7 - Arithmétique des entiers relatifs

Jeremy Daniel

οἱ πρῶτοι ἀριθμοι 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 ; 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 $r \in [\![0, b-1]\!]$ tels que $a = bq + r$.

Définition 1.5 (Quotient et reste)
On dit que q est le quotient dans la division euclidienne de a par b et que r est son 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)
Soit $(a, b) \in \mathbb{Z}^2 - \{(0, 0)\}$. 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 : $\forall n \in \mathbb{Z}^*, 0 \wedge n = |n|$ et $1 \wedge n = 1$.

Théorème 1.9 (Identité de Bachet-Bézout)
Soit $(a, b) \in \mathbb{Z}^2 - \{(0, 0)\}$. 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, soit $(a, b) \in \mathbb{Z}^2 - \{(0, 0)\}$. 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

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

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)
Soit $(a_1, \ldots, a_k) \in \mathbb{Z}^k - \{(0, 0, \ldots, 0)\}$. Leur pgcd, noté $a_1 \wedge \cdots \wedge a_k$ est le plus grand entier naturel divisant chacun des a_i.

Théorème 1.15 (Identité de Bachet-Bézout)
Soit $(a_1, \ldots, a_k) \in \mathbb{Z}^k - \{(0, 0, \ldots, 0)\}$. Il existe des entiers relatifs $u_1, \ldots, u_k$ tels que

$$a_1u_1 + \cdots + a_ku_k = a_1 \wedge \cdots \wedge a_k.$$

Corollaire 1.16
Le pgcd $a_1 \wedge \cdots \wedge a_k$ est l'unique entier naturel tel que

$$\forall d \in \mathbb{Z}, \Big(\forall i \in [\![1, k]\!], d \mid a_i\Big) \iff d \mid a_1 \wedge \cdots \wedge a_k.$$

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 (algorithme récursif) :

```
def pgcd(a,b):
    if b == 0:
        return a
    else:
        return pgcd(b,a%b)
```

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. En Python (algorithme récursif) :

```
def BB(a,b):
    if b == 0:
        return (1,0,a)
    else:
        q = a//b
        r = a%b
        (u,v,d) = BB(b,r)
        return (v,u-q*v,d)
```

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

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

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

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

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 $a_1, \ldots, a_k$ sont premiers entre eux dans leur ensemble si $a_1 \wedge \cdots \wedge a_k = 1$.

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.

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 sur les produits données en début d'année.

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.

Remarque 2.13
On peut étendre la notation à $\mathbb{Z}$. Si $n \in \mathbb{Z} \setminus \mathbb{N}$, on note $v_p(n) = v_p(|n|)$; et si $n = 0$, on convient que $v_p(0) = +\infty$.

Proposition 2.14 (Propriétés des valuations)
Soient a et b deux entiers naturels non nuls. Soit p un nombre premier.
- $v_p(ab) = v_p(a) + v_p(b)$
- $v_p(a \wedge b) = \min(v_p(a), v_p(b))$;
- $v_p(a \vee b) = \max(v_p(a), v_p(b))$.

Proposition 2.15
Si a et b sont deux entiers, on a $a \mid b \iff \forall p \in \mathbb{P}, v_p(a) \leq v_p(b)$.

Remarque 2.16
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, $a^{p-1} \equiv 1 \mod [p]$.

Remarque 3.8
Une deuxième forme du théorème est équivalente : pour tout $a \in \mathbb{Z}$, $a^p \equiv a \mod [p]$. On retiendra cependant la première forme, qui présente 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 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.
On commence par faire la division euclidienne de N par $p-1$: on écrit $N = (p-1)q + N'$, avec $N' \in [\![0, p-2]\!]$. Par le petit théorème de Fermat et les opérations sur les congruences :

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

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 cherche le plus petit exposant $k > 0$ tel que $a^k \equiv 1\,[n]$ (un tel k existe toujours, cf. remarque précédente). Puis on calcule le reste N' de N dans la division euclidienne par k. Alors, $a^N \equiv a^{N'}\,[n]$.
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 ?

Exercice 3.12
Quel est le dernier chiffre de 3^{2049} ?

3.3 Théorème des restes chinois - HP

Théorème 3.13 (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

$$\begin{cases} x & \equiv a\,[n] \\ x & \equiv b\,[m] \end{cases}$$

admet une solution, unique modulo nm.

Remarque 3.14
L'affirmation d'unicité signifie que deux solutions x et y sont congrues modulo nm.

Remarque 3.15
On peut généraliser ce théorème à un nombre fini de congruences modulo $n_1, \ldots, n_k$ si les entiers n_i sont deux à deux premiers entre eux. Attention ! il ne suffit pas aux n_i d'être premiers dans leur ensemble : considérer le système $x \equiv 1\,[6]$, $x \equiv 2\,[10]$, $x \equiv 3\,[15]$. (la première congruence implique que x est impair, la deuxième que x est pair)

Addendum. Pour compléter la discussion du mercredi 13 novembre, on ajoute un théorème qui généralise le théorème des restes chinois, au cas où n et m ne sont pas premiers entre eux.

Théorème 3.16
Soient n et m deux entiers naturels non nuls. Soient a et b deux entiers relatifs. Le système de congruence

$$\begin{cases} x & \equiv a\,[n] \\ x & \equiv b\,[m] \end{cases}$$

admet une solution ssi $a \equiv b\,[n \wedge m]$. Le cas échéant, la solution est unique modulo $n \vee m$.

Démonstration. Supposons qu'une solution x existe. Alors, comme $n \wedge m$ divise n, la première congruence implique $x \equiv a\,[n \wedge m]$; de même la deuxième congruence implique $x \equiv b\,[n \wedge m]$. Ceci montre la nécessité de la condition $a \equiv b\,[n \wedge m]$ pour qu'une solution au système de congruences existe.
Réciproquement, on suppose cette condition vérifiée. Considérons $x \in \mathbb{Z}$ et notons $y = x - a$. Alors,

$$\begin{cases} x & \equiv a\,[n] \\ x & \equiv b\,[m] \end{cases} \iff \begin{cases} y & \equiv 0\,[n] \\ y & \equiv b-a\,[m] \end{cases}$$

Comme 0 et $b - a$ sont divisibles par $n \wedge m$, ce système est encore équivalent à :

$$n \wedge m \mid y \text{ et } \begin{cases} \dfrac{y}{n \wedge m} & \equiv 0 \left[\dfrac{n}{n \wedge m}\right] \\ \dfrac{y}{n \wedge m} & \equiv \dfrac{b-a}{n \wedge m} \left[\dfrac{m}{n \wedge m}\right] \end{cases}$$

Comme $\dfrac{n}{n \wedge m}$ et $\dfrac{m}{n \wedge m}$ sont premiers entre eux, on peut appliquer le théorème des restes chinois : il existe $c \in \mathbb{Z}$ tel que la ligne précédente est équivalente à

$$n \wedge m \mid y \text{ et } \frac{y}{n \wedge m} \equiv c \left[\frac{nm}{(n \wedge m)^2}\right],$$

ce qui est encore équivalent à $y \equiv c\,\big[\dfrac{nm}{n \wedge m}\big]$, c'est-à-dire à $y \equiv c\,[n \vee m]$. Finalement, le système de congruence est équivalent à $x \equiv c + a\,[n \vee m]$, ce qui conclut le théorème.
□