R1.06 : Mathématiques discrètes

Première année - iut informatique

Chapitre 2 : L'arithmétique

Cours : Aude Maignan *aude.maignan@univ-grenoble-alpes.fr*

L'art de calculer, de faire des opérations

La division euclidienne sur $\mathbb{N}$ et les bases de numérations

La division euclidienne

Theorem 1.

Soient $a \in \mathbb{N}$ et $b \in \mathbb{N}^*$
alors il existe un unique couple d'entiers naturels (q, r) tel que

$$a = bq + r \quad et \quad 0 \leqslant r < b$$

q se nomme le quotient et r est le reste de ***la division euclidienne*** *de a (le dividende) par b (le diviseur).*

Quand $r = 0$ on a $a = bq$ et l'on dit que b ***divise*** a. On le note $b|a$.
On dit aussi que a est *multiple* de b.

Exemple

Soit $a = 67$ et $b = 5$, On pose la division classique et on obtient $67 = 5 \times 13 + 2$, d'où $q = a\,div\,b = 13$ et $r = a\,mod\,b = 2$

On remarque que

- $67 = 5 \times 14 - 3$ n'est pas obtenu grâce à la division euclidienne.
- 67 n'est pas multiple de 5 car 67 mod 5 =2. Mais 65 est multiple de 5.

Petite preuve

Prouvons que si q divise 2 entiers a et b (avec a>b) alors il divise a+b.
$q|a$ donc $\exists d \in \mathbb{N}, a = dq$
de même, $q|b$ donc $\exists e \in \mathbb{N}, b = eq$.
Du coup $a + b = (d + e)q$ et $d + e \in \mathbb{N}$ donc $q|(a + b)$.
Plus généralement,

Proposition

Si $q|a$ et $q|b$ alors $q|(ax + by)$ avec $(x \in \mathbb{Z}, y \in \mathbb{Z})$

Proposition

Si $q|a$ et $q|b$ alors $q|(ax + by)$ avec $(x \in \mathbb{Z}, y \in \mathbb{Z})$

Example 2.

Si $a|10$ et $a|3$

alors $a|(10 - 3 \times 3)$

c'est-à-dire $a|1$

autrement dit $a = 1$.

Application : Bases de numération

On a l'habitude de noter les nombres à l'aide de 10 chiffres. En fait, le nombre 10 est arbitraire, et l'on aurait pu choisir n'importe quel entier supérieur ou égal à 2.

Definition 3.

Etant donné un entier b strictement supérieur à 1 et un entier a, il existe un nombre $n \in \mathbb{N}$ et une suite d'entiers $\{\alpha_i, 0 \leqslant i \leqslant n\}$ déterminés de façon unique tels que :

$$a = \sum_{i=0}^{n} \alpha_i b^i$$

et $\alpha_i < b$.
On appelle b la base de numération pour l'écriture des nombres entiers et on représente l'entier a par la suite $< \alpha_n, \alpha_{n-1}, \ldots, \alpha_0 >_b$.

Méthode de calcul des α_i

- α_0 est le reste de la division de a par b.
- On pose $a - \alpha_0 = q_1 b$, α_1 est le reste de la division de q_1 par b.
- et ainsi de suite...

Remarque :

- L'écriture de b en base b est toujours 10. En effet $b = 1.b + 0 =< 1, 0 >_b$.
- Les bases supérieurs à 11 : A partir de 10 on remplace les nombres par des lettres pris par ordre alphabétique.

Les nombres premiers

Nombres Premiers

Definition 4.

On dit qu'un entier naturel p différent de 1 est premier s'il n'a que 2 diviseurs qui sont 1 et p.

Ainsi les entiers 1,6, 25, 63 ne sont pas premiers.
Les entiers 2, 3, 5, 7, 11, 13, 17... sont premiers. Il existe une infinité de nombres premiers.

La recherche des nombres premiers

Il n'existe pas de formule algèbrique pour représenter un nombre premier. La méthode d'Ératosthène permet de déterminer tous les nombres premiers inférieurs à un entier n. Elle consiste à supprimer tous les multiples des nombres premiers déjà trouvés.

- on se donne la grille des nombres entiers de 2 à n.
- Commençant à 2, on supprime tous les multiples de 2.
- l'entier 3 n'a pas été supprimé et il ne peut être multiple des entiers qui le précèdent, sinon on l'aurait supprimé ; il est donc premier : supprimons alors tous les multiples de 3.
- L'entier 5 n'a pas été supprimé, il est donc premier. Et ainsi de suite... tous les nombres non supprimés sont premiers.

Remarque : Pour prouver qu'un nombre n est premier, il suffit de prouver qu'aucun des nombres premiers inférieurs à $\sqrt{n}$ ne divise n.

Preuve Supposons que n est divisible par un nombre premier q et $n > q > \sqrt{n}$ alors $\exists q' \in \mathbb{N}, n = qq'$ avec $1 < q' < \sqrt{n}$ et $\exists p < \sqrt{n}$ et p premier,$1 < p < \sqrt{n}$ et $q' = pp'$ et $p|n$.
Autrement dit, si n admet un diviseur premier plus grand que $\sqrt{n}$, il admet un diviseur premier plus petit que $\sqrt{n}$.

Factorisation

Theorem 5 (fondamental de l'arithmétique).

Pour tout entier $n \in \mathbb{N} - \{0, 1\}$, on appelle décomposition primaire (ou en facteurs premiers) une suite $((q_1, \alpha_1), ..., (q_r, \alpha_r))$ où
1) $r \in \mathbb{N}^*$;
2) q_i est premier et ($i < j$ implique $q_i < q_j$) ;
3) $\alpha_i \in \mathbb{N}^*$;
4) $n = {q_1}^{\alpha_1} ... {q_r}^{\alpha_r}$.
Alors, tout entier différent de 0 possède une ***unique décomposition*** *en facteur premier.*

Exemple : $2200 = 2^3 \times 5^2 \times 11$
$1236 = 2 \times 618 = 2^2 \times 309 = 2^2 \times 3 \times 103$
Prouvons que 103 est premier $[\sqrt{103}] = 10$, il suffit de vérifier que 103 n'est pas divisible par 2,3,5 et 7.

Lemme

[Euclide] Soit p un nombre premier, et a, b deux nombres entiers relatifs. Si p divise ab, alors p divise soit a soit b

PGCD–PPCM,
nombres premiers entre eux,
Bachet-Bézout

Soit $a \in \mathbb{N}^*$, on note $\mathcal{D}(a)$ l'ensemble des diviseurs positifs de a et $\mathcal{M}(a)$ l'ensemble des multiples de a.

Definition 6 (PGCD–PPCM).

1. L'ensemble $\mathcal{D}(a, b)$ des diviseurs communs à a et b possède un plus grand élément d, appelé **Plus Grand Commun Diviseur** de a et b et l'on note

$$d = \text{pgcd}(a, b)$$

2. L'ensemble $\mathcal{M}(a, b)$ des multiples communs à a et b possède un plus petit élément m appelé **Plus Petit Commun Multiple** de a et b et l'on note

$$m = ppcm(a, b)$$

Example 7.

Les diviseurs de 15 sont : $\mathcal{D}(15) = \{1, 3, 5, 15\}$.

Les diviseurs de 18 sont : $\mathcal{D}(18) = \{1, 2, 3, 6, 9, 18\}$.

Donc les diviseurs communs sont $\mathcal{D}(15, 18) = \{1, 3\}$ donc

$\text{pgcd}(15, 18) = 3$.

Les multiples de 15 sont : $\mathcal{M}(15) = \{15, 30, 45, 60, 75, 90, 105, ...\}$.

Les diviseurs de 18 sont : $\mathcal{M}(18) = \{18, 36, 54, 72, 90, 108, ...\}$.

Donc les multiples communs sont $\mathcal{M}(15, 18) = \{90, 180, 270, ...\}$ et donc

$ppcm(15, 18) = 90$.

Definition 8.

Deux entiers naturels non nuls a et b sont dits ***premiers entre eux*** si $\text{pgcd}(a, b) = 1$.

Example 9.

9 et 8 sont premiers entre eux ; $\text{pgcd}(9, 8) = 1$.

Propriétés du PGCD

Pour tout a, b et k dans $\mathbb{N}^*$ on a

1. commutativité : $\text{pgcd}(a, b) = \text{pgcd}(b, a)$
2. associativité : $pgcd(a, pgcd(b, c)) = pgcd(pgcd(a, b), c)$
3. distributivité : $\text{pgcd}(ka, kb) = k\ \text{pgcd}(a, b)$
4. $pgcd(a, 1) = 1, pgcd(a, 0) = a$
5. Si $a|b$ alors $\text{pgcd}(a, b) = a$ et $ppcm(a, b) = b$
6. $\text{pgcd}(a, b)|ppcm(a, b)$

7. Soient $d = \text{pgcd}(a, b)$ et a', b' tels que $a = da'$ et $b = db'$ alors $\text{pgcd}(a', b') = 1$
8. $\text{pgcd}(a, b) = \text{pgcd}(a, b \pm ka)$

Calcul pratique du pgcd : L'algorithme d'Euclide

Cet algorithme récursif est basé sur la proposition suivante :

Theorem 10.

Etant donné 2 entiers a et b tels que $0 < b < a$*, l'ensemble des diviseurs communs à a et b est le même que l'ensemble des diviseurs communs à b et à a mod b. Donc pgcd(a,b)=pgcd(b,a mod b).*

Preuve Si $b = 0$, L'ensemble des diviseurs de a et 0 : $D(a, 0) = \{n : n \in \mathbb{N} \text{ et } n|a\}$ donc pgcd(a,0)=a
Si $b \neq 0$, par division euclidienne, $a = bq + r$. Si $d|a$ et $d|b$ alors $d|r$.
Inversement si $d|b$ et $d|r$ alors $d|a$, ce qui démontre la proposition.

Exemple

Calculons pgcd(1236,96) avec l'algorithme d'Euclide.

$$\begin{array}{cc} 1236 & 96 \\ 96 & 84 \\ 84 & 12 \end{array} \qquad \begin{array}{l} 1236 = 96 \times 12 + 84 \\ 96 = 84 + 12 \\ 84 = 12 \times 7 + 0 \end{array}$$

Ces calculs peuvent etre présenté dans un tableau

a	b	r	q
1236	96	84	12
96	84	12	1
84	12	0	7

12 est le dernier reste non nul Donc pgcd(1236,96)= 12.

L'algorithme d'Euclide

Soit a et b deux entiers, $a > b$. la première division euclidienne donne :

$a = bq_1 + r_1$ avec $0 \leqslant r1 < b$	$pgcd(a, b) = pgcd(b, r_1)$
$b = r_1 q_2 + r_2$ avec $0 \leqslant r2 < r1$	$pgcd(a, b) = pgcd(r_1, r_2)$
...	
$r_{n-2} = r_{n-1} q_n + r_n$ avec $0 \leqslant r_n < r_{n-1}$	$pgcd(a, b) = pgcd(r_{n-1}, r_n)$
$r_{n-1} = r_n q_{n+1} + 0$ avec $r_{n+1} = 0$	$pgcd(a, b) = pgcd(r_n, 0) = r_n$

Le pgcd de a et b est le dernier reste non nul de l'algorithme d'Euclide.

L'identité de Bézout

Theorem 11.

Soient a, b dans $\mathbb{N}^*$.
***Si** l'on note $d = pgcd(a, b)$ **alors** il existe deux entiers relatifs u et v tels que*

$$au + bv = d$$

REMARQUE : les entiers relatifs u et v du théorème ne sont pas uniques
Exemple : $a = 7$ et $b = 11$, on a : $(-3) \times 7 + 2 \times 11 = 8 \times 7 - 5 \times 11 = 1$
Plus généralement :

$$au + bv = a(u + kb) + b(v - ka) \text{ est valable pour tout } k$$

Calcul de u et v tel que $au + bv = \text{pgcd}(a, b)$

Le calcul de u et v se fait à partir de l'algorithme d'Euclide.
Exemple a=32 et b=12.
$a = 2b + 8$, soit $r_1 = 8 = a - 2b$
$b = r_1 + 4$, soit $r_2 = 4 = b - r_1 = b - (a - 2b) = 3b - a$
$r_1 = 2r_2 + 0$, $r_2 = pgcd(a, b) = 3b - a$, d'ou u=-1 et v=3.

Calcul de u et v tel que $au + bv = \text{pgcd}(a, b)$: Algorithme d'Euclide-Bézout

Initialisation : Notons $a = r_{-1}$, $b = r_0$, $(u_{-1}, v_{-1}) = (1, 0)$ et $(u_0, v_0) = (0, 1)$
(donc $r_{-1} = u_{-1} \times a + v_{-1} \times b$ et $r_0 = u_0 \times a + v_0 \times b$)
à chaque itération nous devons

- Calculer par division euclidienne les restes et les quotients succéssifs r_i et q_i et
- Calculer le couple (u_i, v_i) tel que $r_i = u_i \times a + v_i \times b$

A la fin, le dernier reste non nul étant le pgcd, nous obtiendrons
$pgcd(a, b) = r_n = u_n \times a + v_n \times b$.
Proposition : Pour $i \geqslant 1$, $(u_i, v_i) = (u_{i-2} - q_i u_{i-1}, v_{i-2} - q_i v_{i-1})$

Preuve par récurrence

A chaque niveau, nous devons avoir : $r_i = u_i a + v_i b$.

- Cette propriété est vraie au rang -1 et au rang 0.
- Supposons la vraie à un rang $k-1$ et k : $r_{k-1} = u_{k-1}a + v_{k-1}b$ et $r_k = u_k a + v_k b$

La division euclidienne nous permet d'obtenir

$$r_{k-1} = q_{k+1} r_k + r_{k+1}$$

d'où $r_{k+1} = -q_{k+1} r_k + r_{k-1}$
$\Leftrightarrow r_{k+1} = -q_{k+1}(u_k a + v_k b) + u_{k-1}a + v_{k-1}b$
$\Leftrightarrow r_{k+1} = (u_{k-1} - q_{k+1}u_k)a + (v_{k-1} - q_{k+1}v_k)b$
d'où $u_{k+1} = u_{k-1} - q_{k+1}u_k$ et $v_{k+1} = v_{k-1} - q_{k+1}v_k$

Exemple

a	b	r	q	u	v
		1236		1	0
	1236	96		0	1
1236	96	84	12	1	-12
96	84	12	1	-1	13
84	12	0	7		

Du coup $12 = -1236 + 13 \times 96$

Theorem 12 (Bachet–Bézout).

Soient $a, b \in \mathbb{N}^*$.

a et b sont premiers entre eux si et seulement si il existe deux entiers relatifs u et v tels que

$$au + bv = 1$$

Theorem 13 (Gauss).

Soient $a, b \in \mathbb{N}^*$.

Si $a|bc$ *et* $pgcd(a, b) = 1$ ***alors*** $a|c$.

Démonstration

pgcd$(a, b) = 1$ donc d'après le théorème de Bachet-Bézout, $\exists(u, v)$ tels que $au + bv = 1$.
En multipliant à gauche et à droite par c on obtient

$$auc + bvc = c$$

or $a|bc$ donc $\exists k$ tel que $bc = ka$ donc en remplaçant

$$auc + kav = c \quad \text{soit} \quad a(uc + kv) = c$$

cela signifie que $a|c$. □

Une propriété importante en découlant est que

$$\text{pgcd}(a, b) \times ppcm(a, b) = ab$$

Preuve : Notons $\nu = ppcm(a; b)$ et $\sigma = pgcd(a; b)$.
Il existe a' et b' tel que $a = \sigma a'$ et $b = \sigma b'$.
On va montrer que $\nu = \sigma a' b'$

- $\sigma a' b'$ est un multiple de a et de b donc par définition $\nu | \sigma a' b'$.
- Réciproquement : notons u et v les entiers tels que $\nu = au = bv$.
  On obtient $\nu = \sigma a' u = \sigma b' v$ et donc $a' u = b' v$ ce qui implique b' divise $a' u$ or a' et b' sont premiers entre eux donc d'après le théorème de Gauss b' divise u donc il existe q tel que $u = b' q$. En remplaçant u dans l'équation $\nu = au$ on obtient alors $\nu = \sigma a' b' q$ et donc $\nu | \sigma a' b'$.
- Finalement $\nu | \sigma a' b'$ et $\nu | \sigma a' b'$ donc $\nu = \sigma a' b'$

Les congruences

C'est un outil efficace en arithmétique.
Soit n un entier naturel non nul.

Definition 14.

Soient a et b deux entiers relatifs. On dit que a ***est congru à*** b ***modulo*** n si et seulement si $n|(a-b)$.

On note

$$a \equiv b (mod\ n)$$

Example 15.

On a $24 \equiv 0 (mod\, 2)$ ou encore $24 \equiv 10 (mod\, 2)$ ou $24 \equiv -2 (mod\, 2)$

REMARQUE : pour un entier a fixé, il n'y a pas unicité de b tel que $a \equiv b (mod\, n)$.

En effet $a \equiv b(\mod n)$ est équivalent à $\exists k \in \mathbb{Z}, a = b + nk$.
Le plus souvent on choisira (par efficacité) b comme étant le reste de la division euclidienne de a par n et on aura dans ce cas $0 \leqslant b < n$.

Propriétés

1. On suppose $a \equiv b \pmod{n}$ et $c \equiv d \pmod{n}$ alors
   - $ax + cy \equiv bx + dy \pmod{n}$
   - $ac \equiv bd \pmod{n}$

2. Pour tout $m \in \mathbb{N}^*$ si $a \equiv b \pmod{n}$ alors $a^m \equiv b^m \pmod{n}$

3. $ac \equiv bc \pmod{n} \Leftrightarrow a \equiv b \pmod{n/\delta}$ où $\delta = \text{pgcd}(c, n)$

4. Soient n_1 et $n_2 \in \mathbb{N}^*$ alors

$$\left.\begin{array}{l} a \equiv b \pmod{n_1} \\ a \equiv b \pmod{n_2} \end{array}\right\} \Leftrightarrow a \equiv b \pmod{ppcm(n_1, n_2)}$$

Calculs avec congruence

Comment fait-on pour

1. Calculer efficacement $7^{122} (mod\, 13)$
2. Montrer que $10^6 - 1$ est un multiple de 7

Le petit théorème de Fermat et le théorème d'Euler

Le petit théorème de Fermat, énoncé en 1640 et prouvé par Euler en 1736

Theorem 16.

Soit $a \in N$ et p un nombre premier. Alors on a :

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

Si de plus $p \nmid a$, il est équivalent de dire que

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

Exercice : Montrer que $5^{44} - 4$ est divisible par 7.

Definition 17.

La fonction $\varphi(n)$ (phi de n) d'Euler est ainsi définie :

$$\varphi(n) = \text{ le nombre d'entiers naturels inférieurs à } n \text{ ET premiers avec } n$$

Example 18.

$\varphi(8) = 4$ car 1, 3, 5 et 7 sont premiers avec 8.

$\varphi(9) = 6$ car 1, 2, 4, 5, 7 et 8 sont premiers avec 8.

Propriétés :

1. Si p est premier alors $\varphi(p) = p - 1 =$ tous les entiers entre 1 et $< p$
2. Si p est premier alors $\varphi(p^k) = (p-1)p^{k-1}$
3. Si $\text{pgcd}(m, n) = 1$ alors $\varphi(mn) = \varphi(m) \times \varphi(n)$.

Conséquence pratique : *si on connait* la décomposition en facteurs premiers de n

$$n = p_1^{k_1} \times ... \times p_r^{k_r}$$

alors on peut calculer très rapidement $\varphi(n)$ à l'aide de la formule suivante :

$$\varphi(n) = (p_1 - 1)p_1^{k_1 - 1} \times ... \times (p_r - 1)p_r^{k_r - 1}$$

On a $8 = 2^3$ donc $\varphi(8) = (2-1) \times 2^{3-1} = 2^2 = 4$.

On a $75 = 3 \times 5^2$ donc $\varphi(75) = 2 \times 4 \times 5 = 40$.

On a $3087 = 3^2 \times 7^3$ donc $\varphi(3087) = 2 \times 3 \times 6 \times 7^2 = 1764$.

Le théorème d'Euler

Theorem 19.

Soit un entier n non nul et a un entier tel que $pgcd(a, n) = 1$ alors

$$a^{\varphi(n)} \equiv 1 \pmod{n}$$

Remarque : l'exposant $\varphi(n)$ donné par le théorème n'est pas toujours optimal, dans le sens où ce n'est pas toujours le plus petit.

Par exemple le théorème nous donne que $5^8 \equiv 1 \pmod{24}$ or on a mieux $5^2 \equiv 1 \pmod{24}$;

Calculer $3^{49}(mod\ 35)$.
$\Phi(35) = 4 \times 6 = 24$ et $pgcd(3, 35) = 1$ donc d'après le théorème d'Euler,
$3^{24} \equiv 1(mod\ 35)$ et $3^{49} \equiv (3^{24})^2 \times 3 = 1 \times 3 \equiv 3(mod\ 35)$