159	Algorithme d'Euclide dans $\mathbb{Z}$. Calcul de PGCD et de coefficients de Bézout. Applications.	Chiffrement affine (Terracher)	Terracher TS Damphousse Monier Alg MPSI

I. Algorithme d'Euclide: calcul du Pgcd.

Th. et Def.1 (TER): Soient a et b deux entiers naturels non nuls. La suite de divisions euclidiennes:

de a par b : $a = bq_0 + r_0$

de b par r_0 (si $r_0 \neq 0$) : $b = r_0 q_1 + r_1$

de r_0 par r_1 (si $r_1 \neq 0$) : $r_0 = r_1 q_2 + r_2$

: :

de r_{n-1} par r_n (si $r_n \neq 0$) : $r_{n-1} = r_n q_{n+1} + r_{n+1}$

finit par s'arrêter, un des restes r_i étant nul.
Le **dernier reste non nul** est alors le **PGCD de a et b**.
(Si $r_0 = 0$, c'est b).
Le processus itératif mis en œuvre est appelé **Algorithme d'Euclide** (1).

*Ce processus était connu des Grecs sous le nom d'**Anthyphérèse** (c'est-à-dire "action d'enlever tour à tour"; pour trouver le Pgcd de 70 et 18, on enlevait 18 de 70 autant de fois que possible, etc...).*

Exemple (DAM): Calcul de Pgcd(5767;4453)
5767 = 1 × 4453 + 1314
4453 = 3 × 1314 + 511
1314 = 2 × 511 + 292
511 = 1 × 292 + 219
292 = 1 × 219 + 73
219 = 3 × 73 + 0
On en déduit Pgcd(5767;4453) = 73.

Rque 1: Si a<b, la 1ére ligne de l'algorithme a pour effet d'échanger a et b.

Rque 2: Il existe au moins un autre algorithme de calcul du Pgcd, "l'algorithme des différences successives", qui s'appuie sur Pgcd(a,b) = Pgcd(b,a-b).

II. Développement en fractions continues.

Def.2 (DAM): Une **fraction continue simple** (2) est une expression de la forme:

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ldots + \cfrac{1}{a_n}}}} = [a_1, a_2, \ldots, a_n].$$

Remarque: On peut considérer que:
$[a_1, a_2, \ldots, a_n] = [a_1, a_2, \ldots, a_n, 0, 0 \ldots, 0]$.
(avec une suite infinie de zéros). (3)

Pté.1 (DAM): Soient a∈ℕ, b∈ℕ*.
Si q,q_1, q_2, q_3,...,q_{k+3} est la suite de quotients obtenus dans **l'algorithme d'Euclide** (avec r_{k+2}=0), on a:

$$\frac{a}{b} = [q, q_1, q_2, \ldots, q_{k+3}, 0, 0, \ldots]. \quad (4)$$

L'algorithme d'Euclide permet donc aussi de développer un nombre rationnel (5) en fraction continue.

III. Coefficients de Bézout, applications.

A. Calcul des coefficients de Bézout. (MON) (157)

Les coefficients de Bézout peuvent se calculer en utilisant "**l'algorithme d'Euclide étendu**". C'est un algorithme de calcul d'un couple (u,v) t.q. au+bv=1, (a,b) étant donné tel que $a \wedge b = 1$.

Soit (a,b)∈ℤ*×ℕ* t.q. $a \wedge b = 1$.
D'après l'algorithme d'Euclide, il existe N∈ℕ, q_1, r_1, q_2, r_2,...q_N, r_N, q_{N+1} dans ℤ tels que:

$$\begin{cases} a = bq_1 + r_1 \\ 0 < r_1 < b \end{cases}, \begin{cases} b = r_1 q_2 + r_2 \\ 0 < r_2 < r_1 \end{cases}, \ldots \begin{cases} r_{N-2} = r_{N-1} q_N + r_N \\ 0 < r_N < r_{N-1} \end{cases}, r_{N-1} = r_N q_{N+1}$$

et $r_N = a \wedge b = 1$.
On dispose ainsi des égalités:

$r_{N-2} = r_{N-1} q_N + 1$, $r_{N-3} = r_{N-2} q_{N-1} + r_{N-1}$

⋮

$b = r_1 q_2 + r_2$, $a = bq_1 + r_1$

Ce qui permet de faire apparaître un couple (u,v) de $\mathbb{Z}^2$ tq 1 = au + bv. (6)

Exercice: Calculer des coefficients de Bézout pour a=693 et b=680. (7)

B. Chiffrement affine. (TER). 103-302-304.

On assimile les lettres de l'alphabet A, B, ...Z aux nombres 0,1,...,25, et on code ces nombres par la fonction de "hachage": $f : \begin{cases} \{0,1,\ldots,25\} \to \{0,1,\ldots,25\} \\ x \mapsto f(x) \equiv 17x + 22 \,[26] \end{cases}$.
f(x) est le reste de la division Euclidienne de (17x+22) par 26.
Jules César utilisait un chiffrement affine f(x)=1x+3.

IV. Equation ax+by = Pgcd(a,b) (TER).

Qd on a à résoudre ax+by=c dans $\mathbb{Z}^2$, on divise membre à membre par Pgcd(a,b), ce qui ns ramène à a'x+b'y=c', avec a' et b' premiers entre eux: c'est ce qui permettra l'application du th. de Gauss et donc la résolution. Si Pgcd(a,b) ne divise pas c, l'équation n'a pas de solution. (Method'S TS)

A. Un exemple "à la main": 62x + 43y = 1. (8)

1°) On écrit l'algo. d'Euclide avec les entiers 62 et 43.

2°) On "remonte" dans l'algorithme pour trouver un couple de coefficients de Bézout: on exhibe ainsi une solution particulière $(x_0,y_0) = (-9, 13)$.
3°) L'équation équivaut alors à: $62x+43y=62x_0+43y_0$, i.e. $62(x-x_0) = 43(y_0-y)$.
4°) Le théorème de Gauss permet de conclure à un ensemble des solutions de la forme:

$\begin{cases} x = x_0 + 43k \\ y = y_0 - 62k \end{cases}, k \in \mathbb{Z}$, c'est-à-dire:

$S = \{(-9+43k, 13-62k), k \in \mathbb{Z}\}$.

B. Avec un tableur. (dvt 306)

Etude de l'équation $ax+by=D$, où $D = P\gcd(a,b)$.

On note $r_0, \ldots r_{n+1}$ les restes succesifs de l'algorithme d'Euclide appliqué à a et b, avec $r_n = P\gcd(a,b)$.

- Pour tout k $(0 \le k \le n)$, il existe deux entiers u_k et v_k tels que $au_k + bv_k = r_k$. On le montre par récurrence sur k. On a $u_0=1$ et $v_0=-q_0$, $u_1=-q_1$ et $v_1=1+q_0.q_1$ et pour k>1: $u_{k+2} = u_k - u_{k+1}q_{k+2}$, et $v_{k+2} = v_k - v_{k+1}q_{k+2}$.
- Puisque $au_n + bv_n = r_n = P\gcd(a,b)$, le couple (u_n,v_n) est une solution particulière de l'équation.
- En pratique sur un tableur:

	A	B	C	D	E	F
1	**a**	**b**	**q(k)**	**r(k)**	**u(k)**	**v(k)**
2	78	35	2	8	1	-2
3			4	3	-4	9
4			2	2	9	-20
5			1	1	-13	29
6			2	0	Pgcd: dernier reste non nul	

Initialisation: (k=0 et k=1)
C2:=QUOTIENT(A2;B2)
D2:=MOD(A2;B2)
E2:=1
F2:=-C2
C3:=QUOTIENT(B2;D2)
D3:=MOD(B2;D2)
E3:=SI(D3=0;" ";-C3)
F3:=SI(D3=0;" ";1+C2*C3)

Relations de récurrence:
C4:= SI(D3=0;" ";QUOTIENT(D2;D3))
D4:= SI(D3=0;" ";MOD(D2;D3))
E4:= SI(D4=0;" ";E2-C4*E3)
F4:= SI(D4=0;" ";F2-C4*F3)
Ces relations sont étendues vers le bas du tableur, aussi loin que l'on veut.

Le dernier reste non nul est le Pgcd (ici en D5).
Sur la ligne du pgcd, on a une solution particulière, ici: 78×(-13)+35×29=1.

V. Notes.

(1) **Algorithme d'Euclide**.
Les inégalités $b > r_0 > r_1 > \ldots > r_n > \ldots \ge 0$ montrent que (r_n) est une suite strictement décroissante d'entiers naturels, donc, comme "*toute partie de $\mathbb{N}$ non vide admet un plus petit élément*" – axiome - cette suite est finie.
D'autre part, considérons l'égalité $a = bq_0 + r_0$:

- tout diviseur de a et b divise $a - bq_0$, soit r_0 : c'est un diviseur de b et r_0.
- tout diviseur de b et r_0 divise $bq_0 + r_0$, soit a : c'est un diviseur de a et b.

Ainsi, les diviseurs de a et b sont ceux de b et r_0, et il en va de même pour le plus grand d'entre eux:
$PGCD(a,b) = PGCD(b,r_0)$.
On peut appliquer ce raisonnement à chaque égalité; si r_i est le premier reste nul, on a:

$$P\gcd(a,b) = P\gcd(b,r_0) = P\gcd(r_0,r_1) \ldots = P\gcd(r_{i-2},r_{i-1})$$

Or $r_{i-2} = r_{i-1}q_i + 0$, donc r_{i-1} divise r_{i-2}; par suite, ce dernier Pgcd est r_{i-1}.

(2) **Fraction continue "simple":** On dit ça qd tous ses numérateurs sont égaux à 1. Sinon c'est une fraction continue "généralisée".

(3) **Fraction infinie "de zéros":**
Si l'on assimile $\frac{1}{\infty}$ à 0, et $\frac{1}{0}$ à ∞, on a:

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ldots + \cfrac{1}{a_n + \cfrac{1}{0 + \cfrac{1}{\ldots \frac{1}{0}}}}}}} = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ldots + \cfrac{1}{a_n}}}}$$

(4) **Développement d'un rationnel en farction continue:**
On a, d'après l'algorithme d'Euclide:

$$\frac{a}{b} = q + \frac{r}{b} = q + \frac{1}{\left(\frac{b}{r}\right)} = q + \frac{1}{q_1 + \left(\frac{r_1}{r}\right)} = q + \frac{1}{q_1 + \left(\frac{r}{r_1}\right)}$$

$$= q + \frac{1}{q_1 + \cfrac{1}{q_2 + \left(\frac{r_2}{r_1}\right)}} = q + \frac{1}{q_1 + \cfrac{1}{q_2 + \left(\frac{r_1}{r_2}\right)}} = \ldots$$

$$\ldots = q + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \cfrac{1}{\ldots + \cfrac{1}{q_{k+3}}}}}}$$

On note cette dernière: $q + \frac{1}{q_1 +} \frac{1}{q_2 +} \ldots$

pour des raisons évidentes d'encombrement.

(5) **Développement d'un REEL:** Il faut considérer la partie entière. Si $s < \alpha$, de partie entière $[\alpha]$ et de partie fractionnaire $\langle \alpha \rangle$, il vient:

$$\alpha = [\alpha] + < \alpha > = [\alpha] + \frac{1}{< \alpha >^{-1}}$$

$$= [\alpha] + \frac{1}{\left[< \alpha >^{-1} \right] + \left\langle < \alpha >^{-1} \right\rangle} = \ldots.$$

Exemple:

$$\frac{4}{\pi} = 1 + \frac{1}{2+} \frac{4}{2+} \frac{9}{2+} \frac{25}{2+} \ldots$$ (Lord Brouncker/Wallis)

Utilisation des fractions continues (Wikipedia):

- ➔ Résolution d'équations Diophantiennes.
- ➔ Automate planétaire d'Huygens.

Christian Huygens souhaite construire, à l'aide d'un mécanisme de type horlogerie un automate représentant le mouvement des planètes autour du soleil. La difficulté à laquelle il est confronté est liée au rapport de la durée d'une année terrestre et de celle de Saturne. En un an, la Terre tourne de 359° 45' 40'' 30''' et Saturne de 12° 13' 34'' 18'''. Le rapport est égal à 77 708 431/2 640 858. Combien faut-il de dents sur les deux engrenages supportant respectivement la Terre et Saturne ?

Huygens sait que les fractions continues offrent le meilleur compromis, ce qu'il exprime ainsi : « Or, lorsqu'on néglige à partir d'une fraction quelconque les derniers termes de la série et celles qui la suivent, et qu'on réduit les autres plus le nombre entier à un commun dénominateur, le rapport de ce dernier au numérateur sera voisin de celui du plus petit nombre donné au plus grand ; et la différence sera si faible qu'il serait impossible d'obtenir un meilleur accord avec des nombres plus petits. »

(6) **NON UNICITE des coefs de Bézout:** On peut montrer par récurrence forte sur |a| + b que cet algorithme fournit (si |a|≥2) le couple $(u,v) \in \mathbb{Z}^2$ tel que:

$au + bv = 1$, et $|u| < b, |v| < |a|$.

(7) **Solution:**

Pour a=693 et b=680.

693=680x1+13 (3)

680=13x52+4 (2)

13=4x3+1 (1)

(4=1x4+0)

(1) → 1=13-**4**x3

On remplace 4 par sa valeur issue de (2): 4=680-13x52

Il vient: 1=**13**-[680-**13**x52]x3.

On remplace 13 par sa valeur issue de (3): 13=693-680x1

Il vient: 1=(693-680x1)-[680-(693-680x1)x52]x3.

Finalement: 1=693-680-680.3+693.52.3-680.52.3

i.e. 1=693(1+52.3)-680(1+3+52.3)

i.e. 1=157.693+ (-160).680

(8) **Enoncé du th. de Gauss:**

$$\forall (a,b,c) \in (\mathbb{Z}^*)^3, \left(\begin{cases} a \mid bc \\ a \wedge b = 1 \end{cases} \Rightarrow a \mid c \right)$$

Solution détaillée: 62x+43y=1 (E).

1°) Algorithme d'Euclide avec 62 et 43:

62 = 43 × 1 + 19 (4)

43 = 19 × 2 + 5 (3)

19 = 5 × 3 + 4 (2)

5 = 4 × 1 + 1 (1)

En particulier, Pgcd(62,43)=1, donc le théorème de Bézout assure que l'équation admet des solutions.

2°) Recherche d'une solution particulière.

5 = 4 × 1 + 1 (1')

→On élimine le reste 4 dans (2);

comme (1') contient 4 × 1, on multiplie (2) par 1:

19**×1** = 5 × 3**×1** + 4**×1**

19×1 = **5** × 3 + **5** - 1 d'après (1')

19×1 = **5** × 4 - 1 (2')

→On élimine le reste 5 dans (3);

comme (2') contient 5 × 4, on multiplie (3) par 4:

43**×4** = 19 × 2**×4** + 5**×4**

43×4 = **19** × 2×4 + **19** + 1 d'après (2')

43×4 = **19** × 8 + **19** + 1

43×4 = **19** × 9 + 1 (3')

→On élimine le reste 19 dans (4);

comme (3') contient 19 × 9, on multiplie (4) par 9:

62**×9** = 43**×9** + 19**×9**

62×9 = **43**×9 + **43**×4 - 1 d'après (3')

62×9 = **43**×13 – 1 (4')

Finalement, 62×(-9) + 43×(13) = 1.

Le couple (-9;13) est une solution particulière de (E).

3°) L'équation équivaut alors à: $62x+43y=62x_0+43y_0$, car ceci traduit "1 = 1".

On a donc $62(x-x_0) = 43(y_0-y)$. (E')

4°) Ainsi $62 | 43(y_0-y)$, mais $62 \wedge 43 = 1$, donc (th. de Gauss) $62 | (y_0-y)$, i.e. $\exists k \in \mathbb{Z}^*$ t.q. $y_0-y=62k$.

De la même manière, $\exists p \in \mathbb{Z}^*$ t.q. $x-x_0=43p$.

Alors (E') s'écrit: 62×43p = 43×62k, donc p = k.

D'où la forme des solutions:

$\begin{cases} x = x_0 + 43k \\ y = y_0 - 62k \end{cases}, k \in \mathbb{Z}$, c'est-à-dire:

$$S = \{(-9+43k, 13-62k), k \in \mathbb{Z}\}.$$

NB: Si le 2nd membre est une constante autre que 1, multiple du Pgcd(a,b), il suffit de multiplier membre à membre par cette constante.