Agrégation interne de mathématiques **RK**

Séance n° 3

Thème : Arithmétique

Document en cours de rédaction (v.4b) (modif /v.4 : exercice 2 corrigé)

Table des matières

1 Notes de cours

1.1 Anneau, morphismes, sous-anneau, sous-anneau premier, caractéristique

Par convention, tous les anneaux sont supposés munis d'un élément unité. Tous les anneaux considérés seront commutatifs. On note $\mathcal{U}_A$ l'ensemble des éléments inversibles de A (encore appelé ensemble des unités).

Revoir éventuellement les notions d'anneau, de sous-anneau, de morphisme d'anneau (en particulier, un morphisme d'anneaux $f : A \to B$ vérifie $f(1_A) = 1_B$). L'image directe par un morphisme d'un

anneau est un sous-anneau, l'image réciproque par un morphisme d'un sous-anneau est un sous-anneau. Une intersection de sous-anneaux d'un anneau A est un sous-anneau, d'où, pour une partie $S \subset A$ donnée, l'existence d'un plus petit sous-anneau de A contenant S et appelé sous-anneau engendré par S et noté $\mathbb{Z}[S]$. On a

$$\mathbb{Z}[S] = \{P(a_1, a_2, \ldots, a_m),\ m \in \mathbb{N},\ P \in \mathbb{Z}[X_1, \ldots, X_m],\ \ a_1, a_2, \ldots, a_m \in S\}$$

En particulier, le sous anneau engendré par un élément a de A est :

$$\mathbb{Z}[a] = \{P(a),\ P \in \mathbb{Z}[X]\}$$

(si $P = \lambda_n X^n + \lambda_{n-1} X^{n-1} + \ldots + \lambda_0$, on pose $P(a) = \lambda_n.a^n + \lambda_{n-1}.a^{n-1} + \ldots + \lambda_0.1_A$)
Noter que si a satisfait une relation de la forme $Q(a) = 0$, où $Q \in \mathbb{Z}[X]$ est unitaire (de coefficient dominant égal à 1) et de degré m, alors

$$\mathbb{Z}[a] = \{P(a),\ P \in \mathbb{Z}_{m-1}[X]\}$$

(où $\mathbb{Z}_{m-1}[X]$ désigne l'ensemble des polynômes de degré au plus $m-1$)
Par exemple, on appelle anneau des entiers de Gauss le sous-anneau de $\mathbb{C}$ engendré par i :

$$\mathbb{Z}[i] = \{x + iy, x, y \in \mathbb{Z}\}$$

Parmi tous les sous-anneaux de A, il en existe un contenu dans tous les autres, appelé sous-anneau premier. C'est le sous-anneau engendré par la partie vide, qui vaut

$$\{k.1_A, k \in \mathbb{Z}\}$$

et qui est aussi l'image du morphisme $\begin{array}{ccc} \mathbb{Z} & \to & A \\ k & \mapsto & k.1_A \end{array}$.
Le noyau de ce morphisme est un idéal de $\mathbb{Z}$, donc de la forme $s\mathbb{Z}$, $s \in \mathbb{N}$ et le sous-anneau premier de A est isomorphe à $\dfrac{\mathbb{Z}}{s\mathbb{Z}}$ (voir partie suivante). L'entier s s'appelle la caractéristique de l'anneau A. Par conséquent :

A de caractéristique nulle $\iff \forall k \in \mathbb{Z},\ k.1_A = 0 \iff k = 0.$
A de caractéristique $s > 0$ $\iff \forall k \in \mathbb{Z},\ k.1_A = 0 \iff k \equiv 0\ [s].$

Dans le second cas, noter que $k.a = 0_A$ pour tout $a \in A$ et $k \in \mathbb{Z}$ multiple de s.

1.2 Idéaux, anneau quotient

Si $f : A \to B$ est un morphisme, on a, pour tous $a, x \in A$, $f(ax) = f(a)f(x)$ et donc $f(x) = 0 \implies f(ax) = 0$. Par conséquent, $I = \mathrm{Ker}(f)$, qui est un sous-groupe additif de A, possède aussi la propriété :

$$\forall a \in A,\ \forall x \in I,\ ax \in I$$

Un sous-groupe additif I de A qui possède cette propriété est qualifié d'idéal de A. Ce qui suit montrera que, réciproquement, tout idéal est le noyau d'un morphisme d'anneaux.

Notons tout de suite un fait évident. Soit I un idéal de A. Alors

$$I = A \iff 1_A \in A \iff I \cap \mathcal{U}_A \neq \emptyset$$

On en déduit par exemple qu'un morphisme d'anneaux dont l'anneau de départ est un corps est injectif.

Soit $\mathcal{R}$ une relation d'équivalence sur un anneau A. Lorsqu'elle est compatible avec les lois $+$ et $\times$ (et seulement dans ce cas), on peut munir l'ensemble $A/\mathcal{R}$ de deux lois quotients en posant

$$[x]_\mathcal{R} + [y]_\mathcal{R} = [x+y]_\mathcal{R} \qquad [x]_\mathcal{R}[y]_\mathcal{R} = [xy]_\mathcal{R}$$

On vérifie immédiatement que $A/\mathcal{R}$ est alors muni d'une structure d'anneau. La surjection canonique $\pi : A \to A/\mathcal{R}$ est un morphisme d'anneaux et l'on a : $x\mathcal{R}y \iff \pi(x) = \pi(y) \implies x - y \in \mathrm{Ker}(\pi)$. Ainsi la relation $\mathcal{R}$ n'est autre que la congruence modulo l'idéal $I = \mathrm{Ker}(\pi)$. Plutôt que $x\mathcal{R}y$, on écrit $x \equiv y\ [I]$.

Réciproquement, pour tout idéal I de A, la congruence modulo I est compatible[1] avec les lois de A et l'ensemble quotient est naturellement muni d'une structure d'anneau, dit anneau quotient et noté A/I.

Il faut se familiariser avec le travail modulo I (ou modulo a lorsque $I = (a)$). Calculer dans A modulo I revient exactement à calculer dans A/I. On dira par exemple que $x \in A$ est inversible modulo I si il existe $y \in A$ tel que $xy \equiv 1_A\ [I]$. Il revient au même de dire que $[x]_I$ est inversible dans A/I. Voici un exercice élémentaire démontrant l'efficacité de ces notations : prouver[2] que pour tout $P \in K[X]$, $P - X$ divise $P \circ P - X$.

Si $f : A \to B$ est un morphisme d'anneaux et I un idéal de A, f « passe au quotient modulo I » si et seulement si $I \subset \mathrm{Ker}(f)$. Dans ce cas, f induit un morphisme $\overline{f} : A/I \to B$ pour laquelle $f = \overline{f} \circ \pi$.

Une intersection d'idéaux est un idéal, d'où, pour une partie S donnée, l'existence d'un plus petit idéal contenant S appelé idéal engendré par S et noté (S). On a[3]

$$(S) = \left\{ \sum_{i=1}^{n} \lambda_i a_i,\ n \in \mathbb{N}, a_1, \ldots, a_n \in S,\ \lambda_1, \ldots, \lambda_n \in A \right\}$$

En particulier, l'idéal engendré par a est $(a) = aA$. Un tel idéal est dit monogène ou principal. Un anneau dont tous les idéaux sont principaux est dit principal.
Si I et J sont deux idéaux, alors $I + J = \{a + b, a \in I,\ b \in J\}$ est un idéal, appelé idéal somme. Plus généralement, si $(I_\lambda)_{\lambda\in\Lambda}$ est une famille (fini ou non) d'idéaux, on note $\sum_{\lambda\in\Lambda} I_\lambda$ l'ensemble des éléments de la forme $\sum_{j=1}^{m} a_j$, où chaque a_j appartient à l'un des I_λ. Avec cette notation on a :

$$(S) = \sum_{s\in S} (s)$$

Exemples :
Un idéal I est égal à A si et seulement si il contient un élément inversible).
Les idéaux de $\mathbb{Z}$ sont les $a\mathbb{Z}$, $a \in \mathbb{N}$ ($\mathbb{Z}$ est principal).
Les idéaux de $K[X]$ sont les $PK[X]$, $P \in K[X]$ ($K[X]$ est principal).

Un idéal I est dit premier si $ab \in I \implies a \in I$ ou $b \in I$.

[1] Pour l'addition c'est connu. Pour le produit : si $x - x' \in I$ et $y - y' \in I$ alors $xx' - yy' = (x - x')y + x'(y - y') \in I$.
[2] Solution : $P \equiv X\ [P - X]$ donc $P \circ P = P(P) \equiv P(X) \equiv X\ \ [P - X]$.
[3] Noter la similitude formelle avec le sous-espace vectoriel engendré par une partie. Elle n'est pas fortuite. Si on regarde A comme A-module (exactement comme on peut voir un corps K comme une K-espace vectoriel), les idéaux de A sont les sous-modules de A.

Un idéal I est dit maximal si $I \subsetneq A$ et, pour tout idéal J, $I \subset J \subset A \implies J = I$ ou $J = A$.

On vérifie :

A/I est un intègre si et seulement si I est premier.

A/I est un corps si et seulement si I est maximal.

Par exemple, l'application $\begin{array}{rccc} f : & \mathbb{R}[X] & \to & \mathbb{C} \\ & P & \mapsto & P(i) \end{array}$ est un morphisme surjectif d'anneaux. Son noyau est (X^2+1). Donc f induit un isomorphisme de $\mathbb{R}[X]/(X^2+1)$ dans $\mathbb{C}$.

1.3 Généralités sur la relation de divisibilité

On s'accorde généralement à dire que la structure minimale pour faire de l'arithmétique est celle d'anneau intègre. Rappelons qu'un anneau $(A, +, \times)$ est dit intègre s'il commutatif et sans diviseur de 0. Sauf mention explicite du contraire, A désigne dans la suite de cette partie un tel anneau.

L'objet de toutes les attentions est la relation de divisibilité : $a|b$ lorsque qu'il existe c tel que $b = ac$. Cette relation n'est pas d'ordre en général, puisqu'a priori non antisymétrique. Mais on peut la regarder comme relation d'ordre par le procédé suivant : deux éléments a et a' sont dits associés si $a|a'$ et $a'|a$. C'est un exercice facile de vérifier que a et a' sont associées si et seulement si il existe $u \in \mathcal{U}_A$ tel que $a' = ua$ (c'est faux dans un anneau non intègre). L'association est une relation d'équivalence et, si a a' sont associés ainsi que b, b', alors $a|b \iff a'|b'$, de sorte que la relation de divisibilité peut être regardée comme une relation entre classes d'association. C'est de ce point de vue une relation d'ordre (partiel). C'est la raison pour laquelle beaucoup d'énoncés sont à comprendre « à association près ».

Dans $\mathbb{Z}$ par exemple, les classes d'association sont les $\{-s, s\}$, $s \in \mathbb{N}$. Si on choisit l'élément positif de chaque classe pour la représenter, la relation de divisibilité est maintenant « lue » comme étant une relation d'ordre sur $\mathbb{N}$.
Dans $K[X]$ (où K est un corps), la classe d'association de P est λP, $\lambda \in K^*$. On représente généralement chaque classe non réduite à $\{0\}$ par le seul élément unitaire (coefficient dominant = 1) qu'elle contient.

Notons que la relation $a|b$ peut s'exprimer en termes d'idéaux, puisque

$$a|b \iff (b) \subset (a)$$

La relation d'association aussi puisque a associé à b équivaut à $(a) = (b)$.

Puisque la divisibilité est maintenant une relation d'ordre, les notions de borne inférieure et de borne supérieure d'une partie S de A ont un sens, mais elles sont définies à association près et on les appelle pgcd et ppcm. Précisément, si S est une partie de A, on dit que $\delta \in A$ est un pgcd de S si

$$\forall x \in S,\ \delta|x \quad \text{et} \quad \forall d \in A, (\forall x \in A, d|x) \implies d|\delta$$

On écrit abusivement dans ce cas $\delta = \mathrm{pgcd}(S)$. Si δ est un pgcd de S, l'ensemble des pgcd de S est la classe d'association de δ.
De même, on dit que μ est un ppcm de S si

$$\forall x \in S,\ x|\mu \quad \text{et} \quad \forall m \in A, (\forall x \in A, x|m) \implies \mu|m$$

On écrit abusivement dans ce cas $\mu = \mathrm{ppcm}(S)$. Si μ est un ppcm de S, l'ensemble des ppcm de S est la classe d'association de μ.

En termes d'idéaux, S admet δ pour pgcd si et seulement si (δ) est le plus petit idéal principal contenant $(S) = \sum_{s\in S}(s)$, et μ est un ppcm de S si et seulement si μ est le plus grand idéal principal contenu dans $\bigcap_{s\in S}(s)$ (noter que rien n'assure de l'existence de tels idéaux).

Soient S une partie de A et $\lambda \in A$. Si S et λS admettent un pgcd, alors $\mathrm{pgcd}(\lambda S) = \lambda \,\mathrm{pgcd}(S)$ (à association près naturellement). En effet, $\lambda \,\mathrm{pgcd}(S)$ est un diviseur commun de λS. Donc $\lambda \,\mathrm{pgcd}(S)$ divise $\mathrm{pgcd}(\lambda S)$. Par ailleurs, λ est un diviseur commun de λS. Donc $\lambda | \,\mathrm{pgcd}(\lambda S)$ et il existe a tel que $\mathrm{pgcd}(\lambda S) = \lambda a$. Comme λa divise chaque élément de λS, a divise chaque élément de S et $a | \,\mathrm{pgcd}(S)$ d'où $\mathrm{pgcd}(\lambda S) | \lambda \,\mathrm{pgcd}(S)$.

Deux élément a, b d'un anneau A sont dit premiers entre eux si $\mathrm{pgcd}(a, b) = 1$, c'est-à-dire si les seuls diviseurs communs à a et b sont les inversibles. Les éléments d'une partie S sont dits premiers entre eux dans leur ensemble si $\mathrm{pgcd}(S) = 1$.

Soit $a \in A \setminus \{0\}$, non inversible. On dit :
Que a est irréductible si $a = bc$ entraîne b ou c inversible. L'élément a est irréductible si et seulement si l'idéal (a) est maximal dans l'ensemble des idéaux principaux.
Que a est premier si $a|bc$ entraîne $a|b$ ou $a|c$. L'élément a est premier si et seulement si l'idéal (a) est premier donc si et seulement si $A/(a)$ est un anneau intègre.
Tout élément premier est irréductible, mais la réciproque est fausse en général. Par exemple dans $\mathbb{Z}[i\sqrt{5}] = \{x + iy\sqrt{5},\ x, y \in \mathbb{Z}\}$, on a

$$2 \times 3 = (1 - i\sqrt{5})(1 + i\sqrt{5})$$

alors que 2, 3, $1 - i\sqrt{5}$ et $1 - i\sqrt{5}$ sont irréductibles (voir exercice 38).

Un anneau A est dit euclidien s'il existe une application $\phi : A \to \mathbb{N}$ telle que :

$$\phi(0_A) = 0 \text{ et } \forall a \in A, \forall b \in A \setminus \{0\},\ \exists (q, r) \in A^2;\ a = qb + r, \phi(r) < \phi(b)$$

Noter qu'on exige pas l'unicité. Une telle application est affublée du joli nom de stathme. Noter aussi que $\phi(a) = 0 \iff a = 0$.

Les anneaux suivants sont euclidiens : $\mathbb{Z}$, $K[X]$ (K corps), $\mathbb{Z}[i]$. Pour les deux premiers, c'est classique. Pour $\mathbb{Z}[i]$, on peut prendre $\phi(z) = |z|^2$. C'est bien un stathme car si $a \in \mathbb{Z}[i]$, $b \in \mathbb{Z}[i]$, il existe $q \in \mathbb{Z}[i]$ tel que $|a/b - q| \leqslant \dfrac{1}{\sqrt{2}}$ (faire un dessin !). En posant $r = a - qb$, il vient $|r|^2 = |a - bq|^2 \leqslant \dfrac{|b|^2}{2}$.

Tout anneau euclidien est principal : Soit I un idéal non réduit à $\{0\}$ d'un anneau A euclidien (pour un stathme ϕ). Considérons un élément b de $I \setminus \{0\}$ tel que $\phi(r) = \min_I \phi$. Pour tout x de I il existe $q, r \in A$ tels que $x = qb + r$, $\phi(r) < \phi(b)$. Comme $r = x - bq \in I$, $\phi(r) < \phi(b)$ entraîne $r = 0$, d'où $x \in (b)$. On en déduit $I = (b)$.

1.4 Arithmétique dans un anneau principal

Les anneaux $\mathbb{Z}$, $K[X]$ et $\mathbb{Z}[i]$ sont euclidiens, donc principaux. C'est la raison pour laquelle les arithmétiques des trois anneaux sus-mentionnés sont similaires.
Le théorème clef est le suivant :

Théorème 1 *(Bezout) Dans un anneau principal, toute partie S admet un* pgcd *et un* ppcm. *On a :*

$$\delta = \mathrm{pgcd}(S) \iff (\delta) = \sum_{s\in S}(s) \quad \text{et} \quad \mu = \mathrm{ppcm}(S) \iff \mu = \bigcap_{s\in S}(s)$$

Pour important qu'il soit, ce théorème est une évidence, puisque $\sum_{s\in S}(s)$ et $\bigcap_{s\in S}(s)$ sont des idéaux principaux.
Noter qu'il en résulte immédiatement que, dans un anneau principal A, a et b sont premiers entre eux si et seulement si

$$\text{il existe } u, v \in A \text{ tels que } ua + vb = 1_A$$

De même, $a_1, \ldots, a_p \in A$ sont premiers entre eux dans leur ensemble si et seulement si

$$\exists\, u_1, u_2, \ldots, u_p \in A \text{ tels que } u_1a_1 + u_2a_2 + \ldots + u_pa_p = 1_A$$

Corollaire 1 *Dans un anneau principal :*
1. Lemme de Gauss : Si $a|bc$ et $\mathrm{pgcd}(a,b) = 1$ alors $a|c$.
2. Lemme d'Euclide : tout élément irréductible est premier (et donc irréductible $\iff$ premier).
3. Si a et b sont premiers entre eux ainsi que a et c alors a et bc sont premiers entre eux. En particulier, a^n et b^n sont premiers entre eux.
4. Si $a|c$, $b|c$ et $\mathrm{pgcd}(a,b) = 1$ alors $ab|c$.

Tout ceci se prouve aisément :
1. Par Bezout, il existe u et v tels que que $au + bv = 1_A$, d'où $c = acu + bcv$ et $a|c$.
2. Soit a irréductible. Supposons $a|bc$ et posons $d = \mathrm{pgcd}(a,b)$. Comme a est irréductible, on a (à association près) $d = 1_A$ ou $d = a$. Dans le premier cas, $a|c$ par le lemme de Gauss. Dans le cas, $a|b$.
3. Par Bezout, il existe u, v, u', v' tels que $ua+vb = 1_A$ et $u'a+v'c = 1_A$ d'où $(ua+vb)(u'a+v'c) = 1_A$ puis $(uu'a + uv'c + u'vb)a + vv'bc = 1_A$ et $\mathrm{pgcd}(a, bc) = 1$.
4. On écrit $c = ac'$. Alors $b|ac'$ et $\mathrm{pgcd}(a,b) = 1$ donc, par le lemme de Gauss, $b|c'$ d'où $ab|c$.

Théorème 2 *Un anneau principal est factoriel.*

Rappelons qu'on appelle ainsi un anneau intègre dans lequel tout élément non nul admet une décomposition unique à l'ordre des facteurs près (et à association près) en produit d'éléments irréductibles (noter que dans un tel anneau, tout élément irréductible est premier). En d'autres termes, si l'on choisit un ensemble $\mathcal{P}$ d'irréductibles contenant un unique représentant par classe d'association d'irréductibles, alors pour tout $a \in A \setminus \{0\}$, il existe un unique $u \in \mathcal{U}_A$ et une unique famille d'entiers naturels $(\nu_p)_{p\in\mathcal{P}}$ vérifiant $\nu_p = 0$ pour tous p sauf au plus un nombre fini d'entre eux (on dit que $(\nu_p)_{p\in\mathcal{P}}$ est presque nulle), telle que

$$a = u \prod_{p\in\mathcal{P}} p^{\nu_p}$$

La preuve utilise essentiellement le lemme de Gauss et une propriété de finitude :

Proposition 1 *Dans un anneau principal, il n'existe*[4] *pas de suite strictement décroissante pour la relation de divisibilité.*

[4]Plus généralement, il n'existe pas de suite strictement croissante d'idéaux, ce qu'on traduit en disant que l'anneau est noethérien.

Il revient au même de dire que si une suite $(a_k)_k$ d'éléments de A principal vérifie $a_{k+1}|a_k$ pour tout k, alors elle est stationnaire à association près. On a en effet pour une telle suite $(a_k) \subset (a_{k+1})$, donc $\bigcup_k (a_k)$ est un idéal, et il existe $b \in A$ tel que $(b) = \bigcup_k (a_k)$. Mais il existe alors p tel que $b \in (a_p)$, d'où $(b) = (a_p)$ et $(a_p) = (a_{p+1}) = \ldots = (b)$.

Pour prouver le théorème de factorialité, introduisons la définition suivante : si p est un élément premier de A, on désigne par p-valuation de $a \in A$:

$$v_p(a) = \sup\{k \in \mathbb{N}; p^k|a\} \quad \in \mathbb{N} \cup \{+\infty\}$$

On a en fait $v_p(a) < +\infty$ si $a \neq 0$, car si p^k divise a pour tout $k \in \mathbb{N}$, alors en posant $a = p^k a_k$ on obtient une suite $(a_k)_k$ strictement décroissante pour la relation de divisibilité.

On a les propriétés suivantes, aisées à établir :

$v_p(ab) = v_p(a) + v_p(b)$
$v_p(a+b) \geqslant \min(v_p(a), v_p(b))$, avec égalité dès que $v_p(a) \neq v_p(b)$.
$v_p(p^n) = n$, $v_p(q^n) = 0$ (où p et q sont des irréductibles distincts).
$v_p(u) = 0$ pour tout $u \in \mathcal{U}_A$.

Preuve de l'unicité (dans le théorème 2)
Supposons $a = u \prod_{p \in \mathcal{P}} p^{\nu_p}$ (où $(\nu_p)_{p\in\mathcal{P}}$ est presque nulle). Alors, pour tout $q \in \mathcal{P}$, $v_q(a) = v_p(u) + \sum_{p\in\mathcal{P}} v_q(p^{\nu_p}) = \nu_p$.

Preuve de l'existence (dans le théorème 2) Soit $a \in A \setminus \{0\}$. L'ensemble des $p \in \mathcal{P}$ tel que $v_p(a) > 0$ est fini, sinon on construit aisément une suite strictement décroissante (pour $|$) d'éléments de A. Comme $p^{v_p(a)}|a$ pour tout p et que deux tels éléments sont premiers entre eux, $\prod_{p\in\mathcal{P}} p^{v_p(a)}$ divise a (ce produit est fini !). Écrivons $a = u \prod_{p\in\mathcal{P}} p^{v_p(a)}$. Alors $v_p(u) = 0$ pour tout irréductible p et le lemme suivant permet de conclure :

Lemme 1 *Dans un anneau principal, tout élément non inversible admet au moins un diviseur irréductible.*

En effet, si $u \in A\setminus\{0\}$ est non inversible et n'admet aucun diviseur irréductible, il n'est pas irréductible lui-même, on peut donc écrire $a = a_1 b_1$, où a_1 est un diviseur strict non inversible de a. L'élément a_1 n'admet aucun diviseur irréductible. On peut donc construire par récurrence une suite strictement décroissante pour $|$: contradiction.

Noter qu'il existe des anneaux factoriels non principaux. Le théorème suivant permet d'en construire aisément :

Théorème 3 *(Hilbert) Si A est un anneau factoriel, alors $A[X]$ est factoriel.*

Ainsi, $\mathbb{Z}[X]$ ou $K[X,Y]$ (K corps) sont factoriels mais non principaux.

Soit A un anneau principal et $a \in A$. On a les équivalences :

$$A/(a) \text{ est intègre} \iff a \text{ est premier} \iff a \text{ est irréductible} \iff A/(a) \text{ est un corps.}$$

La dernière équivalence peut être vue comme conséquence du fait que A/I est un corps si et seulement si I est maximal. Plus directement, et surtout de manière plus explicite, en supposant a irréductible, si x est un élément non nul modulo a alors $\text{pgcd}(x,a)=1$ d'où l'existence de u, v tels que $ux+va=1_A$. Il vient $ux\equiv 1_A\ [a]$: u est un inverse de A modulo a et $A/(a)$ est un corps. Réciproquement, si $A/(a)$ est un corps alors $A/(a)$ est intègre donc $a|bc$ entraîne $a|b$ ou $a|c$: a est premier, donc irréductible.

Rappelons au passage que si A est un anneau fini, alors A est intègre si et seulement si A est un corps (si A est fini et intègre, alors, pour $a\in A\setminus\{0\}$ fixé, $x\mapsto ax$ est injective donc bijective et il existe $b\in A$ tel que $ab=1_A$).

La recherche d'un couple de Bezout associé à un couple (a,b) tel que $\text{pgcd}(a,b)=1$ peut être importante. Rappelons que dans un anneau euclidien, l'algorithme d'Euclide[5] permet d'en trouver un.

1.5 L'anneau $\mathbb{Z}/n\mathbb{Z}$

D'après ce qui précède,

$$\mathbb{Z}/n\mathbb{Z}\text{ intègre}\iff\mathbb{Z}/n\mathbb{Z}\text{ est un corps}\iff n\text{ est premier}$$

Lorsque n n'est pas premier, les éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$ sont les $[k]_n$, où k est tel que $\text{pgcd}(n,k)=1$ (ce sont donc les générateurs du groupe additif). La relation de Bezout permet, comme on vient de le voir, d'obtenir l'inverse d'un élément inversible. En particulier, $\left|\mathcal{U}_{\mathbb{Z}/n\mathbb{Z}}\right|=\phi(n)$ (où ϕ est l'indicatrice d'Euler). La structure du groupe $\mathcal{U}_{\mathbb{Z}/n\mathbb{Z}}$ sera élucidée un peu plus loin.

L'application du théorème de lagrange dans $\mathcal{U}_{\mathbb{Z}/n\mathbb{Z}}$ mène immédiatement au théorème de Fermat et sa généralisation par Euler : Si $p\in\mathbb{Z}$ est premier et $a\in\mathbb{Z}$ premier avec p alors, puisque $\mathcal{U}_{\mathbb{Z}/p\mathbb{Z}}$ est d'ordre $p-1$, on a $[a]_p^{p-1}=[1_A]_p$, c'est-à-dire

$$\forall a\in\mathbb{Z},\ \text{pgcd}(a,p)=1\implies a^{p-1}\equiv 1\ [p]$$

De manière équivalente

$$\forall a\in\mathbb{Z},\ a^p\equiv a\ [p]$$

Pour $n\in\mathbb{N}^*$ quelconque, on obtient :

$$\forall a\in\mathbb{Z},\ \text{pgcd}(a,n)=1\implies a^{\phi(n)}\equiv 1\ [n]$$

Le bon vieux théorème de Wilson est tout aussi immédiat si on l'interprète dans $\mathcal{U}_{\mathbb{Z}/p\mathbb{Z}}$. Ce théorème affirme :

$$\text{Pour tout } p\in\mathbb{N}^*\text{ premier},\quad (p-1)!\equiv -1\ [p]$$

En effet, $[(p-1)!]_p=\prod_{k=1}^{p-1}[k]_p$ est le produit de tous les éléments de $\mathcal{U}_{\mathbb{Z}/p\mathbb{Z}}$. Or ceux-ci, à l'exception de $[1]_p$ et $[-1]_p$ qui sont les solutions (éventuellement confondues) de l'équation $x^2=1_{\mathbb{Z}/p\mathbb{Z}}$, peuvent se

[5] Brièvement : on pose $r_0=a$, $r_1=b$ puis, tant que $r_k\neq 0$ on effectue la division euclidienne de r_{k-1} par r_k : $r_{k-1}=q_kr_k+r_{k+1}$. Alors le dernier reste non nul, disons r_n, est égal à $\text{pgcd}(a,b)$ et l'on obtient un couple de Bezout pour a,b (ie u,v tels que $ua+vb=\text{pgcd}(a,b)$) en écrivant $\text{pgcd}(a,b)=r_{n-2}-q_{n-1}r_{n-1}$ puis en éliminant r_{n-1} grâce à la relation $r_{n-3}=q_{n-2}r_{n-2}+r_{n-1}$, etc.

grouper par paire de la forme $\{x, x^{-1}\}$, lesquelles se simplifient dans le produit. Donc $[(p-1)!] = [-1]_p$.

Le théorème chinois se prolonge à la structure d'anneau. En effet, l'application

$$\begin{array}{ccc} \mathbb{Z} & \to & \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \\ x & \mapsto & ([x]_n, [x]_m) \end{array}$$

est un morphisme d'anneaux dont le noyau est $\mathrm{ppcm}(n,m)\mathbb{Z}$. Si $\mathrm{pgcd}(n,m) = 1$, alors cette application induit un isomorphisme de l'anneau $\mathbb{Z}/nm\mathbb{Z}$ sur l'anneau $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$.
Comme les inversibles d'un anneau produit sont les couples d'inversibles, on a (il s'agit d'isomorphisme de groupes)

$$\mathrm{pgcd}(n,m) = 1 \implies \mathcal{U}_{\mathbb{Z}/nm\mathbb{Z}} \simeq \mathcal{U}_{\mathbb{Z}/n\mathbb{Z}} \times \mathcal{U}_{\mathbb{Z}/m\mathbb{Z}}$$

D'après le théorème Chinois, il suffit de connaître la structure des groupes $\mathcal{U}_{\mathbb{Z}/p^s\mathbb{Z}}$, p premier, pour connaître celle de $\mathcal{U}_{\mathbb{Z}/n\mathbb{Z}}$ en général. Le résultat est le suivant :

Théorème 4 *Soient $p \in \mathbb{N}$ un nombre premier et $s \in \mathbb{N}^*$.*
Si $p \geqslant 3$, alors $\mathcal{U}_{\mathbb{Z}/p^s\mathbb{Z}}$ est cyclique (d'ordre $\phi(p^s) = p^{s-1}(p-1)$).
$\mathcal{U}_{\mathbb{Z}/2^s\mathbb{Z}}$ est cyclique pour $s = 1$ ou $s = 2$.
Pour $s \geqslant 3$, on a $\mathcal{U}_{\mathbb{Z}/2^s\mathbb{Z}} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{s-2}\mathbb{Z}$

Pour voir que $\mathcal{U}_{\mathbb{Z}/p^s\mathbb{Z}}$ est cyclique quand $p \geqslant 3$, il suffit, puisque l'ordre de ce groupe vaut $p^{s-1}(p-1)$, de trouver un élément a d'ordre p^{s-1} et un élément b d'ordre $(p-1)$ (ab est alors d'ordre $p^{s-1}(p-1)$ car $\mathrm{pgcd}(p^{s-1}, p-1) = 1$ et $ab = ba$).
Pour trouver un tel a, c'est « simple » : on vérifie que $(p+1)$ est d'ordre p^{s-1} modulo p^s. Dire ceci revient à affirmer $(p+1)^{p^{s-1}} \equiv 1\ [p^s]$ et, si $s \geqslant 2$, $(p+1)^{p^{s-2}} \not\equiv 1\ [p^s]$ (car si $(p+1)^{p^{s-1}} \equiv 1\ [p]$, alors l'ordre de $p+1$ modulo p^s divise p^s, donc est de la forme p^k, $0 \leqslant k \leqslant s$). La première relation s'écrit $(p+1)^{p^{s-1}} = 1 + u_s p^s$, $u_s \in \mathbb{Z}$. La seconde signifie $p \not| u_{s-1}$. On a donc à établir, pour tout $s \geqslant 1$, l'existence de $u_s \in \mathbb{Z}$, premier avec p, vérifiant $(p+1)^{p^{s-1}} = 1 + u_s p^s$. C'est immédiat pour $s = 1$ et si c'est vrai au rang $s \geqslant 1$ alors

$$(p+1)^{p^s} = (1 + u_s p^s)^p = 1 + u_s p^{s+1} + \sum_{k=2}^{p^s} \left(\begin{array}{c} p^s \\ k \end{array} \right) u_s^k p^{ks}$$

Mais si $k \geqslant 3$ ou $s \geqslant 2$, alors $ks \geqslant s+2$ et $p^{s+2} | p^{ks}$, tandis que lorsque $k = 2$ et $s = 1$, on a $\left(\begin{array}{c} p^s \\ k \end{array} \right) p^{ks} = p^3 \dfrac{p-1}{2} = p^{s+2} \dfrac{p-1}{2}$. On peut donc mettre p^{s+2} en facteur du « Σ »pour obtenir une relation de la forme $(p+1)^{p^s} = 1 + (u_s + pv)p^{s+1}$ et le résultat.

Pour montrer l'existence de b, on procède par récurrence sur $s \geqslant 1$. Pour $s = 1$, on utilise le fait que $\mathbb{Z}/p\mathbb{Z}$ est un corps. Car on sait que tout sous-groupe fini du groupe des inversible d'un corps est cyclique. Donc $\mathcal{U}_{\mathbb{Z}/p\mathbb{Z}}$ est cyclique et admet un élément d'ordre $p-1$. On considère ensuite le morphisme naturel $\pi : \mathbb{Z}/p^s\mathbb{Z} \to \mathbb{Z}/p^{s-1}\mathbb{Z}$ (obtenu en considérant la surjection canonique de $\mathbb{Z}$ dans $\mathbb{Z}/p^{s-1}\mathbb{Z}$, en constatant qu'elle est compatible avec la congruence modulo p^s – car $p^s\mathbb{Z} \subset p^{s-1}\mathbb{Z}$ –, et en « passant au quotient » modulo p^s). Ce morphisme est surjectif et si $c \in \mathbb{Z}/p^{s-1}\mathbb{Z}$ est d'ordre $p-1$, il existe $d \in \mathbb{Z}/p^s\mathbb{Z}$ tel que $\pi(d) = c$. L'ordre ω de d est un multiple de $p-1$ (car $c^\omega = \pi(d^\omega) = 1_{\mathbb{Z}/p^{s-1}\mathbb{Z}}$). Donc le sous-groupe (cyclique) engendré par d contient un élément b d'ordre $p-1$.

La preuve, dans le cas $p = 2$ est laissée à la sagacité du lecteur (qui pourra vérifier que 5 est d'ordre 2^{s-2} modulo 2^s).

1.6 Arithmétique de $\mathbb{Z}[i]$

On pose, pour $z \in \mathbb{Z}[i]$, $N(z) = z\bar{z}$. On a vu que $\mathbb{Z}[i]$ est euclidien pour le stathme N. Il est donc principal et par conséquent factoriel. L'application N induit en outre un morphisme pour le produit de $\mathbb{Z}[i] \setminus \{0\}$ dans $\mathbb{N}^*$: $N(zz') = N(z)N(z')$. Il en résulte que $N(z)$ « porte » certaines informations sur le statut arithmétique de z. Par exemple on vérifie immédiatement

$$z \text{ inversible} \iff N(z) = 1 \iff z \in \{-1, 1, -i, i\}$$

ou bien

$$N(z) \text{ premier (dans } \mathbb{N}) \implies z \text{ premier (dans } \mathbb{Z}[i])$$

C'est ainsi que, par exemple, $2 = (1+i)(1-i)$, donc $(1-i)$ et $(1+i)$ sont premiers dans $\mathbb{Z}[2]$. Notons que, puisque $(1-i) = -i(1+i)$, ces deux irréductibles sont associés. La décomposition en produit d'irréductibles de 2 est donc

$$2 = -i(1+i)^2$$

Si l'on cherche à déterminer tous les éléments premiers de $\mathbb{Z}[i]$, on peut faire la remarque suivante : soit $z \in \mathbb{Z}[i]$ premier. Alors dans l'anneau $\mathbb{Z}[i]$, z divise $N(z)$. Or $N(z)$ est un produit d'entier naturels premiers. Donc z divise un entier naturel premier. On obtiendra donc tous les éléments premiers de $\mathbb{Z}[i]$ en considérant les diviseurs premiers (dans $\mathbb{Z}[i]$) des entiers naturels premiers (dans $\mathbb{Z}$). Cette remarque et le théorème suivant permettent de dresser la liste de tous les éléments premiers de $\mathbb{Z}[i]$:

Théorème 5 *Soit p un entier naturel premier (dans $\mathbb{Z}$). Alors :*

soit p est premier dans $\mathbb{Z}[i]$,

soit il existe w premier dans $\mathbb{Z}[i]$ tel que $p = w\bar{w}$.

De plus :

p est premier dans $\mathbb{Z}[i] \iff$ p n'est pas somme de deux carrés de $\mathbb{Z}$.

Preuve du théorème : Soit donc $p \in \mathbb{Z}$ premier. On peut décomposer p en produit d'éléments premiers de $\mathbb{Z}[i]$:

$$p = u \prod_{j=1}^{s} q_j^{\alpha_j} \prod_{k=1}^{r} w_k^{\beta_k}$$

où u est inversible, les $q_j \in \mathbb{N}$ et les $w_j \in \mathbb{Z}[i] \setminus \mathbb{Z}$ sont premiers dans $\mathbb{Z}[i]$. Mais la conjugaison possède la propriété suivante : $\forall z, z' \in \mathbb{Z}[i], z|z' \implies \bar{z}|\bar{z'}$. Donc les $w_j^{\bar{\beta_j}}$ sont des diviseurs de z et il est facile de vérifier que $\bar{w_j}$ est encore premier dans $\mathbb{Z}[i]$. On vérifie sans mal que $\bar{w_j}$ n'est pas associé à w_j, sauf si w_j est associé à $(1+i)$. On peut donc, à l'exception éventuelle d'un w_j conjugué à $(1+i)$, grouper deux à deux par conjugaison les termes $w_j^{\beta_j}$. Quitte à modifier u, à isoler l'éventuel terme en $(1+i)$ et à renuméroter les $(w_j)_j$, il vient :

$$p = u(1+i)^{\gamma} \prod_{j=1}^{s} q_j^{\alpha_j} \prod_{k=1}^{r'} N(w_k)^{\beta_k}$$

Puisque $p \in \mathbb{N}$ et $u \in \{-1, 1, -i, i\}$, γ est pair (on posera $\gamma = 2\delta$) et :

$$p = 2^{\delta} \prod_{j=1}^{s} q_j^{\alpha_j} \prod_{k=1}^{r'} N(w_k)^{\beta_k}$$

Enfin, p étant premier dans $\mathbb{Z}$,

soit $s = 1, r' = 0, \delta = 0$ et p est irréductible dans $\mathbb{Z}[i]$,

soit $s = 0, r' = 1, \delta = 0$ ou $s = 0, r' = 0, \delta = 1$ et $p = w\bar{w}$, w irréductible dans $\mathbb{Z}[i]$.

Dans le second cas on voit, en posant $w = u + iv$ (où $u, v \in \mathbb{Z}$), que $p = u^2 + v^2$ est la somme de deux carrés. Réciproquement, si $p = u^2 + v^2$, $u, v \in \mathbb{Z}$, alors en posant $w = u + iv$ on a $p = w\bar{w}$. Le nombre w est bien irréductible dans $\mathbb{Z}[i]$ car $N(w)$ est premier dans $\mathbb{Z}$.

Il reste à repérer les p premiers dans $\mathbb{N}$ qui sont somme de deux carrés. Le résultat est le suivant :

Proposition 2 *Soit $p \in \mathbb{N}$ un entier naturel premier. On a :*

$$p \text{ est la somme de deux carrés } \iff -1 \text{ est un carré modulo } p \iff p = 2 \text{ ou } p \equiv 1\ [4]$$

Vérifions la première équivalence. Si $p = u^2 + v^2$, alors $v \not\equiv 0\ [p]$ (sinon p divise u^2, donc divise i et p^2 divise $u^2 + v^2$). Donc v est inversible modulo p. Soit donc v' tel que $vv' \equiv 1\ [p]$. On a $u^2v'^2 + 1 \equiv 0\ [p]$ et $-1 \equiv -(uv')^2\ [p]$.
Réciproquement, si -1 est un carré modulo p, il existe $a, k \in \mathbb{Z}$ tels que $-1 = a^2 + kp$, d'où $p|(a+i)(a-i)$. Si p était premier dans $\mathbb{Z}[i]$, on en déduirait $p|(a+i)$ par exemple et, par conjugaison, $p|(a-i)$. Or la relation $(a+i)-(a-i) = 2i$ montre que $\mathrm{pgcd}(a+i, a-i)$ est un diviseur de 2. Donc $p|2$ (cette relation est à lire dans $\mathbb{Z}[i]$ a priori, mais on voit aisément qu'elle alors valable dans $\mathbb{Z}$ aussi), puis $p = 2$, ce qui est absurde (2 n'est pas premier dans $\mathbb{Z}[i]$). Donc p n'est pas premier dans $\mathbb{Z}[i]$. Le théorème 5 montre alors que p est somme de deux carrés.

Vérifions maintenant la seconde équivalence. Comme elle est évidente pour $p = 2$, on peut supposer $p \geqslant 3$. On commence par caractériser les carrés modulo p. Considérons l'application

$$\begin{array}{rccc} \xi : & \mathcal{U}_{\mathbb{Z}/p\mathbb{Z}} & \to & \mathcal{U}_{\mathbb{Z}/p\mathbb{Z}} \\ & x & \mapsto & x^2 \end{array}$$

C'est un morphisme de groupes dont le noyau $\{x \in \mathbb{Z}/p\mathbb{Z};\ x^2 = 1\} = \{-1_{\mathbb{Z}/p\mathbb{Z}}, 1_{\mathbb{Z}/p\mathbb{Z}}\}$ est d'ordre 2 et l'on a $\mathrm{Im}(\xi) \simeq (\mathbb{Z}/p\mathbb{Z})/\mathrm{Ker}(\xi)$. Donc $\mathrm{Im}(\xi)$ est un sous-groupe d'ordre $\dfrac{p-1}{2}$. Mais comme le groupe $\mathcal{U}_{\mathbb{Z}/p\mathbb{Z}}$ est d'ordre $p-1$, on a, pour tout $x \in \mathrm{Im}(\xi)$: $x^{\frac{p-1}{2}} = 1_{\mathbb{Z}/p\mathbb{Z}}$. Ainsi le polynôme $X^{\frac{p-1}{2}} - 1_{\mathbb{Z}/p\mathbb{Z}} \in \mathbb{Z}/p\mathbb{Z}[X]$ admet exactement $\dfrac{p-1}{2}$ racines, qui les carrés de $\mathcal{U}_{\mathbb{Z}/p\mathbb{Z}}$. Finalement, $x \in \mathbb{Z}/p\mathbb{Z}$ est un carré si et seulement si $x = 0$ ou $x^{\frac{p-1}{2}} = 1$. En particulier, -1 est un carré modulo p si et seulement si $(-1)^{\frac{p-1}{2}} \equiv 1\ [p]$, ce qui équivaut à $p \equiv 1\ [4]$.

Voici une seconde preuve, très algébrique, de la première équivalence (preuve qu'il est tout sauf indispensable de maîtriser !) : p n'est pas somme de deux carrés si et seulement si, on l'a vu, p est premier dans $\mathbb{Z}[i]$. Donc si et seulement si $(\mathbb{Z}[i])/(p)$ est intègre. Or (attention à ne pas regarder cette suite d'équivalences comme un calcul formel un peu fumeux : chaque isomorphisme peut être explicité)

$$(\mathbb{Z}[i])/(p) \simeq (\mathbb{Z}[X]/(X^2+1))/(p) \simeq \mathbb{Z}[X]/(p, X^2+1) \simeq (\mathbb{Z}[X]/(p))/(X^2+1) \simeq (\mathbb{Z}/p\mathbb{Z})[X]/(X^2+1)$$

et ce dernier anneau est intègre si et seulement si $X^2 + 1$ est premier dans $\mathbb{Z}/p\mathbb{Z}$, c'est-à-dire si -1 n'est pas un carré modulo p.

2 Annexe

2.1 Relations d'ordre

Soit $\mathcal{R}$ une relation binaire sur un ensemble E.
$\mathcal{R}$ est qualifiée de relation d'ordre si $\mathcal{R}$ est réflexive, antisymétrique et transitive.

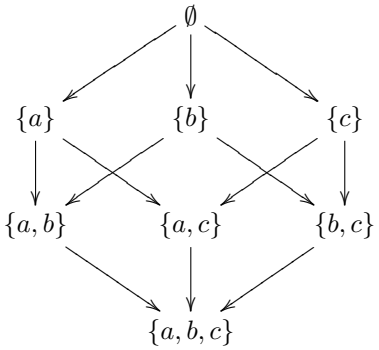
Elle est dite totale si elle vérifie en outre

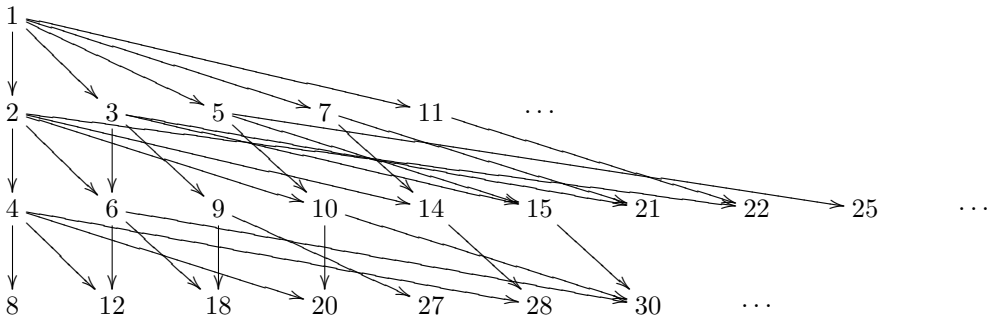
$$\forall x, y \in E,\ x\mathcal{R}y \text{ ou } y\mathcal{R}x.$$

L'expression "relation d'ordre partiel" est équivalente à "relation d'ordre" (l'adjectif "partiel" vient surtout rappeler qu'une relation d'ordre n'est pas nécessairement totale). On choisit généralement un symbole évocateur tel que $\leqslant$ ou $\preccurlyeq$ pour représenter une relation d'ordre. Dans ce cas, l'expression $x < y$ (ou $x \prec y$) signifie $x \leqslant y$ et $x \neq y$ (ou $x \preccurlyeq y$ et $x \neq y$).

Exemples :
- Si X est un ensemble et $\mathcal{P}(X)$ est l'ensemble des parties de X, la relation d'inclusion $\subset$ est une relation d'ordre sur $\mathcal{P}(X)$.
- La relation de divisibilité sur $\mathbb{N}$ ($a|b \iff \exists c \in \mathbb{Z};\ b = ac$) est une relation d'ordre. La relation de divisibilité peut être définie sur $\mathbb{Z}$ ou, plus généralement, sur un anneau commutatif. Elle est alors réflexive et transitive mais généralement pas antisymétrique (une relation réflexive et transitive est dite de préordre).
- La relation, ou plutôt les relations, usuellement notées $\leqslant$ sur $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, ou $\mathbb{R}$ sont des relations d'ordre total.
- Si $\preccurlyeq$ est une relation d'ordre sur E, alors la relation $\succcurlyeq$ définie par $x \succcurlyeq y \iff y \preccurlyeq x$ est aussi une relation d'ordre.
- Si $\mathcal{R}$ est une relation d'ordre sur E et si F est une partie de E, on peut considérer la restriction $\mathcal{S}$ de $\mathcal{R}$ à F (définie par $\forall x, y \in F,\ x\mathcal{S}y \iff x\mathcal{R}y$). C'est une relation d'ordre sur F appelée ordre induit sur F.
- Si $(E, \leqslant)$ est un ensemble ordonné (ie muni d'une relation d'ordre), alors on définit sur E^p l'ordre lexicographique $\preccurlyeq$ par $(x_1, x_2, \ldots, x_p) \preccurlyeq (y_1, y_2, \ldots, y_p) \iff (x_1, x_2, \ldots, x_p) = (y_1, y_2, \ldots, y_p)$ ou $\exists k \in [\![1, p-1]\!];\ x_1 = y_1, \ldots, x_k = y_k$ et $x_{k+1} < y_{k+1}$

Pour se faire une bonne intuition de ce qu'est une relation d'ordre partiel, on peut avoir à l'esprit l'image d'un graphe orienté ne comportant pas de cycle. Les noeuds du graphe représentent les éléments de l'ensemble et l'on a $x\mathcal{R}y$ lorsque y est un "descendant" de x. Ainsi les diagrammes suivants schématisent-ils respectivement la relation d'inclusion sur $\mathcal{P}(\{a, b, c\})$ et la relation de divisibilité sur $\mathbb{N}$.





Un certain nombre de définitions doivent être connues. Soit $(E, \leqslant)$ un ensemble ordonné, A une partie de E et $a \in E$.

– On dit que a est un majorant de A si
$$\forall x \in A, x \leqslant a$$
– On dit que a est un (le) plus grand élément de A si $a \in A$ et si a est un majorant de A. Si A possède un plus grand élément, il est unique et on le note $\max(A)$.
– On dit que a est un élément maximal de A si $a \in A$ et si A ne contient aucun élément strictement plus grand que a :
$$\forall x \in A,\ a \leqslant x \implies x = a$$
– a est une (la) borne supérieure de A si a est un plus petit majorant de A (ie petit élément de l'ensemble des majorants de A). Si A possède une borne supérieure, elle est unique et on la note $\sup(A)$.

On définit de même les notions de minorant, plus petit élément (noté $\min(A)$), élément minimal et borne inférieure (notée $\inf(A)$). Bien sûr, si A admet un plus grand élément, celui-ci est alors aussi la borne supérieure de A.

Exemples

– Dans $\mathbb{R}$ muni de l'ordre usuel, $[0, 1[$ admet 0 pour plus petit élément mais n'a pas de plus grand élément. L'ensemble de ses majorants est $[1, +\infty[$. Donc 1 est borne supérieure de $[0, 1[$.
– Dans $\mathbb{R}$ toujours, $\mathbb{N}$ n'est pas majoré. Donc $\mathbb{N}$ n'admet pas de plus grand élément.
– Dans $\mathbb{Q}$, $A = \{x \in \mathbb{Q}_+; x^2 < 2\} = [0, \sqrt{2}[\cap \mathbb{Q}$ admet pour ensemble de majorant $]\sqrt{2}, +\infty[\cap \mathbb{Q}$, qui n'admet pas de plus petit élément. Donc A n'admet pas de borne supérieure.
– Soit A une partie non vide de $\mathbb{R}$ et $a \in \mathbb{R}$. Alors
$$a = \sup A \iff (\forall x \in A,\ x \leqslant a) \text{ et } (\forall \epsilon > 0,\ \exists x \in A; a - \epsilon \leqslant x)$$
– Parmi les axiomes de $\mathbb{N}$, on trouve : "Toute partie non vide de $\mathbb{N}$ admet un plus petit élément. Toute partie non vide et majorée de $\mathbb{N}$ admet un plus grand élément".
– Parmi les axiomes de $\mathbb{R}$, on trouve : "Toute partie non vide et majorée de $\mathbb{R}$ admet une borne supérieure".
– Soit X un ensemble et $E = \mathcal{P}(X)$ qu'on ordonne par l'inclusion. Soit Z une partie de E. Alors $B \subset X$ majore Z si et seulement si B contient tous les éléments de Z (ces éléments sont des parties de X !), c'est-à-dire si B contient la réunion des éléments de Z. Donc Z admet une borne supérieure : $\sup Z = \bigcup_{A \in Z} A$. De même, Z admet une borne inférieure (l'intersection des éléments de Z).

– Dans $\mathbb{N}$ muni de la relation de divisibilité, les éléments minimaux de $\mathbb{N}^* \setminus \{1\}$ sont les naturels premiers.
– Soient $a_1, a_2, \ldots, a_p \in \mathbb{N}$. On définit $\mathrm{pgcd}(a_1, a_2, \ldots, a_d)$ comme étant, dans l'ensemble des diviseurs communs de $a_1, a_2, \ldots, a_d$, le plus grand *pour la relation de divisibilité*. On ne commettrait pas d'erreur en utilisant ici la relation d'ordre usuelle $\leqslant$ plutôt que la divisibilité, mais cette définition a l'avantage d'être généralisable à un anneau commutatif quelconque (en prenant en compte les problèmes d'association et en prenant garde à ce que l'existence du pgcd n'est pas acquise a priori).
– Étant donnée une famille $(x_i)_{i\in I}$ de vecteurs d'un espace vectoriel E, les propriétés suivantes sont équivalentes :

- $(x_i)_{i\in I}$ est une base.

- $(x_i)_{i\in I}$ est une famille libre maximale (ie est un élément maximal de l'ensemble des familles libres ordonné par l'inclusion).

- $(x_i)_{i\in I}$ est une famille génératrice minimale.

– Dans un espace vectoriel, un hyperplan est, par définition, un sous-espace strict maximal (dans l'ensemble des sous-espaces stricts et pour la relation d'inclusion).
– Soit $(E, \preccurlyeq)$ un ensemble ordonné non vide. Une chaîne de E est une partie totalement ordonnée. Le théorème de Zorn affirme que si toute chaîne de E est majorée, alors E admet un élément maximal (la preuve de ce théorème nécessite l'axiome du choix).
Appliqué à l'ensemble des familles libres d'un espace vectoriel, ordonné par "inclusion", il prouve l'existence de bases. Appliqué à l'ensemble des idéaux stricts d'un anneau A contenant un idéal strict donné, il montre que tout idéal strict est contenu dans un idéal maximal (théorème de Krull)

3 Exercices

1. Soit A un anneau dans lequel, pour tout x, y, $xy = yx$ ou $xy = -yx$. Montrer que A est commutatif (indice : considérer la réunion de deux sous-groupes).

2. (a) Soit A un anneau intègre. Si deux éléments quelconques admettent un pgcd et un ppcm, on dit que A est un anneau à pgcd-ppcm. Montrer que dans un tel anneau, $\mathrm{pgcd}(a, b)\,\mathrm{ppcm}(a, b) = ab$.

   (b) Montrer qu'un anneau factoriel est un anneau à pgcd-ppcm.

   (c) Dans un anneau factoriel, vérifier (distributivité de pgcd sur ppcm et vice-versa) :

$$\mathrm{pgcd}(a, \mathrm{ppcm}(b, c)) = \mathrm{ppcm}(\mathrm{pgcd}(a, b), \mathrm{pgcd}(a, c))$$
$$\mathrm{ppcm}(a, \mathrm{pgcd}(b, c)) = \mathrm{pgcd}(\mathrm{ppcm}(a, b), \mathrm{ppcm}(a, c))$$

3. Soit E un ensemble fini, et K un corps. On considère l'anneau $A = K^E$. Pour toute partie F de E, on pose $I_F = \{f \in A;\ \forall x \in F,\ f(x) = 0\}$. Montrer que I_F est un idéal principal de A et que tout idéal de A est de cette forme. Quels sont les idéaux maximaux de K^E ? Identifier K^E/I lorsque I est maximal.

4. Soit A un anneau commutatif et I un idéal de A. On dit que I est premier si $ab \in I \implies a \in I$ ou $b \in I$. On dit que I est maximal si $I \neq A$ et si il n'existe pas d'idéal J tel que $I \subsetneq J \subsetneq A$.
   À quelle condition un idéal principal (a) est-il premier ? Montrer que I est premier si et seulement si A/I est intègre. Montrer que I est maximal si et seulement si A/I est un corps. Que dire si A est fini ?

5. Déterminer les sous-anneaux de $\mathbb{Q}$ et leurs idéaux.

6. Soient a et b deux entiers naturels premiers entre eux. Montrer qu'une solution de l'équation $ax + by = c$ est :
$$x = ca^{\phi(b)-1},\ y = -c\frac{a^{\phi(b)} - 1}{b}$$

7. Soient $n, m \in \mathbb{N}^*$, $a, b \in \mathbb{Z}$. A quelle condition le système : $\begin{cases} x \equiv a\ [n] \\ x \equiv b\ [m] \end{cases}$ est-il soluble ? Donner la forme de l'ensemble des solutions et indiquer une méthode permettant d'en trouver une.

8. Soient $x, y, z \in Z$ tels que $x^2 + y^2 = z^2$.
   (a) Montrer que l'on peut supposer x, y et z premiers deux à deux entre eux (ce que l'on suppose par la suite).
   (b) Montrer que des deux entiers x et y, l'un est pair, l'autre impair (raisonner modulo 4 ; on suppose par la suite x pair et y impair).
   (c) Montrer que $\frac{z+y}{2}$ et $\frac{z-y}{2}$ sont des entiers premiers entre eux.
   (d) Montrer l'existence de deux entiers premiers entre eux u et v pour lesquels :
$$\begin{cases} x = 2uv \\ y = u^2 - v^2 \\ z = u^2 + v^2 \end{cases}$$

9. Résoudre l'équation d'inconnues n, m : $1! + 2! + .. + n! = m^2$.
   Indication : tout le monde n'est pas un carré modulo r.

10. (a) Peut-on trouver 1000 entiers consécutifs non premiers ?
    (b) Peut-on trouver 1000 entiers consécutifs qui tous ont un facteur premier de valuation au moins égale à deux (utiliser le théorème chinois) ?

11. (a) Quels sont les entiers naturels n tels que n, $n+2$, $n+4$ soient premiers ?
    (b) Quels sont les entiers naturels n tels que n, $n+6$, $n+12$, $n+18$, $n+24$ soient premiers ?

12. (a) Soient p, k des entiers naturels, $1 \leqslant k \leqslant n-1$, p premier. Montrer que p divise C_p^k.
    (b) Soient p, n, k des entiers naturels, p premier. Montrer que p^n divise $kC_{p^n}^k$, mais que, si $0 < k \leqslant p^n$, $p^{(n+1)}$ ne le divise pas.
    (c) Soient p, n, k naturels, p premier. Montrer que $C_{p^n-1}^k \equiv (-1)^k [p]$.

13. (a) Établir, pour $a, b \in \mathbb{N}^*$: $a \wedge b = 1 \Rightarrow (2^a - 1) \wedge (2^b - 1) = 1$.
    (b) On pose $u_0 = 2$, $u_{n+1} = 2^{u_n} - 1$. Montrer que si $n \neq m$ alors $u_n \wedge u_m = 1$.
    (c) En déduire une démonstration de l'existence d'une infinité de nombres premiers.

14. En s'inspirant de la preuve d'Euclide de l'existence d'une infinité de nombres premiers (voir aussi les exercices 34 et 35) :
    (a) Montrer qu'il existe une infinité de nombres premiers de la forme $4n - 1$.
    (b) Montrer qu'il existe une infinité de nombres premiers de la forme $6n - 1$.

15. Soient n, p des entiers, p premier. Établir la formule de Legendre :
$$v_p(n!) = \sum_{k=1}^{\infty} \left[\frac{n}{p^k}\right]$$
    Retrouver que $n!$ divise le produit de n entiers consécutifs.

16. Quelle est la somme des chiffres de la somme de chiffres de la somme des chiffres de 1999^{1999} ?
17. Montrer qu'il existe, parmi les entiers 1, 31, 331, $3331, \ldots$, une infinité de nombres composés.
18. Soit n un entier non multiple de 3 ni de 5. Montrer qu'il existe un multiple de n dont l'écriture décimale ne contient que des 1.
19. Montrer que pour tout entier $n > 6$, $\phi(n) \geqslant \sqrt{n}$ (où ϕ est la caractéristique d'Euler).
20. Déterminer tous les entiers n divisibles par tous les entiers inférieurs ou égaux à $\sqrt{n}$.
21. Soit p un nombre premier, $x_1, x_2, .., x_n$ des entiers. Montrer que :

$$(x_1 + x_2 + ... + x_n)^p \equiv x_1^p + x_2^p + ... + x_n^p \ [p]$$

En déduire une nouvelle preuve du petit théorème de Fermat.

22. Donner une preuve par récurrence du petit théorème de Fermat.
23. Soient p et q deux premiers distincts, $a \in \mathbb{Z}$ premier avec pq. Montrer que $a^{\text{ppcm}(p-1,q-1)} \equiv 1 \ [pq]$.
24. Calculer le reste dans la division euclidienne de 3^{100} par 17 ? De 2^{52} par 37 ? De 55^{142} par 143 ? De 3^{2000} par 85 ? De 2^{1000} par 133 ?
25. Montrer que pour tout entier naturel n, $3^{6n} \equiv 2^{6n} \ [35]$.
26. Résoudre dans $\mathbb{N}$: $1 + 2^n + 3^n + 4^n \equiv 0 \ [5]$.
27. Résoudre dans $\mathbb{Z}$ les équations :
    (a) $x^{35} + 5x^{19} + 11x^3 \equiv 0 \ [17]$
    (b) $304x^{303} + 204x^{202} - 104x^{101} \equiv 0 \ [101]$
28. Montrer que pour tous entiers m et n, $mn(m^{60} - n^{60})$ est divisible par 56786730.
29. Soit $n \in \mathbb{N}^*$ impair. Prouver : $n|(2^{n!} - 1)$.
30. Prouver la réciproque du théorème de Wilson.
31. On propose la preuve de Lagrange du théorème de Wilson. Soient p un nombre premier et P le polynôme $P(X) = (X-1)(X-2)...(X-(p-1))$. On pose : $P(X) = X^{p-1} + a_1X^{p-2} + ... + a_{p-2}X + a_{p-1}$.
    (a) Vérifier : $(X-1)P(X-1) = (X-p)P(X)$.
    (b) En déduire $a_1 \equiv a_2 \equiv ... \equiv a_{p-2} \equiv 0 \ [p]$.
    (c) Retrouver le théorème de Wilson.
32. Soit p un entier premier. Montrer que $(p-1)!+1$ ne peut être une puissance d'un nombre premier que si $p = 2, 3$ ou 5.
33. Montrer que 1997 divise le numérateur de $1 - \dfrac{1}{2} + \dfrac{1}{3} - ... - \dfrac{1}{1330} + \dfrac{1}{1331}$
Indication : Chercher à généraliser cet énoncé.
34. Soit p un entier premier impair. En considérant les applications $x \mapsto x^2$ et $x \mapsto x^{\frac{p-1}{2}}$ de $(\mathbb{Z}/p\mathbb{Z})^*$ dans lui-même, montrer que -1 est un carré modulo p si et seulement si $p \equiv 1 \ [4]$. En déduire l'existence d'une infinité de nombres premiers p congrus à 1 modulo 4 (considérer $n!^2 + 1$).
35. Soit p un nombre premier > 3.
    (a) Donner un condition nécessaire et suffisante pour que l'équation $x^2 + ax + b \equiv 0 \ [p]$ admette une solution.
    (b) En considérant l'équation $x^2 + x + 1 = 0$, trouver une condition nécessaire et suffisante pour que (-3) soit un carré modulo p. En déduire l'existence d'une infinité de nombres premiers p congrus à 1 modulo 3.

36. (a) Soit $z \in \mathbb{N}^*$. Prouver qu'il existe x et $y \in \mathbb{N}$ tels que $z = x^2 + y^2$ si et seulement si , dans la décomposition en facteurs premiers de z, à chaque facteur congrus à 3 modulo 4 est associé un exposant pair. Préciser, en fonction de z, le nombre de solutions dans $\mathbb{Z}^2$ de l'équation $z = x^2 + y^2$.

    (b) À quelle condition un entier naturel peut-il s'écrire comme somme des carrés de deux entiers premiers entre eux ?

37. Soient x et y deux entiers relatifs vérifiant : $x^2 + 1 = y^3$.

    (a) Prouver que x est pair.

    (b) Prouver que $(x + i)$ et $(x - i)$ sont premiers entre eux dans $\mathbb{Z}[i]$.

    (c) Établir que $(x + i)$ est un cube dans $\mathbb{Z}[i]$.

    (d) Déterminer x et y.

38. L'anneau $\mathbb{Z}[i\sqrt{5}]$ (à rédiger)

39. Cet exercice porte sur la notion d'ensemble ordonné. On y démontre un théorème de point fixe et on en déduit le théorème de Cantor-Bernstein.

    (a) Soit $(E, \leqslant)$ un ensemble ordonné dans lequel toute partie admet une borne supérieure et $f : E \to E$ une application croissante. Montrer que f admet un point fixe (on pourra considérer $X = \{x \in E;\ x \leqslant f(x)\}$, montrer que X admet un plus grand élément

    (b) Soient E, F deux ensembles. On suppose qu'il existe deux applications injectives $f : E \to F$ et $g : F \to E$. On souhaite établir l'existence d'une bijection de E dans F. Pour toute partie A de E vérifiant ${}^cA \subset g(F)$, on définit $h_A : E \to F$ en posant $h(x) = f(x)$ si $x \in A$ et $g(h(x)) = x$ si $x \notin A$.
    Montrer que A est telle que ${}^cA \subset g(F)$ et h_A bijective si et seulement si $(g \circ f)(A) \cup {}^c(g(F)) = A$. Conclure.

4 Problèmes

4.1 La loi de réciprocité quadratique

Soit p un nombre premier, et $x \in \mathbb{Z}$, premier avec p. On dit que x est un carré modulo p (ou que x est un résidu quadratique modulo p, ce qui est nettement moins clair) si il existe $y \in \mathbb{Z}$ tel que $x \equiv y^2\ [p]$. On convient de poser $\left(\frac{x}{p}\right) = 1$ si x est un carré modulo p, $\left(\frac{x}{p}\right) = -1$ sinon.
La surprenante loi de réciprocité quadratique, énoncée par Euler en 1783 et démontrée par Gauss en 1801, relie, pour deux nombres premiers distincts p, q différents de 2, les nombres $\left(\frac{p}{q}\right)$ et $\left(\frac{q}{p}\right)$:

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$$

Elle est complétée par les formules (où p est premier différent de 2) :

$$\begin{cases} \left(\dfrac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} \\ \left(\dfrac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} \end{cases}$$

Cette loi a trouvé au XXième siècle de nombreux et subtils prolongements, qui se trouvent au coeur de la théorie des nombres moderne. Elle a fasciné de nombreux mathématiciens, à tel point qu'on en

trouve, paraît-il, plus de 160 démonstrations différentes (Gauss lui-même en proposa 7). Celle que nous donnerons, dans la quatrième partie de ce problème, est due à G. Rousseau. Elle est fort récente, puisqu'elle date de 1991.

4.1.1 Interprétation et mise en oeuvre

1. Calculer "à la main", les valeurs de $\left(\frac{x}{7}\right)$ (pour $1 \leqslant x \leqslant 6$).
2. Soit p un nombre premier différent de 2.
   (a) Soit $x \in \mathbb{Z}$, premier avec p. Indiquer la signification, dans le groupe $\left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)^*$, de la relation $\left(\frac{x}{p}\right) = 1$.
   (b) Montrer que l'ensemble des carrés de $\left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)^*$ est un sous-groupe, que l'on note C_p. Quel est son cardinal (on pourra introduire l'application $x \mapsto x^2$ de $\left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)^*$ dans lui-même) ?
   (c) Soit $a \in \left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)^* \setminus C_p$. Montrer que C_p et aC_p forment une partition de $\left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)^*$.
   (d) Soit p un nombre premier, x et y deux entiers relatifs premiers avec p. Montrer que
   $$\left(\frac{xy}{p}\right) = \left(\frac{x}{p}\right)\left(\frac{y}{p}\right)$$
   Dans la suite de cette partie, on admet la loi de réciprocité quadratique énoncée ci-dessus.
3. Soient p et q deux nombres premiers différents de 2, et (E_1), (E_2) les énoncés :
   (E_1) : "p est un carré modulo q" $\quad$ (E_2) : "q est un carré modulo p"
   Indiquer, en fonction des valeurs de p et q modulo 4, le lien logique liant (E_1) et (E_2).
4. Décomposer "à la main" 713 et 1009 en facteurs premiers (on expliquera le procédé utilisé, mais on ne reportera pas tous les calculs sur la copie). En utilisant la loi de réciprocité quadratique et la conclusion de **1.**, déterminer si 713 est un carré modulo 1009.
5. Soit p un nombre premier distinct de 2 et de 3. Montrer que -3 est un résidu quadratique modulo p si et seulement si $p \equiv 1\ [3]$.

4.1.2 Critère d'Euler et première formule complémentaire

Soit p un nombre premier différent de 2.

1. On considère les applications $\phi, \psi : \left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)^* \to \left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)^*$ définies par $\phi(x) = x^2$, $\psi(x) = x^{\frac{p-1}{2}}$.
   (a) Montrer que ϕ et ψ sont des morphismes. Montrer que l'image de ψ est $\{-1, 1\}$. En déduire $\mathrm{Im}(\phi) = \mathrm{Ker}(\psi)$.
   (b) Soit x un entier relatif premier avec p. Établir le critère d'Euler :
   $$\left(\frac{x}{p}\right) \equiv x^{\frac{p-1}{2}}\ [p]$$
2. Prouver la première formule complémentaire $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$.

4.1.3 Un lemme, et la seconde formule complémentaire

1. Soit A un anneau commutatif de caractéristique différente de 2. On note A^* l'ensemble des éléments inversibles de A.

   Nous dirons qu'une partie X de A^* possède la propriété $(\mathcal{R})$ si

   $$\begin{cases} X \cup (-X) = A^* \\ X \cap (-X) = \emptyset \end{cases}$$

   (a) Soit $x \in A^*$. Montrer que $-x \in A^*$ et que $-x \neq x$.

   (b) Soient X et Y deux parties de A^* possèdant la propriété $(\mathcal{R})$. Montrer que

   $$\prod_{x \in X} x = \epsilon \prod_{y \in Y} y$$

   où $\epsilon = (-1)^{|X \cap (-Y)|}$.

2. On établit ici la seconde formule complémentaire. Soit p un entier naturel premier distinct de 2. On note A l'anneau $\dfrac{\mathbb{Z}}{p\mathbb{Z}}$.

   $$X = \{1, 2, \ldots, \frac{p-1}{2}\} \qquad Y = \{2, 4, 6, \ldots, p-1\}$$

   (a) Montrer que les ensembles $\overline{X}$ et $\overline{Y}$ des classes modulo p d'éléments de X et Y respectivement sont des parties de A^* qui possèdent la propriété $(\mathcal{R})$.

   (b) En déduire la seconde formule complémentaire $\left(\dfrac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$.

4.1.4 Preuve de la loi de réciprocité quadratique

p et q désignent deux entiers premiers distincts et différents de 2. On note A l'anneau $\dfrac{\mathbb{Z}}{p\mathbb{Z}} \times \dfrac{\mathbb{Z}}{q\mathbb{Z}}$.

1. Montrer que $A^* = \left(\dfrac{\mathbb{Z}}{p\mathbb{Z}}\right)^* \times \left(\dfrac{\mathbb{Z}}{q\mathbb{Z}}\right)^*$.
2. On pose $X = \left\{([i]_p, [j]_q),\ 1 \leqslant i \leqslant p-1,\ 1 \leqslant j \leqslant \dfrac{q-1}{2}\right\}$.

   (a) Montrer que X possède la propriété $(\mathcal{R})$.

   (b) Établir $\displaystyle\prod_{x \in X} x = [(-1)^{\frac{q-1}{2}}]_p, [(-1)^{\frac{p-1}{2}}(-1)^{\frac{p-1}{2}\frac{q-1}{2}}]_q)$.
3. On pose $Y = \left\{([k]_p, [k]_q), 1 \leqslant k \leqslant \dfrac{pq-1}{2},\ \text{pgcd}(pq, k) = 1\right\}$.

   (a) Montrer que Y possède la propriété $(\mathcal{R})$.

   (b) Établir $\displaystyle\prod_{y \in Y} y = \left(\left[(-1)^{\frac{q-1}{2}}\left(\frac{q}{p}\right)\right]_p, \left[(-1)^{\frac{p-1}{2}}\left(\frac{p}{p}\right)\right]_q\right)$.
4. Conclure.

4.2 Entiers N-adiques

L'objet de ce problème est l'étude des propriétés élémentaires de l'ensemble $\mathbb{Z}_N$ des entiers N-adiques. Pour une introduction divertissante de ces objets, et en favoriser une certaine intuition, voici une illustration informelle des entiers 10-adiques. Chacun sait qu'un entier naturel non nul a admet une écriture en base 10, de la forme :

$$a = a_0 + 10a_1 + 10^2 a_2 + \ldots + 10^q a_q$$

où $0 \leqslant a_k \leqslant 9$. Un entier 10-adique est un "nombre" défini par un semblable développement, mais infini :

$$a = a_0 + 10a_1 + 10^2 a_2 + \ldots$$

Bien sûr, cela demande une définition précise, cette "somme" ne devant certainement pas être interprétée comme une série de nombres réels (mais c'est bien une série dans un certain sens, voir 4.2.4.4.). Malgré cela, il semble qu'il y ait moyen de définir de manière naturelle l'addition et le produit des entiers 10-adiques. Par exemple :

$$\begin{array}{cccccccc} & \ldots & 1 & 1 & 1 & 1 & 1 \\ + & \ldots & 9 & 9 & 9 & 9 & 9 \\ \hline & \ldots & 1 & 1 & 1 & 1 & 0 \end{array} \qquad \begin{array}{cccccccc} & \ldots & 1 & 1 & 1 & 1 & 1 \\ \times & \ldots & 9 & 9 & 9 & 9 & 9 \\ \hline & \ldots & 9 & 9 & 9 & 9 & 9 \\ & \ldots & 9 & 9 & 9 & 9 & . \\ & \ldots & 9 & 9 & 9 & . & . \\ & \ldots & 9 & 9 & . & . & . \\ & \ldots & 9 & . & . & . & . \\ \hline & \ldots & 8 & 8 & 8 & 8 & 9 \end{array}$$

On s'attachera donc dans ce problème a rendre tout cela précis et rigoureux, et à étudier la structure obtenue. Loin d'être anecdotiques, les nombres N-adiques, découverts par le mathématicien Hensel au début du XXième siècle, constituent un outil fondamental en arithmétique comme en analyse.

4.2.1 Définitions

Soit $N \in \mathbb{N} \setminus \{0, 1\}$. On appelle suite N-adique une suite $a = (a_0, a_1, a_2, \ldots) \in [\![0, N-1]\!]^{\mathbb{N}}$. On appelle k-ième somme partielle de a l'élément S_k de $\dfrac{\mathbb{Z}}{N^{k+1}\mathbb{Z}}$ défini par :

$$S_k(a) = [a_0 + a_1 N + a_2 N^2 + \ldots + a_k N^k]_{N^{k+1}}$$

Et on désigne, pour tout k, par π_k l'application de $\mathbb{Z}/N^{k+1}\mathbb{Z}$ dans $\mathbb{Z}/N^k\mathbb{Z}$ définie par (vérifier qu'elle est bien définie !)

$$\begin{array}{rccc} \pi_k & : \mathbb{Z}/N^{k+1}\mathbb{Z} & \to & \mathbb{Z}/N^k\mathbb{Z} \\ & [\xi]_{N^{k+1}} & \mapsto & [\xi]_{N^k} \end{array}$$

On désignera aussi par A_N l'anneau produit $\dfrac{\mathbb{Z}}{N\mathbb{Z}} \times \dfrac{\mathbb{Z}}{N^2\mathbb{Z}} \times \dfrac{\mathbb{Z}}{N^3\mathbb{Z}} \times \ldots$ (un élément de A_N est donc une suite $(U_0, U_1, U_2, \ldots)$, où $U_k \in \dfrac{\mathbb{Z}}{N^k\mathbb{Z}}$; la somme et le produit se font composante par composante).
Pour éviter les confusions, on utilisera, comme ci-dessus, des lettres minuscules pour désigner une suite N-adique, et des lettres majuscules pour désigner un élément de A_N par ses composantes dans les $\dfrac{\mathbb{Z}}{N^k\mathbb{Z}}$. Mais un élément U de A_N est aussi une suite de la forme $U = ([\alpha_0]_N, [\alpha_1]_{N^2}, [\alpha_2]_{N^3}, \ldots)$, où les α_k sont des entiers relatifs. On utilisera systématiquement des lettres grecques dans cette circonstance.

1. Vérifier que π_k est correctement définie. Montrer que c'est un morphisme d'anneaux. Quel est son noyau ?
2. On note Z_N, et on appelle ensemble des entiers N-adiques, l'ensemble des suites $U = (U_0, U_1, U_2, \ldots) \in A_N$ telles que, pour tout $k \geqslant 1$, $\pi_k(U_k) = U_{k-1}$. Montrer que Z_N est un sous-anneau de A_N. À quelle condition une suite $U = ([\alpha_0]_N, [\alpha_1]_{N^2}, [\alpha_2]_{N^3}, \ldots)$ (où $\alpha_k \in \mathbb{Z}$) est-elle élément de $\mathbb{Z}_N$?
3. Étant donnée une suite N-adique $a = (a_0, a_1, a_2, \ldots) \in [\![0, N-1]\!]^{\mathbb{N}}$, on définit la suite $S(a) \in A_N$ par :
$$S(a)_k = [a_0 + a_1 N + a_2 N^2 + \ldots + a_k N^k]_{N^{k+1}}$$
Montrer $S(a) \in \mathbb{Z}_N$. Prouver que l'application $a \mapsto S(a)$ est une bijection de $[\![0, N-1]\!]^{\mathbb{N}}$ dans $\mathbb{Z}_N$.

On a ainsi correctement défini la notion d'entier N-adique, chacun d'entre eux pouvant être représenté de manière unique par une suite N-adique.

4. Quelle suite N-adique représente l'entier N-adique $-1_{\mathbb{Z}_N}$ (opposé de $1_{\mathbb{Z}_N}$ dans $\mathbb{Z}_N$) ?
5. Montrer que $\mathbb{Z}_N$ contient un (unique) sous-anneau isomorphe à $\mathbb{Z}$.

On identifiera désormais un entier relatif et son image dans $\mathbb{Z}_M$. On pourra, par exemple écrire

$$1 = ([1]_N, [1]_{N^2}, [1]_{N^3}, \ldots)$$

6. Soit $U \in \mathbb{Z}_N$ représenté par la suite N-adique a. Quelle est la représentation N-adique de NU ?
7. (a) Soient N et M deux entiers naturels. On suppose $N|M$. Montrer que l'application
$$\begin{array}{ccc} \dfrac{\mathbb{Z}}{M\mathbb{Z}} & \to & \dfrac{\mathbb{Z}}{N\mathbb{Z}} \\ [\xi]_M & \mapsto & [\xi]_N \end{array}$$
(où $\xi \in \mathbb{Z}$) est bien définie, et que c'est un morphisme d'anneaux.
   (b) Soient N et M deux entiers naturels vérifiant $N|M$. Montrer qu'il existe un morphisme naturel de l'anneau $\mathbb{Z}_M$ dans l'anneau $\mathbb{Z}_N$.
   (c) Soient N et M deux entiers naturels premiers entre eux. Montrer que $\mathbb{Z}_N \times \mathbb{Z}_M \approx \mathbb{Z}_{NM}$ (comme anneaux).
   (d) Soit N un entier naturel et $s \in N^*$. Montrer que $\mathbb{Z}_{N^s} \approx \mathbb{Z}_N$.
   (e) Montrer que $\mathbb{Z}_N$ est intègre si et seulement si N est une puissance d'entier premier.

Pour ces raisons, on étudie généralement les anneaux $\mathbb{Z}_p$, où p est un entier premier. L'étude générale de l'anneau des d'entiers N-adiques s'en déduit immédiatement.

4.2.2 Arithmétique de $\mathbb{Z}_p$

p désigne un entier premier.

1. Montrer que $(U_0, U_1, \ldots) \in \mathbb{Z}_p$ est inversible si et seulement si $U_0 \neq 0$. Soit $a \in [\![0, p-1]\!]^{\mathbb{N}}$. À quelle condition $S(a)$ est-il inversible dans $\mathbb{Z}_p$? Quel est l'inverse de $1-p$ dans $\mathbb{Z}_p$? Quelle est la suite p-adique le représentant ?
2. Montrer que tout élément non nul U de $\mathbb{Z}_p$ s'écrit de manière unique sous la forme $U = Vp^k$, où V est un inversible de $\mathbb{Z}_p$ et $k \in \mathbb{N}$ (k s'appelle la p-valuation de U. On le note $v_p(U)$). Que vaut $v_p(U)$ lorsque $U \in \mathbb{Z}$?

3. Montrer que p est irréductible[6] dans $\mathbb{Z}_p$, et que c'est, à multiplication par un inversible près, l'unique élément irréductible[7] de $\mathbb{Z}_p$.

L'arithmétique de $\mathbb{Z}_p$ est donc très simple, la plus simple que l'on puisse imaginer après celle d'un corps qui elle est triviale (au sens propre).

4.2.3 Distance ultra-métrique

Soit X un ensemble. On appelle distance ultra-métrique sur X une application $d : X \times X \to \mathbb{R}_+$ vérifiant :

$$\begin{aligned}&\forall U, V \in X,\ d(U,V) = d(V,U)\\ &\forall U, V \in X,\ d(U,V) = 0 \implies U = V\\ &\forall U, V, W \in X,\ d(U,W) \leqslant \max(d(U,V), d(V,W))\end{aligned}$$

Une distance ultra-métrique est donc une distance. Un ensemble muni d'une telle distance est appelé un espace ultra-métrique. On se donne dans la suite de cette partie un espace ultra-métrique (X, d). Ce qui suit montre que dans un tel espace, l'intuition est mise à rude épreuve.

1. Soient $U, V \in X$, et $r > 0$. Montrer que si $d(U,V) < r$, alors $B_r(U) = B_r(V)$. En déduire que deux boules ouvertes de X sont disjointes ou confondues.
2. Soit $(U^n)_n$ une suite de points de X. Montrer que U est une suite de Cauchy si et seulement si

$$\lim_{n\to+\infty} d(U^n, U^{n+1}) = 0$$

4.2.4 Topologie de $\mathbb{Z}_p$.

On convient que $v_p(0) = +\infty$. Et on pose, pour $U \in \mathbb{Z}_p$,

$$|U|_p = p^{-v_p(U)} \in \mathbb{R}_+$$

(donc $|0|_p = 0$). Enfin, on pose $d(U,V) = |U - V|_p$.

1. Montrer que $v_p(U+V) \geqslant \min(v_p(U), v_p(V))$, que l'égalité a lieu dès que $v_p(U) \neq v_p(V)$.
2. Établir

$$\begin{aligned}&\forall U,\ |U|_p = 0 \iff U = 0\\ &\forall U, V, |UV|_p = |U|_p |V|_p\\ &\forall U, V, |U+V| \leqslant \max(|U|_p, |V|_p)\end{aligned}$$

3. Montrer que d est une distance ultra-métrique sur $\mathbb{Z}_p$. On munit dans la suite $\mathbb{Z}_p$ de cette distance ultra-métrique.
4. Soit $a = (a_0, a_1, a_2, \ldots)$ une suite p-adique, et $U = S(a)$. Montrer que dans $\mathbb{Z}_p$,

$$U = \sum_{k=0}^{+\infty} a_k p^k$$

(c'est-à-dire $U = \lim_{n\to+\infty} \sum_{k=0}^{n} a_k p^k$).

On peut ainsi écrire, sans complexe,

$$\frac{1}{1-p} = \sum_{k=0}^{+\infty} p^k$$

[6] C'est-à-dire que si $p = VW$, alors V ou W est inversible.

[7] Un inversible n'est pas considéré comme étant irréductible.

5. *Soit $(U^n)_n$ une suite d'éléments de $\mathbb{Z}_p$.*
   (a) Montrer que l'on peut trouver des applications $\phi_k : \mathbb{N} \to \mathbb{N}$ strictement croissante ($k \in \mathbb{N}$), telles que, pour tout k, la suite $(U_k^{\phi_0 \circ \phi_1 \circ \ldots \circ \phi_k(n)})_n$ soit constante (on construira les ϕ_k par récurrence).
   (b) Montrer que l'application $\phi : \mathbb{N} \to \mathbb{N}$ définie par $\phi(n) = \phi_0 \circ \phi_1 \circ \ldots \circ \phi_n(n)$ est strictement croissante et que, pour tout k, la suite $(\phi(n))_{n \geqslant k}$ est extraite de la suite $(\phi_0 \circ \phi_1 \circ \ldots \circ \phi_k(n))_n$.
   (c) Montrer que la suite $U^{\phi(n)}$ converge et en déduire que $\mathbb{Z}_p$ est compact.
6. Montrer que $\mathbb{Z}_p$ est complet. Soit $(U^n)_n$ une suite de $\mathbb{Z}_p$. Montrer que la série $\sum_{n=0}^{\infty} U_n$ converge si et seulement si $\lim_{n \to +\infty} U_n = 0$.

Conclusion

Il y aurait encore beaucoup à dire sur ce sujet, mais ce problème prendrait alors des proportions excessives. En particulier, il faudrait parler du corps $\mathbb{Q}_p$ des nombres p-adiques, qui est à $\mathbb{Z}_p$ ce que $\mathbb{Q}$ est à $\mathbb{Z}$ (son corps des fractions). Les éléments de $\mathbb{Q}_p$ sont de la forme Up^k, où U est un inversible de $\mathbb{Z}_p$ et $k \in \mathbb{Z}$. La "valeur absolue" $|.|_p$ se prolonge sans difficulté à $\mathbb{Q}_p$, et on obtient ainsi une extension de corps de $\mathbb{Q}$ qui s'avère complète pour $|.|_p$. En fait, $\mathbb{Q}_p$ est à $\mathbb{Q}$ pour $|.|_p$ ce que $\mathbb{R}$ est à $\mathbb{Q}$ pour la valeur absolue ordinaire, son "complété". Comme (thm d'Ostrowski) $|.|$ et $|.|_p$ sont essentiellement les seules valeurs absolues sur $\mathbb{Q}$, on voit que $\mathbb{Q}_p$ est une structure très naturelle et non, comme on pourrait le penser, une chose d'artificielle conçue pour enrichir les marchands d'aspirine.