer le pgcd de $a$ et $b$. Quitte à les échanger, on peut supposer que $a \geq b$.

On sait que $a \wedge b = b \wedge r$. Comme $r < b \leq a$, on s'est ramené à un couple d'entiers plus petits. Il suffit de réitérer le procédé : c'est *algorithme d' Euclide*.

**Algorithme d'Euclide :**

*Entrées* : $(a,\ b) \in \mathbb{N}\times \in \mathbb{N}^*$

*Sortie* : $a \wedge b$

Etape 1 $x \leftarrow max(a,\ b)$

Etape 2 $y \leftarrow \min(a,\ b)$

Etape 3 Tant que $y \neq 0$ faire

3.a $r \leftarrow$ reste de la division de $x$ par $y$

3.b $x \leftarrow y$

3.c $y \leftarrow r$

**Fin de la boucle Tant que**

Etape 4 **Retourner** : $x$.

**FIN.**

Vérifier qu'un algorithme est correct revient à vérifier

. qu'il se termine en temps fini ;

. qu'il retourne bien le résultat annoncé.

4.9 Exercice Vérifier que cet algorithme est correct, puis appliquer le pour calculer $12 \wedge 15$ et $598 \wedge 414$.

# 5 Théorème de Bézout

5.1 Théorème (Théorème de Bézout)

Soit $a$ et $b$ *deux entiers relatifs*. Il existe des entiers relatifs $u$ *et* $v$ tels que

$$au\ + bv = a\ \wedge b.$$

---

5.2 Remarque

- Les coefficients $u$ et $v$ du théorème sont loin d'être uniques. En général, il y en a une infinité. Essayer d'en trouver rapidement quelques uns pour $a = 3$ et $b = 2$.
- On peut trouver une paire de coefficients $(u,\ v)$ convenables (on parle de *coefficients de Bézout*) à l'aide de l'algorithme d'Euclide.
- Reprenons l'exemple $a = 598$ et $b = 414$ :

  . $598 = 1\times\ 414+184$

  . $414 = 2\times\ 184+46$

  . $184 = 4 \times 46 + 0$

  Pour trouver les coefficients $u$ et $v$ tels que $46 = 598u + 414v$, on effectue maintenant la "remontée" :

  . $414 = 2 \times 184 + 46 \Rightarrow 46 = 414 - 2 \times 184$

  . $598 = 1 \times 414 + 184 \Rightarrow 184 = 598 - 414 \Rightarrow 46 = 414 - 2 \times (598 - 414)$

  . donc finalement :

  $$46 = -2 \times 598 + 3 \times 414.$$

5.3 Exercice Appliquer cette méthode aux couples $(12, 15)$ et $(598, 414)$.

Le théorème de Bézout permet de déduire les corollaires suivants, dont la démonstration est en exercice.

5.4 Corollaire (Identité de Bézout)
*Les entiers $a$ et $b$ sont premiers entre eux si et seulement si il existe $(u, v) \in \mathbb{Z}^2$ tels que $au + bv = 1$*

---

5.5 Corollaire
*Les diviseurs communs à $a$ et $b$ sont les diviseurs de $a \wedge b$.*

---

5.6 Corollaire (Théorème de Gauss)
*. Soient $a$, $b$ et $c$ des entiers non nuls. .*

- *Si $a|bc$ et $a \wedge b = 1$ alors $a|c$.*
- *Si $a|c$, $b|c$ et $a \wedge b = 1$ alors $ab|c$.*

---

5.7 Exercice Chacune des hypothèses du théorème de Gauss est importante.

- Trouver trois entiers $a$, $b$, $c$ tels que $a|bc$ mais $a \nmid b$ et $a \nmid c$.
- Trouver trois entiers $a$, $b$, $c$ tels que $a|c$ et $b|c$ mais $ab \nmid c$.

# 6 PPCM

Soient $a$ et $b$ deux entiers relatifs. Si $ab \neq 0$, alors l'ensemble des multiples strictement positifs communs à $a$ et $b$ est une partie de $\mathbb{N}$, non vide car elle contient $|ab|$.

6.1 Définition
*Le PPCM de $a$ et $b$, noté $a \vee b$ ou $ppcm(a, b)$ est :*
*. le plus petit des multiples strictement positifs communs à $a$ et $b$ lorsque $ab \neq 0$ ;*
*. $0$ si $a = 0$ ou $b = 0$.*

---

On a vu comment calculer le pgcd de deux entiers. A partir de là, il est aisé de trouver leur ppcm.

6.2 Lemme
*Si $a \wedge b = 1$ alors $a \vee b = ab$.*

*Démonstration:* Dans le cas où $ab = 0$, c'est évident.
On suppose donc maintenant que $a \neq 0$ et $b \neq 0$.
Si $m$ est un multiple strictement positif de $a$ et $b$, alors d'après le théorème de Gauss, $m$ est un multiple de $ab$. Donc en particulier $ab \leq m$.
Tout multiple strictement positif commun à $a$ et à $b$ est plus grand que ab, et ab est bien un multiple strictement commun à $a$ et à $b$ : c'est donc bien le ppcm. ∎

6.4 LEMME
*Si $d = a \wedge b$, soient $a'$ et $b'$ tels que $a = da'$ et $b = db'$. Alors $a' \wedge b' = 1$.*

*Démonstration:* Par l'absurde, si $u > 1$ est un diviseur commun à $a'$ et $b'$, alors on écrit $a' = ua$" et $b' = ub$ ". Alors $a = (du)a$ " et $b = (du)b$ ", ce qui montre que $du$ est un diviseur commun à $a$ et $b$ avec $du > d$. Ceci contredit le fait que $d$ soit le pgcd de $a$ et $b$. ■

6.6 LEMME
*Soient a et b deux entiers. On note d leur pgcd. Soient $a'$ et $b'$ les entiers premiers entre eux tels que $a = da'$ et $b = db'$. Alors*

$$a \vee b = da'b'.$$

*Démonstration:* Il est évident que $da'b' = ab' = a'b$ est un multiple commun de $a$ et $b$.

Soit $m$ un multiple de $a$ et de $b$. C'est donc un multiple de $d$ et on écrit $m = dm'$.

On a par hypothèse $da'|dm'$ avec $d \neq 0$ donc $a'|m'$. De même $b'|m'$. Comme $a' \wedge b' = 1$, le théorème de Gauss nous dit que $a'b'|m'$ et donc que $da'b'|dm'$. ■

6.8 PROPOSITION
*Soient a et b des entiers relatifs, on a*

$$ab = (a \wedge b)(a \vee b).$$

*Démonstration:* Exercice ■

6.10 COROLLAIRE
*Les multiples communs à a et b sont les multiples de $a \vee b$.*

---

*Démonstration:* Exercice ■

# 7 Equations aux congruences

Les démonstrations de cette partie sont à faire en exercice.

## 7.1 Inverse modulaire

7.1 THÉORÈME
*Soit $N > 1$ un entier et c un entier relatif.*

L'équation $cx \equiv 1 (\text{mod } N)$ *admet une solution si et seulement si c et N sont premiers entre eux.*

Dans ce cas là, on dit que *c est inversible modulo N* et qu'une solution $x$ est un inverse de $c$ modulo $N$.

---

*Démonstration:* Indication : utiliser l'identité de Bézout. ■

7.3 Exercice Résoudre les équations suivantes :

- $2x \equiv 1 (\text{mod } 3)$,
- $2x \equiv 1 (\text{mod } 4)$,
- $18x \equiv 1 (\text{mod } 53)$.

7.4 PROPOSITION
*Si $a$ est inversible modulo $N$, alors*

$$ax \equiv ay \ (\text{mod } N) \Leftrightarrow x \equiv y \ (\text{mod } N)$$

7.5 Exercice Trouver $x$ tel que $2x \equiv 0 (\text{mod } 6)$ mais $x \not\equiv 0 (\text{mod } 6)$

## 7.2 Résolution de l'équation $ax \equiv b (\text{mod } n)$

Soient $a$, $b$ et $n$ trois entiers avec $a$ et $n$ non nuls. On pose $d = pgcd(a, n)$.

7.6 PROPOSITION
Si $d \not| b$, alors l'équation $ax \equiv b (\text{mod } n)$ *n'admet pas de solution*.

7.7 PROPOSITION
Si $b$ est un multiple de $d$, soient $a'$, $b'$ et $n'$ tels que $a = da'$, $b = db'$ et $n = dn'$.
On *a alors*

$$ax \equiv b \ (\text{mod } n) \Leftrightarrow a'x \equiv b' \ (\text{mod } n')$$

7.8 PROPOSITION
*Si $A$ et $N$ sont premiers entre eux*, alors les solutions de l'équation $Ax \equiv B (\text{mod } N)$ *sont les entiers $x$ tels que $x \equiv BU (\text{mod } N)$, où $U$ est l'inverse de $A$ modulo $N$.*

7.9 Exercice Résoudre l'équation $3x \equiv 2 (\text{mod } 5)$.
Résoudre l'équation $6x \equiv 4 (\text{mod } 10)$.

## 7.3 Résolution dans $\mathbb{Z} \times \mathbb{Z}$ de $ax + by = c$

Soient $a$, $b$ et $c$ trois entiers relatifs, avec $a$ et $b$ non nuls.
On considère léquation $E : ax + by = c$. On note $S$ l'ensemble de ses solutions, c'est-à-dire

$$S = \{(x, y) \in \mathbb{Z}^2 \mid ax + by = c\}.$$

On pose $d$ le pgcd de $a$ et $b$, et $a'$ et $b'$ les entiers tels que $a = a'd$ et $b = b'd$.

7.10 PROPOSITION
*Si $d \not| c$ alors $S = \emptyset$.*

On suppose dans la suite que $d|c$ et soit $c'$ tel que $c = c'd$.

7.11 PROPOSITION

$$ax + by = c \Leftrightarrow a'x + b'y = c'.$$

7.12 PROPOSITION
*L'algorithme d'Euclide permet de trouver une paire $(x_0, y_0)$ solution de $E$.*

7.13 PROPOSITION

*L'ensemble des solutions de l'équation E est*

$$S = \{(x_0 + b'k,\ y_0 - a'k) | k \in \mathbb{Z}\}.$$

7.14 Exercice Résoudre dans $\mathbb{Z} \times \mathbb{Z}$

$$27x + 45y = 63.$$