Chapitre 6 : Arithmétique

Table des matières

1 Introduction **2**

2 Divisibilité dans $\mathbb{Z}$ **2**
2.1 Multiples et diviseurs . . . 2
2.2 La division euclidienne . . . 2

3 Le PGCD et l'algorithme d'Euclide **3**
3.1 PGCD et PPCM d'un couple d'entiers . . . 3
3.2 L'algorithme d'Euclide . . . 3

4 Entiers premiers entre eux **4**
4.1 Généralités . . . 4
4.2 Propriétés . . . 5
4.3 Applications . . . 6

5 Nombres premiers **6**
5.1 Définitions . . . 6
5.2 Crible d'Erathostène . . . 7
5.3 Décomposition en facteur premiers d'un entier naturel . . . 9
5.4 Valuations p-adiques d'un entier . . . 9

6 Congruences **10**
6.1 Généralités . . . 10
6.2 Congruences et opérations . . . 11
6.3 Inverse modulo n . . . 11
6.4 Petit théorème de Fermat . . . 11

1 Introduction

L'Arithmétique est la branche des mathématique dont l'étude porte sur les propriétés des nombres entiers. La notion fondamentale de qui s'y rattache est celle de **diviseur**. Une question classique d'Arithmétique est par exemple de déterminer une condition nécessaire et suffisante sur un entier pour savoir s'il est divisible par 9. Nous répondrons à cette question dans le chapitre.

Nous terminons cette partie par l'étude des nombres premiers qui sont les "briques" fondamentales avec lesquels tous les nombres premiers sont construits. En effet, nous verrons que tout entier naturel se décompose de manière unique comme produit de nombres premiers.

2 Divisibilité dans $\mathbb{Z}$

2.1 Multiples et diviseurs

Définition: Multiple et diviseurs

Soit $a \in \mathbb{N}$. On dit que :

- l'entier d est un **diviseur** de a s'il existe $k \in \mathbb{N}$ tel que $a = d \times k$, note aussi $d|a$.
- l'entier m est un **multiple** de a si a est un diviseur de m.
- Si d divise à la fois a et $b \in \mathbb{N}$, on dit que d est **un diviseur commun de a et b.**
- On note $Div(a)$ l'ensemble des diviseurs de a et $Div(a, b) = Div(a) \cap Div(b)$.

Exemple

- 2 est un diviseur de 128.
- 51 est un multiple de 17.

Proposition

Soient a et b deux entiers naturels. Alors :

1. Si d divise b et que b divise a, alors d divise a.
2. Si d divise a et b alors d divise toute combinaison linéaire entière de a et b :

$$\forall m, n \in \mathbb{Z}, \quad d|(a \times m + b \times n)$$

Exercice 1 *Traduire l'énoncé de la proposition précédente uniquement en terme de multiples et plus en fonctions de diviseurs.*

2.2 La division euclidienne

Définition: (Proposition) Division euclidienne

Soient $a, b \in \mathbb{N}$. La division euclidienne est a par b est l'écriture de a sous la forme unique :

$$a = b \times q + r$$

où $q \in \mathbb{N}$ et r est un entier naturel tel que $0 \leq r < b$.

Exemple

Effectuons la division euclidienne de 23 par 4.

1. On détermine l'entier k tel que $23-4k$ soit positif et strictement inférieur à 4. Or $23-4=19$, $23-2.4=15$, ...,$0 \leq 23-5\times 4=3<4$.
2. On en déduit que le reste de la division euclidienne de 23 par 4 est $r=3$ et $q=5$.
3. La division euclidienne de 23 par 4 est donc :

$$23=5\times 4+3$$

Exercice 2 *Déterminer la division euclidienne de* 52 *par* 7.

Proposition

Soit $a\in\mathbb{Z}$ et $b\in\mathbb{N}^\star$. Notons $r\in\{0;1;\ldots;b-1\}$ le reste de la division euclidienne de a par b. Alors a est divisible par b si et seulement si $r=0$.

3 Le PGCD et l'algorithme d'Euclide

3.1 PGCD et PPCM d'un couple d'entiers

Définition: PGCD et PPCM

Soient a et b deux entiers. On appelle :

- **plus grand diviseur commun** de a et b, noté $a\wedge b$, le maximum de l'ensemble $Div(a,b)=\{d\in\mathbb{N}\mid d|a \text{ et } d|b\}$.
- **plus petit multiple commun** de a et b, noté $a\vee b$, le minimum de l'ensemble $Mul(a,b)=\{m\in\mathbb{N}\mid a|m \text{ et } b|m\}$.

Exemple

Soient $a=189=3^3\times 7$ et $b=114=2\times 3\times 19$. On a alors :

- $a\wedge b=3$ car $Div(a,b)=\{1,3\}$.
- $a\vee b=2\times 19\times 9\times 7=2394$

Proposition

Pour $a,b\in\mathbb{Z}$ et $k\in\mathbb{N}^\star$ on a :

$$(ka)\wedge(kb)=k.(a\wedge b).$$

3.2 L'algorithme d'Euclide

Comment calculer le PGCD de deux entiers naturels ? La question est simple à résoudre lorsque nous disposons, comme dans l'exemple de la partie précédente, des diviseurs de a et de b. Ceci est une donnée sur les nombres qui n'est pas simplement accessible en pratique et nous devons chercher un autre moyen de calculer le $PGCD$ de deux nombres, on utilise pour cela *l'algorithme d'Euclide.*

Proposition

Soient a, $b\in\mathbb{N}$ deux entiers et $a=bq+r$ la division euclidienne de a par b. Alors :

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

Démonstration :

L'algorithme d'Euclide consiste à réaliser une suite de division euclidienne jusqu'à ce que le reste soit 0. Le dernier reste non nul obtenu est le PGCD des deux entiers initiaux. Nous devons d'abord vérifier que la suite des division euclidiennes de l'algorithme termine bien.

Méthode

Algorithme d'Euclide

Soient $a = a_0$ et $b = b_0$ deux entiers naturels ainsi que $q = q_0$, $r = r_0$ les entiers quotient et reste de la division euclidienne de a par b : $a = bq + r$. Alors les suites d'entiers naturels définies par récurrence (a_n), (b_n), (q_n) et (r_n) comme suit n'ont qu'un nombre fini de termes. Pour tout $n \in \mathbb{N}$:

1. Si $r_n = 0$ l'algorithme termine.
2. Si $r_n > 0$, on pose $a_{n+1} = b_n$, $b_{n+1} = r_n$, q_{n+1} et r_{n+1} quotient et reste de la division euclidienne de a_{n+1} par b_{n+1}.

Argument :

Théorème: Calcul du PGCD par l'algorithme d'Euclide

Soient $a = a_0$ et $b = b_0$ deux entiers naturels. Supposons que la suite (r_n) contienne $n+1$ termes. Alors $r_{n-1} = a \wedge b$.

Exemple

Déterminons à l'aide de cet algorithme le PGCD de 41 et 12.

1. $41 = 12 \times 3 + 5$
2. $12 = 5 \times 2 + 2$
3. $5 = 2 \times 2 + 1$
4. $2 = 1 \times 2 + 0$

On en déduit d'après l'algorithme d'Euclide que $41 \wedge 12 = 1$.

Exercice 3 *À l'aide de l'algorithme d'Euclide, déterminer le pgcd de* 135 *et* 15.

Une application de ce résultat est la proposition suivante.

Théorème: Bezout

Soient a et b deux entiers naturels. Il existe alors $m, n \in \mathbb{Z}$ tels que :

$$am + bn = a \wedge b$$

La démonstration de ce résultat est effective et passe par l'algorithme d'Euclide étendu (voir feuille).

Exercice 4 *Déterminer deux entier* u *et* v *tels que* $150.u + 54.v = 6$.

4 Entiers premiers entre eux

4.1 Généralités

Définition: Entiers premiers entre eux
Soit a et b deux entiers. On dit que (a, b) est un couple d'entiers *premiers entre eux* si $a \wedge b = 1$.

Exemple
— Les entiers 5 et 12 sont premiers entre eux.
— Le couple $(6, 12)$ n'est pas formé par des entiers premiers entre eux car $6 \wedge 12 = 6$.

Proposition
Tout nombre rationnel s'écrit comme un quotient de deux entiers premiers entre eux. On dit alors qu'il est mis sous forme *irréductible*.

Exemple
Le nombre $r = \dfrac{6}{12}$ s'écrit sous forme irréductible $r = \dfrac{1}{2}$.

4.2 Propriétés

Théorème: Bezout
Soit (a, b) un couple d'entiers.
Alors, a et b sont premiers entre eux si et seulement si il existe deux entiers relatifs n et m tels que :

$$a.n + b.m = 1.$$

Corollaire
On considère trois entiers relatifs a, b et c.
Les entiers a et bc sont premiers entre eux si et seulement si a est premier avec b et c.

Remarque 1 *Cette propriété s'étend à un produit fini d'entiers. En effet, un entier a est premier avec un produit d'entiers si et seulement si il est premier avec chacun de ses facteurs.*

Théorème: Lemme de Gauss
Soit a, b et c trois entiers. Si a et b sont premiers entre eux et que $a|bc$ alors $a|c$.

Corollaire
Soit a, b, c trois entiers. Si a et b divisent c et (a, b) est couple d'entiers premiers entre eux, alors ab divise c.

On peut généraliser la notion de couple premiers entre eux à plusiers entier avec le concept de *premiers entre eux dans son ensemble.*

Définition: Entiers premiers entre eux dans leur ensemble

Soit $a_1, a_2, \ldots, a_n$ des entiers non nuls. On dit qu'ils sont :

- **premiers entre eux dans leur ensemble** si leur plus grand diviseur commun dans les entiers naturels est 1.
- **premiers deux à deux** si pour tout couple (i, j) d'entiers distincts entre 1 et n on a $a_i \wedge a_j = 1$.

4.3 Applications

Théorème: Factorisation

Soit a, b deux entiers et $d = a \wedge b$. Il existe alors un couple d'entiers premiers entre eux (a', b') tels que $a = d \times a'$ et $b = d \times b'$.

Théorème: Produit du PGCD et du PPCM

Soit a, b des entiers. Le produit du PGCD de a et b par le PPCM de a et b est égal au produit ab :

$$(a \wedge b) \times (a \vee b) = ab.$$

5 Nombres premiers

5.1 Définitions

Définition: Nombre premier

Soit $n \in \mathbb{N}$. On dit que n est un nombre **premier** si $Div(n) = \{1, n\}$ et $n > 1$.
Dans le cas contraire, on dit que n est *composé*.

Remarque 2 *Un caractérisation alternative de la notion de nombre premier est la suivante :*

$$p \geq 2 \text{ est premier si } \forall a, b \in \mathbb{N}; (p = ab \implies a = 1 \text{ ou } b = 1)$$

On note $\mathcal{P}$ **l'ensemble des nombres premiers**. On peut déduire du précédent théorème un critère de primalité :
Un entier naturel n est premier si et seulement s'il n'est pas divisible par un nombre premier compris entre 2 et $\sqrt{n}$.

Exemple

Le nombre $n = 137$ est premier car $\sqrt{137} \approx 11,7$ à 10^{-1} près et on vérifie que $2, 3, 5, 7$ et 11 ne divisent pas 137.

Théorème: (Euclide) Infinité des nombres premiers

Il existe une infinité de nombres premiers

Démonstration :

Méthode

Pour montrer qu'un entier naturel supérieur ou égal à 2 est premier il suffit de montrer qu'il n'est divisible par aucun nombre premier p vérifiant $2 \leq p \leq \sqrt{n}$.

Exemple

Les entiers $2; 3; 5; 7; 9; 11$ sont les premiers nombres premiers.

Exercice 5 *À l'aide de la méthode précédente, montrer que* 97 *est un nombre premier.*

Le théorème fondamental concernant les nombres premiers est le fait qu'un nombre premier est "une brique de base" de n'importe quel nombre entier.

5.2 Crible d'Erathostène

Le crible d'Erathostène est un moyen simple de calculer les premiers nombre premiers en affaçant dans un tableau d'entiers naturels les multiples des premiers entiers $n \geq 2$. Il ne reste que les nombres premiers.

Exercice 6

1. *Barrer le nombre* 1 *(il n'est pas premier) et entourer 2 puis barrer tous les multiples de* 2*. Le premier entier non barré supérieur à 2 est premier. (Pourquoi ?). On entoure ainsi* 3 *et on barre tous les multiples de* 3*, etc..*
2. *On a ainsi entouré* $2, 3, 5, \ldots, p$.
   Soit q le premier entier non barré supérieur à p. Est-il premier ? Quel est le premier multiple de q qui n'a pas été encore barré ?
   En déduire le moment où le processus s'arrête.
3. *Déterminer tous les nombres premiers entre* 2 *et* 100*.*

Proposition

Si $p \in \mathcal{P}$, alors p est premier avec tous les entiers qu'il ne divise pas. En particulier, on a :

$$\forall k \in [\![1; p-1]\!]; pgcd(k, p) = 1$$

Démonstration :admise

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
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

Théorème: Existence d'un diviseur premier
Tout entier naturel strictement supérieur à 1 admet un diviseur premier.
Si n n'est pas premier, il admet un diviseur premier p vérifiant $2 \leq p \leq \sqrt{n}$.

5.3 Décomposition en facteur premiers d'un entier naturel

Théorème: Décomposition d'un entier en produit de facteurs premiers
Soit $n \in \mathbb{N}^\star$. Il existe une unique famille de nombres :

- $p_1 < p_2 < \cdots < p_r$ premiers.
- $\alpha_1, \ldots, \alpha_r$ entiers naturels.

tels que :

$$n = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \cdots \times p_r^{\alpha_r}$$

Les nombres premiers $p_1, \ldots, p_r$ s'appellent les **facteurs premiers** de n et pour tout $i \in [\![1, r]\!]$, on appelle α_i la **valuation p_i-adique de** n et on note $\alpha_i = v_{p_i}(n)$.

Démonstration :Sur feuille.

Exemple
$7007 = 7 \times 7 \times 11 \times 13$

Une application de la décomposition d'un entier sous la forme d'un produit de facteurs premiers est la simplification d'une fraction sous sa forme irréductible. Par exemple, puisque $525 = 3 \times 5^2 \times 7$ et $1960 = 2^3 \times 5 \times 7^2$, on a :

$$\frac{525}{1960} = \frac{3 \times 5^2 \times 7}{2^3 \times 5 \times 7} = \frac{15}{56}.$$

Remarque 3 *Cette dernière méthode est peu efficace lorsque les entiers sont grands car cela nécessite beaucoup de calculs. Mieux vaut en général passer par le calcul du PGCD du numérateur et du dénominateur via l'algorithme d'Euclide.*

5.4 Valuations p-adiques d'un entier

Proposition
Soit deux entiers n_1 et n_2 ainsi que p un nombre premier.
La valuation p-adique de $n_1 n_2$ est égale à la somme des valuations p-adiques de n_1 et n_2 :

$$v_p(n_1 n_2) = v_p(n_1) + v_p(n_2).$$

On peut donc dégager un critère de divisibilité a pat b à partir de leur valuations p-adiques :

Proposition
Soit a et b deux entiers. On a b qui divise a si et seulement si pour tout diviseur premier p de b, p est un diviseur premier de a et $v_p(b) \leq v_p(b)$.

Théorème: Expression du PGCD et du PPCM en fonction des valuations p-adiques

Soit n et m deux entiers naturels supérieurs à 2. En notant :
$p_1 < p_2 < \cdots < p_r$ premiers apparaissant dans la décomposition en produit de facteurs premiers de n et m tels que :

$$n = p_1^{v_{p_1}(n)} \times p_2^{v_{p_2}(n)} \times \cdots \times p_r^{v_{p_r}(n)} \quad et \quad m = p_1^{v_{p_1}(m)} \times p_2^{v_{p_2}(m)} \times \cdots \times p_r^{v_{p_r}(m)}$$

On a alors :
- $n \wedge m = p_1^{\min(v_{p_1}(n),v_{p_1}(m))} \times p_2^{\min(v_{p_2}(n),v_{p_2}(m))} \times \cdots \times p_r^{\min(v_{p_r}(n),v_{p_r}(m))}$
- $n \vee m = p_1^{\max(v_{p_1}(n),v_{p_1}(m))} \times p_2^{\max(v_{p_2}(n),v_{p_2}(m))} \times \cdots \times p_r^{\max(v_{p_r}(n),v_{p_r}(m))}$

Exemple

Puisque $525 = 2^0 \times 3^1 \times 5^2 \times 7^1$ et $1960 = 2^3 \times 3^0 \times 5^1 \times 7^2$, on a :
- $525 \wedge 1960 = 2^0 \times 3^0 \times 5 \times 7^1 = 35$
- $525 \vee 1960 = 2^3 \times 3^1 \times 5^2 \times 7^2 = 29400$

6 Congruences

6.1 Généralités

Définition: Egalité modulo n

Soit $n \in \mathbb{N}$ un entier supérieur ou égal à 2 et a, b deux entiers relatifs.
On dit que a est congru à b modulo n, et on écrit $a \equiv b[n]$, si $a - b$ est divisible par n.

Exemple

- $2023 \equiv 23[10]$.
- $34 \equiv -131[5]$.
- Pour obtenir tous les entiers congrus à 5 modulo 6 on compte "de 6 en 6" à partir de 5 : ... ; -19 ;-13 ; -7 ; -1 ;5 ;11 ;..

Proposition

Soit n un entier supérieur ou égal à 2, a, b et c trois entiers relatifs. On a alors :
1. $a \equiv a[n]$ (réflexivité).
2. Si $a \equiv b[n]$ et $b \equiv c[n]$ alors $a \equiv c[n]$ (transitivité).
3. Si $a \equiv b[n]$ alors $b \equiv a[n]$ (symétrie).

Théorème:

Soit n un entier supérieur ou égal à 2 et a un entier relatif. Si r est le reste de la division euclidienne de a par n alors :

$$a \equiv r[n]$$

De manière directe on a que $a \equiv 0[n]$ si et seulement si $n|a$.

Remarque 4 *Une conséquence de ce théorème est de pouvoir définir une partition de $\mathbb{Z}$ en n "classes" qui chacune contient un unique élément de $[\![0, n]\!]$.*

Exemple

Modulo 2, $\mathbb{Z}$ se partitionne en 2 parties :
- les entiers dont le reste de la division euclidienne par 2 est 0.
- les entiers dont le reste de la division euclidienne par 2 est 1.

6.2 Congruences et opérations

La relation de "congruence modulo n" est compatible avec l'addition et la multiplication sur $\mathbb{Z}$.

Proposition

Soit n un entier naturel supérieur à 2. Si $a \equiv a'[n]$ et $b \equiv b'[n]$ alors :
- $a \times b \equiv a' \times b'[n]$.
- $a + b \equiv a' + b'[n]$.

Remarque 5 *En particulier si $k \in Z$ et $a \equiv b[n]$ alors $ka \equiv kb[n]$ et $a^k \equiv b^k[n]$.*

Exercice 7 *À l'aide d'une table de multiplication, déterminer l'ensemble des entier x tels que :*

$$3x \equiv 2[7].$$

6.3 Inverse modulo n

Définition: Inverse modulo n

Soit $n \in \mathbb{N}$ et un entier x. On dit que l'entier y est un *inverse de x modulo n* si :

$$x \times y \equiv 1[n]$$

Exemple

Si $x \equiv 3[4]$ et $y \equiv 3[4]$ alors $xy \equiv 9[4]$ et comme $9 = 2 \times 4 + 1$ il vient que $xy \equiv 1[4]$. Finalement , 7 est un inverse modulo 4 de 3.

Risque d'erreur

Tous les entiers n'admettent pas forcément d'inverse modulo n ni d'inverse unique. Par exemple 2 n'admet pas d'inverse modulo 4.

Méthode

Déterminer un inverse modulo n :
Soit k et n deux entiers. Pour déterminer, s'il existe, un inverse de k modulo n, on calcule pour $x \in [\![0, n-1]\!]$ la valeur de kx modulo n (que l'on peut consigner dans un tableau par exemple.
Les inverses sont les x tels que $kx \equiv 1[n]$.

6.4 Petit théorème de Fermat

Le petit théorème de Fermat (le grand n'a été démontré qu'en 1993 !) est un résultat permettant de déterminer un inverse de de tout entier a modulo p où p est un nombre premier qui ne divise pas a.

Théorème: Petit théorème de Fermat

Soit p un nombre premier. Pour tout entier relatif a, on a :

$$a^p \equiv a[p]$$

Si de plus, p ne divise pas a alors :

$$a^{p-1} \equiv 1[p].$$

Ce théorème est un des ingrédients de base de l'algorithme de cryptographie RSA (voir TD).