

9 - Arithmétique des entiers relatifs

Jeremy Daniel

οἱ πρῶτοι ἀριθμοὶ πλείους εἰσὶ παντὸς τοῦ προτεθέντος πλήθους πρώτων ἀριθμῶν.¹

Euclide, *Éléments*, IX-Prop. 20

1 Divisibilité dans \mathbb{Z}

1.1 Division euclidienne

DÉFINITION 1.1 (Divisibilité)

Soient $a, b \in \mathbb{Z}$. On dit que a divise b (ou que a est un diviseur de b ; ou que b est un multiple de a ; ou que b est divisible par a) s'il existe $k \in \mathbb{Z}$ tel que $b = ka$.

NOTATION 1.2

On écrit alors $a \mid b$.

REMARQUE 1.3

1 et -1 divisent tous les entiers; 0 est divisible par tous les entiers (mais 0 ne divise que 0).

THÉORÈME 1.4 (Division euclidienne)

Soient $a \in \mathbb{Z}$, $b \in \mathbb{N}^*$. Il existe un unique couple d'entiers (q, r) , avec $r \in \llbracket 0, b - 1 \rrbracket$ tels que $a = bq + r$.

DÉFINITION 1.5 (Quotient et reste)

Avec les notations précédentes, q est le quotient dans la division euclidienne de a par b ; r est le reste.

COROLLAIRE 1.6

Un entier $b > 0$ divise $a \in \mathbb{Z}$ ssi le reste dans la division euclidienne de a par b est nul.

1. Il y a davantage de nombres premiers que dans toute multitude donnée de nombres premiers.

1.2 PGCD

DÉFINITION 1.7 (PGCD)

Soient a et b deux entiers relatifs, non tous les deux nuls. Le pgcd de a et b , noté $a \wedge b$, est le plus grand (pour l'ordre usuel) entier naturel divisant à la fois a et b .

REMARQUE 1.8

En particulier :

$$\forall n \in \mathbb{Z}^*, 0 \wedge n = |n| \text{ et } 1 \wedge n = 1.$$

THÉORÈME 1.9 (Identité de Bachet-Bézout)

Soient a et b deux entiers relatifs, non tous les deux nuls. Il existe deux entiers relatifs u et v tels que

$$au + bv = a \wedge b.$$

COROLLAIRE 1.10

Soit k un entier naturel non nul, soient a, b deux entiers relatifs non tous les deux nuls. On a

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

COROLLAIRE 1.11 (Diviseurs du pgcd)

Le pgcd $a \wedge b$ est l'unique entier naturel tel que

$$\forall d \in \mathbb{Z}, \left((d \mid a) \text{ et } (d \mid b) \right) \iff d \mid a \wedge b.$$

REMARQUE 1.12

Ainsi, pour l'ordre sur \mathbb{N} donné par la relation de divisibilité, $a \wedge b$ est le plus grand élément de l'ensemble des diviseurs communs à a et b .

REMARQUE 1.13

On constate que si $a = b = 0$, $d = 0$ satisfait la propriété précédente. On peut donc convenir que $0 \wedge 0 = 0$.

DÉFINITION 1.14 (PGCD, généralisation à un nombre fini d'entiers)

Soient a_1, \dots, a_k des entiers relatifs, non tous nuls. Leur pgcd, noté $a_1 \wedge \dots \wedge a_k$ est le plus grand entier naturel divisant chacun des a_i .

THÉORÈME 1.15 (Identité de Bachet-Bézout)

Soient a_1, \dots, a_k des entiers relatifs, non tous nuls. Il existe des entiers relatifs u_1, \dots, u_k tels que

$$a_1 u_1 + \dots + a_k u_k = a_1 \wedge \dots \wedge a_k.$$

COROLLAIRE 1.16

Le pgcd $a_1 \wedge \dots \wedge a_k$ est l'unique entier naturel tel que

$$\forall d \in \mathbb{Z}, \left(\forall i \in \llbracket 1, k \rrbracket, d \mid a_i \right) \iff d \mid a_1 \wedge \dots \wedge a_k.$$

1.3 Aspects algorithmiques

MÉTHODE 1.17 (Calcul du pgcd par l'algorithme d'Euclide)

Pour calculer le pgcd de a et b , on procède par divisions euclidiennes successives. Si r est le reste dans la division euclidienne de a par b , on a $a \wedge b = b \wedge r$. On fait ainsi jouer le rôle du couple (a, b) à (b, r) et on s'arrête quand le reste est nul. Le pgcd $a \wedge b$ est le dernier reste non nul.

En Python :

```
def pgcd(a, b):
    r, r' = a, b
    while r' != 0:
        r, r' = r', r%r'
    return r
```

MÉTHODE 1.18 (Calcul d'une relation de Bézout)

Si on cherche en plus des coefficients u, v tels que $au + bv = a \wedge b$, on commence par écrire l'algorithme d'Euclide. Puis on part du dernier reste non nul (le pgcd), qu'on écrit comme combinaison linéaire des deux restes précédents; et on continue par substitution jusqu'à avoir exprimé le pgcd comme combinaison des deux premiers restes, à savoir a et b .

D'un point de vue algorithmique, il est plus malin de calculer des relations de Bézout au fur et à mesure (pour ne pas stocker les étapes de calcul notamment). On écrit un programme qui calcule des coefficients u_0, v_0, u_1, v_1 tels que, à chaque étape du calcul, avec les notations de l'algorithme précédent, on ait :

$$au_0 + bv_0 = r \text{ et } au_1 + bv_1 = r'.$$

On renvoie finalement les coefficients u_0, v_0 et le dernier reste non nul (correspondant à r).

En Python :

```
def BB(a, b):
    r, r' = a, b
    u0, v0 = 1, 0
    u1, v1 = 0, 1
    while r' != 0:
        quot = r//r'
        r, r' = r', r%r'
        (u0, u1) = (u1, u0-quot*u1)
        (v0, v1) = (v1, v0-quot*v1)
    return (u0, v0, r)
```

1.4 Entiers premiers entre eux

DÉFINITION 1.19 (Entiers premiers entre eux)

Deux entiers a et b sont premiers entre eux si $a \wedge b = 1$.

REMARQUE 1.20

On peut aussi dire que a est premier avec b .

REMARQUE 1.21

Écrire une fraction sous forme irréductible, c'est l'écrire avec un quotient et un dénominateur premiers entre eux.

THÉORÈME 1.22 (Bézout)

Deux entiers a et b sont premiers entre eux ssi il existe deux entiers u et v tels que

$$au + bv = 1.$$

PROPOSITION 1.23 (Lemme de Gauss)

Soient a, b, c trois entiers tels que $a \mid bc$. Si a est premier avec b , alors $a \mid c$.

PROPOSITION 1.24

Soient a, b, c trois entiers tels que $a \mid c$ et $b \mid c$. Si a et b sont premiers entre eux, alors $ab \mid c$.

PROPOSITION 1.25

Soient a, b, c trois entiers. Si a et b sont premiers avec c , alors ab est premier avec c .

DÉFINITION 1.26 (ppcm)

Soient a et b deux entiers non nuls. Leur ppcm, noté $a \vee b$ est le plus petit (pour l'ordre usuel) entier naturel non nul multiple de a et de b .

THÉORÈME 1.27 (Propriétés du ppcm)

Soient a et b deux entiers non nuls.

– $a \vee b$ est l'unique entier naturel tel que

$$\forall m \in \mathbb{Z}, \left((a \mid m) \text{ et } (b \mid m) \right) \iff a \vee b \mid m.$$

– $(a \vee b)(a \wedge b) = ab$.

REMARQUE 1.28

On peut étendre la définition du ppcm en considérant que si a ou b est nul, alors $a \vee b = 0$. Ceci est compatible avec les deux propriétés ci-dessus.

DÉFINITION 1.29 (Entiers premiers entre eux dans leur ensemble)

Des entiers a_1, \dots, a_k sont premiers entre eux dans leur ensemble si $a_1 \wedge \dots \wedge a_k = 1$.

ATTENTION !

Il s'agit d'une notion moins forte que de demander que les entiers soient deux à deux premiers entre eux. Considérer $a_1 = 6$; $a_2 = 10$ et $a_3 = 15$, qui sont premiers dans leur ensemble : deux quelconques ne sont pas premiers entre eux.

2 Nombres premiers

2.1 Généralités

DÉFINITION 2.1 (Nombre premier)

Soit $n \geq 2$ un entier naturel. On dit que n est premier si les seuls diviseurs positifs de n sont 1 et n .

NOTATION 2.2

On note \mathbb{P} l'ensemble des nombres premiers.

PROPOSITION 2.3

Un nombre premier p est premier avec tout nombre qu'il ne divise pas, en particulier avec tout nombre premier distinct q .

COROLLAIRE 2.4 (Lemme d'Euclide)

Soient p un nombre premier, a et b deux entiers relatifs. Si $p \mid ab$, alors $p \mid a$ ou $p \mid b$.

PROPOSITION 2.5

Un entier $n \geq 2$ est premier ou admet un diviseur premier $p \leq \lfloor \sqrt{n} \rfloor$.

MÉTHODE 2.6 (Crible d'Ératosthène)

La proposition précédente peut être utilisée pour déterminer si un nombre est premier, en testant successivement s'il est divisible par tout entier jusqu'à sa racine carrée.

Si l'on souhaite plutôt construire la liste des nombres premiers strictement inférieurs à un certain N , on applique le crible d'Ératosthène. On considère la liste des entiers de 2 à $N - 1$. On entoure 2 et on barre tous ses multiples ; puis on entoure 3 et on barre tous ses multiples, non déjà barrés ; et on continue en entourant à chaque fois le premier nombre non barré de la liste, parcourue de gauche à droite.

cf. TP d'informatique.

THÉORÈME 2.7 (Infinité des nombres premiers)

L'ensemble \mathbb{P} des nombres premiers est infini.

2.2 Théorème fondamental de l'arithmétique

REMARQUE 2.8 (Sur les faux produits infinis)

Soit I un ensemble d'indices. Soit $(u_i)_{i \in I}$ une famille de nombres tels que l'ensemble

$$J = \{i \in I \mid u_i \neq 1\}$$

est fini. On convient de noter

$$\prod_{i \in I} u_i = \prod_{i \in J} u_i.$$

Cette convention est compatible avec les règles de calcul données plus tôt.

On procèdera de même avec les sommes dont tous les termes sont nuls, sauf un nombre fini d'entre eux.

THÉORÈME 2.9 (Théorème fondamental de l'arithmétique)

Soit n un entier naturel non nul. Il existe une unique (à l'ordre près des facteurs) décomposition de n en produit de nombres premiers.

Plus précisément, avec la convention précédente : il existe une unique famille $(v_p(n))_{p \in \mathbb{P}}$ d'entiers naturels telle que :

$$n = \prod_{p \in \mathbb{P}} p^{v_p(n)}.$$

DÉFINITION 2.10 (Valuation p -adique)

Avec les notations précédentes, on appelle $v_p(n)$ la valuation p -adique de n .

REMARQUE 2.11

En particulier, $p \mid n$ ssi $v_p(n) \geq 1$.

REMARQUE 2.12

Donner la décomposition de n en produit de facteurs premiers revient donc à donner la valuation p -adique de n pour tout nombre premier p .

PROPOSITION 2.13 (Propriétés des valuations)

Soient a et b deux entiers naturels non nuls. Soit p un nombre premier.

- $v_p(ab) = v_p(a) + v_p(b)$;
- $v_p(a \wedge b) = \min(v_p(a), v_p(b))$;
- $v_p(a \vee b) = \max(v_p(a), v_p(b))$.

REMARQUE 2.14

On généralise immédiatement ces relations à un produit/pgcd/ppcm d'un nombre fini d'entiers naturels non nuls.

3 Arithmétique modulaire

3.1 Congruences

DÉFINITION 3.1 (Congruence modulo n)

Soit n un entier naturel non nul. Soient a et b deux entiers relatifs. On dit que a et b sont congrus modulo n , et on note $a \equiv b [n]$ si n divise $a - b$.

EXEMPLE 3.2

Le reste r dans la division euclidienne de a par n vérifie $a \equiv r [n]$.

PROPOSITION 3.3 (Compatibilité des opérations avec les congruences)

Soient a, b, c, d des entiers relatifs, soit n un entier naturel non nul. On suppose que $a \equiv c [n]$ et $b \equiv d [n]$. Alors,

- $-a \equiv -c [n]$;
- $a + b \equiv c + d [n]$;
- $ab \equiv cd [n]$;
- $\forall k \in \mathbb{N}, a^k \equiv c^k [n]$.

ATTENTION !

On ne peut pas diviser des congruences, même quand les quotients tombent juste. Dans le doute, on reviendra toujours à la définition.

DÉFINITION 3.4 (Inverse modulo n)

Soit a un entier relatif, soit n un entier naturel non nul. On dit que x est un inverse de a modulo n si $ax \equiv 1 [n]$.

THÉORÈME 3.5 (Existence d'un inverse modulo n)

Avec les notations précédentes, il existe un inverse de a modulo n ssi a est premier avec n .

En particulier, si p est un nombre premier, les nombres admettant un inverse modulo p sont les nombres qui ne sont pas multiples de p .

REMARQUE 3.6

Pour exhiber un inverse, on cherche une relation de Bézout : $au + bn = 1$ et u convient.

3.2 Petit théorème de Fermat

THÉORÈME 3.7

Soit p un nombre premier. Soit a un entier premier à p . Alors,

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

REMARQUE 3.8

On en déduit aisément une deuxième forme : $a^p \equiv a \pmod{p}$, valable pour tout entier a . On retiendra cependant la première forme, plus utile et présentant davantage de généralisations.

REMARQUE 3.9

L'énoncé est faux si p n'est pas premier. Par exemple, $3^{4-1} = 27$ n'est pas congru à 1 modulo 4. On verra plus tard en exercice qu'il faut remplacer l'exposant $p - 1$, par l'indicatrice d'Euler de n , pour avoir un résultat général.

MÉTHODE 3.10 (Congruence d'une puissance)

On se donne un entier a , un (grand) entier N et un nombre premier p (ne divisant pas a). On cherche à déterminer la valeur de a^N modulo p (sous la forme d'une congruence $a^N \pmod{p}$, où r est petit – le plus souvent, le reste de a^N dans la division euclidienne par p).

On commence par faire la division euclidienne de N par $p-1$: on écrit $N = (p-1)q + N'$, avec $N' \in \llbracket 0, p-2 \rrbracket$. Par le petit théorème de Fermat et les opérations sur les congruences :

$$a^N \equiv (a^{p-1})^q a^{N'} \equiv a^{N'} \pmod{p}.$$

Une fois ramené à une puissance plus petite, on peut calculer directement, en ne gardant à chaque que la valeur des restes modulo p .

Si on remplace p par un entier n non premier (et premier à a , pour simplifier), le principe est le même mais on ne dispose plus du petit théorème de Fermat. On commence par chercher le plus petit exposant $k > 0$ tel que $a^k \equiv 1 \pmod{n}$ (un tel k existe toujours, cf. remarque précédente). Puis on calcule le reste N' de N dans la division euclidienne par k . Alors, $a^N \equiv a^{N'} \pmod{n}$.

Le théorème des restes chinois peut aussi permettre d'accélérer les calculs.

EXERCICE 3.11

- Quel est le reste de 7^{2022} dans la division euclidienne par 13 ?
- Quel est le dernier chiffre de 3^{2049} ?

3.3 Théorème des restes chinois - HP

THÉORÈME 3.12 (Théorème des restes chinois)

Soient n et m deux entiers naturels non nuls premiers entre eux. Soient a et b deux entiers quelconques. Le système de congruence

$$\begin{cases} x \equiv a \pmod{n} \\ x \equiv b \pmod{m} \end{cases}$$

admet une solution, unique modulo nm .

REMARQUE 3.13

L'affirmation d'unicité signifie que deux solutions x et y sont congrues modulo nm .

REMARQUE 3.14

On peut généraliser ce théorème à un nombre fini de congruences modulo n_1, \dots, n_k si les entiers n_i sont deux à deux premiers entre eux. Attention! il ne suffit pas d'être premiers dans leur ensemble : considérer $x \equiv 1 [6]$, $x \equiv 2 [10]$, $x \equiv 3 [15]$. (la première congruence implique que x est impair, la deuxième que x est pair)

EXERCICE 3.15

Quel est le dernier chiffre de 3^{2049} ?