Université de Clermont1
IUT d'Informatique
1ère année - 2002-2003
Benoît GUGGER - Denis RICHARD - Jerzy TOMASIK

ALGORITHME D'EUCLIDE

ET

ÉQUATIONS DIOPHANTIENNES

Algorithme d'Euclide et Équations diophantiennes

1 Divisibilité

Définition 1.1 (Rappel) *: On dira que* x *divise* y *(ou* x|y*) ssi il existe* q *tel que*
$$y = qx.$$

Le ***plus grand commun diviseur*** *de* $a_1, \ldots, a_n$ *(noté* **PGCD** $(a_1, \ldots, a_n)$*) est le diviseur commun aux* a_i *qui est le plus grand.*

Le ***plus petit commun multiple*** *de* $a_1, \ldots, a_n$ *(noté* **PPCM** $(a_1, \ldots, a_n)$*) se définit naturellement : c'est le multiple commun aux* a_i *qui est le plus petit possible.*

Un entier p *est PREMIER dans* $\mathbb{N}$ *ssi* p *possède exactement deux diviseurs* (1 *et* p).

Un entier p *est dit PREMIER dans* $\mathbb{Z}$ *ssi* |p| *est premier dans* $\mathbb{N}$. *L'ensemble des entiers premiers de* $\mathbb{N}$ *est noté* $\mathbb{P}$.

Exemples :

$2, 3, 5, 7, 11, 13, \ldots,$
$2^1 - 1, 2^3 - 1, 2^7 - 1, 2^{13} - 1, 2^{17} - 1, 2^{19} - 1,$
$2^{31} - 1, 2^{61} - 1, 2^{89} - 1, \ldots, 2^{19937} - 1, \ldots$
(les $2^n - 1$ premiers avec n premiers sont les nombres de MERSENNE).

L'importance extrême des premiers tient au :

Théorème 1.1 (fondamental de l'arithmétique)
Pour tout entier $n \in \mathbb{N}^*$*, on appelle décomposition primaire (ou en facteurs premiers) une suite* $((q_1, \alpha_1), \ldots, (q_r, \alpha_r))$ *où*

1) $r \in \mathbb{N}^*$ *;*

2) $q_i \in \mathbb{P}$ *et* $(i < j$ *implique* $q_i < q_j)$ *;*

3) $\alpha_i \in \mathbb{N}^*$ *;*

4) $n = q_1^{\alpha_1} \ldots q_r^{\alpha_r}$.

Alors, tout entier $\neq 0$ *possède une UNIQUE DÉCOMPOSITION PRIMAIRE.*

Égalité de Bezout dans $\mathbb{Z}$,
Algorithme d'Euclide, Équations Diophantiennes

À propos du contenu
Si "l'identité de Bezout" (expression à laquelle nous préfèrerons "théorème de Bezout" car il n'y a pas *une* mais des égalités équivalentes de ce type) ne figure dans les programmes que parce qu'elle sert dans la démonstration du théorème de Gauss, on aurait pu se dispenser de l'introduire. En fait, et rares sont les manuels qui insistent sur ce point, la détermination des coefficients dont l'existence est assurée par le théorème de Bezout, équivaut à la résolution dans $\mathbb{Z}$ d'équations à n inconnues, à coefficients entiers et à celle de certains systèmes d'équations qui se ramènent à des systèmes de congruences. C'est donc un point de vue délibérément pratique (mais non exempt de considérations et d'applications théoriques) que nous adoptons ici.

2 Algorithme d'Euclide

• Soit $n \in \mathbb{N}^*$. Pour tout $(a_1, a_2, \dots a_n) \in \mathbb{Z}^n$, il existe $d \in \mathbb{N}$, unique tel que $a_1\mathbb{Z} + \cdots + a_n\mathbb{Z} = d\mathbb{Z}$. Par définition ce d est appelé PGCD$(a_1, a_2, \dots a_n)$.

• La détermination pratique du PGCD s'effectue par divisions successives. Nous rappelons que si $(a, b) \in \mathbb{Z} \times \mathbb{Z}^*$ et si $a = bq$, $q \in \mathbb{Z}$ alors PGCD$(a, b) = |b|$. Sinon on peut, avec des notations évidentes, trouver $k \in \mathbb{N}^*$ tel que :

$$\begin{array}{ll} a = bq_1 + r_1 & 0 < r_1 < |b| \\ b = r_1q_2 + r_2 & 0 < r_2 < r_1 \\ r_1 = r_2q_3 + r_3 & 0 < r_3 < r_2 \\ & \\ r_{k-2} = r_{k-1}q_k + r_k & 0 < r_k < r_{k-} \\ r_{k-1} = r_kq_{k+1} & \end{array}$$

ce qui détermine $r_k = \text{PGCD } (a, b)$.

2.1 Introduction aux équations diophantiennes.

La notion d'entiers premiers entre eux (et le théorème fondamental de Bezout qui s'y rapporte) surgit naturellement dès que l'on se propose de résoudre des équations diophantiennes, ou des systèmes d'équations diophantiennes, c'est-à-dire d'équations à coefficients et ensemble de solutions contenus dans $\mathbb{Z}$.

1) Une équation diophantienne $\alpha x + \beta y = \gamma$ (1), avec $\alpha \neq 0$ ou $\beta \neq 0$ n'a de solutions que si $d = \text{PGCD } (\alpha, \beta)$ divise γ. L'ensemble des solutions de (1) est alors, dans ce cas, celui de

$$ax + by = c \tag{2}$$

en posant $a = \alpha/d$, β/d et $c = \gamma/d$. Remarquons dès maintenant que :

(A) Nous pouvons résoudre (2) en trouvant une solution particulière (x_0, y_0) de (2), et en constatant qu'alors toute solution (x, y) vérifie (3) $a(x-x_0) = b(y_0-y)$ avec PGCD $(a, b) = 1$. Le théorème de Gauss nous permettra de résoudre (3).

(B) Si c divise a et b, on peut essayer de résoudre $(a/c)x + (b/c)y = 1$ avec PGCD $(\frac{a}{c}, \frac{b}{c}) = 1$. Cela revient au problème plus général de trouver, pour $(a, b) \in \mathbb{Z}^2$ avec PGCD $(a, b) = 1$, les couples $(u, v) \in \mathbb{Z}^2$ tels que $au + bu = 1$.

(C) Si c ne divise pas a et b, nous pouvons cependant affirmer, en posant
$\delta = \text{PGCD}(a, b, c)$, $a_1 = a/\delta$, $a_2 = b/\delta$, $a_3 = c/\delta$, que les solutions de (1) sont celles de :

$$a_1x + a_2y - a_3 = 0 \quad \text{avec} \quad \text{PGCD}(a_1, a_2, a_3) = 1.$$

Nous sommes ici ramenés au problème plus général de la détermination de $(u_1, u_2, u_3) \in \mathbb{Z}^3$ tels que a_1, a_2 et a_3 étant des entiers de PGCD égal à 1, on ait

$$a_1u_1 + a_2u_2 + a_3u_3 = 1.$$

2) Considérons maintenant des systèmes de deux équations comme

$$I \begin{cases} x + 2y = 5 \\ x + 4z = 6 \end{cases} \qquad II \begin{cases} x + 8y = 5 \\ x + 27z = 6. \end{cases}$$

Ces systèmes d'équations conduisent aux systèmes de congruences suivants :

$$I' \begin{cases} x \equiv 5(2) \\ x \equiv 6(4) \end{cases} \qquad II' \begin{cases} x \equiv 5(8) \\ x \equiv 6(27). \end{cases}$$

Pour I' remarquons que PGCD $(2, 4) = 2$ et pour II' que PGCD $(8, 27) = 1$. Or le *système I'* (donc le système I) *n'a pas de solution* sinon il existerait $(k, k') \in \mathbb{Z}^2$ tels que $x = 2k+5 = 4k'+6$, ce qui est impossible car un nombre pair ne peut être égal à un nombre impair. *Quant au système II', il y a des solutions car* -75 et 141, par exemple conviennent, de sorte que le système II lui admet aussi des solutions comme $(-75, 10, 3)$ et $(141, -17, -5)$.

Moralité de cette introduction.
Les problèmes posés par la résolution de l'équation diophantienne $\alpha x + \beta y = \gamma$ se ramènent à la détermination d'entiers :

- (u, v) tels que $au + bv = 1$ avec $\text{PGCD}(a, b) = 1$,
- (x, y) tels que $ax + by = C$ avec $\text{PGCD}(a, b) = 1$,
- (u_1, u_2, u_3) tels que $a_1u_1 + a_2u_2 + a_3u_3 = 1$ avec $\text{PGCD}(a_1, a_2, a_3) = 1$.

l'ensemble des solutions de

$$\begin{cases} x + ay = a' \\ x + bz = b' \end{cases}$$

peut être vide si PGCD $(a, b) \neq 1$.
Si PGCD $(a, b) = 1$, nous avons pu constater sur un exemple que l'ensemble des solutions peut ne pas être vide.
Étudions donc le comportement des entiers relatifs de PGCD égal à 1.
[Sauf mention expresse du contraire, on entend dans tout le développement qui suit par entiers, des entiers relatifs, c'est-à-dire éléments de $\mathbb{Z}$.]

3 Théorème de Bezout et Applications

Définition 3.1
Des entiers $\text{a}_1, \text{a}_2, \ldots, \text{a}_\text{n}(\text{n} \geq 2)$ *sont dits premiers entre eux dans leur ensemble (ou premiers entre eux) si leur PGCD est 1.*

Exemples : Les ensembles suivants sont des ensembles d'entiers premiers entre eux :

$$\{2, 5\}, \qquad \{3, 10\}, \qquad \{2, 4, 3, 6\}$$

alors que ce n'est pas le cas pour

$$\{2, , \}, \qquad \{2, 6\}, \qquad \{867, 969\}.$$

Remarques :
• Si des entiers sont premiers entre eux, ils ne sont pas tous nuls. Si $(a, b) \in \mathbb{Z}^2$ sont premiers entre eux et $a = 0$, alors $|b| = 1$.

• Des entiers $\{a_1, \dots a_n\}(n \geq 2)$ peuvent être premiers entre eux, mais ne pas être, deux à deux, premiers entre eux, ainsi PGCD $(2, 4, 3, 6) = 1$ et PGCD $(2, 4) = 2$, PGCD $(3, 6) = 3$.
Le théorème fondamental de cette leçon donne deux critères pour reconnaître si des entiers sont premiers dans leur ensemble. Ces critères s'expriment d'une part en termes d'équations diophantiennes et, d'autre part, en termes de relation entre sous-groupes de $\mathbb{Z}$.

Théorème 3.1 (de Bezout)
Des entiers $\mathrm{a}_1, \mathrm{a}_2, \dots \mathrm{a}_\mathrm{n}(\mathrm{n} \geq 2)$ *sont premiers dans leur ensemble si et seulement s'ils vérifient une des conditions équivalentes suivantes :*

(1) Il existe des entiers $\mathrm{u}_1, \dots, \mathrm{u}_\mathrm{n}$ *tels que*

$$\sum_{\mathrm{i}=1}^{\mathrm{n}} \mathrm{a_i u_i} = 1.$$

(2) $\mathrm{a}_1\mathbb{Z} + \mathrm{a}_2\mathbb{Z} + \cdots + \mathrm{a}_\mathrm{n}\mathbb{Z} = \mathbb{Z}$.

Conséquence : L'entier d est PGCD des entiers $a_1, a_2, \dots a_n$ si et seulement si les reels $a_1/d, a_2/d, \dots, a_n/d$ sont des entiers entre eux.

Exercices : Démontrer, par deux méthodes, mais sans calculer de PGCD , que $\{2, 4, 3, 6\}$ sont premiers entre eux.

Donnons maintenant deux théorèmes dont le second est le célébre théorème de Gauss.

Théorème 3.2 *Si un entier* a *est premier avec chacun des entiers* $\mathrm{b}_1, \mathrm{b}_2, \dots, \mathrm{b}_\mathrm{n}(\mathrm{n} \geq 2)$, *il est premier avec leur produit, et réciproquement.*

La réciproque - conséquence immédiate du théorème de Bezout - est toujours dans les manuels élémentaires.

Théorème 3.3 (de Gauss)
Soient a, b *et* c *des entiers. Si* a *divise* bc *et si* a *est premier avec* b, *alors* a *divise* c.

4 Étude de $E = \{(u, v) \in \mathbb{Z}^2/((au + bv) = 1$ et PGCD $(a, b) = 1)\}$

Proposition 4.1 *Soit* (a, b) *un couple d'entiers et* E *l'ensemble des* $(\mathrm{u}, \mathrm{v}) \in \mathrm{Z}^2$ *tels que* $au+bv = 1$.

(1) Si a *et* b *ne sont pas premiers entre eux,* $\mathrm{E} = \emptyset$.

(2) Si a *et* b *sont premiers entre eux,* E *n'est pas vide, et pour tout élément* $(\mathrm{u}, \mathrm{v}) \in \mathrm{E}$, *on a* $\mathrm{E} = \{(\mathrm{u} - \mathrm{zb}, \mathrm{v} + \mathrm{za}) \in \mathbb{Z}^2(\mathrm{z} \in \mathbb{Z})\}$.

"L'identité" de Bezout, $au + bv = 1$ ne détermine donc pas un couple (u, v). C'est pour cela que nous préférons parler de théorème de Bezout, ou de relations de Bezout. Comme il n'y a pas d'unicité de (u, v), nous allons imposer des conditions supplémentaires assurant l'unicité d'un couple (u, v). Les conditions qu'on trouve, en exercices ou dans le texte, des manuels élémentaires sont souvent *fausses*. Ainsi :

• $(a,b) \in \mathbb{N}^2$, PGCD $(a,b) = 1$, $au + bv = 1$, $|u| < b$, $|v| < a$ n'assure pas l'unicité de (u,v). Contre-exemple :

$$2.2 + (-1).3 = 1 = (-1)2 + 1.3.$$

• $(a.b) \in \mathbb{N}^{*^2}$. PGCD $(a,b) = 1$, $au_0 - bv_0 = 1$, $0 < u_0 < b$, $0 < v_0 < a$ n'assure même pas l'existence du couple (u,v) si on considère, par (contre)-exemple, $a = 1$, $b \in \mathbb{N}^*$.

Le résultat qui suit, parfois appelé théorème de Bezout dans $\mathbb{N}^*$, servira de lemme pour établir des conditions d'unicité.

Proposition 4.2 *Soit* (a,b) *un couple d'entiers naturels, autres que 0 et 1, premiers entre eux. Il existe un couple* $(\mathrm{u},\mathrm{v}) \in \mathbb{N}^2$ *et un seul tel que :*

$$0 < \mathrm{u} < \mathrm{b}, \qquad 0 < \mathrm{v} < \mathrm{a} \qquad \textit{et} \qquad \mathrm{au} - \mathrm{bv} = 1.$$

Théorème 4.1 (Conditions d'unicité de (u,v))
Soit (a,b) *un couple d'entiers, différents de 0, 1 et* -1, *premiers entre eux. Alors il existe un couple* $(\mathrm{u},\mathrm{v}) \in \mathbb{Z}^2$, *unique, tel que* $\mathrm{au} + \mathrm{bv} = 1$, *avec :*

$$\begin{array}{llllll} 0 < \mathrm{u} < \mathrm{b}, & -\mathrm{a} < \mathrm{v} < 0 & \textit{si} & \mathrm{a} > 1 & \textit{et} & \mathrm{b} > 1, \\ \mathrm{b} < \mathrm{u} < 0, & 0 < \mathrm{v} < -\mathrm{a} & \textit{si} & \mathrm{a} < -1 & \textit{et} & \mathrm{b} < -1, \\ \mathrm{b} < \mathrm{u} < 0, & -\mathrm{a} < \mathrm{v} < 0 & \textit{si} & \mathrm{a} > 1 & \textit{et} & \mathrm{b} < -1. \end{array}$$

Détermination pratique : Montrons par récurrence finie, que l'algorithme d'Euclide (voir rappels pour les notations) permet de déterminer des coefficients u et v tels que $au + bv = 1$ lorsque a et b sont des entiers premiers entre eux. On a $r_1 = a.1 + b(-q)$, $r_2 = 1.b + r_1(-q_2)$.

Supposons que $r_{p-2} = au_{p-2} + bv_{p-2}$
$r_{p-1} = au_{p-1} + bv_{p-1}$
pour $2 \leqq p \leqq k$, u_{p-2}, u_{p-1}, v_{p-2} et v_{p-1} entiers. On a :

$$\begin{array}{rcl} r_p & = & r_{p-2} - r_{p-1}q_p \\ & = & a(u_{p-2} - q_p u_{p-1}) + b(v_{p-2} - q_p v_{p-1}) = au_p + bv_p. \end{array}$$

Remarques :

1) Cette détermination redémontre de façon constructive[1] (i.e. en prouvant non seulement l'existence d'un couple (u,v), mais en donnant une méthode de calcul) le théorème de Bezout dans la cas des deux entiers.

2) Le cas de n entiers se ramène à celui de deux entiers d'après le théorème 3.

Exemple et mode de présentation des calculs :
Calculer un couple $(u,v) \in \mathbb{Z}^2$ tel que $au + bv = 1$ avec $a = 99099$ et $b = 43928$.

5 Applications aux résolutions diophantiennes

Équation $ax + by = c$ (1), avec PGCD $(a,b) = d$.

Théorème 5.1 *Soit* S *l'ensemble des solutions dans* $\mathbb{Z}$ *de (1).*

- *Si PGCD* (a,b) *ne divise pas* c, *alors* $\mathrm{S} = \emptyset$.
- *Si PGCD* $(\mathrm{a},\mathrm{b}) = \mathrm{d}$ *divise* c, *alors pour tout couple* $(\mathrm{u},\mathrm{v}) \in \mathbb{Z}^2$ *tel que* $\dfrac{\mathrm{a}}{\mathrm{b}}\mathrm{u} + \dfrac{\mathrm{b}}{\mathrm{d}}\mathrm{v} = 1$,

$$\mathrm{S} = \left\{ \left(\frac{\mathrm{cu}}{\mathrm{d}} - \frac{\mathrm{kd}}{\mathrm{d}}, \frac{\mathrm{cv}}{\mathrm{d}} + \frac{\mathrm{ka}}{\mathrm{d}} \right) \in \mathbb{Z}^2 (\mathrm{k} \in \mathbb{Z}) \right\}.$$

[1] La démonstration par récurrence *finie* permet évidemment de *construire l'objet* dont on prouve l'existence.

Le théorème 5.1 montre donc que la résolution d'une équation diophantienne à deux variables se ramène à la détermination *d'un* couple (u, v) tel que $\alpha u + v\beta = 1$, pour α et β premiers entre eux. Le théorème qui suit va ramener l'étude d'une équation diophantienne à n variables ($n > 2$) à celle d'équations diophantienne à deux variables, donc, d'après ce qu'on vient de voir, au théorème de BEZOUT.

Théorème 5.2 *Soit* $a_1x_1 + a_2x_2 + \cdots + a_nx_n = b (n \geqq 3)$ *une équation diophantienne dont* S *est l'ensemble des solutions.*

- *Si PGCD* $(a_1, a_2, \ldots, a_n)$ *ne divise pas* b, $S = \emptyset$.
- *Si PGCD* $(a_1, a_2, \ldots, a_n) = d$ *divise* b, *alors* S *est l'ensemble des solutions du système :*

$$a_1x_1 + \cdots + a_{n-1}x_{n-1} = PGCD(a_1, \ldots, a_{n-1})y \quad (1)$$
$$PGCD(a_1, \ldots, a_{n-1})y + a_nx_n = b. \quad (2)$$

Exercice : Résoudre dans $\mathbb{Z}$, $10x_1 + 15x_2 + 6x_3 = 73$.[2]

Systèmes de congruences
Les anciens Chinois savaient résoudre, en nombres entiers, le problème astronomique suivant : calculer l'instant t, *le plus proche de l'instant présent, de la conjonction de deux astres* A_1 *et* A_2 *de périodes respectives* p_1 *et* p_2, *connaissant deux instants de passage respectifs* t_1 *et* t_2 *de ces astres en un même azimut. La solution éventuelle vérifie* $t \equiv t_1(p_1)$ *et* $t \equiv t_2(p_2)$.
Nous avons vu dans l'introduction que si p_1 *et* p_2 *ne sont pas premiers, il peut ne pas y avoir de solution.*[3]

Théorème 5.3 *Soient* a.b *des entiers premiers entre eux,* $(u, v) \in \mathbb{Z}^2$ *un couple tel que* $au+vb = 1$ *et* $(x_0, x_1) \in \mathbb{Z}^2$.
Le système :

$$x \equiv x_0(a)$$
$$x \equiv x_1(b)$$

admet pour ensemble de solutions $S = aux_1 + vbx_0 + ab\mathbb{Z}$.

Corollaire 5.1 *Si* a *et* b *sont premiers entre eux, les anneaux* $\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$ *et* $\mathbb{Z}/ab\mathbb{Z}$ *sont isomorphes.*

De plus si $\Psi(n)$ *désigne le nombre d'éléments inversibles de* $\mathbb{Z}/n\mathbb{Z}$, $\Psi(ab) = \Psi(a)\Psi(b)$ (la fonction d'EULER est *multiplicative* pour des entiers premiers entre eux).

Nous venons de voir que le théorème de BEZOUT fournit la solution de certains systèmes de deux congruences et prouve un théorème important sur les anneaux $\mathbb{Z}/n\mathbb{Z}$. Mais ce théorème de BEZOUT permet aussi de résoudre des systèmes de n congruences quand les modules de congruence sont premiers deux à deux. En effet le théorème 9 nous montre comment un tel système de n congruences se ramène à $n - 1$ systèmes de deux congruences.

Théorème 5.4 *Soient* $a_1, \ldots, a_n (n > 2)$ *des entiers premiers deux à deux,* $(x_1, \ldots, x_n) \in \mathbb{Z}^n$ *et le système* Σ *:*

$$x \equiv x_1(a_1),\ x \equiv x_2(a_2), \ldots, x \equiv x_n(a_n).$$

Soit y_i *une solution du système :*

$$\begin{cases} x \equiv 1(a_i) \\ x \equiv 0(a_1a_2 \ldots a_{i-1}a_{i+1} \ldots a_n) \end{cases}$$

pour tout $i \in [1, n] \cap \mathbb{N}$. *L'ensemble* S *des solutions du système* Σ *est :*

$$S = x_1y_1 + x_2y_2 + \cdots + x_ny_n + a_1a_2 \ldots a_n\mathbb{Z}.$$

[2] On trouvera une *autre* résolution de cette équation dans $\mathbb{N}$ à l'exercice 39 de *Mathématiques du CAPÉS* (HERMANN).
[3] Vérifiez qu'il peut aussi y en avoir.

6 Interpolation géométrique

Soit A un point de coordonnées entières (a, b) du plan affine euclidien rapporté à un repère $(O, \vec{i}, \vec{j})$. Supposons que PGCD $(a, b) = 1$. Les couples $(u, v) \in E$ s'interprètent alors comme coordonnées des points M tels que $\overrightarrow{OA}.\overrightarrow{OM} = 1$. L'ensemble E sera donc contenu dans l'ensemble des points à coordonnées entières de la perpendiculaire à OA passant par le point H défini par $\overrightarrow{OH} = \frac{\overrightarrow{OA}}{OA^2}$.

7 Démonstration

Exemples : Calculs de PGCD .

Théorème 3.1 de Bezout :
Les deux conditions énoncées sont évidemment équivalentes et la seconde est la traduction même de PGCD $(\mathrm{a}_1, \mathrm{a}_2, \ldots, \mathrm{a}_\mathrm{n}) = 1$.

Conséquence :
Immédiatement prouvée par la définition du PGCD , et la condition (1) du théorème 3.1.

Exercice :
- On a $(-1)2 + 0.4 + 1.3 + 0.6 = 1$ et la condition (1) du théorème 3.1 permet de conclure.
- On a aussi $2\mathbb{Z} + 4\mathbb{Z} = 2\mathbb{Z}$ car $4\mathbb{Z} \subset 2\mathbb{Z}$.

De même $3\mathbb{Z} + 6\mathbb{Z} = 3\mathbb{Z}$. Enfin $2\mathbb{Z} + 3\mathbb{Z} = \mathbb{Z}$ car, pour tout $z \in \mathbb{Z}$, $(-2)z + 3z = z$.
La condition (2) du théorème 3.1 achève la preuve.

Théorème 3.2 :
- *Si* a *est premier avec deux entiers* b_1 *et* b_2 *respectivement, il existe des entiers* $\mathrm{u}_1, \mathrm{u}_2, \mathrm{v}_1, \mathrm{v}_2$ *tels que*

$$\mathrm{u}_1\mathrm{a} + \mathrm{v}_1\mathrm{b}_1 = 1 \qquad \textit{et} \qquad \mathrm{u}_2\mathrm{a} + \mathrm{v}_2\mathrm{b}_2 = 1,$$

d'où $(\mathrm{u}_1(\mathrm{u}_2\mathrm{a} + \mathrm{v}_2\mathrm{b}_2) + \mathrm{u}_2\mathrm{v}_1\mathrm{b}_1)\mathrm{a} + (\mathrm{v}_1\mathrm{v}_2)\mathrm{b}_1\mathrm{b}_2 = 1$, *ce qui prouve que* a *et* $\mathrm{b}_1\mathrm{b}_2$ *sont premiers entre eux.*

- *Si* $\mathrm{n} > 2$, *comme* a *est premier avec* $\mathrm{b}_1, \mathrm{b}_2, \ldots, \mathrm{b}_{\mathrm{n}-1}$, *on peut supposer par hypothèse de récurrence que* a *est premier avec* $\mathrm{b}_1\mathrm{b}_2 \ldots \mathrm{b}_{\mathrm{n}-1} = \mathrm{B}_1$.
Par utilisation du résultat précédent, a *est premier avecs* $\mathrm{B}_1\mathrm{b}_\mathrm{n}$. CQFD

La réciproque résulte de l'existence de $(u, v) \in \mathbb{Z}^2$ tel que $\mathrm{au} + \mathrm{vb}_1\mathrm{b}_2 \ldots \mathrm{b}_\mathrm{n} = 1$.

Théorème 3.3 de Gauss :
Il existe $(\mathrm{u}, \mathrm{v}) \in \mathbb{Z}^2$ *tel que* $\mathrm{au} + \mathrm{bv} = 1$, *donc tel que* $\mathrm{auc} + \mathrm{bvc} = \mathrm{c}$.
D'une part a *divise évidemment* auc, *et d'autre part, comme* a *divise* bc, *il divise* bvc.
L'entier a *divise donc* $\mathrm{auc} + \mathrm{bvc} = \mathrm{c}$.

Remarque :
Il n'y a pas lieu, comme le montre la preuve ci-dessus, d'exclure le cas où b est nul comme le font certains livres. En effet si $b = 0$, comme a et b sont premiers entre eux, $a = 1$ ou $a = -1$ et le théorème tient.

Proposition 1 :
1)*D'après le théorème de* Bezout, *si* $\mathrm{E} \neq \emptyset$, *alors* a *et* b *sont premiers entre eux, donc, dans le cas contraire,* $\mathrm{E} = \emptyset$.

2) Si a *et* b *sont premiers entre eux, le théorème de* Bezout *affirme encore que* $\mathrm{E} \neq \emptyset$.
Si $\mathrm{a} = 0$, *alors* $\mathrm{b} = 1$ *ou* $\mathrm{b} = -1$ *et* $\mathrm{E} = \mathbb{Z} \times \{1\}$ *ou* $\mathrm{E} = \mathbb{Z} \times \{-1\}$ *respectivement.*
Résultat analogue si $\mathrm{b} = 0$, *car* $\mathrm{a} = 1$ *ou* $\mathrm{a} = -1$.

Supposons maintenant $|a| \geq 1$ *et* $|b| \geq 1$.
Soient (u, v) *et* (x, y) *des éléments de* E. *Comme* $au + bv = 1 = ax + by$, *on a aussi* $a(x - u) = b(v - y)$. *Le théorème de* Gauss *assure l'existence d'un* $z \in \mathbb{Z}$ *tel que* $v - y = za$, *donc tel que* $v = y + za$.
Par suite $a(x - u) = zab$ *et* $u = x - zb$, *en simplifiant par* $a \neq 0$.

Proposition 2 :
On peut évidemment supposer $a > b$ *et alors il existe* $(x, y) \in (\mathbb{N}^*)^2$ *tel que* $ax - by = 1$ *(vérifiez-le).*
Soient $(q, u) \in \mathbb{N}^2$ *tel que* $x = bq + u$ *avec* $0 \leq u < b$. *On a alors* $au - b(y - aq) = 1$.
Si $u = 0$, *alors* $b = 1$ *ce qui n'est pas, donc* $0 < u < a$.
Posons $v = y - aq$. *Comme* $bv = au + 1$, *il vient* $v > 0$. *Comme* $a > b$, *il est vrai, puisque* $u \leq b - 1$, *que :*

$$v = \frac{au + 1}{b} \leq a + \frac{b - a}{b},$$

d'où $v < a$, *ce qui achève ce raisonnement.*

Théorème 4.1 : Laissé au lecteur.

Détermination pratique : Un exemple par divisions successives :

$$\begin{array}{rcrcrr}
99099 & = & 43928 & \times 2 & + & 11243 \\
43928 & = & 11243 & \times 3 & + & 10199 \\
11243 & = & 10199 & & + & 1044 \\
10199 & = & 1044 & \times 9 & + & 803 \\
1044 & = & & & + & 241 \\
803 & = & 241 & \times 3 & + & 80 \\
241 & = & 80 & \times 3 & + & 1.
\end{array}$$

Posons maintenant $a = 99099$, $b = 43928$, $r_1 = 11243$, $r_2 = 10199$, $r_3 = 1044$, $r_4 = 803$, $r_5 = 241$ et $r_6 = 80$; il vient :

$$\begin{array}{rcl}
r_1 & = & a - 2b \\
r_2 & = & b - 3r_1 = -3a + 7b \\
r_3 & = & r_1 - r_2 = 4a - 9b \\
r_4 & = & r_2 - 9r_3 = -39a + 88b \\
r_5 & = & r_3 - r_4 = 43a - 97b \\
r_6 & = & r_4 - 3r_5 = -168a + 379b \\
1 & = & r_5 - 3r_6 = -547a - 1234b \ (= 54207153 - 54207152).
\end{array}$$

(Les tableaux de présentation de l'algorithme d'Euclide qu'on trouve dans la littérature ne dispensent pas des reports successifs effectués ci-dessus. Ces tableaux sont donc inutiles.)

Théorème 5.1 :

- *Comme PGCD* (a, b) *divise* $ax + by$, *pour tout* $(x, y) \in \mathbb{Z}^2$, *il divise* c *si* $S \neq \emptyset$.

- *Les solutions de* $ax + by = c$ *sont exactement celles de* $\frac{a}{d}x + \frac{b}{d}y = \frac{c}{d}$ *si* d *divise* c.

Mais PGCD $\left(\frac{a}{d}, \frac{b}{d}\right) = 1$ *(conséquence citée du théorème 3.1), donc il existe* $(u, v) \in \mathbb{Z}^2$ *tel que* $\frac{a}{d}u + \frac{b}{d}v = 1$, *donc tel que* $a\frac{cu}{d} + b\frac{vc}{d} = c$ *et* $(x, y) = \left(\frac{cu}{d}, \frac{cv}{d}\right)$ *est une solution particulière de* $ax + by = c$. *Si* $(x, y) \in S$ *on a*

$$ax + by = c = ax_0 + by_0 \qquad et \qquad \frac{a}{d}(x - x_0) = \frac{b}{d}(y_0 - y).$$

D'après le théorème de Gauss $x - x_0 = \frac{kb}{d}$ *et* $y_0 - y = \frac{ka}{d}$. *Par suite*

$$S \subset \left\{ \left(\frac{cu}{d} + \frac{kb}{d}, \frac{cv}{d} - \frac{ka}{d} \right) (k \in \mathbb{Z}) \right\}.$$

Réciproquement tout élément du premier ensemble écrit est dans S car

$$a\left(\frac{cu}{d}+\frac{kb}{d}\right)+b\left(\frac{cv}{d}-\frac{ka}{d}\right)=\left(\frac{au}{d}+\frac{bv}{d}\right)c=c.$$

Théorème 5.2 :

• *Comme précédemment* $\mathrm{S}\neq\emptyset$ *implique PGCD* $(\mathrm{a}_1,\ldots,\mathrm{a}_\mathrm{n})$ *divise* b.

• *Soit* $(\mathrm{x}_1,\mathrm{x}_2,\ldots,\mathrm{x}_{\mathrm{n}-1},\mathrm{x}_\mathrm{n})$ *un élément de l'ensemble* S' *des solutions du système. En ajoutant membre à membre les équations (1) et (2) du système on voit que* $(\mathrm{x}_1,\mathrm{x}_2,\ldots\mathrm{x}_\mathrm{n})\in\mathrm{S}$.

Réciproquement le réel y tel que

$$y\mathrm{PGCD}(a_1,\ldots,a_{n-1})=x_1a_1+x_2a_2+\cdots+x_{n-1}a_{n-1}$$

est un entier qui vérifie (1). Comme $x_1a_1+\cdots+x_{n-1}a_{n-1}+x_na_n=b$ l'équation (2) est aussi vérifiée par (y,x_n). Par suite

$$(x_1,x_2,\ldots,x_{n-1},y_1,y_n)\in S'.$$

Exercice : Considérons le système

$$\begin{cases}10x_1+15x_2=5y & (1)\\ 5y+6x_3=73. & (2)\end{cases}$$

C'est un système de 2 équations à 2 inconnues que nous savons résoudre séparement.
Les solutions de (2) sont $\{(-73-6k,(k\in\mathbb{Z})\}$.
Les solutions de (1) sont $\{(-y-3k',y+2k')\in\mathbb{Z}^2(k'\in\mathbb{Z})\}$.
Les solutions de l'équation de départ sont donc, d'après le théorème 5.2.

$$\{(73+6k-3k',\ -73-6k+2k',\ 73+5k)\text{ avec }(k,k')\in\mathbb{Z}^2\}$$

encore inclus, en posant $p=24+2k-k'$ et $q=-37-3k+k'$, à

$$\{(1+3p,\ 1+2q,\ 3+5(1-p-q))\text{ avec }(p,q)\in\mathbb{Z}^2\}.$$

Toutes ces solutions, réciproquement conviennent.

Théorème 5.3 :
Si x *et* x′ *sont deux solutions*

$$\mathrm{x}-\mathrm{x}'\in\mathrm{a}\mathbb{Z}\cap\mathrm{b}\mathbb{Z}\ ;\qquad or\qquad \mathrm{a}\mathbb{Z}\cap\mathrm{b}\mathbb{Z}=P.P.C.M.(a,b)\mathbb{Z}=ab\mathbb{Z}.$$

Par suite si α *est une solution particulière du système* $\mathrm{S}=\alpha+\mathrm{ab}\mathbb{Z}$.
Or $\alpha=\mathrm{aux}_1+\mathrm{bvx}_0$ *est une telle solution puisque, du fait que* $\mathrm{au}\equiv1(\mathrm{b})$ *et* $\mathrm{bv}\equiv1(\mathrm{a})$, *on trouve* $\alpha\equiv\mathrm{x}_0(\mathrm{a})$ *et* $\alpha\equiv\mathrm{x}_1(\mathrm{b})$.

Corollaire[4] **5.1** :
D'après le théorème précédent, pour tout $(\alpha,\beta)\in\mathbb{Z}/\mathrm{a}\mathbb{Z}\times\mathbb{Z}/\mathrm{b}\mathbb{Z}$, *il existe* $\mathrm{x}\in\mathbb{Z}$ *tel que* $\mathrm{x}\in\alpha$ *et* $\mathrm{x}\in\beta$.
Notons $\bar{\mathrm{z}}$, $\bar{\bar{\mathrm{z}}}$ *et* z *les classes respectives de* z *dans* $\mathbb{Z}/\mathrm{a}\mathbb{Z}$, $\mathbb{Z}/b\mathbb{Z}$ *et* $\mathbb{Z}/\mathrm{ab}\mathbb{Z}$. *Ainsi on a* $\bar{\mathrm{x}}=\alpha$ *et* $\bar{\bar{\mathrm{x}}}=\beta$.
Soit f : $\mathbb{Z}/\mathrm{a}\mathbb{Z}\times\mathbb{Z}/\mathrm{b}\mathbb{Z}\longrightarrow\mathbb{Z}/\mathrm{ab}\mathbb{Z}$ *la* ***correspondance*** *définie par* $\mathrm{f}(\bar{\mathrm{x}},\bar{\mathrm{x}})=\mathrm{x}$.
Montrons que f *est une* ***application*** *et qu'elle est* ***injective*** :

$$\mathrm{x}=\mathrm{x}'\Leftrightarrow\mathrm{x}-\mathrm{x}'\in\mathrm{ab}\mathbb{Z}\Leftrightarrow\mathrm{x}-\mathrm{x}'\in\mathrm{a}\mathbb{Z}\cap\mathrm{b}\mathbb{Z}\Leftrightarrow\bar{\mathrm{x}}=\bar{\mathrm{x}'}\quad et\quad\bar{\bar{\mathrm{x}}}=\bar{\bar{\mathrm{x}'}}$$

qui équivaut à $(\bar{\mathrm{x}},\bar{\bar{\mathrm{x}}})=(\bar{\mathrm{x}'},\bar{\bar{\mathrm{x}'}})$.
L'application f *est évidemment* ***surjective*** *car pour tout* $\mathrm{x}\in\mathbb{Z}/\mathrm{ab}\mathbb{Z}$, $\mathrm{f}(\bar{\mathrm{x}},\bar{\mathrm{x}})=\mathrm{x}$.
Que f *soit un homomorphisme d'anneaux est évident.*

Théorème 5.4 :
Si x *et* x' *sont des solutions,*

$$\mathrm{x}-\mathrm{x}'\in\mathrm{a}_1\mathbb{Z}\cap\mathrm{a}_2\mathbb{Z}\cap\ldots\cap\mathrm{a}_\mathrm{n}\mathbb{Z}=\mathrm{P.P.C.M.}(\mathrm{a}_1,\ldots,\mathrm{a}_\mathrm{n})\mathbb{Z}=\mathrm{a}_1\mathrm{a}_2\ldots\mathrm{a}_\mathrm{n}\mathbb{Z},$$

d'où $\mathrm{S}=\alpha+\mathrm{a}_1\mathrm{a}_2\ldots\mathrm{a}_\mathrm{n}\mathbb{Z}$ *pour une solution particulière* α.
Vérifions maintenant que $\mathrm{x}_1\mathrm{y}_1+\cdots+\mathrm{x}_\mathrm{n}\mathrm{y}_\mathrm{n}$ *est une telle solution.*
Si $\mathrm{i}\neq\mathrm{j}$ $(1\leqq\mathrm{i}\leqq\mathrm{n},\ l\leqq j\leqq n)$, *alors* a_i *figure dans le produit* $\mathrm{a}_1\ldots\mathrm{a}_{\mathrm{j}-\mathrm{l}}\mathrm{a}_{\mathrm{j}+\mathrm{l}}\ldots\mathrm{a}_\mathrm{n}$ *donc* $\mathrm{y}_\mathrm{j}\equiv0(\mathrm{a}_1\ldots\mathrm{a}_{\mathrm{j}-\mathrm{l}}\mathrm{a}_{\mathrm{j}+\mathrm{l}}\ldots\mathrm{a}_\mathrm{n})$ *implique* $\mathrm{y}_\mathrm{i}\equiv0(\mathrm{a}_\mathrm{i})$. *Comme de plus* $\mathrm{y}_\mathrm{i}\equiv\mathrm{l}(\mathrm{a}_\mathrm{i})$, *alors* $\mathrm{x}_\mathrm{i}\mathrm{y}_\mathrm{i}\equiv\mathrm{x}_\mathrm{i}(\mathrm{a}_\mathrm{i})$.
Le résultat annoncé en découle.

[4] On l'appelle corollaire, mais c'est un résultat fondamental de théorie des groupes.

Programmation de l'algorithme d'EUCLIDE

(extrait de *The art of computer programming*
de Donald E.KNUTH (vol 1, Addison - Wesley))

By 1950, the word algorithm was most frequently associated with "Euclid's algorithm," a process for finding the greatest common divisor of two numbers which appears in Euclid's *Elements* (Book 7, Propositions 1 and 2.) It will be instructive to exhibit Euclid's algorithm here :

Agorithm E (*Euclid's algorithm*). Given two positive integers m and n, find their greatest common divisor, i.e., the largest positive integer which evenly divides both m and n.

E1. [Find remainder.] Divide m by n and let r be the remainder. (We will have $0 \leq r < n$.)
E2. [Is it zero ?] If $r = 0$, the algorithm terminates ; n is the answer.
E3. [Interchange.] Set $m \leftarrow n$, $n \leftarrow r$, and go back to step E1.

Algorithm E (*Extended Euclid's algorithm*). Given two positive integers m and n, we compute their greatest common divisor d and two integers a and b, such that $am + bn = d$.

E1. [Initilize.] Set $a' \leftarrow b \leftarrow 1$, $a \leftarrow b' \leftarrow 0$, $c \leftarrow m$, $d \leftarrow n$.
E2. [Divide.] Let q, r be the quotient and remainder, respectively, of c divided by d. (We have $c = qd + r$, $0 \leq r < d$.)
E3. [Remainder zero ?] If $r = 0$, the algorithm terminates ; we have in this case $am + bn = d$ as desired.
E4. [Recycle.] Set $c \leftarrow d$, $d \leftarrow r$, $t \leftarrow a'$, $a' \leftarrow a$, $a \leftarrow t - qa$, $t \leftarrow b'$, $b' \leftarrow b$, $b \leftarrow t - qb$, and go back to E2.

If we suppress the variables a, b, a', and b' from this algorithm and use m, n for the auxiliary variables c, d, we have our old algorithm, 1.1E. The new version does a little more, by determining the coefficients a, b. Suppose that $m = 1769$ and $n = 551$; we have successively (after step E2) :

a'	a	b'	b	c	d	q	r
1	0	0	1	1769	551	3	116
0	1	1	−3	551	116	4	87
1	−4	−3	13	116	87	1	29
−4	5	13	−16	87	29	3	0.

The answer is correct : $5 \times 1769 - 16 \times 551 = 8845 - 8816 = 29$, the greatest common divisor of 1769 and 551.

The problem is to *prove* that this algorithm works properly for all m and n. We can try to set this up for the method of mathemetical induction by letting $P(n)$ be the statement "Algorithm E works for n and all integers m." However, this doesn't work out so easly, and we need to prove some extra facts. After a little study, we find that something must be proved about a, b, a', and b', and the appropriate fact is that

$$a'm + b'n = c, \qquad am + bn = d \tag{6}$$

always holds whenever step E2 is executed. We may prove Eqs. (6) directly by observing that it is certainly true the first time we get to E2, and step E4 does not change the validity of (6). (See exercices 1.2.1-6.)
Now we are ready to show that Algorithm E is valid, by induction on n. If m is a multiple of n, the algorithm obviously works properly, since we are done immediately at E3 the first time. This case always occurs when $n = 1$. The only case remaining is when $n > 1$ and m is not a multiple of n. In this case, the algorithm proceeds to set $c \leftarrow n$, $d \leftarrow r$ after the first execution, and since $r < n$, *we may assume by induction* that the final value of d is the g.c.d. of n and r. By the argument given in Section 1.1, the pairs m, n and n, r have the same common divisors, and, in particular, they have the same greatest common divisor. Hence d is the g.c.d. of m and n, and by Eq. (6), $am + bn = d$.

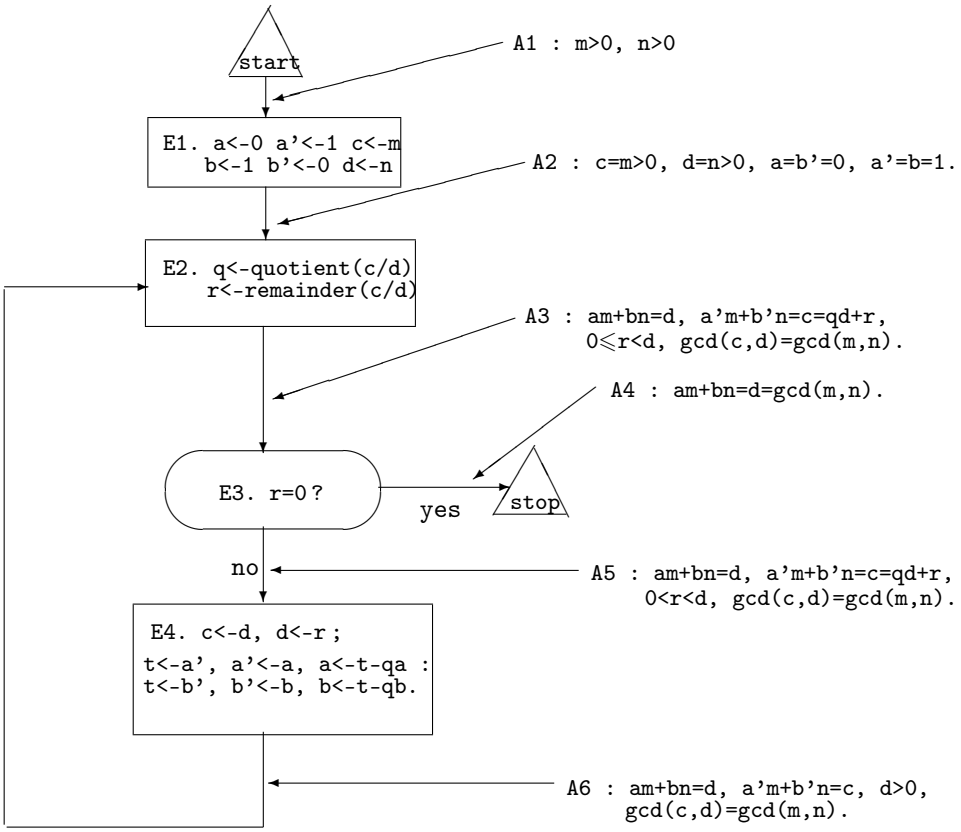

Fig. 4 Flow chart for Algorithm E, labeled with assertions which prove the validity of the algorithm.