Outils arithmétiques pour la géométrie discrète

Gaëlle Largeteau-Skapin, Isabelle Debled-Rennesson

Chapitre 2 Traité IC2 Géométrie discrète et Images numériques : Outils Arithmétiques pour la Géométrie Discrète

Ce chapitre a été rédigé par Gaëlle **Largeteau-Skapin** et Isabelle **Debled-Rennesson**

1 Introduction

La géométrie discrète définit et étudie les objets géométriques au moyen de grandeurs numériques et d'équations. Les nombres utilisés dans le cadre de la géométrie discrète sont des entiers et les équations sont diophantiennes (à coefficients entiers et également à solutions entières). Le premier objet de l'arithmétique est justement l'étude de l'ensemble des nombres entiers relatifs $\mathbb{Z}$, et principalement l'étude du problème de la divisibilité dans $\mathbb{Z}$. En effet, contrairement à l'addition, la soustraction et la multiplication, la division n'est pas une opération interne à cet ensemble.

L'objectif de ce chapitre est de présenter les notions de base de l'arithmétique couramment utilisées en géométrie discrète, des approfondissements pouvant être trouvés dans de nombreux ouvrages [RS97,Samuel67].

2 Structure de $\mathbb{Z}$

L'ensemble des entiers relatifs (ou nombres entiers) est l'union des entiers naturels $\mathbb{N}$ (0, 1, 2, ...) et de leurs opposés (-1, -2, -3, ...). Cet ensemble est noté $\mathbb{Z}$, qui vient de l'allemand **Zahlen** (nombres). L'ensemble $\mathbb{Z}$ muni de l'addition et de la multiplication $(\mathbb{Z}, +, *)$ est un **anneau commutatif** :

$+$ est une loi de composition interne telle que : il existe un élément neutre 0 ($a+0 = 0+a = a$) ; pour tout a il existe un inverse $-a$ tel que ($a+(-a) = 0$) ; la loi est associative $(a + b) + c = a + (b + c)$ et commutative $a + b = b + a$.

$*$ est une loi de composition interne telle que : il existe un élément neutre 1 ($a * 1 = 1 * a = a$) ; la loi est associative ($(a * b) * c = a * (b * c)$), commutative ($a * b = b * a$) et distributive par rapport à $+$: $(a * (b + c) = a * b + a * c)$.

$\mathbb{Z}$ est de plus **intègre**, c'est-à-dire qu'il vérifie la propriété suivante : $ab = 0 \Rightarrow a = 0$ ou $b = 0$.

En revanche, $\mathbb{Z}$ n'est pas un corps. Pour qu'un anneau soit un corps, il faut que tout élément admette un inverse pour l'opération $*$: $\forall x \in \mathbb{Z},\ \exists y \in \mathbb{Z},\ x * y = 1$. Les seuls éléments inversibles de $\mathbb{Z}$ sont -1 et 1.

Le plus petit corps contenant $\mathbb{Z}$ est l'ensemble des nombres **rationnels** $\mathbb{Q}$. Un nombre rationnel peut s'écrire sous forme de fraction $\frac{a}{b}$ où a et b sont des éléments de $\mathbb{Z}$. L'ensemble $\mathbb{Q}$ est muni de deux opérations : l'addition ($\frac{a}{b} + \frac{c}{d} = \frac{ad+cb}{bd}$) et la multiplication ($\frac{a}{b} * \frac{c}{d} = \frac{ac}{bd}$). Dans cet ensemble, chaque élément admet un inverse pour l'addition ($\frac{a}{b} + \frac{-a}{b} = 0$) et pour la multiplication ($\frac{a}{b} * \frac{b}{a} = 1$)(pour $\frac{a}{b} \neq 0$ bien sûr).

Une fraction $\frac{a}{b}$ est dite **irréductible** si il n'existe pas une fraction $\frac{c}{d}$ o $|c| < |a|$ et $0 < d < b$ telle que $\frac{a}{b} = \frac{c}{d}$. Chaque élément de $\mathbb{Q}$ peut être représenté par une fraction irréductible.

Il existe des nombres qui ne peuvent pas être écrits sous forme de fraction, comme π et $\sqrt{2}$ par exemple. Ces nombres sont dits **irrationnels**. L'ensemble de tous les nombres (rationnels et irrationnels) est l'ensemble des réels $\mathbb{R}$.

Les nombres réels peuvent représenter n'importe quelle grandeur physique (distance, poids, temps etc...). En théorie, ils peuvent être représentés par un développement décimal fini ou infini ($\pi = 3 \times 10^0 + 1 \times 10^{-1} + 4 \times 10^{-2}$...) mais en pratique, ce développement est tronqué pour les calculs (souvent deux chiffres après la virgule pour les calculs mentaux, plus pour les calculs par ordinateur suivant les principes des codages en virgule fixe ou en virgule flottante). Dans tous les cas, le nombre réel devient rationnel ($\pi \simeq 3,14 = \frac{314}{100}$), l'erreur commise par la troncature dépend du nombre de chiffres conservés et permet de donner une mesure de précision du résultat.

Des librairies spécialisées ont été élaborées pour répondre aux problèmes dépendant de la taille du mot-machine. La librairie GMP[1](GNU Multiple Precision Arithmetic Library) , diffusée sous licence GNU LGPL[2], permet des calculs en précision arbitraire sur les nombres entiers signés, les nombres rationnels et les nombres en virgule flottante. Par ailleurs, la librairie MPFR[3], basée sur la bibliothèque GMP, se distingue des autres logiciels de calcul flottant en précision arbitraire par la notion d'*arrondi correct*. Ainsi, le résultat de chaque opération est parfaitement spécifié, ce qui permet d'écrire des programmes dont le comportement est rigoureusement identique, indépendamment de la taille du mot-machine (32 ou 64 bits).

3 Notion de divisibilité dans $\mathbb{Z}$

3.1 Définition

On dit que a est **divisible** par b si la division de a par b a pour résultat un quotient entier et un reste nul.

[1] http://www.swox.com/gmp/
[2] http://www.gnu.org/copyleft/lesser.html
[3] http://www.mpfr.org/

Définition 1 *Soient a et b deux entiers relatifs. b divise a si il existe un entier k tel que $a = b * k$*

La divisibilité est une relation réflexive (a divise a), transitive (a divise b et b divise c implique a divise c) et antisymétrique (a divise b et b divise a implique $a = b$). On a, de plus, les propriétés suivantes : a divise 0 et 1 divise a.

On appelle *critères de divisibilité* les tests qui permettent de savoir facilement si un nombre a est un multiple de b, sans avoir à poser la division. Voici quelques critères, parmi d'autres :

- 2 divise a si le chiffre des unités de a est pair.
- 3 divise a si la somme des chiffres qui composent a est divisible par 3.
- 8 divise a si le nombre formé des trois derniers chiffres de a est divisible par 8 ...

On note $n\mathbb{Z}$ l'ensemble des entiers relatifs qui sont divisibles par l'entier n. L'arithmétique modulaire est définie à partir de ces ensembles. L'**arithmétique modulaire** est une arithmétique où l'on ne raisonne pas directement sur les nombres mais sur leurs restes respectifs par la division euclidienne par un certain entier : le modulo. On parle alors de **congruence**:

Définition 2 *Deux entiers a et b sont dits **congruents modulo** n et on note $a \equiv b(n)$, avec n un entier non nul différent de 1 et -1, si il existe $k \in \mathbb{N}$ tel que $a = b + k * n$.*

La congruence est une relation d'équivalence : elle est réflexive ($a \equiv a(n)$), symétrique ($a \equiv b(n) \Leftrightarrow b \equiv a(n)$) et transitive ($a \equiv b(n)$ et $b \equiv c(n)$ alors $a \equiv c(n)$). On peut donc définir des classes d'équivalence : la classe d'équivalence de l'entier a est l'ensemble des entiers b tels que $b \equiv a \pmod{n}$. On la note $[a]_n$, ou $a + n\mathbb{Z}$. On peut utiliser les règles de calcul suivantes : $[a]_n + [b]_n = [a + b]_n$ et $[a]_n * [b]_n = [ab]_n$. L'ensemble de ces classes d'équivalence, noté $\mathbb{Z}/n\mathbb{Z}$, est un anneau commutatif à n éléments.

3.2 Nombres premiers

Un **nombre premier** est un entier strictement supérieur à 1, n'admettant que 1 et lui-même comme diviseurs. L'ensemble des nombres premiers est parfois noté $\mathbb{P}$. La nature première ou non d'un nombre est appelée sa **primalité**. Un entier (> 1) qui n'est pas premier est dit **composé** car il peut être décomposé (on dit aussi factorisé) en un produit de puissances de nombres premiers. Chaque nombre composé admet une unique décomposition en facteurs premiers, par exemple $90 = 2 * 3^2 * 5$.

Les nombres premiers inférieurs à 100 sont 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97.

La méthode la plus classique pour trouver les nombres premiers inférieurs à un entier donné n est le **crible d'Ératosthène**. L'algorithme correspondant

consiste à écrire l'ensemble des entiers de 2 à n puis à rayer successivement les pultiples des nombres premiers. Le premier entier non rayé est premier, les multiples de cet entier sont rayés. Pour trouver les nombres premiers plus petits que 10, on note 2,3,4,5,6,7,8,9,10. Le premier entier non rayé est 2, il est premier, 4,6,8 et 10 sont rayés. L'entier non rayé suivant est 3, il est donc premier et on raye 6 et 9. L'entier suivant est 5, on raye 10. Le dernier nombre premier inférieur à 10 est 7.

Une autre approche pour obtenir des nombres premiers serait de trouver une formule pour les construire. Plusieurs tentatives pour trouver un algorithme de construction de nombres premiers ont été réalisées, en voici quelques-unes.

La première idée des mathématiciens pour construire un nombre premier n est qu'il ne soit pas divisible par les entiers plus petits que lui. Ils proposent donc la formule basée sur la factorielle (notée !) : $n = k! + 1$. Il existe cependant des contre-exemples : pour $k = 4$, on a $4! = 24$ et $4!+1 = 25$ n'est évidement pas premier. Pour $k = 7$, $k! + 1 = 4033 = 37 * 109$ mais pour $k = 1, 2, 3, 5, 6$, $k! + 1$ est premier. Un nombre premier obtenu par cette formule est dit **factoriel**. Le plus grand nombre premier factoriel connu à ce jour est $34790! - 1$.

La formule a été modifiée pour ne prendre en compte que le produit des k premiers nombres premiers : $n = (2 * 3 * 5 * ... * k) + 1$. Cette méthode ne fournit toutefois pas toujours un nombre premier : $2 * 3 * 5 * 7 * 11 * 13 + 1 = 30031 = 59 * 509$. Un nombre premier obtenu par cette méthode est dit **primoriel**.

Les nombres premiers de la forme $F_n = 2^{2^n} + 1$ sont appelés les nombres premiers de **Fermat**. $F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$ et $F_4 = 65537$ sont les seuls nombres premiers de **Fermat** connus ($F_5 = 4294967297 = 6700417 * 641$).

Une autre méthode de construction consiste à utiliser la suite dite d'**Euclide-Mullin** définie de la façon suivante : $u_1 = 2$, et u_{n+1} est le plus petit nombre premier diviseur de $u_1 * u_2 * \cdots * u_n + 1$. Les premiers termes de cette suite sont : 2, 3, 7, 43, 13, 53, 5, 6221671, 38709183810571, 139, 2801, 11, 17,... On ne connaît que les 43 premiers termes de cette suite et on ignore si tous les nombres premiers y apparaissent mais **Shanks** a conjecturé en 1991 [Shanks93] que tel était le cas.

3.3 PGCD et PPCM

Le **plus grand commun diviseur** (**PGCD**) noté $pgcd(a, b)$ ou $a \wedge b$, de deux entiers non nuls a et b, est le plus grand nombre entier naturel qui divise les deux entiers :

Définition 3 $\forall (a, b) \in \mathbb{Z}^2,\ pgcd(a, b) = max\{c \in \mathbb{N}^* \mid c\ divise\ a\ et\ c\ divise\ b\}$.

Deux nombres entiers sont dits **premiers entre eux** si leur plus grand commun diviseur est 1.

Le **plus petit commun multiple** (**PPCM**) noté $ppcm(a, b)$ ou $a \vee b$, de deux entiers, est le plus petit entier naturel qui est multiple des deux entiers. Si l'un des deux entiers est nul, le PPCM est égal à 0.

Définition 4 $\forall (a,b) \in \mathbb{Z}^2,\ ppcm(a,b) = min\{c \in \mathbb{N}^* \mid a \text{ divise } c \text{ et } b \text{ divise } c\}$.

Le PPCM de deux entiers se déduit de leur pgcd de la manière suivante :

$$ppcm(a,b) = \frac{|a * b|}{pgcd(a,b)}$$

3.4 Algorithme de calcul du PGCD

L'algorithme d'**Euclide** pour le calcul du PGCD de deux entiers est basé sur la propriété suivante : soient a et b deux entiers avec $a \geq b$, si r est le reste de la division de a par b, alors $pgcd(a,b) = pgcd(b,r)$. On calcule donc des divisions euclidiennes, jusqu'à ce qu'on trouve un reste nul. Le dernier reste non nul est le pgcd de a et b.

Théorème 1 *(**Bézout**) Le PGCD de deux entiers a et b est une combinaison linéaire (à coefficients entiers relatifs) de a et b : il existe deux entiers relatifs u et v tels que* $pgcd(a,b) = a * u + b * v$.

Une modification de l'algorithme d'**Euclide** (que l'on appelle algorithme d'**Euclide** étendu ou algorithme de **Blankinship**) permet de calculer ces coefficients u et v en même temps que le PGCD. La méthode de **Blankinship** consiste à utiliser l'algorithme d'**Euclide** sur la matrice

$$M = \begin{bmatrix} a & 1 & 0 \\ b & 0 & 1 \end{bmatrix} \qquad \begin{array}{rcccc} a & = & 1*a & + & 0*b \\ b & = & 0*a & + & 1*b \end{array}$$

pour conserver la trace des u et v successifs.

Données: a_{init},b_{init} entiers dont on veut calculer le pgcd
Résultat: Les coefficients de Bézout u_{final} et v_{final} ainsi que le *pgcd*
$a := a_{init}$, $b := b_{init}$, $u_1 := 1$, $v_1 := 0$, $u_2 := 0$, $v_2 := 1$; /*matrice initiale*/
tant que $b \neq 0$ **faire**
  /*variables auxiliaires pour le calculs des nouvelles valeurs*/
  $reste := a \bmod b$;
  $quotient := a/b$;
  $n\_u_2 := u_1 - quotient * u_2$;
  $n\_v_2 := v_1 - quotient * v_2$;
  /*mise à jour de la matrice*/
  $u_1 := u_2$;
  $v_1 := v_2$;
  $u_2 := n\_u_2$;
  $v_2 := n\_v_2$;
  $a := b$;
  $b := reste$;
fin
$u_{final} := u_1$;
$v_{final} := v_1$;
$pgcd := a$; /*$pgcd(a_{init}, b_{init}) = a_{init} * u\_final + b_{init} * v\_final$*/

Algorithm 1: Algorithme de **Blankinship** [B63].

Exemple : Recherche du PGCD de 6744 et 432

$$\begin{bmatrix} 6744 & 1 & 0 \\ 432 & 0 & 1 \end{bmatrix}, \begin{array}{r|l} 6744 & 432 \\ \hline 264 & 15 \end{array} \Rightarrow \begin{bmatrix} 432 & 0 & 1 \\ 264 & 1 & -15 \end{bmatrix}, \begin{array}{r|l} 432 & 264 \\ \hline 168 & 1 \end{array} \Rightarrow \begin{bmatrix} 264 & 1 & -15 \\ 168 & -1 & 16 \end{bmatrix},$$

$$\begin{array}{r|l} 264 & 168 \\ \hline 96 & 1 \end{array} \Rightarrow \begin{bmatrix} 168 & -1 & 16 \\ 96 & 2 & -31 \end{bmatrix}, \begin{array}{r|l} 168 & 96 \\ \hline 72 & 1 \end{array} \Rightarrow \begin{bmatrix} 96 & 2 & -31 \\ 72 & -3 & 47 \end{bmatrix},$$

$$\begin{array}{r|l} 96 & 72 \\ \hline 24 & 1 \end{array} \Rightarrow \begin{bmatrix} 72 & -3 & 47 \\ 24 & 5 & -78 \end{bmatrix}, \begin{array}{r|l} 72 & 24 \\ \hline 0 & 3 \end{array} \Rightarrow \begin{bmatrix} \mathbf{24} & \mathbf{5} & \mathbf{-78} \\ 0 & -18 & 125 \end{bmatrix}$$

Résultat : $6744 * 5 - 432 * 78 = pgcd(6744, 432) = 24$.

4 Équation diophantienne

4.1 Définition et exemples

Une **équation diophantienne** est une égalité entre deux polynômes à coefficients dans $\mathbb{Z}$ avec un nombre quelconque d'inconnues. Un **problème diophantien** est une équation diophantienne dont on ne cherche que les solutions entières. Une **équation diophantienne linéaire** est une équation entre deux sommes de monômes de degré zéro ou un : $ax + by = c$ (nous omettrons l'opérateur $*$ dans la suite du document si cela ne prête pas à confusion).
Voici quelques exemples d'équations diophantiennes remarquables :

- Équation de **Catalan** : $x^n - y^m = 1$, admet une seule solution non nulle: $3^2 - 2^3 = 1$.
- Identité de **Bézout** : $au + bv = pgcd(a, b)$, admet toujours une solution.
- Équation de **Pythagore** : $x^2 + y^2 = z^2$, admet une infinité de solutions.
- Équation de **Fermat-Wiles** : $x^n + y^n = z^n,\ n > 2$, n'admet aucune solution non nulle.
- Équations de **Pell** : $x^2 - ny^2 = \pm 1\ \sqrt{n} \notin \mathbb{N}$. L'équation $x^2 - ny^2 = 1$ admet une infinité de solutions (x, y) telles que $\frac{x}{y}$ donne une approximation de $\sqrt{n}$; plus x et y sont grands, meilleure est l'approximation. L'équation $x^2 - ny^2 = -1$ n'a pas nécessairement de solution dans $\mathbb{Z}$.
- Équations de **Thue** : $\sum_{i=0}^{n} a_i x^i y^{n-i} = c,\ n > 3, c \neq 0$ que l'on peut généralement résoudre.

La résolution d'une équation diophantienne produit un système de la forme $\begin{cases} x = \lambda_1 + \lambda_2 k \\ y = \lambda_3 + \lambda_4 k \end{cases}, \forall i \lambda_i \in \mathbb{Z}, k \in \mathbb{Z}$

Si k parcours $\mathbb{R}$, ce système est une représentation paramétrique d'une droite. L'ensemble des points de coordonnées entières de cette droite fournit les solutions de l'équation diophantienne.

4.2 Méthodes de résolutions

Soit $ax + by = c,\ a, b, c \in \mathbb{Z}$, une équation diophantienne d'inconnues x et y. On note $\mathcal{S}$ l'ensemble des solutions entières de cette équation. Il existe une solution de cette équation ($\mathcal{S} \neq \emptyset$) si et seulement si le pgcd de a et b divise c ($pgcd(a, b)$ divise c).

Supposons qu'il existe une solution, donc $\mathcal{S} \neq \emptyset$. On peut simplifier l'équation par $pgcd(a, b)$. On a alors $a'x + b'y = c',\ a' = \frac{a}{pgcd(a,b)},\ b' = \frac{b}{pgcd(a,b)},\ c' = \frac{c}{pgcd(a,b)},\ pgcd(a', b') = 1$.

Considérons l'équation $a'x + b'y = 0$ dite équation **homogène**. Les solutions de cette équation sont évidentes et sont $\mathcal{S}_H = \{(-b'k, a'k),\ k \in \mathbb{Z}\}$.

On peut obtenir une solution particulière de l'équation $a'x + b'y = c'$ en considérant la relation de Bézout associée à a' et b' : comme $pgcd(a', b') = 1$, il existe u et v tels que $a'u + b'v = 1$. En multipliant l'égalité par c' on obtient : $a'uc' + b'vc' = c'$ et donc $x_0 = uc'$ et $y_0 = vc'$ est une solution de l'équation.

L'ensemble des solutions de l'équation peut alors être construit de la manière suivante :

$$\mathcal{S} = \{(x_0 - b'k, y_0 + a'k),\ k \in \mathbb{Z}\} = \{(x_0 - \frac{b}{pgcd(a,b)}k, y_0 + \frac{a}{pgcd(a,b)}k),\ k \in \mathbb{Z}\}$$

Exemple : Soit l'équation $12x + 15y = 51$. On a $pgcd(12, 15) = 3$ et $51 = 3 \times 17$.

Il existe donc au moins une solution à notre problème. Divisons les coefficients par 3, on obtient : $4x + 5y = 17$ avec $pgcd(4, 5) = 1$.

Considérons l'équation homogène : $4x + 5y = 0$, les solutions sont

$$\mathcal{S}_H = \big\{(-5k, 4k),\ k \in \mathbb{Z}\big\}.$$

La solution particulière est déterminée par la résolution de l'équation $4x+5y = 1$ par l'algorithme de **Blankinship**, puis on multiplie par $c' = 17$ d'o : $x_0 = -1 \times 17$, $y_0 = 1 \times 17$. L'ensemble des solutions de l'équation est donc :

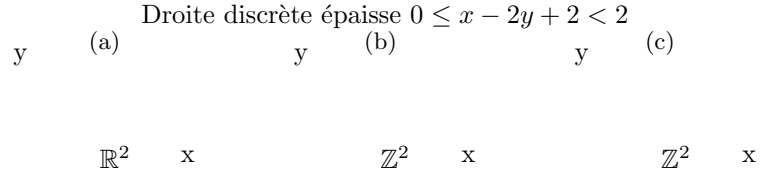
$$\mathcal{S} = \big\{(-17 - 5k, 17 + 4k),\ k \in \mathbb{Z}\big\}.$$

Difficultés : Pour les équations diophantiennes de degré supérieur, il n'existe pas de méthode générale pour en trouver les solutions : le $10^{\text{ème}}$ problème de **Hilbert** consiste à définir un algorithme acceptant comme paramètre une équation diophantienne D et donnant comme réponse le fait que D admette ou non des solutions. En 1970, **Matiyasevic** [Mat70] montra qu'il était impossible qu'un tel algorithme existe, la résolution générale des équations diophantiennes étant un problème indécidable.

4.3 Lien avec la géométrie discrète

Dans l'espace réel $\mathbb{R}^2$, une droite est un ensemble de points (x, y) défini par une équation de la forme $ax + by + c = 0$ avec $pgcd(a, b) = 1$. En ne considérant que les points de coordonnées entières de cette droite, on définit un sous-ensemble de $\mathbb{Z}^2$, appelé **droite discrète**. Cette droite discrète est définie par l'équation diophantienne $ax + by + c = 0$.

(a) Droite Euclidienne $x - 2y + 2 = 0$. (b) Droite discrète $x - 2y + 2 = 0$. (c) Droite discrète épaisse $0 \leq x - 2y + 2 < 2$



Sur l'exemple de la figure 4.3, on remarque que cette droite n'est pas définie pour tout $x \in \mathbb{Z}$. Pour obtenir un résultat défini pour tous les entiers relatifs, il faut "épaissir" la droite en considérant aussi les points entiers solutions de $x - 2y + 2 = 1$ (fig 4.3 (c)). On obtient alors une droite discrète d'épaisseur 2 définie par les deux équations diophantiennes :

$$\begin{cases} x - 2y + 2 = 0 \\ x - 2y + 2 = 1 \end{cases} \Leftrightarrow 0 \leq ax + by + c < 2.$$

Plus généralement, on peut définir une droite d'épaisseur quelconque w par le

système d'équations diophantiennes :

$$\begin{cases} ax+by+c=0 \\ ax+by+c=1 \\ \quad\dots \\ ax+by+c=w-1 \end{cases} \Leftrightarrow 0 \leq ax+by+c < w.$$

Les droites discrètes et leurs propriétées sont traitées plus en détail dans le chapitre **??**(Droites et plans discrets).

5 Partie entière

5.1 Définitions

La partie entière notée $\lfloor x \rfloor$ (ou E(x)) est le plus grand entier relatif inférieur ou égal à x. Ainsi, $\lfloor 3,4 \rfloor = 3$ et $\lfloor -3,4 \rfloor = -4$. La partie entière supérieure, notée $\lceil x \rceil$, est le plus petit entier relatif supérieur ou égal à x. La troncature (notée $trunc(x)$) consiste à couper le nombre à la virgule ($trunc(0,5) = trunc(-0,5) = 0$), elle est généralement utilisée dans les langages de programmation. La troncature a la propriété d'être symétrique par rapport à 0 ce qui peut être utile, mais induit une singularité en 0 et enlève à la fonction sa propriété d'invariance par translation.

Graphes des fonctions partie entière, partie entière supérieure et troncature.

La partie entière peut aussi être définie comme la fonction :

$$E : \mathbb{R} \to \mathbb{Z},\ \forall x \in [0,1[,\ \lfloor x \rfloor = 0 \text{ et } \forall x \in I\!R,\ \lfloor x+1 \rfloor = \lfloor x \rfloor + 1.$$

5.2 Propriétés et calcul avec des parties entières

La première propriété de la partie entière est que le réel x est encadré par sa partie entière et sa partie entière augmentée de 1 : $\lfloor x \rfloor \leq x < \lfloor x \rfloor + 1$.

De plus, pour tout entier k et pour tout réel x, la partie entière possède les propriétés suivantes : d'une part, $\lfloor x+k \rfloor = \lfloor x \rfloor + k$ et d'autre part, $\lfloor k/2 \rfloor + \lceil k/2 \rceil = k$.

Une troisième propriété de cette fonction fait le lien entre la partie entière et la partie entière supérieure : $\lfloor -x \rfloor = -\lceil x \rceil$.

La fonction partie entière est souvent utilisée en analyse pour approcher des réels : étant donné un nombre réel x, la suite de nombres décimaux $\frac{\lfloor 10^n x \rfloor}{(10^n)}$ converge vers x.

Théorème 2 *La partie entière d'une fraction rationnelle* $\frac{a}{b},\ a \in \mathbb{Z},\ b \in \mathbb{Z}$ *est le quotient de la division euclidienne de a par b :*

$$a = \left\lfloor \frac{a}{b} \right\rfloor b + r,\ 0 \leq r < b.$$

5.3 Introduction aux applications quasi-affines

Si on considère une application affine rationnelle:

$$F : \mathbb{Z}^2 \longrightarrow \mathbb{Z}^2$$
$$\begin{pmatrix} x \\ y \end{pmatrix} \mapsto \begin{cases} x' = \frac{\lambda_1 x + \lambda_2 y + \lambda_3}{\omega} \\ y' = \frac{\lambda_4 x + \lambda_5 y + \lambda_6}{\omega} \end{cases}, \forall i \lambda_i \in \mathbb{R}, \omega \in \mathbb{R}$$

Une application quasi-affine est la partie entière de cette application :

$$F : \mathbb{Z}^2 \longrightarrow \mathbb{Z}^2$$
$$\begin{pmatrix} x \\ y \end{pmatrix} \mapsto \begin{cases} x' = \left\lfloor \frac{\lambda_1 x + \lambda_2 y + \lambda_3}{\omega} \right\rfloor \\ y' = \left\lfloor \frac{\lambda_4 x + \lambda_5 y + \lambda_6}{\omega} \right\rfloor \end{cases}, \forall i \lambda_i \in \mathbb{R}, \omega \in \mathbb{R}$$

Les principales propriétés des applications affines (conservation des barycentres, transformation d'une droite en une droite, existence d'un point fixe) ne sont pas toujours vérifiées lorsque l'on considère l'application quasi-affine associée. Nous verrons dans le chapitre **??** (Transformations affines discrètes) les propriétés spécifiques aux applications quasi-affines.

6 Arbre de Stern-Brocot et suites de Farey

Les résultats présentés dans cette section sont détaillés et approfondis dans les ouvrages [GKP94] et [HW89].

6.1 Définitions et premières propriétés

Une méthode pour engendrer toutes les fractions irréductibles positives $\frac{m}{n}$, à partir des nombres entiers et donc de construire $\mathbb{Q}$ à partir de $\mathbb{Z}$, a été découverte indépendamment par Moriz **Stern** [Stern58] et Achille **Brocot** [Brocot60], la structure qui en résulte est appelée l'**arbre de Stern-Brocot**.

L'idée est de commencer avec les deux fractions $\frac{0}{1}$, $\frac{1}{0}$ et ensuite de répéter l'opération suivante autant de fois qu'on le désire : insérer $\frac{m+m'}{n+n'}$ entre deux fractions adjacentes $\frac{m}{n}$ et $\frac{m'}{n'}$.

La nouvelle fraction $\frac{m+m'}{n+n'}$ est appelée le **médian** de $\frac{m}{n}$ et de $\frac{m'}{n'}$. On notera $\frac{m}{n} \oplus \frac{m'}{n'} = \frac{m+m'}{n+n'}$. Entre $\frac{0}{1}$ et $\frac{1}{0}$ on construit $\frac{1}{1}$, on a alors la suite $(\frac{0}{1}, \frac{1}{1}, \frac{1}{0})$ à l'étape suivante, deux fractions sont construites et on obtient $(\frac{0}{1}, \frac{1}{2}, \frac{1}{1}, \frac{2}{1}, \frac{1}{0})$, ensuite quatre fractions sont insérées $(\frac{0}{1}, \frac{1}{3}, \frac{1}{2}, \frac{2}{3}, \frac{1}{1}, \frac{3}{2}, \frac{2}{1}, \frac{3}{1}, \frac{1}{0})$, et ainsi de suite ... Cette construction peut être vue comme un arbre binaire infini dont une partie est représentée sur la figure 6.1.

Début de la construction de l'arbre de **Stern-Brocot**.

Chaque fraction $\frac{m+m'}{n+n'}$ de l'arbre est telle que $\frac{m}{n}$ est son plus proche ancêtre droit et $\frac{m'}{n'}$ est son plus proche ancêtre gauche.

Propriété 1 (GKP94) *A chaque étape de la construction de l'arbre de* ***Stern-Brocot****, si* $\frac{m}{n}$ *et* $\frac{m'}{n'}$ *sont deux fractions consécutives, alors* $m'n - n'm = 1$.

De manière similaire, les **suites de Farey** permettent d'énumérer et représenter de manière ordonnée toutes les fractions rationnelles positives irréductibles.

Définition 5 *La suite de* ***Farey*** *d'ordre* n*, notée* $\mathcal{F}_n$*, est la suite croissante des fractions rationnelles irréductibles comprises entre* 0 *et* 1 *dont le dénominateur est inférieur ou égal à* n.
Par exemple, $\mathcal{F}_5 = \{\frac{0}{1}, \frac{1}{5}, \frac{1}{4}, \frac{1}{3}, \frac{2}{5}, \frac{1}{2}, \frac{3}{5}, \frac{2}{3}, \frac{3}{4}, \frac{4}{5}, \frac{1}{1}\}$.

La construction des suites de Farey se fait récursivement à partir de $\mathcal{F}_1 = \{\frac{0}{1}, \frac{1}{1}\}$: la suite de **Farey** d'ordre n est calculée à partir de la suite de **Farey** d'ordre $n-1$ en ajoutant les médians de dénominateurs inférieurs ou égaux à n, calculés à partir des fractions consécutives de $\mathcal{F}_{n-1}$.
En fait, la suite de **Farey** d'ordre n définit un sous-arbre dans l'arbre de **Stern-Brocot** et la propriété 1 est donc vérifiée pour 2 fractions consécutives de $\mathcal{F}_n$.

6.2 Arbre de Stern-Brocot et fractions continues

Chaque nœud de l'arbre de **Stern-Brocot** peut être représenté par une suite de déplacements en partant du nœud $\frac{1}{1}$:

$$D^{q_0}\ G^{q_1}\ D^{q_2}\ G^{q_3}\ ...\ D^{q_{n-1}}\ G^{q_n}$$

avec,

- D un déplacement vers le fils droit,
- G un déplacement vers le fils gauche,
- $q_0 \in \mathbb{N}$ et $q_i \in \mathbb{N}^*$ pour tout $i > 0$, q_i étant le nombre de fois o le déplacement est itéré.

Par exemple, le nœud $\frac{3}{7}$ est représenté par les déplacements $G^2\ D^2$: $q_0 = 0$, $q_1 = 2$, $q_2 = 2$.

Propriété 2 *Un nœud de l'arbre de* ***Stern-Brocot*** *caractérisé par les déplacements* $D^{q_0}\ G^{q_1}\ D^{q_2}\ G^{q_3}\ ...\ D^{q_{n-1}}\ G^{q_n}$ *a la représentation en fraction continue,*

$$q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \cfrac{1}{\ldots + \cfrac{1}{q_n + \frac{1}{1}}}}} = [q_0; q_1, q_2, ..., q_n + 1]$$

Remarquons aussi que $[q_0; q_1, q_2, ..., q_n + 1] = [q_0; q_1, q_2, ..., q_n, 1]$. Par exemple, $\frac{3}{7} = 0 + \frac{1}{2+\frac{1}{2+\frac{1}{1}}} = [0; 2, 3] = [0; 2, 2, 1]$.

Il existe aussi un lien (montré dans [GKP94]) entre l'algorithme d'**Euclide** et le parcours dans l'arbre de **Stern-Brocot** jusqu'au nœud correspondant à la fraction $\frac{m}{n}$. En effet, il y a $\lfloor \frac{m}{n} \rfloor$ déplacements D, puis $\lfloor \frac{n}{m \ mod \ n} \rfloor$ déplacements G, puis $\lfloor \frac{m \ mod \ n}{n \ mod \ m \ mod \ n} \rfloor$ déplacements D, etc. Ces nombres $m \ mod \ n$, $n \ mod (m \ mod \ n)$, ... sont ceux utilisés dans l'algorithme d'**Euclide**.

6.3 Réseaux entiers

Dans [HW89], une interprétation géométrique de certaines propriétés des fractions continues ainsi que des résultats très intéressants sur les réseaux entiers sont proposés. Nous en citons deux et les illustrons ci-après sans les démontrer.

Considérons trois points O, P et Q non colinéaires dans le plan $\mathbb{Z}^2$. Le parallélogramme engendré par ces trois points (cf. figure 6.3) permet, en prolongeant ses cotés par des droites et en les reproduisant parallèlement, d'engendrer un **réseau** infini de droites. En considérant les points d'intersection entre ces droites, un ensemble infini de points est obtenu, appelé **réseau de points**. Deux différents réseaux qui déterminent le même réseau de points sont dits **équivalents** (cf. figure 6.3).

En traits pleins le réseau engendré par O, P, Q et en traits pointillés un réseau équivalent engendré par O, R, S.

Le réseau formé par les parallèles aux axes Ox et Oy à une unité de distance est appelé le **réseau fondamental** et le réseau de points correspondant **réseau de points fondamental**, il est noté Λ.
Un point P de Λ est dit **visible** depuis le point origine O de Λ si il n'existe pas de points de Λ sur OP entre O et P.

Théorème 3 *Considérons P et Q des points visibles depuis O de Λ et δ l'aire du parallélogramme J défini par OP et OQ. Alors,*

- (i) *Si $\delta = 1$, il n'y a pas de point de Λ dans J;*
- (ii) *Si $\delta > 1$, il y a au moins un point de Λ dans J, et à moins que ce point soit le point d'intersection de diagonales de J, au moins 2 points, un dans chaque triangle délimité par PQ.*

Illustration du théorème précédent; de gauche à droite cas (i) et (ii).

Théorème 4 ***(Minkowski)*** *Toute région convexe R de Λ, symétrique par rapport à O, d'aire supérieure à 4, contient des points de Λ autres que O.*

Un autre résultat permet de calculer simplement l'aire d'un polygone simple construit sur le réseau fondamental (cf. figure 6.3) :

Théorème 5 *(**Pick**, 1899) Soit P un polygone simple dont les sommets sont des points entiers, I le nombre de points intérieurs du polygone et B le nombre de points du bord du polygone alors :*

$$\mathcal{A}ire(P) = I + \frac{1}{2}B - 1$$

Illustration du théorème de **Pick**, ici $I = 9$, $B = 11$, et l'aire du polygone est égale à 13.5.

Ce résultat peut être généralisé aux polygones plus généraux en utilisant la caractéristique d'**Euler** de P à la place de -1 dans la formule précédente. De plus pour les dimensions supérieures, le nombre de points entiers d'un polyèdre convexe à sommets entiers peut être caractérisé en utilisant les polynmes d'**Ehrhart** [EHR72].