Chap. Annexe 2 Congruences – théorème de Bézout

1. Identité de Bézout

Si l'on se donne trois nombres réels a, b et c, avec a et b non nuls, on sait que l'équation :
(1) $xa + yb = c$
admet une infinité des solutions réelles, il suffit de se donner x arbitrairement et de calculer y par la formule : $y = (c - xa)/b$
Par contre si a et b sont des entiers , et si on cherche les entiers (x, y) qui sont solution de (1), le problème dévient beaucoup plus difficile (avant c'était de l'algèbre, maintenant c'est de l'arithmétique), car x ne peut plus être choisi arbitrairement.

Nous allons commencer par chercher quand l'équation (1) a des solutions, puis nous donnerons une méthode permettant de trouver une solution particulière, enfin nous montrerons comment on peut en déduire toutes les autres solutions.

Théorème 1

Soient $a_1, a_2, \ldots, a_n$ des entiers fixés. Alors l'ensemble des nombres de la forme : $x_1a_1 + x_2a_2 + \ldots + x_na_n$, où $x_1, x_2, \ldots, x_n$ sont des entiers relatifs quelconques, coïncide avec l'ensemble des multiples $a_1 \wedge a_2 \wedge \ldots \wedge a_n$.

Démo : *L'ensemble E des entiers de la forme : $x_1a_1 + x_2a_2 + \ldots + x_na_n$ possède deux propriétés importantes : si u est dans E, tout multiple de u est dans E, si u et v sont dans E, leur différence $u - v$ est dans E.*
Notons c le plus petit élément strictement positif de E et u un élément quelconque de E. Alors la division euclidienne de u par c donne $u = cq + r$ avec $0 \leq r < c$. Mais cq est dans E, car c est dans E, donc $u - cq$ aussi, et r est un élément de E. Il est forcement nul car il n'existe pas d'élément de E strictement positif inférieur à c. Ceci signifie que c divise tous les éléments de E. Donc E est constitué de multiples de c, et comme tout multiple de c est dans E, les éléments de E sont tous les multiples de c.
A présent démontrons que $c = a_1 \wedge a_2 \wedge \ldots \wedge a_n$. Chaque a_i est dans E ; on le voit en prenant tous les coefficients nuls sauf x_i qui vaut 1. Ces nombres sont donc des multiples de c, et c est un de leurs diviseurs communs. D'autre part tout diviseur commun aux nombres a_i divise n'importe quel élément de E, donc c en particulier. Nous venons de montrer que c est un diviseur commun aux a_i et qu'il est divisible par leur PGCD ; c'est donc $a_1 \wedge a_2 \wedge \ldots \wedge a_n$.
Il résulte de ce théorème qu'une équation du type :
$x_1a_1 + x_2a_2 + \ldots + x_na_n = c$ dans laquelle $a_1, a_2, \ldots, a_n$ et c sont des entiers relatifs connus, $x_1, x_2, \ldots, x_n$ sont des entiers relatifs inconnus, possède des solutions ssi le nombre c est un multiple de $a_1 \wedge a_2 \wedge \ldots \wedge a_n$. Fort improprement on appelle **identité de Bézout** l'équation particulière :
(2) $x_1a_1 + x_2a_2 + \ldots + x_na_n = a_1 \wedge a_2 \wedge \ldots \wedge a_n$.
et le théorème 1 nous dit qu'elle a toujours des solutions.
Maintenant nous allons voir comment on peut trouver toutes les solutions de l'équation
(3) $xa + yb = a \wedge b$.
Sans restreindre le problème nous supposerons que a et b sont deux entiers tels que : $a \geq b > 0$.

Théorème 2

Si l'on calcule $a \wedge b$ par l'algorithme d'Euclide :

$a = bq_1 + r_1$
$b = r_1q_2 + r_2$
$r_1 = r_2q_3 + r_3$
…….
$r_{n-2} = r_{n-1}q_n + r_n$
$r_{n-1} = r_nq_{n+1} + 0$

alors les entiers $A_1, A_2, \ldots, A_{n+1}$ et $B_1, B_2, \ldots, B_{n+1}$ définis par :

(4) $A_{-1} = 0$ $A_0 = 1$ $A_{k+1} = A_kq_{k+1} + A_{k-1}$
(5) $B_{-1} = 1$ $B_0 = 0$ $B_{k+1} = B_kq_{k+1} + B_{k-1}$

vérifient, quel que soit k compris entre –1 et n+1, la relation :

(6) $(-1)^k r_k = A_kb - B_ka$

En particulier :

(7) $a \wedge b = (-1)^n A_nb - (-1)^n B_na$

et une solution de l'équation de (3) est :

(8) $x = (-1)^{n+1}B_n$ $y = (-1)^n A_n$

Démo : *D'abord $r_{-1} = a = B_{-1}a - A_{-1}b$ et $r_0 = b = A_0b - B_0a$. Par conséquent (6) est vérifié pour $k = -1$ et $k = 0$. Ensuite posons $D_k = A_kb - B_ka$, et remplaçons* A_{k+1} et B_{k+1} dans $D_{k+1} = A_{k+1}b - B_{k+1}a$, par des valeurs données dans (4) et (5) ; nous obtenons alors : $D_{k+1} = q_{k+1}D_k + D_{k-1}$. *Si la relation (6) est vraie jusqu'à l'ordre $k\geq 2$ on a : $D_{k+1} = q_{k+1}(-1)^k r_k + (-1)^{k-1}r_{k-1} = (-1)^{k+1}r_{k+1}$ et elle est vraie aussi à l'ordre k+1. par récurrence elle est toujours vraie.*

Il n'est pas inutile de dire d'où sortent les nombres A_k et B_k. D'abord la première division donne $r_1= a - bq_1$, puis la seconde donne $r_2 = b - r_1q_2$ et si l'on remplace l'expression de r_1 qui vient d'être trouvée, on obtient $r2 = b(1+q1q2) - aq_2$. Alors on a l'idée de voir s'il existe des nombres A_k et B_k qui vérifieraient : $(-1)^k r_k = A_kb - B_ka$, puisqu'en les calculant jusqu'à k = n cela résoudrait l'équation de Bézout. On cherche donc quelle relation de récurrence pourrait lier ces nombres, et quelles seraient leurs premières valeurs ; c'est ainsi qu'on arrive à (4) et (5).

Pratiquement, pour calculer A_n et B_n "à la main", on dispose les calculs suivants. on inscrit d'abord les 0 et les 1, puis q_1, q_1, ... et on calcule A_1, B_1, A_2, B_2,... en utilisant (4) et (5).

	q_1	q_2	…	q_k	…	q_{n-1}	q_n	q_{n+1}
0 1 1 0	A_1 B_1	A_2 B_2	… …	A_k B_k	… …	A_{n-1} B_{n-1}	A_n B_n	A_{n+1} B_{n+1}

Exemple 1. *Calcul de PGCD de 791 et 336.*

	2	2	1	4	1	2
0 1 1 0	2 1	5 2	7 3	33 14	40 17	113 48

et on vérifie bien que 17*791 – 40*336 = 7.

Nous allons donner une interprétation des deux nombres A_{n+1} et B_{n+1}.

Théorème 3

Quel que soit k compris entre 0 et n + 1 on a :

(9) $A_kB_{k-1} – A_{k-1}B_k = (-1)^k$

et par conséquent les nombres A_k et B_k sont toujours premiers entre eux. De plus :

(10) $A_{n+1} = a/(a \wedge b)$ $B_{n+1} = b/(a \wedge b)$

Démo : *Posons $D_k = A_kB_{k-1} – A_{k-1} B_k$. L'égalité $D_0 = 1$ est évidemment vraie. Maintenant si l'on remplace A_{k+1} et B_{k+1} dans D_{k+1} par leurs valeurs tirées de (4) et (5) on trouve immédiatement : $D_{k+1} = -D_k$, et par une récurrence immédiate on en déduit que*

$D_k = (-1)^k$.

L'égalité (9) montre que les nombres A_k et B_k sont toujours premiers entre eux. Mais lorsque k = n + 1 l'égalité (6) devient : $A_{n+1}b – B_{n+1}a = (-1)^{n+1}r_{n+1} = 0$, c'est à dire : $bA_{n+1} = aB_{n+1}$. Comme A_{n+1} et B_{n+1} sont premiers entre eux, et comme A_{n+1} divise aB_{n+1}, l'affirmation 1) du lemme de Gauss nous dit que A_{n+1} divise a. Alors si l'on note c l'entier qui vérifie $a = cA_{n+1}$ nous avons : $bA_{n+1} = cA_{n+1} B_{n+1}$, ce qui donne $b = cB_{n+1}$. Mais, puisque $a = cA_{n+1}$ et $b = cB_{n+1}$ avec A_{n+1} et B_{n+1} premiers entre eux la troisième affirmation du théorème 8 du chapitre précédent montre que c = $a \wedge b$.

Exemple 2 *: Dans l'exemple 2 cela donne : 113 = 791/7 et 43 = 336/7.*

Les formules (8) nous ont fourni une solution particulière de (3). Il reste à voir quelles sont les autres, et alors le problème sera complètement résolu.

Théorème 4

Les solutions de l'équation (3) sont :

(11) $X = (-1)^{n+1}(B_n + kB_{n+1})$ $Y = (-1)^n(A_n + kA_{n+1})$

où k désigne un entier relatif quelconque.

Démo : *Notons x et y les solutions de l'équation (3) données par les formules (8). Si l'on a aussi : $Xa + Yb = a \wedge b$ on en déduit que :$(X – x)a = (y – Y)b$ et en divisant les deux membres de cette égalité par $a \wedge b$ on obtient :*

(12) $(X –x)A_{n+1} = (y – Y)B_{n+1}$

Comme B_{n+1} divise le membre de droite il divise aussi le membre de gauche, et puisqu'il est premier avec A_{n+1}, il divise $(X –x)$ d'après la première affirmation du lemme de Gauss. Donc il existe un entier relatif K tel que $(X – x) = K B_{n+1}$, mais pour tomber exactement sur (11) nous poserons $k = (-1)^{n+1}K$, ce qui donne alors : $(X –x) = (-1)^{n+1}k B_{n+1}$. En reportant cette égalité dans (12) on en déduit aussitôt que : $(y – Y) = (-1)^n k A_{n+1}$.

Réciproquement si k est un entier relatif quelconque on vérifie que les nombres X et Y donnés par la formule (11) constituent bien une solution de (3).

La méthode employée pour démontrer ce théorème permet de résoudre toutes les équations du type $xa+yb = a \wedge b$.

Exemple 3 *L'équation : $3x + 5y = 28$ possède des solutions parce que 3 et 5 sont premiers entre eux. Cherchons alors une solution de $3x + 5y = 1$. Les formules (8) donnent $3*2 – 5*1 = 1$. Multiplions les deux membres par 28 ce qui donne $3*56 – 5*28 = 28$; nous avons ainsi la solution particulière de l'équation. Pour chercher la solution générale on fait la différence de deux équations : $3(x – 56) = 5(y + 28)$. Puisque 3 est premier à 5 il divise $y + 28$; donc $y = -28 + 3k$ et $x = 56 + 5k$ pour un certain k. On vérifie facilement que n'importe quel entier k fait l'affaire et l'équation est résolue.*

2. Entiers modulo n.

Dans toute cette partie n désigne un entier supérieur ou égal à 2 qui est fixé. Il est possible d'ajouter, soustraire ou multiplier des entiers relatifs, en faisant "comme si" le nombre n valait 0. Bien évidemment les résultats de ces calculs ne s'expriment pas au moyen de vraies égalités ; c'est pourquoi on utilisera le symbole ≡ à la place de =, et nos fausses égalités s'appelleront des congruences.

Soient a et b deux entiers relatifs ; si a – b est un multiple de n on dit que a est congru à b modulo n et on écrit $a\equiv b \pmod n$. Si r est le reste de la division euclidienne de a par n nous avons : $a \equiv r \pmod n$, et r s'appelle le résidu de a modulo n.

Théorème 5.

1) $a\equiv b \pmod n$ ssi les résidus de a et de b sont les mêmes.
2) La relation $a\equiv b \pmod n$ est une relation d'équivalence sur **Z**.
3) Si a est un entier relatif sa classe d'équivalence est formée des entiers obtenus en lui ajoutant un multiple quelconque de n ; on la note $\overline{a}$ et on dit que a est un représentant de $\overline{a}$.
4) Chaque classe contient un unique entier r vérifiant $0\le r<n$; c'est le résidu commun à tous les éléments de la classe.
5) L'ensemble des classes d'équivalence s'appelle l'ensemble des entiers modulo n, on le note Z/nZ ; il possède n éléments. Plus précisément : $Z/nZ = \{ \overline{0}, \overline{1}, \ldots \overline{n-1}\}$.

Démo : *1) La division euclidienne de a et de b par n donne : $a = nq_1 + r_1$ et $b = nq_2 + r_2$; on a alors : $a – b = n(q_1 – q_2) + (r_1 – r_2)$. Si les restes sont égaux $a – b = n(q_1 – q_2)$ et alors $a\equiv b \pmod n$. Réciproquement si n divise a – b il divise aussi $r_1 – r_2$. Comme $0\le r_1<n$ et $0\le r_2<n$, nous avons $|r_1 – r_2| < n$, mais 0 étant le seul multiple de n dont la valeur absolue soit strictement inférieure à n, on a forcément $r_1 – r_2 = 0$.*
Les affirmations 2) et 3) sont immédiates ; passons à la quatrième. D'après 1) tous les éléments ont le même résidu et ce nombre, qui appartient à la classe, vérifie $0\le r<n$. *Si un autre nombre de la classe vérifie ces inégalités sa différence avec le résidu commun est un multiple de n de valeur absolue inférieure à n, ce ne peut donc être que 0, et on a bien l'unicité. Donc les classes sont caractérisées par le résidu commun à tous leurs éléments.*

Exemple 4
Avec n = 3 il y a trois classes d'équivalence :
$\overline{0} = \{\ldots, -3, 0, 3, 6, \ldots\}$
$\overline{1} = \{\ldots, -2, 1, 4, 7, \ldots\}$
$\overline{2} = \{\ldots, -1, 2, 5, 8, \ldots\}$

Remarque : Dans le cas particulier n = 2 il n'y a que 2 classes ; en prenant comme représentant de ces classes les bits 0 et 1 on identifie Z/2Z avec B.

On notera que les éléments de Z/nZ sont tous les progressions arithmétiques infinies de raison n.

Problème
Sachant que le 1er janvier 1994 est un samedi, quel jour de la semaine tombe le 144ième jour de l'année ?

Chaque jour de la semaine revient tous les 7 jours. Par conséquent, si on numérote les jours de l'année de 1 à 365, deux jours occupent la même position dans la semaine ssi leurs numéros sont congrus modulo 7. 144 mod 7 = 4, donc le 144ième jour de l'année occupe la même position que le 4ième.
samedi = {1, 8, 15, …}
dimanche = {2, 9, 16,…}
lundi = {3, 10, 17, …}
mardi = {4, 11, 18, …,144,…}
mercredi = {5, 12, 19, …}
jeudi = {6, 13, 20, …}
vendredi = {7, 14, 21, …}

Le théorème suivant permet de définir une addition et une multiplication sur Z/nZ appellées addition modulo n et multiplication modulo n.

Théorème 6.

Si $a_1 \equiv a_2 \pmod{n}$ et $b_1 \equiv b_2 \pmod{n}$ alors :
(13) $a_1 + b_1 \equiv a_2 + b_2 \pmod{n}$ (14) $a_1 b_1 \equiv a_2 b_2 \pmod{n}$.

Le théorème de Bézout affirme que le PGCD *d* de deux entiers *a* et *b* est une combinaison linéaire (à coefficients entiers) de *a* et *b* :

$$d = au + bv.$$

Une modification simple de l'algorithme d'Euclide (qu'on appelle alors algorithme d'Euclide *étendu*) permet de calculer ces coefficients *u* et *v*. Remarquons d'abord que l'algorithme d'Euclide calcule une suite définie par une récurrence à deux termes :

$$a_0 = a \text{ , } a_1 = b$$
$$a_{n-1} = q_n a_n + a_{n+1}$$

autrement dit :

$$a_{n+1} = - q_n a_n + a_{n-1} \text{ (*)}$$

donc en posant :

$$a_n = a\, u_n + b\, v_n$$

u_n et v_n vérifient la même récurrence (*) que a_n, avec les conditions initiales :

$$u_0 = 1\ ,\ v_0 = 0$$
$$u_1 = 0\ ,\ v_1 = 1$$

Exemple (suite) :

		u		v
96	= 96 *	1	+ 81 *	0
81	= 96 *	0	+ 81 *	1
15	=	96 - 81		
	= 96 *	(1 - 0)	+ 81 *	(0 - 1)
	= 96 *	1	+ 81 *	-1
6	=	81 - 5 * 15		
	= 96 *	(0 - 5 * 1)	+ 81 *	(1 - 5 * (-1))
	= 96 *	-5	+ 81 *	6
3	=	15 - 2 * 6		
	= 96 *	(1 - 2 * (-5))	+ 81 *	(-1 - 2 * 6)
	= 96 *	11	+ 81 *	-13

Exercices

1) 47u + 111v = 1

111 = 47*2 + 17
47 = 17*2 + 13
17 = 13 + 4
13 = 4*3 + 1,

donc u et v existent

On remonte
1 = 13 – 4*3 = 13 – (17 – 13)*3 = 13 – 17*3 + 13*3 = 13*4 – 17*3 = (47 – 17*2)*4 – 17*3 = 47*4-17*8 – 17*3 = 47*4 –17*11 = 47*4 – (111-47*2)*11 = 47*4 – 111*11 + 47*22 = 47*26 – 111*11
u = 26, v = -11

2) 693u + 680v = 1

693 = 680 + 13
680 = 13*52 + 4
13 = 4*3 + 1

On remonte
1 = 13 – 4*3 = 13 – (680 – 13*52)*3 = 13 – 680*3 + 13*156 = 13*157 – 680*3 = (693 – 680)*157 – 680*3 = 693*157 –680*160
u = 157
v = -160

3) Déterminer

a) le pgcd(1482,1428).

1482 = 1428*1 + 54
1428 = 54*26 + 24
54 = 24*2 + 6
24 = 6*4 + 0 $\Rightarrow$ pgcd(1482,1428) = 6

b) Trouver deux entiers u_0 et v_0 tels que : d = 1482u_0 + 1428v_0

6 = 54 – 24*2
24 = 1428 – 54*26
54 = 1482 – 1428
6 = 1482 – 1428 – (1428 – (1482 – 1428) * 26)*2 = 1482(1+52) + 1428(-1 – 2 –52) =
1482*53 + 1428* (-55)

c) Résoudre dans Z l'équation 1482u + 1428v = d

1482 = 6 * 247
1428 = 6 * 238
Apparemment, 247 et 238 sont premiers entre eux.
Il faut trouver u et v, tels que 1482u + 1428v = 6
247 * 6 *u + 238 * 6 * v = 6
247 * 6 * 53 + 238 * 6 * (-55) = 6

On fait la soustraction :
247 * 6 * (u – 53) + 238 * 6 * (v + 55) = 0

On divise par 6 et on obtient : 247 * (u – 53) + 238 * (v + 55) = 0
C.à.d. que 247 * (u –53) = -238 * (55 + v)

Comme 247 et 238 sont premiers entre eux u – 53 = 238q et -55 – v = 247q

Alors u = 238q + 53 et v = -55 – 247q

Déf.
L'inverse modulo b^{-1} de b est le nombre entier tel que $b \cdot b^{-1}$ (mod n) = 1. Par exemple 7 est l'inverse modulo 9 de 4, car 4·7 (mod 9) = 1.

Pour qu'un nombre b possède un inverse modulo n b^{-1} il faut que b et n soient premiers entre eux.
Démonstration par contradiction.
Imaginons que b et n ne sont pas premiers entre eux et que b possède un inverse modulo n b^{-1}.
Alors b = kl et n = kt, comme b et n ont un pgcd k ≠ 1. b* b^{-1} = k*l* b^{-1} divisible par k, n = kt est divisible par k, donc k ≠ 1 est un diviseur commun de b* b^{-1} et n. Contradiction avec l'énoncé (par définition b* b^{-1} est premier avec n).

L'algorithme d'Euclide étendu permet de calculer l'inverse de *b* modulo *n* s'il existe.
Il faut calculer le pgcd de b et n, en calculant u et v en même temps. Si le pgcd = 1, alors
SI u < 0

b^{-1} = (n + u) mod n
SINON
b^{-1} = u mod n

Exemple
Trouver 15^{-1} modulo 26.

15 = 1*15 + 26*0
26 = 0*15 + 26*1
26 = 15*1 + 11
15 = 11 + 4
11 = 4*2 + 3
4 = 3 + 1
3 = 1*3 + 0
pgcd(26, 15) = 1
Remontons
1 = 4 – 3
3 = 11 – 4*2
1 = 4 – (11 – 4*2)
4 = 15 – 11
1 = (15 – 11) – (11 – 4*2)
4 = 15 – 11
1 = (15 – 11) – (11 – (15 - 11)*2)
11 = 26 – 15
1 = (15 – (26 – 15)) – ((26 – 15) – (15 – (26-15))*2)
1 = 15 – 26 + 15 – 26 + 15 + 15*2 - 26*2 + 15*2
1 = 15*7 +26*(-4)

u = 7
15^{-1} = 7 [26]
7*15 = 105
105 = 26*4 + 1

Exemple
Trouver 5^{-1} modulo 8.
5 = 8*0 + 5
8 = 5*1 + 3
5 = 3*1 + 2
3 = 2*1 + 1
1 = 3 –2*1 = 3 – (5 – 3*1) = 8 –5 – (5 – (8 – 5)) = 8 – 5 – 5 + 8 – 5 = 5*(-3) + 8*1
u = -3
5^{-1} = 8 – 3 = 5 [8]
5*5 = 25
25 = 8*3 + 1