Cours élémentaire d'arithmétique

Valentin Vinoles

décembre 2009

Introduction

« *Wir müssen wissen. Wir werden wissen.* »
(Nous devons savoir. Nous saurons.)
David Hilbert

Voici un document présentant les principales définitions et résultats d'arithmétique élémentaire, dans le sens où l'appel à des notions d'algèbre générale, comme l'anneau $\mathbf{Z}/n\mathbf{Z}$, est exclu. Il s'adresse donc à des terminales et à des premières années d'études supérieures, en L1 scientifique ou en maths sup'.

On y présente tout d'abord les notions de base de l'arithmétique qui sont la divisibilité et la division euclidienne. Tout cela est ensuite interprété dans le puissant langage des congruences. On applique alors tout cela pour établir des critères de divisibilités.
Ensuite, on insiste sur la notion de Plus Grand Commun Diviseur (PGCD) et d'entiers premiers entre eux. On y voit notamment le théorème de Bézout qui établit un lien fondamental entre calcul algébrique et propriété arithmétique. On y présente également une section sur les simplifications et l'inversion dans les congruences et la notion de Plus Petit Commun Multiple (PPCM).
Enfin, avec tous les outils vu jusqu'alors, on étudie les nombres premiers, qui sont en quelques sortes les briques fondamentales permettant de construire les entiers. On y voit notamment le théorème fondamental de l'arithmétique et on expose une démonstration du célèbre théorème de Fermat.
À la fin, on trouve la résolution de l'équation diophantienne $ax + by = c$ qui en quelque sorte résume bien le cours.

J'espère que ce document vous sera utile et j'attends avec plaisir toute remarque, correction et suggestion que vous pouvez m'envoyer sur mon adresse email.

Bonne lecture !

Valentin Vinoles

Table des matières

1 Divisibilité **3**
1.1 Définition . . . 3
1.2 Propriétés . . . 3

2 Division euclidienne **4**
2.1 Définition-théorème . . . 4
2.2 Algorithme de calcul . . . 4

3 Congruences **5**
3.1 Définition . . . 5
3.2 Lien avec la division euclidienne . . . 5
3.3 Propriétés . . . 5
3.4 Critères de divisibilité . . . 6

4 Plus grand commun diviseur **7**
4.1 Définition . . . 7
4.2 Algorithme d'Euclide . . . 7
4.2.1 Théorie algorithmique . . . 7
4.2.2 Calcul pratique, disposition . . . 7
4.3 Propriétés du PGCD . . . 7

5 Entiers premiers entre eux **9**
5.1 Définition . . . 9
5.2 Propriétés . . . 9
5.3 Théorème de Bézout . . . 9
5.3.1 Identité de Bézout . . . 9
5.3.2 Calcul du couple dans l'identité de Bézout . . . 10
5.3.3 Théorème de Bézout . . . 11
5.4 Lemme de Gauss . . . 11
5.5 Simplification et inversion dans les congruences . . . 11

6 Plus petit commum multiple **12**
6.1 Définition . . . 12
6.2 Lien entre PGCD et PPCM . . . 12
6.3 Propriétés du PPCM . . . 12

7 Nombre premier **13**
7.1 Définition . . . 13
7.2 Propriétés . . . 13
7.3 Deux théorèmes fondamentaux . . . 13

8 Théorème de Fermat **16**

9 L'équation diophantienne $ax + by = c$ **17**
Références18

1 Divisibilité

1.1 Définition

Définition. Soient a et b deux entiers. On dit que a *divise* b si, et seulement si, il existe un entier k tel que $b = ak$, et l'on note $a|b$. On dit aussi que b est un *multiple* de a.

Exemple. $3|12$ car $12 = 3 \times 4$.

Définition. Si un entier est divisible par 2, il est dit *pair*, sinon il est dit *impair*.

1.2 Propriétés

Proposition. Ici, a, b, c, a' et b' désignent des entiers quelconques.

1. On a $a|a$, $a|0$ et $1|a$.
2. Si $0|a$, alors $a = 0$ et si $a|1$ alors $a = \pm 1$.
3. Si $a|b$, alors $-a|b$.
4. Si $a|b$ et $b \neq 0$, alors $|a| \leqslant |b|$. Ainsi tout entier admet un nombre fini de diviseurs.
5. Si $a|b$ et $b|a$, alors $|a| = |b|$.
6. Si $a|b$ et $b|c$, alors $a|c$ (transitivité).
7. Si $a|b$ et $a|c$, alors $a|(\lambda b + \mu c)$ avec λ et μ deux entiers quelconques. En particulier, on a$a|(b+c)$, $a|(b-c)$ et $a|(c-b)$.
8. Si $a|b$, alors $a|bc$.
9. Si $a|b$, alors $ac|bc$.
10. Si $a|b$ et $a'|b'$, alors $aa'|bb'$. En particulier $a^n|b^n$ pour n un entier naturel non nul.

Démonstration.

1. Comme $a = 1 \times a$, on a $a|a$. De plus, $0 = 0 \times a$ donc $a|0$. Et $a = a \times 1$ donc $1|a$.
2. Si $0|a$, alors il existe un entier k tel que $a = k \times 0 = 0$, donc $a = 0$. Si $a|1$ alors il existe un entier k tel que $1 = k \times a$, donc nécessairement $a = \pm 1$.
3. Si $a|b$, alors il existe un entier k tel que $b = k \times a$. On a donc $b = (-k) \times (-a)$, c'est-à-dire $-a|b$.
4. Si $a|b$, alors il existe un entier k tel que $b = k \times a$, c'est-à-dire $|b| = |k| \times |a|$. Or $b \neq 0$ et $|k| \geqslant 1$, donc $|a| \leqslant |b|$.
5. D'après 4., si $a|b$ et $b|a$ alors $|a| \leqslant |b|$ et $|b| \leqslant |a|$ d'où $|a| = |b|$.
6. Si $a|b$ et $b|c$, alors il existe deux entiers k et k' tels que $b = k \times a$ et $c = k' \times b$. On a donc $c = (kk') \times a$, c'est-à-dire $c|a$.
7. Si $a|b$ et $b|c$, alors il existe deux entiers k et k' tels que $b = k \times a$ et $c = k' \times b$. Pour deux entiers λ et μ, on a donc $\lambda b + \mu c = (\lambda k + \mu k') \times a$, c'est-à-dire $a|(\lambda b + \mu c)$.
8. Si $a|b$, alors il existe un entier k tel que $b = k \times a$. On a donc $bc = (kc) \times a$, c'est-à-dire $a|bc$.
9. Si $a|b$, alors il existe un entier k tel que $b = k \times a$. On a donc $bc = k \times (ac)$, c'est-à-dire $ac|bc$.
10. Si $a|b$ et $a'|b'$, alors il existe deux entiers k et k' tels que $b = k \times a$ et $b' = k' \times a'$. On a donc $bb' = (kk') \times aa'$, c'est-à-dire $aa'|bb'$. □

2 Division euclidienne

2.1 Définition-théorème

Théorème (Division euclidienne)**.** Soit a un entier et b un entier naturel non nul. Alors il existe deux entiers q (appelé *quotient*) et r (appelé *reste*) tels que $a = bq + r$ et $0 \leqslant r < b$. De plus, les entiers q et r sont uniques.

Démonstration. Démontrons tout d'abord l'existence. Soit E l'ensemble des entiers k tel que $a \geqslant bk$. Si $a \geqslant 0$ alors $0 \in E$ et si $a < 0$, alors $a \in E$. L'ensemble E n'est donc pas vide. Si $a \geqslant 0$, tous les éléments de E sont inférieurs à a. Si $a < 0$, tous les éléments de E sont inférieurs à $-a$. L'ensemble E est donc majoré.
L'ensemble E est une partie de $\mathbf{Z}$ non vide et majorée, il admet donc un plus grand élément noté q. On pose alors $r = a - bq$.
Comme $q \in E$, on a $a \geqslant bq$, donc $r \geqslant 0$. Et comme $q + 1 \notin E$ (car sinon q ne serait pas le plus grand élément de E), on obtient $a < b(q + 1)$ puis $a < bq + b$, d'où $a - bq < b$, c'est-à-die $r < b$. Le couple d'entiers q et r ainsi construit convient.

Démonstrons maintenant l'unicité. Supposons que deux couples d'entiers q, r et q', r' conviennent. On a $a = bq + r = bq' + r'$, d'où $b(q - q') = r' - r$. Or $-b < r' - r < b$ puisque $0 \leqslant r < b$ et $0 \leqslant r' < b$. On déduit des deux relations précédentes que $-1 < q - q' < 1$. Un entier strictement compris entre -1 et 1 est nécessairement égal à 0 donc $q - q' = 0$, c'est-à-dire $q = q'$. De plus, comme $b(q - q') = r' - r$ et $b \neq 0$, on obtient $r - r' = 0$, c'est-à-dire $r = r'$. □

2.2 Algorithme de calcul

En pratique, on effectue la division comme nous l'avons appris à l'école primaire, en nous arrêtant dès que le reste est strictement inférieur au quotient.

Exemple. Effectuons la division euclidienne de 6359 par 17.

$$\begin{array}{cccc|cc} 6 & 3 & 5 & 9 & & 1\ \ 7 \\ \hline & & & & & \\ & & & & & \end{array}$$

$$\begin{array}{cccc|cc} & 6 & 3 & 5 & 9 & & 1\ \ 7 \\ \hline - & 5 & 1 & & & 3 & \\ \hline & 1 & 2 & & & & \end{array}$$

$$\begin{array}{cccc|cc} & 6 & 3 & 5 & 9 & & 1\ \ 7 \\ \hline - & 5 & 1 & & & 3\ \ 7 & \\ \hline & 1 & 2 & 5 & & & \\ - & 1 & 1 & 9 & & & \\ \hline & & & 6 & & & \end{array}$$

$$\begin{array}{cccc|cc} & 6 & 3 & 5 & 9 & & 1\ \ 7 \\ \hline - & 5 & 1 & & & 3\ \ 7\ \ 4 & \\ \hline & 1 & 2 & 5 & & & \\ - & 1 & 1 & 9 & & & \\ \hline & & & 6 & 9 & & \\ & & - & 6 & 8 & & \\ \hline & & & & 1 & & \end{array}$$

Conclusion : $6359 = 17 \times 374 + 1$.

3 Congruences

3.1 Définition

Définition. Soit n un entier naturel non nul et soient a et b deux entiers. On dit que a et b sont *congrus modulo* n si, et seulement si, $n|(b-a)$. On note alors $a \equiv b \pmod{n}$ ou $a \equiv b\ [n]$.

3.2 Lien avec la division euclidienne

Théorème. Soit n un entier naturel non nul et soient a et b deux entiers. Alors $a \equiv b \pmod{n}$ si, et seulement si, a et b ont même reste dans la division euclidienne par n.

En particulier, on remarque que $b|a$ si, et seulement si, $a \equiv 0 \pmod{b}$ si, et seulement si, le reste la division euclidienne de a par b est nul.

Démonstration. Supposons $a \equiv b \pmod{n}$. Il existe un entier k tel que $b-a=kn$. Il existe deux entiers q et r tels que $a=nq+r$ avec $0 \leqslant r < n$. On a donc $b=n(q+k)+r$, toujours avec $0 \leqslant r < n$, ce qui montre que a et b ont le même reste dans la division euclidienne par n.
Réciproquement, supposons que a et b ont le même reste dans la division euclidienne par n. Il existe donc des entiers r, q et q' tels que $a=nq+r$ et $b=nq'+r$ avec $0 \leqslant r < n$. On a donc $b-a=n(q-q')$, c'est-à-dire $n|(b-a)$ et donc $a \equiv b \pmod{n}$. □

3.3 Propriétés

Proposition. Ici, a et b désignent des entiers, et n et m des entiers naturels non nuls.

1. $a \equiv a \pmod{n}$ (réflexivité).
2. $a \equiv b \pmod{n} \iff b \equiv a \pmod{n}$ (symétrie).
3. Si $a \equiv b \pmod{n}$ et $b \equiv c \pmod{n}$, alors $a \equiv c \pmod{n}$ (transitivité).
4. Si $a \equiv b \pmod{n}$ et si $m|n$, alors $a \equiv b \pmod{m}$.

Démonstration.

1. On a $a-a=0$. Or $n|0$, d'où $a \equiv a \pmod{n}$.
2. $a \equiv b \pmod{n} \iff n|(b-a) \iff n|(a-b) \iff b \equiv a \pmod{n}$.
3. Si $a \equiv b \pmod{n}$ et $b \equiv c \pmod{n}$, alors $n|(b-a)$ et $n|(c-b)$ donc $n|((b-a)+(c-b))$, c'est-à-dire $n|(c-a)$, d'où $a \equiv c \pmod{n}$.
4. Si $m|n$, alors il existe un entier k tel que $n=km$, et si $a \equiv b \pmod{n}$, alors il existe un entier k' tel que $b-a=k'n$. On a donc $b-a=kk'm$, c'est-à-dire $m|(b-a)$, d'où $a \equiv b \pmod{m}$. □

Proposition (Règles de calcul avec les congruences)**.** Ici, a, b, c et d désignent des entiers, et n un entier naturel non nul.

1. Si $a \equiv b \pmod{n}$ et $c \equiv d \pmod{n}$, alors $a+c \equiv b+d \pmod{n}$.
2. Si $a \equiv b \pmod{n}$ et $c \equiv d \pmod{n}$, alors $ac \equiv bd \pmod{n}$. En particulier, si $a \equiv b \pmod{n}$, alors $a^k \equiv b^k \pmod{n}$ où k est un entier naturel non nul.

Démonstration.

1. Si $a \equiv b \pmod{n}$ et $c \equiv d \pmod{n}$, alors il existe deux entiers α et β tels que $b-a=\alpha n$ et $d-c=\beta n$. On a donc $(b+d)-(a+c)=(b-a)+(d-c)=(\alpha+\beta)n$, d'où $a+c \equiv b+d \pmod{n}$.
2. Si $a \equiv b \pmod{n}$ et $c \equiv d \pmod{n}$, alors il existe deux entiers α et β tels que $b-a=\alpha n$ et $d-c=\beta n$. On a donc $bd-ac=(a+\alpha n)(c+\beta n)-ac=(\alpha c+\beta a+\alpha\beta n)n$, d'où $ac \equiv bd \pmod{n}$. □

3.4 Critères de divisibilité

Nous avons maintenant les outils nécessaires pour énoncer quelques critères de divisibilités.

Proposition (Critère de divisibilité par 2)**.** Un entier est divisible par 2 si, et seulement si, son chiffre des unités est divisible par 2.

Exemple. 13 484 est divisible par 2 car 4 l'est.

Démonstration. Soit a un entier. Il existe deux entiers q et r tels que $a = 10q + a_0$ avec $0 \leqslant r < 10$. Ici, r est le chiffre des unités de a. Si $2|a$, alors il existe un entier k tel que $a = 2k$. On a donc $r = 2k - 10 \equiv 0 - 0 = 0 \pmod 2$, car $2|2k$ et $2|10$. Réciproquement si $2|r$, alors $a = 10q + r \equiv 0 \pmod 2$, c'est-à-dire $2|a$. □

Proposition (Critère de divisibilité par 3)**.** Un entier est divisible par 3 si, et seulement si, la somme de ses chiffres est divisible par 3.

Exemple. 11 124 est divisible par 3 car $1 + 1 + 1 + 2 + 4 = 9$ l'est.

Démonstration. Soit a un entier. On peut l'écrire sous la forme $a = a_0 + a_1 \times 10 + \ldots + a_n \times 10^n$ avec a_i des entiers vérifiant $0 \leqslant a_i < 10$. Ici, les a_i sont les chiffres de a. Comme $10 \equiv 1 \pmod 3$, on a $a \equiv a_0 + \cdots + a_n \pmod 3$. Ceci montre que $a \equiv 0 \pmod 3$ si, et seulement si, $a_0 + a_1 + \cdots + a_n \equiv 0 \pmod 3$, c'est à dire que $3|a$ si, et seulement si, $3|(a_0 + a_1 + \cdots + a_n)$. □

On montre de la même manière les critères suivants :

Proposition (Critère de divisibilité par 5)**.** Un entier est divisible par 5 si, et seulement si, son chiffre des unités est divisible par 5.

Exemple. 3249 est divisible par 9 car 3+2+4+9=18 l'est. 725 est divisible par 5 car 5 l'est.

Proposition (Critère de divisibilité par 9)**.** Un entier est divisible par 9 si, et seulement si, la somme de ses chiffres est divisible par 9.

Exemple. 13311 est divisible par 9 car $1 + 3 + 3 + 1 + 1 = 9$ l'est.

Proposition (Critère de divisibilité par 11)**.** Un entier est divisible par 11 si, et seulement si, la différence entre la somme de ses chiffres de rang impairs (en partant des unités) et la somme de ses chiffres de rang pairs est divisible par 11.

Exemple. 54 967 est divisible par 11 car $(7 + 9 + 5) - (6 + 4) = 11$ l'est.

4 Plus grand commun diviseur

4.1 Définition

Définition. Soient a et b deux entiers naturels non nuls. On note $\mathcal{D}(a,b)$ l'ensemble des diviseurs positifs communs à a et b. Cet ensemble n'est pas vide (il contient 1) et est majoré par $\max(a,b)$. Il admet donc un plus grand élément appelé *plus grand commun diviseur* de a et b. On le note $a \wedge b$ ou $\mathrm{PGCD}(a,b)$.

On étend la définition pour a et b des entiers relatifs non nuls en posant $a \wedge b = |a| \wedge |b|$.

Exemple. $24 \wedge 36 = 12$.

4.2 Algorithme d'Euclide

4.2.1 Théorie algorithmique

Soient a et b deux entiers naturels non nuls. On suppose que $a \geqslant b$. On va construire un algorithme de calcul de $a \wedge b$.

Supposons $b|a$. Puisque l'on a aussi $b|b$, b est un diviseur commun de a et b, donc appartient à $\mathcal{D}(a,b)$. Et b est clairement le plus grand diviseur de b. On a donc $a \wedge b = b$.
Supposons maintenant que b ne divise pas a. Il existe alors deux entiers naturels q_1 et r_1 tels que $a = bq_1 + r_1$ avec $0 < r_1 < b$.

Montrons que $a \wedge b = b \wedge r_1$. Soit c un entier. Si $c|a$ et $c|b$, alors $c|r_1$ car $r_1 = a - bq_1$. Réciproquement, si $c|b$ et $c|r_1$, alors $c|a$ car $a = bq_1 + r_1$. Ceci montre que $\mathcal{D}(a,b) = \mathcal{D}(b,r_1)$. Ainsi, on a $a \wedge b = b \wedge r_1$.

Si $r_1|b$, alors $a \wedge b = b \wedge r_1 = r_1$ et l'algorithme est terminé. Si r_1 ne divise pas b, on réitère alors le procédé. On a alors $b = r_1 q_2 + r_2$ avec q_2 et r_2 des entiers naturels tels que $0 < r_2 < r_1$; et ainsi de suite, avec $a \wedge b = b \wedge r_1 = r_1 \wedge r_2$, etc...

Or nous avons $b > r_1 > r_2 > \ldots$, c'est-à-dire une suite strictement décroissante d'entiers naturels, qui ne peut donc être infini. Un reste r_{n+1} va donc finir par être nul, alors que r_n ne le sera pas. D'après ce qui précède, on aura alors

$$a \wedge b = b \wedge r_1 = r_1 \wedge r_2 = \ldots = r_{n-1} \wedge r_n = r_n.$$

4.2.2 Calcul pratique, disposition

En pratique on effectue des divisions euclidiennes successives du quotient par le reste de la division euclidienne antérieure et le PGCD est le dernier reste non nul.

Exemple. Calculons $264 \wedge 168$.

$$\begin{aligned} 264 &= 168 \times 1 + 96 \\ 168 &= 96 \times 1 + 72 \\ 96 &= 72 \times 1 + 24 \\ 72 &= 24 \times 3 + 0. \end{aligned}$$

On a donc $264 \wedge 168 = 24$.

4.3 Propriétés du PGCD

Proposition. Ici, a, b et k désignent des entiers non nuls.

1. $a \wedge 1 = 1$ et $a \wedge a = a$.
2. $a \wedge b = b \wedge a$ (symétrie).
3. $a|b \iff a \wedge b = a$.

4. $ka \wedge kb = |k| \times (a \wedge b)$.
5. Si $k|a$ et $k|b$ alors $k|(a \wedge b)$.

Démonstration.

1. Le seul diviseur de 1 est lui-même, donc $a \wedge 1 = 1$. La deuxième propriété découle directement du fait que $a|a$.
2. Évident.
3. Si $a|b$ alors $a \in \mathcal{D}(b)$. Or a est le plus grand diviseur de a, donc $a|b \iff a \wedge b = a$.
4. Lors de l'algorithme d'Euclide, si on multiplie a par k alors tous les restes sont multipliés par $|k|$, et en particulier le dernier reste non nul qui est le PGCD. D'où $ka \wedge kb = |k| \times (a \wedge b)$.
5. Si $k|a$ et $k|b$ alors $k \in \mathcal{D}(a) \cap \mathcal{D}(b)$. En particulier k divise le plus grand élément, donc $k|(a \wedge b)$. □

5 Entiers premiers entre eux

5.1 Définition

Définition. Soient a et b deux entiers non nuls. On dit que a et b sont *premiers entre eux* si, et seulement si, $a \wedge b = 1$.

5.2 Propriétés

Proposition. Ici, a, b et c désignent des entiers non nuls.

1. Tout entier est premier avec 1.
2. Si $a \wedge b = 1$ et $c|b$ alors $a \wedge c = 1$.
3. Soit D un entier naturel non nul. $D = a \wedge b$ si, et seulement si, il existe deux entiers relatifs a' et b' premiers entre eux tels que $a = a'D$ et $b = b'D$.
4. $a \wedge b = 1$ et $a \wedge c = 1$ si, et seulement si, $a \wedge (bc) = 1$.
5. a est premier avec b si, et seulement si, a^n l'est avec b^m pour n et m des entiers naturels non nuls quelconques.

Démonstration.

1. Le seul diviseur de 1 est lui-même, donc pour tout entier non nul a, $a \wedge 1 = 1$.
2. Pour d un entier naturel non nul, si $d|a$ et $d|c$ alors $d|a$ et $d|b$ par transitivité. Donc $d = 1$, et $a \wedge c = 1$.
3. Supposons $D = a \wedge b$. Par définition, $D|a$ et $D|b$. Donc il existe a' et b' dans $\mathbf{Z}$ tels que $a = a'D$ et $b = b'D$. On a donc d'après les propriétés du PGCD :

$$D = a \wedge b = a'D \wedge b'D = |D|(a' \wedge b') = D(a' \wedge b')$$

   Et en simplifiant par D il vient $a' \wedge b' = 1$. Réciproquement, supposons qu'il existe deux entiers relatifs a' et b' premiers entre eux tels que $a = a'D$ et $b = b'D$. Donc $a' \wedge b' = 1$. D'où

$$a \wedge b = a'D \wedge b'D = |D|(a' \wedge b') = D \times 1 = D$$

   donc D est bien le PGCD de a et de b.
4. Supposons $a \wedge b = a \wedge c = 1$. D'après le théorème de Bézout (voir section suivante), il existe u, v, w et x des entiers tels que $au + bv = 1$ et $aw + cx = 1$. On en déduit que

$$1 = (au + bv)(aw + cx) = (auw + vwb + uxc) \times a + (wx) \times (bc)$$

   donc d'après le théorème de Bézout, $a \wedge bc = 1$. Réciproquement, supposons $a \wedge bc = 1$. On a $b|bc$ et $c|bc$ donc d'après la propriété 2, on a $a \wedge b = 1$ et $a \wedge c = 1$.
5. Supposons $a \wedge b = 1$. D'après la proposition précédente, on a donc $a \wedge b^m$, puis $a^n \wedge b^m = 1$. Réciproquement, si $a^n \wedge b^m$ alors d'après la proposition précédente, $a^n \wedge b = 1$ puis $a \wedge b = 1$. □

5.3 Théorème de Bézout

5.3.1 Identité de Bézout

Théorème (Identité de Bézout)**.** Soient a et b deux entiers non nuls. Il existe deux entiers u et v tels que $au + bv = a \wedge b$.

Démonstration. Posons E l'ensemble des $am + bn$ avec m et n parcourant indépendamment $\mathbf{Z}$. On a $E \cap \mathbf{N}^*$ non vide car $a \in E$ (en prenant $m = 1$ et $n = 0$). $E \cap \mathbf{N}^*$ est une partie non vide de $\mathbf{N}^*$ donc admet un plus petit élément d.
Comme $d \in E$ il existe un couple d'entiers u et v tel que $au + bv = d$. Notons D l'ensemble des multiples positifs de d. Clairement on a $D \subset E \cap \mathbf{N}^*$.
Soit $x \in E \cap \mathbf{N}^*$. On effectue la division euclidienne de x par d : $x = dq + r$ avec $(q, r) \in \mathbf{Z}^2$ tel que $0 \leqslant r < d$. Comme $r = x - dq$ on a par différence de deux éléments de E, $r \in E$. Supposons $r \neq 0$. Alors $r \in E \cap \mathbf{N}^*$ ce

qui est absurde car $r < d$ qui est le plus petit élément de E. D'où $r = 0$ et donc $x = dq$ et par suite $x \in D$. Par suite $E \cap \mathbf{N}^* \subset D$ et par suite $D = E \cap \mathbf{N}^*$. Montrons alors que d est le PGCD de a et de b.
Soit $d' = a \wedge b$. On a $d'|a$ et $d'|b$ donc $d'|(au + bv)$ et donc $d'|d$. Comme a et b sont dans E on a $d|a$ et $d|b$ donc $d|d'$ et par suite comme d et d' sont positifs $d = d'$ et donc $d = a \wedge b$. □

5.3.2 Calcul du couple dans l'identité de Bézout

Soient a et b des entiers non nuls. Le théorème de Bézout nous indique qu'il existe deux entiers u et v tels que $au + bv = a \wedge b$. Nous cherchons une méthode pour déterminer u et v.

D'après l'algorithme d'Euclide, on a toute une série de relations de la forme

$$r_{k-1} = q_k r_k + r_{k+1} \qquad \text{où} \quad 0 \leqslant r_k < r_k \quad \text{et} \quad r_{k-1} \wedge r_k = r_k \wedge r_{k+1}$$

pour $k \in \{1, \dots, n\}$ tel que $r_{n+1} = 0$ et $a \wedge b = r_n$.
Posons maintenant la propriété $\mathcal{P}(k)$ suivante : il existe $(u_k, v_k) \in \mathbf{Z}^2$ tel que $r_n = u_k r_k + v_k r_{k-1}$. On va utiliser une récurrence descendante finie.

D'après ce qui précède, on a $r_{n-2} = r_{n-1}q_{n-1} + r_n$, c'est-à-dire $r_n = -q_{n-1}r_{n-1} + r_{n-2}$. Donc en posant $u_{n-1} = -q_{n-1}$ et $v_{n-1} = 1$, $\mathcal{P}(n-1)$ est vraie.

Pour $k \in \{2, \dots, n-1\}$, supposons $\mathcal{P}(k)$ vraie. Il existe donc $(u_k, v_k) \in \mathbf{Z}^2$ tel que $r_n = u_k r_k + v_k r_{k-1}$. Or on a $r_{k-2} = q_{k-1}r_{k-1} + r_k$, ce qui implique que

$$r_n = (-u_k q_{k-1} + v_k) r_{k-1} + u_k r_{k-2}.$$

En posant $u_{k-1} = -u_k q_{k-1} + v_k$ et $v_{k-1} = u_k$, on a $\mathcal{P}(k-1)$ vraie.

Par principe de récurrence, on a $\mathcal{P}(k)$ vraie pour tout $k \in \{1, \dots, n-1\}$. En particulier, pour $k = 1$, on a

$$a \wedge b = r_n = u_1 r_1 + v_1 r_0 = v_1 a + u_1 b.$$

Ceci fournit donc un couple (v_1, u_1) qui vérifie l'identité de Bézout.

En pratique, on effectue l'algorithme d'Euclide de a par b, puis on remonte les divisions successives.

Exemple. Prenons $a = 123$ et $b = 67$. Effectuons alors l'algorithme d'Euclide.

$$\begin{aligned} 123 &= 67 \times 1 + 56 \qquad (L_1) \\ 67 &= 56 + \times 111 \qquad (L_2) \\ 56 &= 11 \times 5 + 1 \qquad (L_3) \end{aligned}$$

Ceci montre tout d'abord que $a \wedge b = 1$. Remontons maintenant les divisions euclidiennes successives. On a d'après (L_3)

$$1 = 56 - 5 \times 11$$

puis en remplaçant 11 grâce à (L_2)

$$1 = 56 - 5 \times (67 - 56 \times 1) = 6 \times 56 - 5 \times 67$$

puis en remplaçant 56 grâce à (L_1)

$$1 = 6 \times (123 - 67) - 5 \times 67.$$

Finalement, on a

$$6 \times 123 + (-11) \times 67 = 1.$$

5.3.3 Théorème de Bézout

Théorème (Théorème de Bézout)**.** Deux entiers non nuls a et b sont premiers entre eux si, et seulement si, il existe $(u, v) \in \mathbf{Z}^2$ tel que $au + bv = 1$.

Démonstration. Si $a \wedge b = 1$ alors l'identité de Bézout montre bien qu'il existe $(u, v) \in \mathbf{Z}^2$ tel que $au + bv = 1$. Réciproquement, supposons qu'il existe $(u, v) \in \mathbf{Z}^2$ tel que $au + bv = 1$. Si il existe un d entier positif qui divise à la fois a et b, on a bien que d divise 1, c'est à dire que $d = 1$ et par suite a et b sont premiers entre eux. □

5.4 Lemme de Gauss

Théorème (Lemme de Gauss)**.** Soient a, b et c des entiers non nuls tels que a divise bc et que a soit premier avec b. Alors a divise c.

Démonstration. On a $a \wedge b = 1$ d'où $ac \wedge bc = |c|$. On a bien que a divise ac et, comme par hypothèse a divise bc, on a bien que $a|(ac \wedge bc)$. D'où a divise $|c|$ et par suite $a|c$. □

5.5 Simplification et inversion dans les congruences

Proposition. Soient $n \in \mathbf{N}^*$ et $a \in \mathbf{Z}^*$ tels que $a \wedge n = 1$. Pour tout $(x, y) \in \mathbf{Z}^2$, on a alors

$$ax \equiv ay \pmod{n} \Longrightarrow x \equiv y \pmod{n}.$$

Démonstration. La congruence implique que $n|[a(y - x)]$. Or $a \wedge n = 1$, donc d'après le théorème de Gauss, $n|(y - x)$, d'où $x \equiv y \pmod{n}$. □

Définition. Soit $n \in \mathbf{N}^*$. On dit $a \in \mathbf{Z}$ est *inversible* modulo n si et seulement s'il existe $b \in \mathbf{Z}$ tel que $ab \equiv 1 \pmod{n}$. Dans ce cas, b est appelé *inverse* de a modulo n.

Proposition. Soit $n \in \mathbf{N}^*$ et soit $a \in \mathbf{Z}$. Alors a est inversible modulo n si et seulement si $a \wedge n = 1$.

Démonstration. Si a admet $b \in \mathbf{Z}$ comme inverse modulo n, alors $ab \equiv 1 \pmod{n}$, d'où l'existence d'un $k \in \mathbf{Z}$ tel que $kn = 1 - ab$, c'est-à-dire $1 = kn + ab$. Le théorème de Bézout implique donc que $a \wedge n = 1$. Réciproquement, si $a \wedge n = 1$, alors d'après le théorème de Bézout, il existe $(u, v) \in \mathbf{Z}^2$ tel que $au + vn = 1$, et en passant modulo n on a $au \equiv 1 \pmod{n}$, c'est-à-dire que a admet u pour inverse modulo n. □

Remarquons que la preuve précédente donne un moyen de calcul explicite d'un inverse de a modulo n via le théorème de Bézout.

6 Plus petit commum multiple

6.1 Définition

Définition. Soient a et b deux entiers naturels non nuls. L'ensemble des multiples communs strictement positifs de a et b est une partie de $\mathbf{N}$ qui n'est pas vide. Il admet donc un plus petit élément appelé *plus petit commun multiple* de a et b. On le note $a \vee b$ ou $\mathrm{PPCM}(a, b)$.
On étend la définition à a et b entiers relatifs non nuls en posant $a \vee b = |a| \vee |b|$.

Exemple. $12 \vee 15 = 60$.

6.2 Lien entre PGCD et PPCM

Théorème. Soient a et b deux entiers non nuls. On a la relation suivante :

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

Démonstration. On pose $D = a \wedge b$. On pose $a' = a/D$ et $b' = b/D$ (c'est à dire que l'on prend le quotient de la division euclidienne de a par D et de b par D, les restes étant nuls car $D|a$ et $D|b$). D'après les propriétés sur le PGCD on a $a' \wedge b' = 1$. Posons m un multiple commun de a et b. Il existe donc deux entiers x et y tels que $m = xa = yb$. Et donc $m = a'Dx = b'Dy$ et par suite $a'x = b'y$.
On a donc $a'|b'y$ mais comme $a' \wedge b' = 1$ d'après le lemme de Gauss $a'|y$. Il existe donc un entier n tel que $y = a'n$. Par suite $m = a'b'Dn$.
Les multiples strictement positifs communs à a et à b sont de la forme $|a'b'|Dn$ pour n parcourant $\mathbf{N}^*$. L'ensemble des multiples communs est aussi l'ensemble des multiples de leur PPCM d'où :

$$(a \vee b) \times (a \wedge b) = |a'b'|D \times D = |a'D| \times |b'D| = |ab|. \qquad \square$$

6.3 Propriétés du PPCM

Proposition. Soient a, b et k des entiers non nuls.

1. $a \vee 1 = a$, $a \vee a = a$.
2. $a \vee b = b \vee a$ (commutativité).
3. $a|(a \vee b)$.
4. $ka \vee kb = |k| \times (a \vee b)$.
5. Si $a|b$ alors $a \vee b = b$.
6. Si $a|k$ et $b|k$ alors $(a \vee b)|k$.

Démonstration.

1. Le plus petit multiple de a est lui-même, et a est un multiple de 1, donc $a \vee 1 = a$. Et également $a \vee a = a$.
2. L'ensemble des multiples commun de a et b est bien celui de b et a.
3. Le plus petit commun multiple de a et b est en particulier un multiple de a, donc $a|(a \vee b)$.
4. Soit k un entier non nul. On sait que $(ka \wedge kb) \times (ka \vee kb) = |ka \times kb| = k^2|ab|$. Donc $(ka \wedge kb) \times (ka \vee kb) = k^2(a \wedge b) \times (a \vee b)$. Or on sait que $(ka \wedge kb) = |k|(a \wedge b)$ donc en simplifiant par $|k| \neq 0$ et $a \wedge b \neq 0$ il vient $ka \vee kb = |k|(a \vee b)$.
5. Si $a|b$, alors b est un multiple de a. C'est aussi un multiple de b. Or tout multiple n de b vérifie $n \geqslant b$. Donc le plus petit commun multiple de a et de b est b.
6. On a $a|k$ et $b|k$, donc k est un multiple de a et de b. Donc par définition, soit $k = 0$ et on a bien $(a \vee b)|k$, soit $k \geqslant (a \vee b)$. On effectue la division euclidienne de k par $a \vee b$ et on obtient un couple d'entiers (q, r) tel que
$$k = (a \vee b)q + r \quad \text{avec} \quad 0 \leqslant r < (a \vee b)$$
On a donc $r = k - (a \vee b)q$, donc comme k est un multiple de a et de b, on en déduit que r est un multiple de a et de b, donc par définition, soit $r = 0$ et on a $k = q(a \vee b)$ donc $(a \vee b)|k$, soit $r \geqslant (a \vee b)$, impossible car par division euclidienne $0 \leqslant r < (a \vee b)$. On a donc bien $(a \vee b)|k$. $\square$

7 Nombre premier

7.1 Définition

Définition. Un entier naturel p est dit *nombre premier* si, et seulement si, il admet deux diviseurs positifs distincts : 1 et lui-même. Le cas échéant il est dit *nombre composé*. On note $\mathbf{P}$ l'ensemble des nombres premiers.

Remarquons que d'après la définition, $1 \notin \mathbf{P}$.

Exemple. Les nombres premiers inférieurs à 100 classés dans l'ordre croissant sont

$$2,\ 3,\ 5,\ 7,\ 11,\ 13,\ 17,\ 19,\ 23,\ 29,\ 31,\ 37,\ 41,\ 43,\ 47,\ 53,\ 59,\ 61,\ 67,\ 71,\ 73,\ 79,\ 83,\ 89 \text{ et } 97.$$

7.2 Propriétés

Proposition. On prend $p \in \mathbf{P}$, a et b des entiers non nuls.

1. On a $p|a$ ou $p \wedge a = 1$.
2. Si $p|ab$ alors $p|a$ ou $p|b$.
3. Si $a \geqslant 2$, a admet un diviseur premier p.
4. Et si $a \notin \mathbf{P}$, alors $2 \leqslant p \leqslant \sqrt{a}$, où p désigne un diviseur premier quelconque de a.

Démonstration.

1. $p \wedge a$ est en particulier un diviseur de p : $(p \wedge a)|p$. Or p est premier donc il n'admet comme diviseurs que 1 et lui-même, donc soit $p \wedge a = 1$, soit $p \wedge a = p$ c'est à dire $p|a$.
2. Par l'absurde, supposons que p ne divise pas a et ne divise pas b. On a alors $p \wedge a = 1$ et $p \wedge b = 1$ par propriété précédente. Le théorème de Bézout indique qu'il existe deux entiers u et v tels que $au+pv = 1$, et en multipliant par b des deux côtés il vient $b = abu + pbv$, et comme $p|ab$ on obtient que $p|b$, absurde. Donc $p|a$ ou $p|b$.
3. Si a est premier alors il admet un diviseur premier : lui-même. Si $a \notin \mathbf{P}$, par définition il admet au moins un diviseur distinct de 1 et a. Soit p le plus petit de ces diviseurs qui vérifie donc $2 \leqslant p < a$. Supposons $p \notin \mathbf{P}$. Alors il admet un diviseur d distinct de 1 et p. Mais d est plus petit que p et divise aussi a, ce qui est en contradiction avec la définition de p. Donc $p \in \mathbf{P}$ et a admet un diviseur premier.
4. On a $p|a$ d'où il existe $k \in \mathbf{Z}$ tel que $a = kp$. k divise donc a et par définition de p, on a donc $2 \leqslant p \leqslant k$. Comme $p > 1$ on obtient $4 \leqslant p^2 \leqslant kp = a$ et par croissance de la fonction racine carrée $2 \leqslant p \leqslant \sqrt{a}$. □

7.3 Deux théorèmes fondamentaux

Théorème. $\mathbf{P}$ est infini.

Démonstration. On va raisonner par l'absurde. Supposons donc $\mathbf{P}$ fini. On écrit donc $\mathbf{P} = \{p_1, p_2, \ldots, p_n\}$ où $n \in \mathbf{N}^*$. On pose

$$N = p_1 \times p_2 \times \cdots \times p_n + 1.$$

D'après les propriétés précédentes comme $N > 2$, N admet un diviseur premier p', qui est l'un des p_i (avec $i \in \{1, \ldots, n\}$) dans la formule explicitant N. D'où

$$p'|p_1 \times p_2 \times \cdots \times p_n.$$

Et par propriété de divisibilité

$$p'|(N - p_1 \times p_2 \times \cdots \times p_n)$$

Donc $p'|1$. Alors $p' = 1$, ce qui est absurde car $1 \notin \mathbf{P}$. Notre supposition est donc fausse et $\mathbf{P}$ est infini. □

Théorème (Théorème fondamental de l'arithmétique)**.** Soit n un entier supérieur ou égal à 2. L'entier n est alors décomposable en un produit, unique à l'ordre des facteurs près, de nombres premiers.
Il existe donc un nombre fini de nombres premiers $p_1, \dots, p_k$ et un nombre fini d'entiers naturels non nuls $a_1, \dots, a_k$ tels que $n = p_1^{a_1} \times \cdots \times p_k^{a_k}$.

Exemple. $6936 = 2^3 \times 3 \times 17^2$.

Démonstration. Montrons d'abord l'existence de la décomposition. Soit donc n entier supérieur ou égal à 2. Nous allons procéder par récurrence forte sur n.
La propriété est vraie au rang 2, car $n = 2$ se décompose bien comme un produit (avec un seul facteur) de nombres premiers (car $2 \in \mathbf{P}$).
Supposons que tout entier compris entre 1 et n se décompose en facteurs premiers. Si $n+1 \in \mathbf{P}$, alors $n+1$ se décompose en un produit d'un seul facteur $n+1$. Si $n+1$ est composé, alors par définition il existe a et b entiers tels que $n+1 = ab$. Or a et b sont compris entre 2 et n, donc par hypothèse ils se décomposent en un produit de nombres premiers. Donc ab, et par égalité $n+1$, se décompose bien en produit de facteurs premiers.
Par propriété de récurrence sur $\mathbf{N}$, on en déduit que tout entier supérieur ou égal à 2 est décomposable en un produit de nombres premiers.

Montrons maintenant l'unicité. De même on procède par récurrence forte sur n. L'unicité est triviale pour $n = 2$.
Supposons qu'il y ait unicité, à l'ordre des facteurs près, des décompositions en facteurs premiers des entiers compris entre 2 et n. Supposons qu'il existe (possible d'après ce qui précède) $p_1, \dots, p_k$ avec $k \in \mathbf{N}^*$ nombres premiers, et $q_1, \dots, q_{k'}$ avec $k' \in \mathbf{N}^*$ nombres premiers tels que $n+1 = p_1 \times \ldots \times p_k = q_1 \times \ldots \times q_{k'}$.
p_1 est premier et divise le produit $p'_1 \times \ldots \times p'_{k'}$. Par nos propriétés précédentes, on a donc que p_1 divise l'un des q_i avec $i \in \{1, \dots, k'\}$. Or q_i est premier, et comme $p_1 \neq 1$ on a nécessairement $p_1 = q_i$.
En réordonnant les termes $q_1, \dots, q_{k'}$, on peut supposer $p_1 = q_1$.
On a donc $p_2 \times \ldots \times p_k = q_2 \times \ldots \times q_{k'} \leqslant n$. Or en appliquant notre hypothèse de récurrence, on obtient $k = k'$ et $p_2 = q_2,\ p_3 = q_3, \dots, p_k = q_{k'}$, ce qui prouve l'unicité de la décomposition en facteurs premiers de $n+1$.
Par propriété de récurrence sur $\mathbf{N}$, on en déduit que l'unicité, à l'ordre des facteurs près, des décompositions en facteurs premiers de tout entier supérieur ou égal à 2. □

La décomposition d'un entier $n \geqslant 2$ nous renseigne immédiatement sur les propriétés arithmétiques de n. En effet, les diviseurs (positifs) de n seront tous les entiers s'écrivant $n = p_1^{\alpha_1} \times \ldots \times p_k^{\alpha_k}$, avec pour tout $i \in \{1, \dots, k\}$, $0 \leqslant \alpha_i \leqslant a_i$.

Exemple. Prenons $n = 36 = 2 \times 2 \times 3 \times 3 = 2^2 \times 3^2$. Les diviseurs positifs de n sont donc

$$\begin{aligned}
2^0 \times 3^0 &= 1 \\
2^0 \times 3^1 &= 3 \\
2^0 \times 3^2 &= 9 \\
2^1 \times 3^0 &= 2 \\
2^1 \times 3^1 &= 6 \\
2^1 \times 3^2 &= 18 \\
2^2 \times 3^0 &= 4 \\
2^2 \times 3^1 &= 12 \\
2^2 \times 3^2 &= 36
\end{aligned}$$

De plus, la décomposition permet de calculer facilement le PGCD et le PPCM de deux entiers n et m. En effet, le PGCD est l'entier composé de tous les facteurs premiers communs à n et m. La décomposition en facteurs premiers du PPCM contient tous les nombres premiers qui apparaissent dans au moins une des décompositions en facteurs premiers de n et m, chacun affecté du plus grand exposant qui apparait dans celles-ci.

Exemple. Prenons $n = 168 = 2 \times 2 \times 2 \times 3 \times 7 = 2^3 \times 3 \times 7$ et $m = 60 = 2 \times 2 \times 3 \times 5 = 2^2 \times 3 \times 5$. On obtient alors

$$n \wedge m = 2^2 \times 3 = 12$$

et

$$n \vee m = 2^3 \times 3 \times 5 \times 7 = 840.$$

8 Théorème de Fermat

Théorème (Théorème de Fermat)**.** Soit $a \in \mathbf{Z}$ et $p \in \mathbf{P}$. Si $a \wedge p = 1$, alors

$$a^{p-1} \equiv 1 \pmod{p}.$$

Démonstration. Notons r_k le reste de la division euclidienne de ka par p, pour $k \in \{1, \dots, p-1\}$.

Si $r_k = 0$, alors $p|ka$. Dans ce cas, soit $p|a$ ce qui est impossible car $a \wedge p = 1$, soit $p|k$, ce qui est impossible car $k < p$. Finalement, $r_k \neq 0$.

On ne peut avoir $r_k = r_{k'}$ pour $k \neq k'$. En effet, si $r_k = r_{k'}$, alors $ka \equiv k'a \pmod{p}$. Or $a \wedge p = 1$, donc il existe $(u, v) \in \mathbf{Z}^2$ tel que $au + pv = 1$, c'est-à-dire $au \equiv 1 \pmod{p}$. Donc en multipliant la congruence $ka \equiv k'a \pmod{p}$ par u, il vient $k \equiv k' \pmod{p}$. Et comme $1 \leqslant k \leqslant p-1$ et $1 \leqslant k' \leqslant p-1$, on a $k = k'$. Donc dès que $k \neq k'$, on a $r_k \neq r_{k'}$.

Par définition des r_k, on a $a \equiv r_1 \pmod{p}$, $2a \equiv r_2 \pmod{p}, \dots, (p-1)a \equiv r_{p-1} \pmod{p}$. En multipliant ces congruences, il vient

$$a \times 2a \times \cdots \times (p-1)a \equiv r_1 \times r_2 \times \cdots \times r_{p-1} \pmod{p}.$$

Or les r_k sont tous distincts, il y en a $p-1$ et à valeurs dans l'ensemble $\{1, \dots, p-1\}$. Donc $r_1 \times r_2 \times \cdots \times r_{p-1} = (p-1)!$. On en déduit que

$$a^{p-1}(p-1)! \equiv (p-1)! \pmod{p}. \qquad (\star)$$

L'entier p est premier avec 1, 2 jusqu'à $p-1$, donc il est premier avec $(p-1)!$. Il existe donc $(u', v') \in \mathbf{Z}^2$ tel que $u'p + v'(p-1)! = 1$, c'est-à-dire $v'(p-1)! \equiv 1 \pmod{p}$. En multipliant par v' la congruence $(\star)$, on a donc

$$a^{p-1} \equiv 1 \pmod{p}. \qquad \square$$

Corollaire. Soit $a \in \mathbf{Z}$ et $p \in \mathbf{P}$. On a

$$a^p \equiv a \pmod{p}.$$

Démonstration. Si $a \wedge p = 1$, alors le théorème de Fermat donne $a^{p-1} \equiv 1 \pmod{p}$, et en multipliant par a il vient $a^p \equiv a \pmod{p}$. Si $a \wedge p \neq 1$, alors $p|a$. On a donc $a \equiv 0 \pmod{p}$, donc $a^p \equiv 0 \equiv a \pmod{p}$. $\square$

9 L'équation diophantienne $ax + by = c$

Soit a, b et c des entiers tels que a et b soient non nuls. On s'intéresse à l'équation diophantienne

$$ax + by = c \qquad (E)$$

d'inconnus x et y *entiers* (d'où le terme *diopantienne*). On pose $d = a \wedge b$.

Théorème. L'équation (E) admet des solutions si, et seulement si, $d|c$ (donc en particulier si $a \wedge b = 1$).

Démonstration. Si $c = 0$, alors $d|c$ et $(x, y) = (0, 0)$ est solution. Supposons donc $c \neq 0$. D'après le théorème de Bézout, il existe $(u, n) \in \mathbf{Z}^2$ tel que $au + bv = d$.
Si (E) admet des solutions $(x_0, y_0) \in \mathbf{Z}^2$, alors comme $d|a$ et $d|b$, on obtient que $d|(ax_0 + by_0)$, d'où $d|c$.
Supposons que $d|c$. Alors $d|cu$ et $d|cv$. En posant x_0 (resp. y_0) le quotient de la division euclidienne de cu (resp. cv) (le reste étant nul), on vérifie que (x_0, y_0) est solution de (E). □

Supposons donc maintenant que $d|c$. D'après le calcul du couple dans l'identité de Bézout, on peut trouver des solutions particulières à (E), que l'on note (x_0, y_0). En divisant (E) par d, on se ramène à une nouvelle équation (E') qui s'écrit

$$a'x + b'y = c'.$$

Comme on avait $a \wedge b = d$, on a maintenant $a' \wedge b' = 1$. Remarquons également que (x_0, y_0) est solution de (E'). Soit (x, y) une solution quelconque de (E'), différente de (x_0, y_0). On a donc

$$c' = a'x + b'y = a'x_0 + b'y_0$$

d'où

$$a'(x - x_0) = b'(y_0 - y).$$

Ceci indique que $b'|a'(x - x_0)$, et comme $a' \wedge b' = 1$ on obtient d'après le lemme de Gauss que $b'|(x - x_0)$. Il existe donc $k \in \mathbf{Z}$ tel que $x = x_0 + b'k$. Puis en réinjectant dans l'égalité ci-dessus, on trouve $y = y_0 - a'k$. Réciproquement, on vérifie que pour tout $k \in \mathbf{Z}$, $(x_0 + b'k, y_0 - a'k)$ est bien solution de (E'). Résumons alors l'étude.

Théorème. Les solutions de (E) sont de la forme

$$\begin{cases} x &= x_0 + \dfrac{kb}{d} \\ y &= y_0 - \dfrac{ka}{d} \end{cases}$$

avec $k \in \mathbf{Z}$ et (x_0, y_0) solution particulière de (E).

Exemple. On cherche à résoudre l'équation $123x + 67y = 10$ noté (E). D'après l'exemple qui précède, on sait que $123 \wedge 67 = 1$ et que $123 \times 6 + 67 \times (-11) = 1$. Donc une solution particulière de (E) est $(x_0, y_0) = (60, -110)$. Soit (x, y) une autre solution distincte de (E). On a alors

$$123(x - 60) = 67(-y - 110).$$

Ainsi, $67|123(x - 60)$, et comme $123 \wedge 67 = 1$ d'après le lemme de Gauss on a $67|x - 60$. Il existe donc $k \in \mathbf{Z}$ tel que $x = 60 + 67k$. En remplaçant, on obtient $y = -110 - 123k$. Réciproquement, on vérifie que les couples $(60 + 67k, -110 - 123k)$ sont bien solutions de (E).

Cette section s'inspire directement de l'ouvrage *Thèmes d'arithmétique* d'Olivier Bordellès.

Références

- *Transmath terminale S - spécialité*, Nathan, 2002.
- *Mathématiques terminale S - enseignement de spécialité*, Bréal, 2002.
- *Maths terminale S spécialité*, collection Contrôle continu, Ellipses, 2004.
- Olivier Bordellès, *Thèmes d'arithmétique*, Ellipses, 2006.
- Marc Lorré, *Maths MPSI*, collection Pas à pas en prépa, Ellipses, 2004.
- Jean-Marie Monier, *Algèbre MPSI*, collection J'intègre, Dunod, 2006.
- Godfrey Harold Hardy & Edward Maitland Wright, *An Introduction of the Theory of Numbers*, Oxford University Press, 1979.
- *http ://wikipedia.org*, version francophone et anglophone.