Mathématiques pour l'informatique

#2 Arithmétique modulaire

par David Albert

GEMA
GRANDES ÉCOLES DES MÉTIERS D'AVENIR

2023

Table des matières

00 Notations

$a \mid b$	a divise b
$\lfloor x \rfloor$	partie entière de x
$PGCD$	plus grand diviseur commun
$PPCM$	plus petit multiple commun
$a \equiv b \ (mod\ N)$	a est congru à b modulo N
$DIV(a, b)$	quotient de la division euvlidienne de a par b
$MOD(a, b)$	reste (ou module) de la division euvlidienne de$a$ par b
$a = \overline{a_k a_{k-1} \dots a_1}^b$	décomposition en base b de a

01

Division euclidienne

Division euclidienne

Théorème - Division euclidienne

Soient $a \in \mathbb{Z}$ et $b \in \mathbb{Z}^*$. Alors a se décompose de façon unique sous la forme:

$$a = bq + r,\ avec\ q \in \mathbb{Z}\ et\ r \in \{0, \ldots, |d| - 1\}$$

Les entiers q et r sont appelés respectivement **quotient** et **reste** de la **division euclidienne** de a par b.

Notation

Soient $a \in \mathbb{Z}$ et $b \in \mathbb{Z}^*$. On note $DIV(a, b)$ (respectivement $MOD(a, b)$) le **quotient** (respectivement le **reste**) de la division euclidienne de a par b.

Exemple : Soient $a = 7$ et $b = 3$.

On a $\underbrace{7}_{a} = \underbrace{3}_{b} \times \underbrace{2}_{q} + \underbrace{1}_{r}$ l'unique décomposition de $a = 7$ quand $b = 3$.

Divisibilité

Définition - Divisibilité

On dit que b est un **diviseur** de a (et on note $b \mid a$) si le reste de la division euclidienne de a par b est nul (égal à 0). On a donc : $a = b \times q$

On dit alors que b **divise** a, que a **est divisible par** b ou que a **est un multiple de** b.

Critère de divisibilité

Un nombre entier est divisible par :

- 2 lorsque son chiffre des unités est 0, 2, 4, 6 ou 8
- 3 lorsque la somme de ses chiffres est divisible par 3
- 4 lorsque le nombre formé par ses deux derniers chiffres est divisible par 4
- 5 lorsque son chiffre des unités est 0 ou 5
- 9 lorsque la somme de ses chiffres est divisible par 9
- 10 lorsque son chiffre des unités est 0

Divisibilité

Propriétés

1. Si a et b sont deux entiers avec $b \neq 0$, b divise a si et seulement si la fraction $\frac{a}{b}$ est un entier.
2. Tous les entiers divisent 0 et sont divisibles par 1.
3. Un entier n est toujours divisible par 1, -1, n et $-n$.
4. Si $a \mid b$, et $b \mid c$, alors $a \mid c$.
5. Si $a \mid b_1, b_2, \ldots, b_n$, alors $a \mid b_1c_1 + b_2c_2 + \ldots + b_nc_n$, quels que soient les entiers $c_1, c_2, \ldots, c_n$.
6. Si a divise b et $b \neq 0$, alors $|a| \leq |b|$.
7. Si a divise b et b divise a, alors $a = \pm b$.
8. Si a et b sont deux entiers tels que $a^n | b^n$ pour un entier $n > 1$, alors $a | b$.

Divisibilité

Exercices

Démontrez la propriété (3), (4) et (8).

Parties entières

Définitions

♡ Définition - Partie entière

Si x est un réel, on appelle **partie entière** de x, et on note $\lfloor x \rfloor$, le plus grand entier inférieur ou égal à x.

Mathématiquement, on a $\lfloor x \rfloor \leq x < \lfloor x \rfloor + 1$.

i Remarque - Partie décimale

On définit aussi la **partie décimale** de x, comme la différence $x - \lfloor x \rfloor$.

Exemples :

- $\lfloor 2,5 \rfloor = 2$
- $\lfloor \pi \rfloor = 2$
- $\lfloor -1,632 \rfloor = -2$
- $\lfloor -\sqrt{19} \rfloor = -5,$

Parties entières

Propriétés

1. Pour tout réel x, on a $x - 1 < \lfloor x \rfloor \leq x$.
2. $\lfloor -x \rfloor = -\lfloor x \rfloor - 1$ sauf si x est entier, auquel cas $\lfloor -x \rfloor = -\lfloor x \rfloor$.
3. Si x et y sont deux réels, $\lfloor x \rfloor + \lfloor y \rfloor \leq \lfloor x + y \rfloor \leq \lfloor x \rfloor + \lfloor y \rfloor + 1$.
4. Si $m > 0$ est un entier, alors il y a exactement $\left\lfloor \frac{x}{m} \right\rfloor$ multiples de m compris entre 1 et x.

Parties entières

Exercices

Exercice 1 : Démontrez les propriétés (1) et (3).

Exercice 2 : Donnez les parties entières des nombres suivants: $0,53$; $123,2453927$; $-1,25$; $-4150,67$; $\frac{2}{3} - \frac{23}{9}$; $\frac{2023}{0,6}$

PGCD / PPCM

Définitions

♡ PGCD

Soient $a, b \in \mathbb{Z}^*$. L'ensemble des diviseurs communs de a et de b est fini et non vide.

Il possède donc un plus grand élément appelé **plus grand commun diviseur (PGCD)** de a et b et noté $PGCD(a, b)$.

Lorsque $PGCD(a, b) = 1$, on dit que a et b sont **premiers entre eux**.

♡ PPCM

Soient $a, b \in \mathbb{Z}^*$. L'ensemble des diviseurs communs de a et de b est fini et non vide.

a et b possèdent un plus petit multiple commun positif, on l'appelle le **plus petit commun multiple (PPCM)** de a et de b et on le note $PPCM(a, b)$.

PGCD / PPCM

Propriétés

1. Si $d = PGCD(a, b)$, alors n divise a et b si et seulement si n divise d.
2. Si $m = PPCM(a, b)$, alors n est un multiple a et de b si et seulement si n est un multiple de m.
3. Si a, b et n sont des entiers non nuls et $n > 0$, alors $PGCD(na, nb) = nPGCD(a, b)$.

   Si de plus n divise a et b, alors $PGCD(\frac{a}{n}, \frac{b}{n}) = \frac{1}{n}PGCD(a, b)$.
4. Si $d = PGCD(a, b)$, on peut écrire $a = da'$ et $b = db'$ pour a' et b' des nombres premiers entre eux.
5. Si a et b sont des entiers, l'égalité $PGCD(a, b) = PGCD(a, a + b)$ est toujours vérifiée lorsqu'elle a un sens. En particulier, le $PGCD$ de deux nombres consécutifs est 1, et plus généralement, le $PGCD$ de a et de $a + n$ est un diviseur positif de n.
6. Plus généralement, si x, y, a, b, a' et b' sont des entiers alors :

   $$PGCD(x, y) \times \mid PGCD(ax + by, a'x + b'y) \mid \times (ab' - ba')PGCD(x, y)$$

   En particulier si $|ab' - ba'| = 1$, alors $PGCD(x, y) = PGCD(ax + by, a'x + b'y)$.

PGCD / PPCM

Exercices

Exercice 1 : Déterminer les valeurs suivantes: $PGCD(20, 36)$, $PGCD(36, 60)$ et $PGCD(116, 78)$

Exercice 2 : Démontrez les propriétés (1), ...

Exercice 3 : Soit $a, b \in \mathbb{Z}^*$. Montrez que $\forall n \in \mathbb{N}^*$, on a $PGCD(a^n, b^n) = PGCD(a, b)^n$

Algorithme d'Euclide

L'algorithme d'Euclide est une méthode pour **trouver le PGCD de deux nombres sans avoir besoin de faire leur décomposition en produit de facteurs premiers**. Il est basé sur la propriété suivante.

Proposition

Si $a, b \in \mathbb{N}$ avec $a \geq b$, si r est le reste de a par b, alors le

$$PGCD(a, b) = PGCD(b, r)$$

On fait donc des divisions euclidiennes, jusqu'à ce qu'on trouve un reste nul. Le dernier reste non nul est le pgcd de a et b.

Exemple : On souhaite calculer le PGCD de 255 et 141. On effectue les divisions euclidiennes successives suivantes :

$$\begin{aligned} 255 &= 1 \times 141 + 114 \\ 142 &= 1 \times 114 + 27 \\ 114 &= 4 \times 27 + 6 \\ 27 &= 4 \times 6 + 3 \\ 6 &= 2 \times 3 + 0 \end{aligned}$$

Le pgcd de 255 et 141 est donc 3.

Algorithme d'Euclide

Algorithm 1 Algorithme d'Euclide

Require: $a, b \in \mathbb{N}_0$

Ensure: $\text{pgcd}(a, b)$

$r \leftarrow \max(a, b),\ s \leftarrow \min(a, b)$

while $s > 0$ **do**

$(r, s) \leftarrow (s, \text{MOD}(r, s))$

end while

return r

Théorème de Bézout

A chaque étape de l'algorithme d'Euclide, on a une égalité de la forme :

$$r_{i-2} = r_{i-1}q_i + r_i$$

où par convention $r_{-2} = a$ et $r_{-1} = b$. A l'avant-dernière étape, on a $r_k = d = PGCD(a, b)$ et donc une égalité de la forme :

$$r_{k-2} = r_{k-1}q_k + d \Rightarrow d = r_{k-2} - r_{k-1}q$$

A l'étape précédente, on a de même : $r_{k-1} = r_{k-3} - r_{k-2}q_{k-1}$
Et donc en réinjectant, on obtient une expression de d comme une combinaison linéaire de r_{k-3} et r_{k-2}. En continuant à remonter, on trouve finalement une égalité de la forme :

$$d = ur - 2 + vr - 1 = au + bv$$

pour des entiers u et v.

♡ **Théorème - Identité de Bachet-Bézout**

Soit $a, b \in \mathbb{Z}$ et $PGCD(a, b) = d$.
Il existe deux entiers relatifs u et v tels que $au + bv = d$.

Théorème de Bézout

♡ Théorème de Bézout

Soit $a, b \in \mathbb{Z}$. a et b sont premiers entre eux si, et seulement si, il existe des entiers relatifs u et v tels que $au + bv = 1$.

Le théorème précédent n'est pas spécifique aux entiers. Il peut être appliqué avec des polynômes :

♡ Théorème de Bézout (appliqué aux polynômes)

Soit A et B deux polynômes de $\mathbb{R}[X]$. Alors A et B sont premiers entre eux si et seulement s'il existe deux polynômes U et V tels que $AU + BV = 1$.

Exemple :

59 et 123 sont premiers entre eux car $12 \times 123 + (-25) \times 59 = 1$

Lemme de Gauss

Lemme de Gauss

Si des entiers a, b et c sont tels que a divise bc et a est premier avec b, alors a divise c.

Démonstration

Comme a est premier avec b, on peut écrire $au + bv = 1$ pour des entiers u et v. Ainsi $auc + bvc = c$ et comme a divise auc (car il divise a) et bvc (car il divise bc), il divise la somme qui vaut c.

Conséquences du lemme:

- Si un nombre premier p divise le produit $a_1 a_2 \dots a_n$, alors il divise l'un des a_i.
- Si deux entiers premiers entre eux a et b divisent n, alors le produit ab divise également n.

02

Nombres premiers

Nombres premiers

Définitions

Définition - Nombre premier

Un nombre entier positif est **premier** s'il admet **exactement deux diviseurs : 1 et lui-même**.

Les entiers 2, 3, 5, 7, 11, 13 sont les premiers nombres premiers.
Le nombre 6, n'est pas premier: il admet 2 et 3 comme autres diviseurs

Remarques

→ **0 n'est pas premier** car il admet **une infinité de diviseurs**.

→ **1 n'est pas premier** car il possède **un seul diviseur** : lui-même.

→ 2 est le seul nombre premier pair car tous les nombres pairs sont divisibles par 2.

Propriété : Il existe une infinité de nombres premiers.

Décomposition en facteurs premiers

Théorème

Théorème - Décomposition en facteurs premiers

Tout entier $n \geq 1$ se décompose d'une seule et unique manière en un produit de nombres premiers.

Autrement dit, pour tout entier $n \geq 1$, il existe des nombres premiers deux à deux distincts $p_1, \ldots, p_k$ et des entiers strictement positifs $\alpha_1, \ldots, \alpha_k$, tels que :

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$$

Le théorème reste bien vrai pour $n = 1$.
Pour cela on remarquera que $p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k} = 1 \times p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$ et on choisira $k = 0$.

Décomposition en facteurs premiers

Exemples

Exemple 1: Décomposer 84 en produits de facteurs premiers.

Exemple 2: Décomposer 2520 en produits de facteurs premiers.

Décomposition en facteurs premiers

Proposition

Si la décomposition en facteurs premiers de l'entier $n \geq 1$ est $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$, alors les diviseurs positifs de n sont les entiers de la forme $p_1^{\beta_1} p_2^{\beta_2} \dots p_k^{\beta_k}$, avec $0 \leq \beta_i \leq \alpha_i$ pour tout $1 \leq i \leq k$

Par conséquence, soient a et b tels que:

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k} \quad et \quad b = p_1^{\beta_1} p_2^{\beta_2} \dots p_k^{\beta_k}$$

où les p_i sont deux à deux distincts, mais les α_i et β_i sont éventuellement nuls, on a:

$$(i)\ PGCD(a,b) = p_1^{\min(\alpha_1,\beta_1)} p_2^{\min(\alpha_2,\beta_2)} \dots p_k^{\min(\alpha_k,\beta_k)}$$

$$(ii)\ PPCM(a,b) = p_1^{\max(\alpha_1,\beta_1)} p_2^{\max(\alpha_2,\beta_2)} \dots p_k^{\max(\alpha_k,\beta_k)}$$

Décomposition en facteurs premiers

Exercices

Exercice : Montrez que $PGCD(a,b) \times PPCM(a,b) = ab$

03

Décomposition en base b

Décomposition en base *b*

Théorème - Décomposition en base *b*

Soit b une base entière, c'est-à-dire un naturel tel que $b \geq 2$. Alors tout entier $a \in \mathbb{N}^*$ se décompose de façon unique sous la forme:

$$a = a_0 + a_1 b + a_2 b^2 + \ldots + a_k b^k$$

où k est un entier, les a_i sont des entiers compris entre 0 et $b-1$ et où $a_k \neq 0$.

Notation

On notera $a = \overline{a_k a_{k-1} \ldots a_0}^{b}$, l'écriture en base *b* de a

Exemples :

$4 = \overline{100}^{2}$ car $4 = \mathbf{1} \times 2^2 + \mathbf{0} \times 2^1 + \mathbf{0} \times 2^0$

$4 = \overline{11}^{3}$ car $4 = \mathbf{1} \times 3^1 + \mathbf{1} \times 3^0$

$4 = \overline{4}^{5}$ car $4 = \mathbf{4} \times 5^0$

$7 = \overline{111}^{2}$ car $7 = \mathbf{1} \times 2^2 + \mathbf{1} \times 2^1 + \mathbf{1} \times 2^0$

$7 = \overline{21}^{3}$ car $7 = \mathbf{2} \times 3^1 + \mathbf{1} \times 3^0$

$7 = \overline{12}^{5}$ car $7 = \mathbf{1} \times 5^1 + \mathbf{2} \times 5^0$

Tableau des bases classiques

b=10 (décimale)	b=2 (binaire)	b=3 (ternaire)	b=8 (octale)	b=16 (hexadécimale)
0	0	0	0	0
1	1	1	1	1
2	10	2	2	2
3	11	10	3	3
4	100	11	4	4
5	101	12	5	5
6	110	20	6	6
7	111	21	7	7
8	1000	22	10	8
9	1001	100	11	9
10	1010	101	12	A
11	1011	102	13	B

Tableau des bases classiques (suite)

b=10 (décimale)	b=2 (binaire)	b=3 (ternaire)	b=8 (octale)	b=16 (hexadécimale)
12	1100	110	14	C
13	1101	111	15	D
14	1110	112	16	E
15	1111	120	17	F
16	10000	121	20	10
17	10001	122	21	11
18	10010	200	22	12
19	10011	201	23	13
20	10100	202	24	14
...	...	...	...	...
100	1100100	10201	144	64
1000	1111101000	1101001	1750	3E8

04

Congruences

Congruences

Avant propos

SUNDAY	MONDAY	TUESDAY	WEDNESDAY	THURSDAY	FRIDAY	SATURDAY
26	27	28	29	30	1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30

Nous avons tous déjà utiliser les congruences sans le savoir.

Imaginons que l'on n'a pas de calendrier sous les yeux. **Sachant qu'aujourd'hui nous sommes mardi 5, comment savoir savoir quel jour seront nous le 28 ?**

Nous savons qu'une semaine est composée de 7 jours donc:

$$Mardi\ 5 \xrightarrow{+7} Mardi\ 12 \xrightarrow{+7} Mardi\ 19 \xrightarrow{+7} Mardi\ 26 \xrightarrow{+1} Mercredi\ 27 \xrightarrow{+1} Jeudi\ 28$$

En faisant cela, on fait des congruences.

On dira que 5 **est congru à** 26 **modulo** 7 et on notera $5 \equiv 26[7]$.

⚠ $a \equiv b[7]$ signifie que $b = a + 7k$

Congruences

Définitions

Définition - Congruence

Soient $n \in \mathbb{N}^*$ et $a, b \in \mathbb{Z}$.
On dit a **et** b **sont congrus modulo** n si et seulement si $\exists k \in \mathbb{N}$ tel que $a = b + nk$.
On notera $a \equiv b\,[n]$.

D'autre part,

$$\begin{aligned} a \equiv b\,[n] &\iff \exists k \in \mathbb{N}; b = a + nk \\ &\iff n \text{ divise } a - b \\ &\iff \text{a et b ont le meme reste dans la division euclidienne par n} \end{aligned}$$

Congruences

Propriétés

Soit $n \in \mathbb{N}^*$, $a, b \in \mathbb{Z}$

1. $a \equiv a\,[n]$
2. $n \equiv 0\,[n]$
3. $a \equiv b\,[n] \Leftrightarrow b \equiv a\,[n]$
4. $a \equiv 0\,[n] \Leftrightarrow n$ divise a
5. Si $a \equiv b\,[n]$ et $b \equiv c\,[n]$, alors $a \equiv c\,[n]$
6. r est le reste de la division euclidienne de a par b si et seulement si :

$$\begin{cases} a \equiv r\,[b] \\ r < |b| \end{cases}$$

Congruences

Opérations sur les congruences

Soient $a, b, a', b' \in \mathbb{Z}$ tels que $a \equiv b\,[n]$ et $a' \equiv b'\,[n]$.

Alors :

1. $a + a' \equiv b + b'\,[n]$
2. $a - a' \equiv b - b'\,[n]$
3. $a \times a' \equiv b \times b'\,[n]$
4. $a^p \equiv b^p\,[n],\ \forall p \in \mathbb{N}$

Conséquences immédiates:

5. $a + k \equiv b + k\,[n],\ \forall k \in \mathbb{Z}$
6. $a - k \equiv b - k\,[n],\ \forall k \in \mathbb{Z}$
7. $a \times k \equiv b \times k\,[n],\ \forall k \in \mathbb{Z}$

(vous pouvez vous amuser à redémontrer toutes ces propriétés)

Congruences

Astuces de calcul

Astuce 1 : *Multiplier au fur et à mesure en simplifiant à chaque fois*

Exemple : Soit $a \in \mathbb{Z},\ a \equiv 34\,[6]$. A quoi est congru $22a$ modulo 6 ?

Astuce 2 : *Aller dans les négatifs.*

Exemple : Soit $a \in \mathbb{Z},\ a \equiv 10\,[11]$. A quoi est congru a^{14} modulo 11 ?

Astuce 3 : : *Trouver une puissance congrue à 1 ou -1*

Exemple : On veut savoir le reste dans la division euclidienne de 2^{1495} par 15.

Congruences

Théorème des restes chinois

Théorème des restes chinois

Soient $n_1, n_2, \ldots, n_k$ des entiers strictement positifs deux à deux premiers entre eux, et $a_1, a_2, \ldots, a_k$ des entiers quelconques. Le système d'équations :

$$\begin{cases} x \equiv a_1 \,[n_1] \\ \vdots \quad \vdots \quad \vdots \\ x \equiv a_k \,[n_k] \end{cases}$$

admet une unique solution modulo $N = n_1 \times \ldots \times n_k$ donnée par la formule :

$$x = a_1 N_1 y_1 + \ldots + x = a_k N_k y_k$$

où $N_i = \frac{N}{n_i}$ et $y_i \equiv \frac{1}{N_i} [n_i]$ pour i compris entre 1 et k.

Congruences

Théorème des restes chinois (exemple)

Problème : Soient des objets en nombre inconnu. Si on les range par 3 il en reste 2. Si on les range par 5, il en reste 3 et si on les range par 7, il en reste 2. Combien a-t-on d'objets ?

Solution

Si x désigne le nombre d'objets total, alors x est le plus petit entier positif tel que :

$$\begin{cases} x \equiv 2\,[3] \\ x \equiv 3\,[5] \\ x \equiv 2\,[7] \end{cases}$$

On applique le théorème chinois : on a $N = 3 \times 5 \times 7 = 105$, $N_1 = \frac{105}{3} = 35$, $N_2 = \frac{105}{5} = 21$ et $N_3 = \frac{105}{7} = 15$. L'inversion de chaque N_i modulo n_i (par l'algorithme d'Euclide) donne $y_1 = 70$, $y_2 = 21$ et $y_3 = 15$

Donc, $x \equiv 2 \times 70 + 3 \times 21 + 2 \times 15[105] \equiv 233[105] \equiv 23[105]$

Ainsi, le nombre d'objets est de la forme $23 + 105k$ avec $k \in \mathbb{N}$.