

Mathématiques discrètes. C5 - Théorie des nombres.

7 mars 2012

1 Théorème de Bachet-Bézout

1.1 PGCD et combinaisons linéaires

Pour tous a et b dans \mathbb{N} non tous nuls, une combinaison linéaire de a et b est un entier de la forme

$$n = au + bv,$$

avec $u, v \in \mathbb{Z}$.

Notons $C(a, b)$ l'ensemble des combinaisons linéaires de a et b :

$$C(a, b) = \{au + bv \mid u, v \in \mathbb{Z}\}.$$

Notons $C^+(a, b)$ l'ensemble des combinaisons linéaires strictement positives de a et b :

$$\begin{aligned} C^+(a, b) &= \{au + bv \mid au + bv > 0, u, v \in \mathbb{Z}\} \\ &= \mathbb{N}^* \cap C(a, b). \end{aligned}$$

Exemple. Pour $(a, b) = (1, 4)$. Quelques combinaisons linéaires :

$$0 = 1 \times 0 + 4 \times 0$$

$$3 = 3 \times 1 + 4 \times 0 = 1 \times (-1) + 4 \times 1$$

$$-3 = 3 \times (-1) + 4 \times 0 = 1 \times 1 + 4 \times (-1).$$

Exercice. Déterminer $C(1, 4)$, $C^+(1, 4)$. Même question pour $(a, b) = (6, 4)$.

Théorème. L'ensemble des combinaisons linéaires strictement positives de a et b coïncide avec à l'ensemble des multiples de $d = PGCD(a, b)$:

$$C^+(a, b) = d\mathbb{N}^*.$$

Preuve.

Notons e le plus petit élément de $C^+(a, b) : e = ak + bl > 0$. Dans un premier temps, on m.q.

$$C^+(a, b) = e\mathbb{N}^*.$$

D'une part, on m.q. e divise $c = au + bv$ pour tous $u, v \in \mathbb{Z}$. Faisons la division euclidienne de c par $e : c = e \times q + r$ avec $0 \leq r \leq e - 1$.

En remplaçant c et e par les combinaisons linéaires de a et b , on a $au + bv = (ak + bl) \times q + r$. Alors, $r = a(u - kq) + b(v - lq)$ est aussi une combinaison linéaire de a et b .

Si $r > 0$, il est un élément de $C^+(a, b) : e = ak + bl > 0$ qui est strictement plus petit que e - contradiction. Alors $r = 0$.

Donc, e divise $c = au + bv$ pour tous entiers u, v . Alors

$$C^+(a, b) \subset e\mathbb{N}^*.$$

D'autre part, un multiple de e s'écrit toujours $n \times e = n(au + bv) = a(nu) + b(nv)$.

Alors tout multiple de e est une combinaison linéaire de a et b .

Donc,

$$e\mathbb{N}^* \subset C^+(a, b).$$

Alors on a l'égalité

$$e\mathbb{N}^* = C^+(a, b).$$

Montrons maintenant que $d = e$.

Prenons $(u, v) = (1, 0)$ et $(0, 1)$, on a e divise a et b , donc, e est un diviseur commun de a et b . Alors e divise d . Inversement, d divise a et b alors d divise $ak + bl = e$. Alors $d = e$.

On a finalement

$$C^+(a, b) = d\mathbb{N}^*.$$

Corollaire. (Identité de Bachet-Bézout) Pour tous entiers naturels a et b non tous nuls dont d est le PGCD, il existe deux entiers u et v t.q.

$$d = au + bv.$$

Preuve. Prenons $(u, v) = (k, l)$ dans la preuve du théorème précédent, on a $au + bv = e = d$.

Exemple. Soient $(a, b) = (21, 6)$. Trouver leur PGCD et le couple (u, v) t.q. $d = au + bv$

a	b	q	r
21	6	3	3
6	3	2	0
3	0		

1.2 Algorithme d'Euclide étendu

Pour trouver $d = PGCD(a, b)$ et u, v t.q. $d = au + bv$, on suit l'algorithme d'Euclide étendu :

1. Initialiser $u = 1, u' = 0, v = 0, v' = 1$.
2. Vérifier si $b = 0$. Si oui, $d = a$ et (u, v) est le couple cherché.
Sinon, effectuer la division euclidienne $a = bq + r, 0 \leq r < b$.
Remplacer :
 - (a, b) par $(b, a - bq)$
 - (u, u') par $(u, u - u'q)$
 - (v, v') par $(v, v - v'q)$
 Retourner à la vérification.

(Faire une figure...)

Exemple. Application pour le couple $(a, b) = (21, 6)$.

a	b	q	r	u	u'	v	v'
21	6	3	3	1	0	0	1
6	3	2	0	0	1	1	-3
3	0			1	-2	-3	7

Conclusion : $d = 3, u = 1, v = -3$. On a $21 \times 1 + 6 \times (-3) = 3$.

Exemple. Trouver d, u, v pour le couple $(a, b) = (120, 23)$.

a	b	q	r	u	u'	v	v'
120	23	5	5	1	0	0	1
23	5	4	3	0	1	1	-5
5	3	1	2	1	-4	-5	21
3	2	1	1	-4	5	21	-26
2	1	2	0	5	-9	-26	47
1	0			-9		47	

On a $PGCD(120, 23) = 1$ et $120 \times (-9) + 23 \times 47 = 1$.

Preuve. Notons les valeurs de $(a, b, q, r, u, u', v, v')$ à l'étape i par $(a_i, b_i, q_i, r_i, u_i, u'_i, v_i, v'_i)$.
Que fait l'algo d'Euclide étendu ?

Initialisation (étape $i = 0$) : $a_i = a, b_i = b, \dots$ Remarquons que l'on a en particulier

$$\begin{cases} au_i + bv_i = a_i \\ au'_i + bv'_i = b_i \end{cases}$$

On montre que cette relation (*) est valable pour toute étape par récurrence en i .

À l'étape $i + 1$, si $b_i \neq 0$, on affecte

$$\begin{aligned} a_{i+1} &= b_i \\ b_{i+1} &= a_i - b_i q_i \\ u_{i+1} &= u'_i \\ u'_{i+1} &= u_i - u'_i q_i \\ v_{i+1} &= v'_i \\ v'_{i+1} &= v_i - v'_i q_i \end{aligned}$$

Alors on a

$$au_{i+1} + bv_{i+1} = au'_i + bv'_i = b_i = a_{i+1}$$

et

$$\begin{aligned} au'_{i+1} + bv'_{i+1} &= a(u_i - u'_i q_i) + b(v_i - v'_i q_i) \\ &= (au_i + bv_i) - (au'_i + bv'_i)q_i \\ &= a_i - b_i q_i \\ &= b_{i+1}. \end{aligned}$$

Donc la relation (*) est valable pour toute étape. À la dernière étape, on a

$$au_n + bv_n = a_n = d.$$

On trouve bien le PGCD du couple (a, b) et le couple (u, v) satisfaisant $au + bv = d$.

1.3 Application dans les équations diophantiennes.

Cet algorithme d'Euclide étendu permet d'étudier la plus simple de toutes les équations diophantiennes, à savoir

$$ax + by = c, \quad a, b, c \in \mathbb{N} \text{ et } x, y \in \mathbb{Z}. \quad (1)$$

Lemme de Gauss. Si c divise ab et a et c sont premiers entre eux, alors c divise b .

Solution. Soit d le PGCD de a et b . Rappelons que par l'algorithme d'Euclide étendu, on peut trouver en même temps d et le couple d'entiers (u, v) t.q. $au + bv = d$.

Etape 1. Si d ne divise pas c , il n'existe pas de solution.

Etape 2. Si d divise c , $c' = c/d$ est un entier.

Etape 2.1. On peut vérifier que $(x_0, y_0) = (c'u, c'v)$ est une solution particulière.

Etape 2.2. À partir de cette solution particulière, on peut construire toutes les solutions : en remplaçant c par $ax_0 + by_0$ dans l'équation originale, on obtient

$$ax + by = ax_0 + by_0.$$

Cela peut être réécrite comme suite

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

Posons $x' = x - x_0$, $y' = y - y_0$, $a' = a/d$, et $b' = b/d$, on obtient l'équation suivante

$$a'x' = b'y'. \quad (2)$$

On a b' divise $a'x'$

or b' et a' sont premiers entre eux

donc d'après le lemme de Gauss, b' divise x' , c.à.d., x' s'écrit

$$x' = kb', k \in \mathbb{Z}.$$

L'équation (2) est équivalente à la suivante

$$a'kb' + b'y' = 0 \iff y' = -ka'.$$

Alors $(x', y') = (kb', -ka'), k \in \mathbb{Z}$.

La solution générale est

$$(x, y) = (x_0 + x', y_0 + y') = (x_0 + kb', y_0 - ka'), k \in \mathbb{Z}.$$

où

$$\begin{cases} d = PGCD(a, b) \\ au + bv = d \\ a' = a/d, b' = b/d, c' = c/d \\ x_0 = c'u, y_0 = c'v \end{cases}$$

Exemple. Résoudre l'équation diophantienne suivante

$$240x + 46y = 10.$$

En appliquant l'algorithme d'Euclide étendu pour le couple $(240, 46)$, on obtient le PGCD $d = 2$:

$$PGCD(240, 46) = 2$$

et le couple $(u, v) = (-9, 47)$ satisfaisant

$$240u + 46v = 2.$$

Alors $c' = \frac{c}{d} = 5$ et une solution particulière est $(x_0, y_0) = (c'u, c'v) = (-45, 235)$.

La solution générale $(x, y) = (x_0 + kb', y_0 - ka'), k \in \mathbb{Z}$ où

$$a' = \frac{a}{d} = 120 \quad \text{et} \quad b' = \frac{b}{d} = 23.$$

Application numérique :

$$(x, y) = (-45 + 23k, 235 - 120k), k \in \mathbb{Z}.$$

2 Congruences.

Définition. Pour tous entiers $a, b, n, n > 0$, on dit que a et b sont *congrus modulo n* et l'on note

$$a \equiv b(\text{modulo } n) \text{ ou } a \equiv b(\text{mod } n)$$

si n divise $a - b$.

Exemple. $3 \equiv 23(\text{mod } 10)$ car $23 - 3 = 20$ est divisible par 10.

2.1 Propriétés.

Réflexivité. $a \equiv a(\text{mod } n)$

Symétrie. $a \equiv b(\text{mod } n)$ ssi $b \equiv a(\text{mod } n)$

Transitivité.

$$\begin{cases} a \equiv b(\text{mod } n) \\ b \equiv c(\text{mod } n) \end{cases} \Rightarrow a \equiv c(\text{mod } n).$$

Et l'on note dans ce cas $a \equiv b \equiv c(\text{mod } n)$.

Autres propriétés.

$$a \equiv b(\text{mod } n) \Rightarrow \begin{cases} a + c \equiv b + c(\text{mod } n) \\ ac \equiv bc(\text{mod } n) \\ a^k \equiv b^k(\text{mod } n) \end{cases}$$

$$\begin{cases} a \equiv b(\text{mod } n) \\ c \equiv d(\text{mod } n) \end{cases} \Rightarrow a + c \equiv b + d(\text{mod } n)$$

$$\begin{cases} a \equiv b(\text{mod } n) \\ m|n \end{cases} \Rightarrow a \equiv b(\text{mod } m)$$

Par les trois propriétés *Réflexivité*, *Symétrie* et *Transitivité*, la congruence modulo n définit une relation d'équivalence.

Exemple. On a $-7 \equiv 3 \equiv 13 \equiv 23(\text{mod } 10)$ alors on dit que $-7, 3, 13, 23$ sont équivalents modulo 10 et on dit de plus que ils appartiennent à la même classe d'équivalence modulo 10.

Les n classes d'équivalence modulo n sont définies comme suite :

$$\begin{cases} C_0 = \{kn, k \in \mathbb{Z}\} - \text{tous les multiples de } n \\ C_1 = \{kn + 1, k \in \mathbb{Z}\} - \text{tous les entiers qui sont congrus à 1 modulo } n \\ \vdots \\ C_{n-1} = \{kn + (n - 1)\} \end{cases}$$

D'une façon générale, pour tous $0 \leq r < n$, C_r se compose de tous les entiers congrus à r modulo n .

Les classes C_0, C_1, \dots, C_{n-1} sont représentées par $0, 1, \dots, n - 1$ respectivement. Et l'on note $\mathbb{Z}/n\mathbb{Z} = \{C_0, C_1, \dots, C_{n-1}\}$, ou encore $\mathbb{Z}/n\mathbb{Z} = \{0, 1, \dots, n - 1\}$, l'ensemble de ces n classes.

Exemple. Pour $n = 10$, on a 10 classes C_0, C_1, \dots, C_9 qui sont représentées par $0, 1, \dots, 9$, $\mathbb{Z}/10\mathbb{Z} = \{0, 1, 2, \dots, 9\}$. Et $-7, 3, 13, 23$ appartiennent à la même classe C_3 .

Addition et multiplication dans $\mathbb{Z}/n\mathbb{Z}$.

On peut définir l'addition et la multiplication dans l'ensemble $\mathbb{Z}/n\mathbb{Z}$. Par exemple, la somme et le produit de 7 et 8 dans $\mathbb{Z}/10\mathbb{Z}$ sont déterminés comme suit :

$7 + 8 = 15 \equiv 5 \pmod{10}$, alors on dit que $C_7 + C_8 = C_5$ ou encore $7 + 8 = 5$ dans $\mathbb{Z}/10\mathbb{Z}$.

$7 \times 8 = 56 \equiv 6 \pmod{10}$, on dit que $C_7 \times C_8 = C_6$ ou encore $7 \times 8 = 6$ dans $\mathbb{Z}/10\mathbb{Z}$.

Formellement,

$C_a + C_b = C_c$ (ou encore $a + b = c$) dans $\mathbb{Z}/n\mathbb{Z}$ si et seulement si $a + b \equiv c \pmod{n}$

$C_a \times C_b = C_c$ (ou encore $a \times b = c$) dans $\mathbb{Z}/n\mathbb{Z}$ si et seulement si $a \times b \equiv c \pmod{n}$.

Opposé et Inverse. Dans $\mathbb{Z}/n\mathbb{Z}$, on dit que

- b est l'opposé de a si $a + b = 0$.
- b est l'inverse de a si $a \times b = 1$. Et on dit que a est inversible.

Exemple. Dans $\mathbb{Z}/10\mathbb{Z}$:

- 4 est l'opposé de 6,
- 3 est l'inverse de 7 car $3 \times 7 = 1$ dans $\mathbb{Z}/10\mathbb{Z}$. On dit que 7 est inversible dans $\mathbb{Z}/10\mathbb{Z}$.

Question : 2 est-il inversible dans $\mathbb{Z}/10\mathbb{Z}$?

Remarque. b est l'inverse de a dans $\mathbb{Z}/n\mathbb{Z}$ ssi $ab \equiv 1(\text{mod } n)$, c.a.d., $ab - 1 = kn$, ou encore $ab - kn = 1$. Alors afin de trouver b l'inverse de a dans $\mathbb{Z}/n\mathbb{Z}$, on applique l'algorithme d'Euclide étendu pour le couple (a, n) .

- Cet algorithme nous donne l'inverse de a si a et n sont premiers entre eux.
- a n'est pas inversible si a et n ne sont pas premiers entre eux.

Exemple. 2 et 10 ne sont pas premiers entre eux, alors 2 n'est pas inversible dans $\mathbb{Z}/10\mathbb{Z}$. Effectivement 2 n'admet pas d'inverse dans $\mathbb{Z}/10\mathbb{Z}$.

2.2 Congruences du premier degré.

Problème. Résoudre l'équation suivante

$$ax \equiv b(\text{mod } n).$$

Solution. Il faut chercher x satisfaisant n divise $ax - b$, c.a.d.

$$ax - b = ny, y \in \mathbb{Z}.$$

On retrouve donc une équation diophantienne qui peut être résolue en appliquant l'algorithme d'Euclide étendu.

Exemple. Trouver $x \in \mathbb{Z}$ t.q.

$$21x \equiv 9(\text{mod } 6).$$

On a ici $a = 21, b = 9, n = 6$ et l'équation diophantienne correspondant est

$$21x - 6y = 9 \leftrightarrow 7x - 2y = 3.$$

L'algorithme d'Euclide étendu pour le couple $(a, n) = (7, 2)$:

a	b	q	r	u	u'	v	v'
7	2	3	1	1	0	0	1
2	1	2	0	0	1	1	-3
1	0			1	-2	-3	7

On obtient $d = PGCD(7, 2) = 1$ et $7 \times 1 + 2 \times (-3) = 1$.

Une solution particulière de l'équation diophantienne est $(1, 3)$. La solution générale est

$$(x, y) = (1 + 2k, 3 + 7k).$$

La solution de l'équation originale est donc

$$x = 1 + 2k, k \in \mathbb{Z}$$

ou

$$x \equiv 1(\text{mod } 2).$$

2.3 Système de congruences.

Problème. Soient a, b, m, n dans \mathbb{Z} t.q. $m > 0, n > 0$. Résoudre le système suivant

$$(S) \begin{cases} x \equiv a(\text{mod } m) \\ x \equiv b(\text{mod } n) \end{cases}$$

Exemple. Résoudre le système de congruences suivant

$$(S_1) \begin{cases} x \equiv 3(\text{mod } 11) \\ x \equiv 2(\text{mod } 27) \end{cases}$$

Théorème chinois. Si m et n sont premiers entre eux il existe un entier c tel que l'on ait l'équivalence suivante

$$(S) \iff x \equiv x_0(\text{mod } mn).$$

Autrement dit, si m et n sont premiers entre eux le système de congruences (S) admet une infinité de solutions dans \mathbb{Z} , ce sont tous les entiers de la forme $x = x_0 + kmn, k \in \mathbb{Z}$.

Preuve. Le système (S) est équivalent à un nouveau système

$$\begin{aligned} & \begin{cases} x = a + km \\ x = b + ln \end{cases} \quad k, l \in \mathbb{Z} \\ \iff & \begin{cases} a + km = b + ln \\ x = a + km \end{cases} \quad k, l \in \mathbb{Z} \\ \iff & \begin{cases} km - ln = b - a \\ x = a + km \end{cases} \quad k, l \in \mathbb{Z} \end{aligned}$$

Il faut résoudre l'équation diophantienne suivante pour les variables k et l

$$km - ln = b - a. \tag{3}$$

Comme m et n sont premiers entre eux, il existe un couple (u, v) t.q.

$$um + vn = 1.$$

D'où,

$$(b-a)um + (b-a)vn = b-a.$$

Alors une solution particulière de l'équation (3) est donnée par

$$(k_0, l_0) = \left((b-a)u, (a-b)v \right).$$

Par conséquent, une solution particulière de notre système (S) est donnée par

$$x_0 = a + k_0m = a + (b-a)um.$$

(S) est équivalent au système suivant

$$\begin{cases} x \equiv x_0 \pmod{m} \\ x \equiv x_0 \pmod{n} \end{cases} \Leftrightarrow \begin{cases} m|(x-x_0) \\ n|(x-x_0) \end{cases} \Leftrightarrow PPCM(m,n)|(x-x_0) \Leftrightarrow mn|(x-x_0)$$

puisque m et n sont premiers entre eux. En conclusion,

$$(S) \Leftrightarrow x \equiv x_0 \pmod{mn}$$

où

$$\begin{cases} x_0 = a + (b-a)um \\ u : um + vn = 1 \end{cases}$$

Une autre façon de calculer x_0 :

$$x_0 = a + (b-a)um = a(1-um) + bum = avn + bum.$$

Exemple. Résoudre le système de congruences suivant

$$(S_1) \begin{cases} x \equiv 3 \pmod{11} \\ x \equiv 2 \pmod{27} \end{cases}$$

Solution. Appliquons l'algorithme d'Euclide étendu pour trouver $d = PGCD(11, 27)$ et le couple (u, v) t.q. $d = 27u + 11v$.

a	b	q	r	u	u'	v	v'
27	11	2	5	1	0	0	1
11	5	2	1	0	1	1	-2
5	2	2	1	1	-2	-2	5
2	1	2	0	-2	5	5	-12
1	0						

Alors $PGCD(11, 27) = 1$ et de plus, $27 \times (-2) + 11 \times 5 = 1$.

Considérons $c = anv + bmu = 2 \times 11 \times 5 + 3 \times 27 \times (-2) = -52$. Alors c est une solution particulière du système de congruences (S) :

$$\begin{cases} -52 \equiv 3(mod\ 11) \\ -52 \equiv 2(mod\ 27) \end{cases}$$

D'après le théorème chinois, (S) est équivalent à l'équation $x \equiv c(mod\ mn)$, c.à.d., $x \equiv -52(mod\ 287)$. Les solutions de (S) sont de la forme $x = c + kmn = -52 + 287k, k \in \mathbb{Z}$.

Exemple. Résoudre le système de congruences suivant

$$(S_2) \begin{cases} x \equiv 5(mod\ 123) \\ x \equiv 5(mod\ 20) \end{cases}$$

Solution. Dans ce cas il est évident que 5 est une solution particulière de (S_2) , on a

$$(S_2) \iff PPCM(120, 23)|(x - 5).$$

Comme 123 et 20 sont premiers entre eux, $PPCM(120, 23) = 123 \times 20 = 2460$.

(S_2) est équivalent à $2460|(x - 5)$, alors les solutions de (S_2) sont $x = 5 + 2460k, k \in \mathbb{Z}$.